



# TeamViewer Security

Comprehensive overview of the company security program

for TeamViewer Tensor and TeamViewer ONE

## Table of contents

|         |                                                                               |    |
|---------|-------------------------------------------------------------------------------|----|
| 1       | Introduction and Security Fundamentals                                        | 6  |
| 1.1     | About TeamViewer                                                              | 6  |
| 1.2     | Fundamentals of TeamViewer Security                                           | 7  |
| 1.3     | Quality Management                                                            | 7  |
| 1.4     | Information Security and Compliance                                           | 7  |
| 1.5     | Data Centers and Backbone                                                     | 7  |
| 1.6     | References                                                                    | 7  |
| 2       | Security Overview                                                             | 7  |
| 3       | Shared Responsibility Model                                                   | 8  |
| 3.1     | TeamViewer Responsibilities                                                   | 8  |
| 3.2     | Customer Responsibilities                                                     | 9  |
| 3.3     | Shared Security Responsibilities                                              | 9  |
| 4       | Security Governance, Certifications and Compliance                            | 11 |
| 4.1     | Security Governance                                                           | 11 |
| 4.2     | Segregation of Corporate and Production Environments                          | 11 |
| 4.3     | Certifications, Attestations and Audits                                       | 11 |
| 4.4     | Compliance and Regulatory Support                                             | 12 |
| 4.5     | Certification Scope Matrix                                                    | 13 |
| 4.6     | Customer Assurance Resources                                                  | 14 |
| 5       | Platform Capabilities and Security Controls                                   | 15 |
| 5.1     | Components                                                                    | 15 |
| 5.1.1   | Clients                                                                       | 15 |
| 5.1.2   | Management Console and Administration                                         | 16 |
| 5.1.3   | TeamViewer ONE Platform                                                       | 16 |
| 5.1.4   | TeamViewer AI and Intelligence Capabilities                                   | 18 |
| 5.2     | Main Use Cases                                                                | 18 |
| 5.2.1   | Secure Attended Access                                                        | 18 |
| 5.2.2   | Secure Unattended Access                                                      | 18 |
| 5.3     | Client Enrollment / Assignment                                                | 19 |
| 5.4     | Connection Authentication and Device Access Control                           | 20 |
| 5.4.1   | Block- and Allowlist                                                          | 20 |
| 5.4.2   | Two-Factor Authentication for Connections (TFA/MFA)                           | 21 |
| 5.4.3   | Access Control for Incoming and Outgoing Connections                          | 21 |
| 5.4.4   | Conditional Access                                                            | 21 |
| 5.4.4.1 | Conditional Access                                                            | 21 |
| 5.4.4.2 | Hybrid Conditional Access (for Segmented and Security-Sensitive Environments) | 21 |
| 5.4.5   | Bring Your Own Certificate (BYOC) for Connection Authentication               | 22 |
| 5.4.6   | Random Password for Connections                                               | 23 |
| 5.5     | Account Authentication                                                        | 24 |
| 5.5.1   | Single Sign-On (SSO)                                                          | 24 |

|         |                                                                  |    |
|---------|------------------------------------------------------------------|----|
| 5.5.2   | Two-Factor Authentication for Account Login (TFA/MFA)            | 24 |
| 5.5.3   | Trusted Devices                                                  | 24 |
| 5.6     | Additional Security Features                                     | 24 |
| 5.6.1   | Security Center                                                  | 24 |
| 5.6.2   | Device Policy and Unified Policies                               | 25 |
| 5.6.3   | Endpoint Management and Security in TeamViewer ONE               | 25 |
| 5.6.4   | Digital Employee Experience (DEX) and Digital Workplace Controls | 26 |
| 5.6.5   | Automations in TeamViewer ONE                                    | 27 |
| 5.6.6   | Black Screen / Privacy Screen                                    | 27 |
| 5.6.7   | Traceability, Auditability and Session Recording                 | 27 |
| 5.6.7.1 | Event Logging                                                    | 27 |
| 5.6.7.2 | Connection Reporting                                             | 28 |
| 5.6.7.3 | Session Recording and Retention                                  | 28 |
| 5.6.7.4 | AI and Tia Auditability                                          | 28 |
| 5.6.8   | Mobile SDK                                                       | 28 |
| 5.6.9   | Security Key Redirection                                         | 29 |
| 5.6.10  | Agentless Access for Operational Technology (OT)                 | 29 |
| 5.6.11  | LAPS Integration                                                 | 31 |
| 5.6.12  | Chat                                                             | 31 |
| 6       | Architecture                                                     | 32 |
| 6.1     | ONE platform architecture                                        | 32 |
| 6.2     | Session Initialization                                           | 33 |
| 6.3     | Modern TLS 1.3 Mutually Authenticated Session Handshake          | 34 |
| 6.4     | Legacy Secure Network Protocol and Backend Connection Flows      | 36 |
| 7       | Encryption and Data Protection                                   | 38 |
| 7.1     | Account Data Protection                                          | 38 |
| 7.2     | Encryption                                                       | 38 |
| 7.3     | TeamViewer ONE, DEX and AI Data Handling                         | 38 |
| 8       | Secure Development and Product Security                          | 40 |
| 8.1     | Our Secure Software Development Lifecycle (S-SDLC)               | 40 |
| 8.2     | Security Testing and Composition Analysis (SCA)                  | 40 |
| 8.3     | Penetration Testing                                              | 40 |
| 8.4     | Code Signing                                                     | 40 |
| 8.5     | Software Bill of Materials (SBOM)                                | 41 |
| 8.6     | Product Security Incident Response Team (PSIRT)                  | 41 |
| 8.7     | Vulnerability Disclosure Program (VDP)                           | 41 |
| 8.8     | Bug Bounty Program                                               | 42 |
| 8.9     | Security Bulletins                                               | 42 |
| 8.10    | Certified Numbering Authority (CNA)                              | 43 |
| 8.11    | Internal Product Vulnerability Management Timeframes             | 43 |
| 9       | Hosting and Infrastructure                                       | 44 |
| 9.1     | Hosting and Infrastructure Overview                              | 44 |

|     |                                                                 |    |
|-----|-----------------------------------------------------------------|----|
| 9.2 | Cloud Providers, Sub-processors and Infrastructure Dependencies | 45 |
| 9.3 | Network Connectivity Requirements                               | 45 |
| 9.4 | Data Residency and Processing Locations                         | 45 |
| 9.5 | Business Continuity and Service Availability                    | 46 |
| 9.6 | Security Incident Management                                    | 46 |
| 10  | Definitions                                                     | 47 |
| 11  | Public Source Links                                             | 54 |

## Table of figures

|                                                                                                       |    |
|-------------------------------------------------------------------------------------------------------|----|
| Figure 1: TeamViewer ONE capabilities map .....                                                       | 17 |
| Figure 2: Secure Unattended Access: TeamViewer Session Initialization and Secure Handshake Flow ..... | 19 |
| Figure 3: Secure Client Enrollment and Assignment Workflow .....                                      | 20 |
| Figure 4: TeamViewer Tensor OT Architecture with Hybrid Conditional Access and Agentless Access.....  | 30 |
| Figure 5: TeamViewer Remote Session Initialization and Certificate Issuance Flow .....                | 33 |
| Figure 6: Modern TLS 1.3 Mutually Authenticated Session Handshake Flow.....                           | 35 |
| Figure 7: Legacy Secure Network Protocol Session Initialization and Backend Connection Flow .....     | 37 |
| Figure 8: High-level product vulnerability response lifecycle .....                                   | 44 |

## Material Revision

| Version | Date    | Author                    | Description                                                                                                                                |
|---------|---------|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| 1.0     | 02/2022 | Product Security          | Initial publication                                                                                                                        |
| 1.1     | 03/2024 | Product Security          | Updated content                                                                                                                            |
| 1.2     | 08/2025 | Product Security          | Added content                                                                                                                              |
| 1.3     | 03/2026 | Customer Trust & Security | Added and updated content                                                                                                                  |
| 2.0     | 08/2026 | Customer Trust & Security | Added TeamViewer ONE, digital workplace, endpoint management, DEX and AI security content; updated Tensor-only references where applicable |

### Notice

This document provides a general, non-binding overview of selected TeamViewer security features and architecture. Feature availability, technical implementation and applicable controls may vary by product, license, version, configuration, region and contractual terms. The applicable product documentation and contractual documents take precedence.

## 1 Introduction and Security Fundamentals

### 1.1 About TeamViewer

TeamViewer is a leading global technology company that provides secure remote connectivity, enterprise remote access, endpoint management, and Digital Employee Experience (DEX) solutions. Since its founding in 2005, TeamViewer has helped organizations connect people, devices, and systems across distributed IT environments, enabling secure remote support, remote work, and unattended access at scale.

Today, TeamViewer's platform combines the secure remote connectivity capabilities of TeamViewer with advanced endpoint visibility, monitoring, automation, and Digital Employee Experience capabilities. Together, these solutions help organizations proactively identify and resolve endpoint

issues, securely manage complex IT and operational technology (OT) environments, improve employee productivity, and strengthen their overall security posture.

In addition, TeamViewer supports digital transformation initiatives through AI-powered capabilities, endpoint management, automation, and augmented reality-based workflows, while integrating with leading enterprise technology platforms and identity providers. TeamViewer is headquartered in Göttingen, Germany, and serves organizations of all sizes across a wide range of industries worldwide.

## 1.2 Fundamentals of TeamViewer Security

Organizations rely on TeamViewer platform capabilities to securely access, support, manage, monitor, and optimize endpoints across distributed IT environments. These capabilities range from attended and unattended remote access to endpoint monitoring, Digital Employee Experience (DEX), automation, and proactive remediation of device and application issues. Depending on the configuration, authorized users can remotely access and control computers and devices in real time, while administrators can gain visibility into endpoint health, performance, compliance, and user experience across their managed environments.

Because these capabilities provide access to critical systems, devices, and operational data, they must be protected by robust security controls and stringent security protocols. Whether enabling remote support, managing enterprise endpoints, or collecting operational telemetry for proactive issue detection and remediation, TeamViewer applies a security-by-design approach across its platform.

Our goal is to ensure that access to systems, devices, and operational insights remains secure, trusted, and transparent. Security is embedded into every layer of the platform, including authentication, authorization, encryption, data protection, auditability, and administrative controls. By combining secure remote connectivity with proactive endpoint visibility and management capabilities, TeamViewer helps organizations improve operational resilience while maintaining a strong security posture.

## 1.3 Quality Management

Security management is inconceivable without an established quality management system. TeamViewer is a leading global vendor in the market with an ISO 9001 certified quality management system (QMS). Our quality management follows internationally recognized standards and is reviewed by external audits on an annual basis.

## 1.4 Information Security and Compliance

TeamViewer deploys industry leading cyber security resources both internally and externally. We are fully dedicated to ensuring the best possible protection of our IT infrastructure. Our 24/7 Security Operations Center (SOC) monitors TeamViewer's system landscape in real time. A Computer Security Incident Response Team (CSIRT) and Product Security Incident Response Team (PSIRT) are poised to respond to threats.

TeamViewer undergoes internal reviews and independent assessments against applicable security and compliance frameworks. Scope, frequency and applicability vary by certification, report, product and service. Additional information can be found in the TeamViewer [Compliance Portal](#) and [Trust Center](#). Product and certification scope can vary by product, service, report period, and region.

## 1.5 Data Centers and Backbone

To provide the highest levels of security, availability, and resilience for TeamViewer services, TeamViewer leverages secure data centers and cloud infrastructure operated in accordance with industry-recognized security standards and best practices. The platform is designed with redundancy across power supplies, network connectivity, and critical infrastructure components to support service continuity and operational resilience.

TeamViewer implements a comprehensive set of [Technical and Organizational Measures \(TOMs\)](#) to protect customer data and systems. These measures include access controls, encryption, network security monitoring, vulnerability management, security incident response processes, business continuity and disaster recovery procedures, change management controls, secure software development practices, and regular security assessments. Controls are reviewed and maintained through TeamViewer's ISMS and related governance processes.

TeamViewer's ISMS is certified to ISO/IEC 27001, the internationally recognized standard for information security management. In addition, TeamViewer undergoes regular independent assessments and audits against recognized security and compliance frameworks, including SOC 2 Type II, CSA STAR, TISAX, and HIPAA/HITECH controls where applicable. Certain TeamViewer services and platforms may also maintain additional certifications or attestations depending on the product scope and service offering.

Specific hosting locations, sub processors, and compliance scopes may vary depending on the applicable product, feature set, geographic region, and contractual requirements. Further information regarding TeamViewer's security, privacy, compliance posture, and sub processors is available through the TeamViewer [Trust Center](#) and [Compliance Portal](#).

## 1.6 References

Leading enterprises across industries - such as financial services, healthcare, government, and other sectors with highly sensitive data - leverage TeamViewer for secure remote access and support, digital workplace operations, IoT, and industrial augmented reality solutions. Customer success stories are available on the [TeamViewer website](#).

# 2 Security Overview

TeamViewer works to create a smarter working world through leading edge remote connectivity and digital workplace capabilities. Customers provide spontaneous support over the internet, access unattended computers and other devices, and use platform capabilities to monitor, manage,

automate, and optimize digital work. Clearly, using this powerful functionality over the internet must be protected with stringent security protocols. As such, we put security at the center of everything we do by engineering our software by security by design. Our goal is to ensure access to computers and other devices is safe. Your security is our highest priority: users only trust secure solutions, and we are fully committed to providing secure solutions to sustain long-term business success. We work diligently to ensure our solutions are secure and aligned with the latest security and data privacy standards.

## 3 Shared Responsibility Model

TeamViewer follows a shared responsibility model in which TeamViewer is responsible for securing and operating the underlying services, infrastructure, and platform controls, while customers remain responsible for the configuration, administration, and usage of their TeamViewer environments. The allocation of responsibilities may vary depending on the deployed products, enabled features, integration architecture, and customer-specific requirements.

Understanding these shared responsibilities helps organizations effectively implement security controls, meet compliance requirements, and align TeamViewer deployments with their internal governance frameworks.

### 3.1 TeamViewer Responsibilities

TeamViewer is responsible for the security and operation of the TeamViewer services and supporting infrastructure used to deliver TeamViewer Remote, Tensor, TeamViewer ONE, DEX, Automation, AI capabilities, and related services.

This includes:

- Development and maintenance of the TeamViewer platform and services
- Secure Software Development Lifecycle (Secure SDLC)
- Vulnerability management and security patching of TeamViewer-operated services
- Product Security Incident Response Team (PSIRT) operations
- Security monitoring, logging, and incident response for TeamViewer-managed environments
- Encryption technologies and cryptographic controls used by TeamViewer services
- Protection of TeamViewer-managed systems and infrastructure
- Business continuity and disaster recovery processes
- Compliance and certification activities applicable to TeamViewer-operated environments
- Administration of TeamViewer cloud services and supporting infrastructure
- Availability and operational resilience of the TeamViewer platform

## 3.2 Customer Responsibilities

Customers remain responsible for the configuration, governance, and secure use of their TeamViewer environment.

This includes:

- User lifecycle management and access approvals
- Identity governance and account management
- Multi-factor authentication (MFA) configuration and enforcement
- Single Sign-On (SSO) integration and configuration
- Conditional Access policy design and administration
- Endpoint hardening and device security
- Operating system and application patch management for customer-managed devices
- User training and security awareness
- Review of audit logs, reports, and recorded session data where applicable
- Classification and protection of customer data processed within TeamViewer environments
- Configuration of retention, governance, and monitoring controls where applicable
- Secure management of integrations with third-party systems

## 3.3 Shared Security Responsibilities

Certain security controls require cooperation between TeamViewer and the customer to achieve the desired security outcome. While TeamViewer secures and operates the underlying platform, infrastructure, and service controls, customers remain responsible for configuring and governing their own environment, identities, users, devices, policies, network controls, and operational processes. The following table illustrates common areas of shared responsibility.

| Security Area                             | TeamViewer Responsibility                                                                                                                      | Customer Responsibility                                                                                                                  |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Infrastructure Security                   | Secure TeamViewer-operated servers, cloud services, data centers, networking, monitoring, and platform infrastructure                          | Evaluate infrastructure suitability for organizational requirements and review available assurance documentation                         |
| Application Security                      | Develop, test, secure, maintain, and patch TeamViewer services and applications through the Secure SDLC and vulnerability management processes | Deploy supported software versions and configure security settings, policies, and controls appropriately                                 |
| Authentication                            | Provide authentication mechanisms, SSO integration, MFA capabilities, and identity integration interfaces                                      | Configure identity providers, MFA policies, account governance, and authentication requirements                                          |
| Access Control                            | Provide RBAC, Conditional Access, Hybrid Conditional Access, device policies, and policy-management capabilities                               | Define and administer access policies, approval processes, least-privilege access, and user authorization                                |
| Encryption and Data Protection            | Implement and maintain encryption technologies, key-management processes, and platform-level data protection controls                          | Protect endpoint devices, credentials, local data, and customer-managed encryption controls where applicable                             |
| Network Security                          | Provide secure connectivity architecture, encrypted communications, and network-security controls for TeamViewer services                      | Configure firewalls, allowlists, proxy settings, network segmentation, and customer-specific network-security controls                   |
| Endpoint Management                       | Provide endpoint-management, monitoring, automation, patch-management, and management capabilities                                             | Configure policies, maintain managed devices, remediate findings, and manage endpoint-security configurations                            |
| Logging and Auditability                  | Provide event logs, connection reports, session recording capabilities, audit trails, and reporting interfaces                                 | Enable, review, retain, monitor, and act upon security-relevant logs and audit information according to internal requirements            |
| Monitoring and Threat Detection           | Monitor TeamViewer-operated environments through the SOC and security operations processes                                                     | Review customer logs, alerts, reports, and monitoring outputs and respond to identified risks and incidents                              |
| AI Capabilities                           | Implement AI security, privacy, governance, tenant-isolation, and administrative controls                                                      | Control AI feature enablement, permissions, acceptable-use policies, governance, and organizational oversight                            |
| Compliance and Certifications             | Maintain TeamViewer certifications, attestations, audits, and compliance programs                                                              | Assess applicability to organizational requirements and implement customer-side compliance controls                                      |
| Business Continuity and Disaster Recovery | Maintain business continuity, disaster recovery, resilience testing, and recovery processes for TeamViewer-operated services                   | Maintain organizational continuity plans and recovery procedures for customer-managed environments                                       |
| Data Retention and Session Recording      | Provide retention and recording capabilities where available and configurable                                                                  | Define retention periods, recording policies, storage locations, and evidentiary requirements in accordance with organizational policies |
| Data Retention and Lifecycle Management   | Provide retention, deletion, export and lifecycle management capabilities where applicable                                                     | Define retention schedules, legal hold requirements, deletion policies and governance requirements                                       |

## 4 Security Governance, Certifications and Compliance

### 4.1 Security Governance

TeamViewer integrates security into its business operations, product development lifecycle, and service delivery processes through a comprehensive governance framework designed to support the secure operation of its products, services, data, and infrastructure.

TeamViewer maintains an Information Security Management System (ISMS) that supports risk management, security governance, continuous improvement, regulatory compliance activities, and the implementation of security controls across applicable business functions. The security governance framework includes documented policies and standards, risk-management processes, security awareness activities, vulnerability management, supplier management, incident response, business continuity management, and compliance oversight.

Security responsibilities are distributed across dedicated teams responsible for information security, product security, privacy, compliance, infrastructure operations, and secure software development. These functions collaborate to support security throughout the product lifecycle, from design and development through deployment, operation, maintenance, and retirement.

Security controls, governance processes, and operational safeguards are regularly reviewed through internal assessments, independent audits, certification activities, penetration testing programs, vulnerability management processes, and continuous monitoring activities.

### 4.2 Segregation of Corporate and Production Environments

TeamViewer maintains logical and administrative separation between corporate environments and production systems used to deliver customer-facing services. This segregation is designed to reduce risk, limit unauthorized access, support least-privilege principles, and strengthen the protection of customer data and service infrastructure.

Access to production environments is restricted to authorized personnel with a legitimate business need and is subject to defined access-management processes, authentication requirements, logging, monitoring, and periodic review activities. Privileged access is governed through security controls designed to help ensure accountability and appropriate oversight of production activities.

Corporate user environments, end-user computing systems, business applications, and productivity services are managed separately from production service environments. Additional technical and administrative controls are implemented to help maintain separation between business operations and customer-facing service infrastructure.

These controls form part of TeamViewer's broader Information Security Management System (ISMS) and are subject to internal governance activities, independent certification assessments, audits, risk-management processes, and continuous monitoring activities. Applicable controls may be evaluated through certifications and assurance activities such as ISO/IEC 27001, SOC 2 Type II, CSA STAR, TISAX, and other independent assessments where relevant.

### 4.3 Certifications, Attestations and Audits

To provide customers with independent assurance regarding the effectiveness of its security and operational controls, TeamViewer maintains a portfolio of certifications, attestations, assessments, and third-party audits.

These independent assessments evaluate applicable governance processes, technical safeguards, operational controls, security management activities, compliance programs, and service delivery controls.

Depending on the applicable service and assessment scope, TeamViewer maintains certifications and assurance programs that may include:

- ISO/IEC 27001
- SOC 2 Type II
- CSA STAR Level 2
- [Cloud Control Matrix \(CCM\) /CAIQ](#)
- HIPAA attestation
- TISAX

- BSI C5
- Cyber Essentials
- Additional security, privacy, and compliance assessments as applicable

Independent certification bodies and auditing organizations periodically assess the effectiveness and operation of controls included within the respective assessment scope.

Because TeamViewer continuously evolves its products, services, and supporting infrastructure, certification boundaries, scope definitions, and covered services may change over time. Customers should therefore refer to the applicable certification reports, attestations, and Trust Center resources for authoritative scope information.

## 4.4 Compliance and Regulatory Support

TeamViewer provides security, privacy, compliance, and governance controls designed to support customers in performing supplier due diligence and meeting their own internal governance and risk-management requirements.

Customers may use TeamViewer's security documentation, certifications, audit reports, compliance artefacts, contractual commitments, and transparency resources as part of their own compliance and vendor-assurance programs.

Additional compliance-related information is available through:

- TeamViewer Trust Center
- TeamViewer Compliance Portal
- Technical and Organizational Measures (TOMs)
- Data Processing Agreements (DPAs)
- Sub-processor disclosures
- Security and compliance documentation

While TeamViewer operates controls intended to support security and compliance requirements, customers remain responsible for determining the applicability of TeamViewer services to their specific legal, regulatory, contractual, and business obligations.

## 4.5 Certification Scope Matrix

The following matrix provides a high-level overview of certifications, attestations, and assurance activities that apply to TeamViewer products and services. The authoritative scope of each certification is defined by the applicable certification report, attestation, or assessment documentation.

|                                                  | TeamViewer Remote                     | TeamViewer Tensor                     | TeamViewer ONE                        |
|--------------------------------------------------|---------------------------------------|---------------------------------------|---------------------------------------|
| <b>Certification / Attestation</b>               |                                       |                                       |                                       |
| ISO/IEC 27001                                    | ✓                                     | ✓                                     | ✓                                     |
| ISO/IEC 9001                                     | ✓                                     | ✓                                     | ✓                                     |
| SOC 2 Type II                                    | ✓                                     | ✓                                     | ✓                                     |
| CSA STAR Level 2                                 | ✓                                     | ✓                                     | ✓                                     |
| HIPAA Attestation                                | ✓                                     | ✓                                     | ✓                                     |
| TISAX                                            | ✓                                     | ✓                                     | x                                     |
| BSI C5                                           | ✓                                     | ✓                                     | x                                     |
| Cyber Essentials                                 | ✓                                     | ✓                                     | x                                     |
| <b>Additional certifications and assessments</b> | Refer to <a href="#">Trust Center</a> | Refer to <a href="#">Trust Center</a> | Refer to <a href="#">Trust Center</a> |

The scope, reporting period, covered services, and applicability of certifications may evolve as TeamViewer products, infrastructure, and certification boundaries change. Customers should consult the underlying assurance documentation for definitive scope information.

Customers requiring certification reports, attestations, audit summaries, or additional assurance artefacts may request access through the TeamViewer Trust Center, Compliance Portal, or their TeamViewer representative, subject to applicable confidentiality requirements.

## 4.6 Customer Assurance Resources

TeamViewer supports customer security-review and supplier-assurance activities through a combination of publicly available security documentation, certification reports, audit artefacts, compliance resources, and customer-facing security materials.

Available resources available on <https://compliance.teamviewer.com/> may include:

- Security whitepapers
- Security architecture documentation
- Encryption documentation
- TeamViewer AI security documentation
- Product security documentation
- Trust Center resources
- Compliance resources and certifications
- Security advisories and vulnerability disclosures

These resources are intended to help customers evaluate TeamViewer's security posture, governance framework, compliance activities, and operational controls as part of their procurement and supplier-assurance processes.

# 5 Platform Capabilities and Security Controls

To get started with TeamViewer security, please familiarize yourself with the most important security recommendations and considerations:

- [Golden Security Rules](#) for TeamViewer accounts and remote access usage.
- [Proper configuration of unattended access](#), including Easy Access, strong authentication, and access restrictions.
- [TeamViewer Security Handbook](#) and [Trust Center](#) resources.
- [Product-specific hardening and configuration guidance](#) for TeamViewer Tensor, TeamViewer Remote, TeamViewer ONE, and associated platform capabilities.
- Customer-side governance, such as least privilege, regular access reviews, identity provider controls, and monitoring of administrative activities.

## Product applicability

This document covers TeamViewer Remote, TeamViewer Tensor and TeamViewer ONE. The remote-connectivity, identity, access-control and session-security sections apply to the relevant TeamViewer products as described in each section. TeamViewer ONE-specific capabilities, including Digital Employee Experience (DEX), endpoint management, Patch Management, Automations, DEX Hub, DEX Insights and certain AI-supported workflows, apply only where the customer has licensed and enabled the corresponding TeamViewer ONE capability. Customers using TeamViewer Tensor without TeamViewer ONE are not affected by DEX or other TeamViewer ONE-specific controls and may disregard those sections.

## 5.1 Components

### 5.1.1 Clients

#### TeamViewer Remote, TeamViewer Tensor and TeamViewer ONE Clients

TeamViewer Remote brings a modern approach to connectivity and improved security standards for remote support, remote work, and remote access. TeamViewer Remote and TeamViewer Tensor clients are native applications available for Windows, macOS and Linux as well as mobile platforms. TeamViewer has also leveraged web technologies to help provide seamless experience between the web and desktop interfaces.

TeamViewer ONE extends this remote connectivity foundation into an integrated digital workplace platform. It brings together secure remote access and support, endpoint management and security, remote monitoring and management, digital employee experience (DEX), hardware and software asset management, patch management, mobile device management, application experience monitoring, automation, analytics, and AI-supported capabilities into a unified platform experience. Availability of specific capabilities depends on the purchased TeamViewer ONE package and applicable add-ons.

### **TeamViewer Web Client and ONE Platform Experience**

TeamViewer has worked to provide a modern and web-first approach to our solution. The TeamViewer web client uses HTML5 to provide secure remote access on the web without the need to download a native application. This works to combine functionality into a unified view that simplifies usability for technicians and administrators. For TeamViewer ONE, this unified platform approach is extended to digital workplace management, endpoint visibility, automation, and DEX workflows so IT teams can manage, support, and optimize digital work from one platform.

### **TeamViewer Automation Client**

The TeamViewer Automation Client is an endpoint component used for supported automation and Tia troubleshooting workflows. For Tia troubleshooting, it operates as a locally integrated extension of the TeamViewer Remote Client. Its endpoint resource use depends on the enabled functionality, configuration, diagnostic activity, and whether it is connected to additional TeamViewer ONE or DEX platform services. Detailed deployment and resource-consumption information is provided in the applicable product documentation.

## **5.1.2 Web Console and Administration**

The [TeamViewer Web Console](#) and web-based administration experiences support user management, device management, policy configuration, connection reporting, and administration of TeamViewer environments. Data transfer is protected using TLS encryption, and sensitive account data is protected using the account data encryption mechanisms described in this document.

TeamViewer ONE administration adds central control for managed devices, policies, automations, DEX and endpoint management workflows, user and role permissions, reporting, and integrations. TeamViewer ONE supports centralized management for distributed teams and integrates with existing IT ecosystems such as ITSM, endpoint management, security, and identity tools where supported by the applicable license and integration package.

## **5.1.3 TeamViewer ONE Platform**

TeamViewer ONE is the digital workplace platform for IT teams. It is designed to help IT teams manage, support, secure, and optimize digital work by bringing together secure remote connectivity, endpoint management, remote monitoring and management, Digital Employee Experience (DEX), automation, analytics, and AI-powered workflows into a single platform. TeamViewer ONE enables organizations to move from reactive support to proactive and increasingly autonomous IT operations.

TeamViewer ONE combines secure attended and unattended remote access, endpoint telemetry, device management, patching, software deployment, asset visibility, experience monitoring, automation, and AI-assisted capabilities. This enables IT teams to securely support users and devices, identify operational issues earlier, automate remediation workflows, reduce manual effort, and validate outcomes across distributed digital workplaces.

## Capabilities areas

## TeamViewer ONE capabilities and security and control relevance

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Secure remote access and support</b>  | Cross-platform remote access and control attended and unattended access, remote support, remote desktop access, web-based access, session reporting, and enterprise remote connectivity capabilities. Uses connection authentication, end-to-end encrypted sessions, access controls, MFA, SSO, Conditional Access, policies, auditability, and optional enterprise security controls.                             |
| <b>Endpoint management and security</b>  | Device monitoring, policy management, patch management, software deployment, asset discovery, endpoint visibility, mobile device management (MDM), remote monitoring and management (RMM), and endpoint protection add-ons where licensed. Supports secure configuration, centralized governance, vulnerability reduction through patching, policy enforcement, and operational visibility across managed devices. |
| <b>Digital Employee Experience (DEX)</b> | Endpoint insights, experience analytics, user feedback, early detection, prioritization, closed-loop remediation, and reporting. Uses role-based access, tenant controls, telemetry processing safeguards, and data minimization to support secure operational insights.                                                                                                                                           |
| <b>Automation</b>                        | Policy-based TeamViewer ONE Automations, remote session automations, script libraries, automated remediation workflows, and operational orchestration. Governed by permissions, policies, execution history, auditability, reviewable artifacts, and administrator controls.                                                                                                                                       |
| <b>AI</b>                                | Session Insights, TeamViewer Intelligent Agent (Tia), AI-assisted scripting, DEX Insights, DEX Hub, Tia Reporting, AI-supported troubleshooting, intelligent recommendations, and natural-language reporting where available. Uses admin-controlled rollout, permissions, policies, encryption, tenant-scoped controls, data minimization, anonymization where applicable, and defined AI processing boundaries.   |
| <b>Integrations and ecosystem</b>        | Uses admin-controlled rollout, permissions, policies, encryption, tenant-scoped controls. Integration access is governed through authentication, authorization, permissions, tenant boundaries and audit capabilities supported by the applicable integration.                                                                                                                                                     |

## TeamViewer ONE capability map

Connectivity & digital workplace capabilities governed by customer security controls

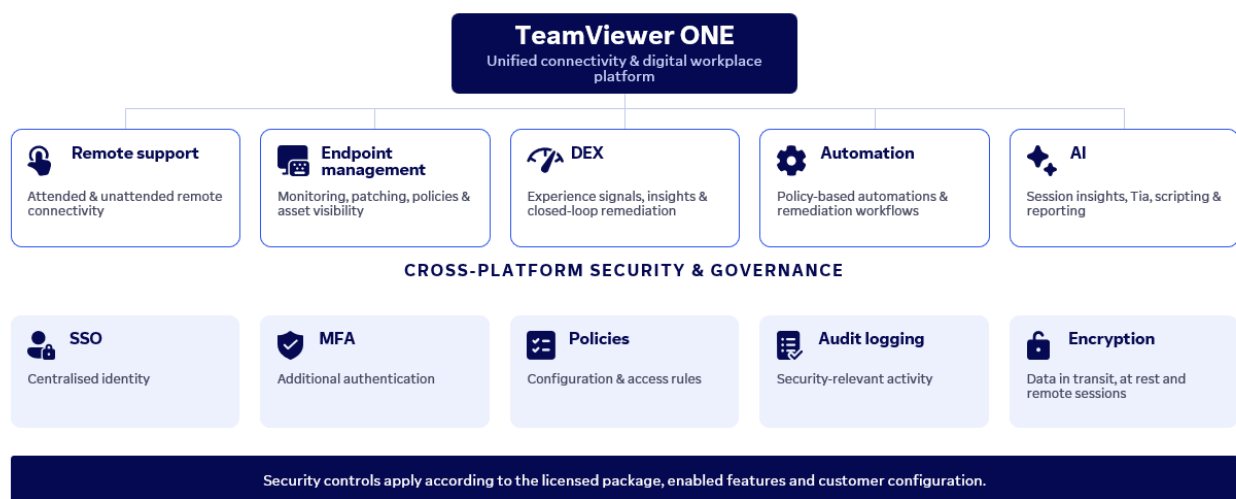


Figure 1: TeamViewer ONE capabilities map

## 5.1.4 TeamViewer AI and Intelligence Capabilities

TeamViewer products offer [several AI-supported capabilities](#). These include TeamViewer AI features for session documentation, in-session troubleshooting with TeamViewer Intelligent Agent (Tia), AI-assisted scripting, DEX Insights, DEX Hub, and Tia Reporting, depending on the product environment and license. TeamViewer AI is designed to support efficiency while keeping customers in control through settings, permissions, policies, role-based controls, data minimization, anonymization where applicable, and encryption in transit and at rest.

Session Insights can generate structured summaries, action steps, and labels for support sessions. Tia can provide guided troubleshooting based on defined inputs, permissions, and read-only diagnostic information. AI-assisted scripting can help draft scripts faster, while execution remains permission-controlled and subject to authorized workflows. In TeamViewer DEX and TeamViewer ONE Enterprise, AI capabilities may support insights, automation libraries, and natural-language reporting based on tenant-scoped DEX data and governed access controls.

For supported Tia troubleshooting scenarios, the TeamViewer Automation Client provides a local endpoint component used to collect diagnostic information requested during the troubleshooting workflow. The Automation Client is locally integrated with the TeamViewer Remote Client. Communication associated with Tia troubleshooting continues to use the TeamViewer Remote Client infrastructure and does not introduce a separate remote-access channel. Access to Tia troubleshooting remains subject to the customer's TeamViewer configuration, permissions, policies, and applicable access controls, including Conditional Access where configured.

For more information, please see our knowledge base articles: [Enable Tia troubleshooting in TeamViewer](#)

Additional information regarding TeamViewer AI security, architecture, data handling, governance controls, and processing workflows is available in the dedicated TeamViewer AI security resources published through the [TeamViewer Trust Center](#) and related [TeamViewer AI security documentation](#). These resources provide detailed architecture diagrams and explanations for TeamViewer AI capabilities, including Session Insights, Tia (TeamViewer Intelligent Agent), AI-assisted scripting, DEX Intelligence Insights, DEX Hub, and Tia Reporting. They also describe relevant administrative controls, data protection mechanisms, encryption, tenant isolation, auditability, anonymization and minimization measures, and AI service boundaries.

Customers who require a deeper technical understanding of TeamViewer AI security and data processing can refer to the following resources:

- [TeamViewer AI security, privacy, and customer control](#)
- [TeamViewer AI Security, Control, and Data Handling for TeamViewer Remote, Tensor, and TeamViewer ONE](#)
- [TeamViewer AI Security, Control, and Data Handling for TeamViewer DEX and TeamViewer ONE Enterprise](#)

These documents include detailed architecture diagrams and security explanations that complement the high-level overview provided in this document. Product availability, feature scope, processing details, and controls may vary depending on the applicable product environment, license, configuration, region, and contractual terms.

## 5.2 Main Use Cases

### 5.2.1 Secure Attended Access

To accomplish [secure attended access](#), TeamViewer leverages Session Codes that use public key cryptography to identify, authenticate and authorize users for accessing devices and combine them with the Access Control feature. With Access Control configuration, mandatory local approval for attended access can then be enforced via Device Policy. Following the zero-trust approach - "never trust, always verify" - access needs to be granted explicitly to specific devices or groups. Access Control provides just-in-time approval by the user on the device to secure attended support sessions.

### 5.2.2 Secure Unattended Access

The [Easy Access feature](#) uses public key cryptography to identify, authenticate and authorize users for accessing devices for unattended access only. Once a user has been granted Easy Access permission on a device, they can connect to the device without a password, using strong public key cryptography instead. Using this connection method instead of a personal password reduces the risk of unauthorized access using exposed or stolen device passwords. Easy Access is built on top of the TeamViewer Account and is commonly supported by SSO and Conditional Access for scalable and robust unattended access control.

In addition, *Access Control for incoming connections*, *Device Policy* and *Conditional Access* can be used to apply further fine-grained access restrictions for device connections. This feature is only for devices that have a TeamViewer service installed on the device.

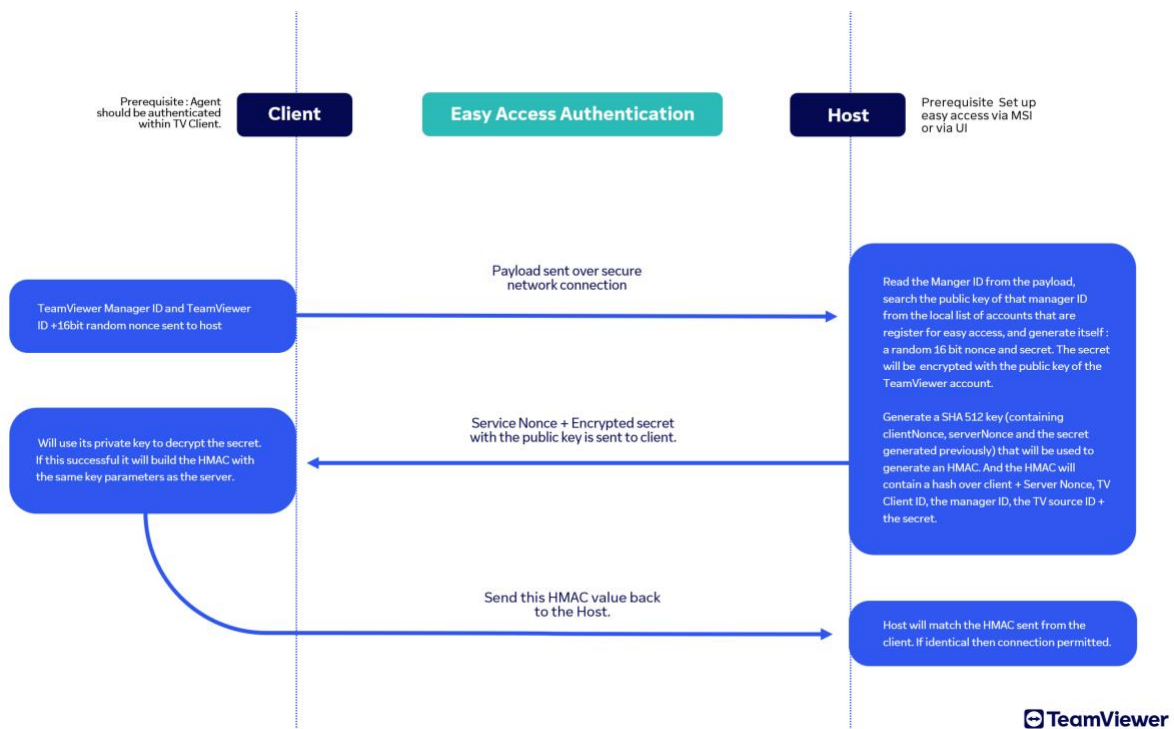


Figure 2: Secure Unattended Access: TeamViewer Session Initialization and Secure Handshake Flow

### 5.3 Client Enrollment / Assignment

The diagram below outlines the secure client enrollment and assignment workflow in TeamViewer, applicable across all major operating systems. While assignments can be initiated manually, deployments are typically performed through software deployment solutions, Mobile Device Management (MDM) platforms, or enterprise rollout tools to ensure consistency and scalability.

The assignment process is designed to ensure that device assignments are authenticated, verified, and securely exchanged between the endpoint and the TeamViewer backend. During enrollment, assignment information is validated and linked to the designated TeamViewer account or company profile, helping to ensure assignment integrity and alignment between local device data and backend records.

Once assigned, the device securely stores the information required to maintain its association with the corresponding TeamViewer environment. This enables centralized administration, policy deployment, access management, inventory visibility, and other management capabilities across TeamViewer Tensor and TeamViewer platform services.

To further support large-scale deployments and environments with intermittent connectivity, TeamViewer also supports offline assignment workflows. In these scenarios, assignment information can be cached locally until the device establishes connectivity with the TeamViewer network, helping to improve deployment success rates in disconnected or unstable environments.

Further information regarding TeamViewer deployment and assignment can be found in the TeamViewer Knowledge Base under [Mass Deployment on Windows – Overview](#).

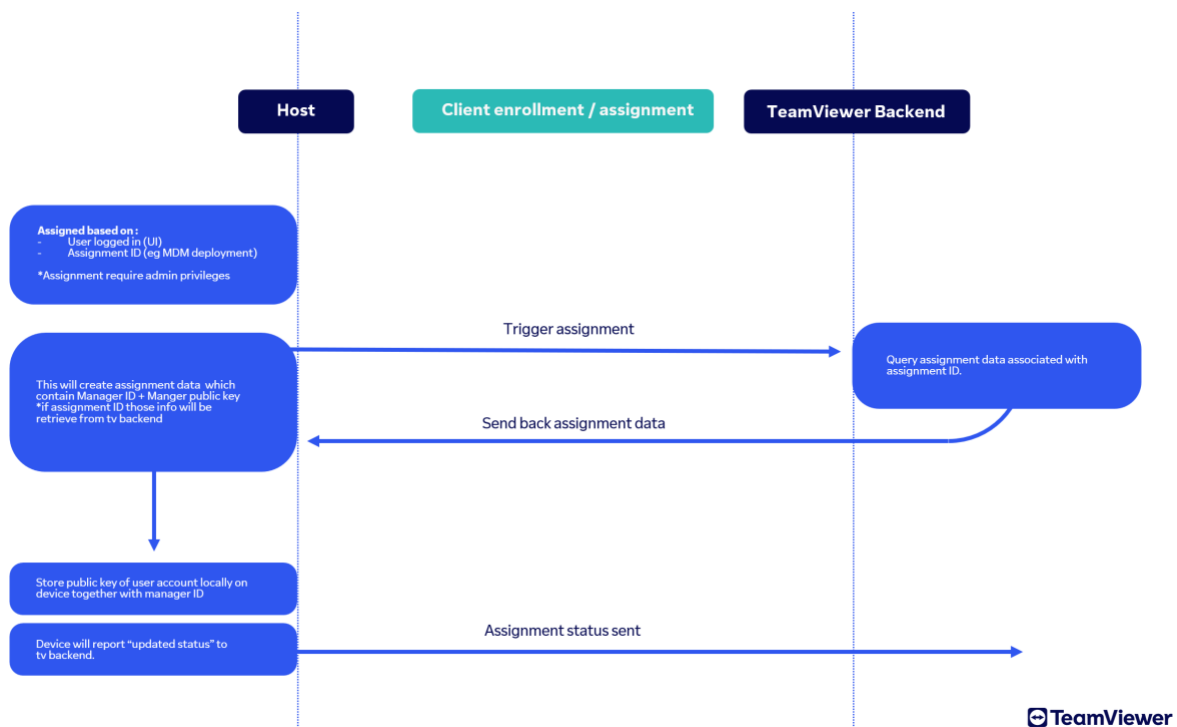


Figure 3: Secure Client Enrollment and Assignment Workflow

## 5.4 Connection Authentication and Device Access Control

### 5.4.1 Block- and Allowlist

Especially when TeamViewer is used for unattended computer or device maintenance and support (i.e., no connection partner is present at the remote computer or device to approve incoming connection requests), the Allowlist provides an additional layer of security. By adding TeamViewer IDs, TeamViewer accounts, or company profiles to an Allowlist, organizations can restrict access to specific devices so that only explicitly authorized users, accounts, or company profiles can establish remote connections.

Even if a device password is exposed or compromised, unauthorized third parties will still be unable to access the device unless they are explicitly included in the Allowlist. Allowlist restrictions can be configured for individual TeamViewer IDs, TeamViewer accounts, or entire company profiles and can be centrally managed through TeamViewer policies.

The Blocklist allows organizations to prevent specific TeamViewer IDs, accounts, or devices from establishing connections to managed computers or devices. Accounts or IDs included in the Blocklist cannot connect to the protected device. However, other authorized users who successfully authenticate through approved access methods may still be granted access according to the configured security settings.

For most enterprise use cases, TeamViewer recommends an Allowlist-based approach as part of a zero-trust access strategy, ensuring that only explicitly authorized users and devices can establish remote connections.

**Note:** Devices, accounts, or partners included in the Blocklist can still be used for outgoing TeamViewer connections initiated from your environment. For more information, please refer to the TeamViewer Knowledge Base article: [Block and allowlist](#)

## 5.4.2 Two-Factor Authentication for Connections (TFA/MFA)

TeamViewer supports Two-Factor Authentication for Connections (TFA/MFA) as an additional security layer for remote access. When enabled, connections to a computer or device must be approved through a push notification sent to designated mobile devices before the session can be established. This helps ensure that only authorized users can initiate remote connections, even if account credentials have been compromised.

For enterprise deployments, this functionality can be further enhanced through Conditional Access. Conditional Access enables organizations to centrally enforce connection approval policies across multiple devices, groups, or environments. Rather than requiring approval at the individual device level, connection authorization can be managed at the account, group, or policy level, providing greater scalability and administrative control for large deployments.

By combining strong user authentication with centralized policy enforcement, organizations can implement a zero-trust approach to remote access, helping ensure that every connection is explicitly verified before access is granted.

For more information, please refer to the TeamViewer Knowledge Base article: [Two-Factor Authentication for Connections](#).

## 5.4.3 Access Control for Incoming and Outgoing Connections

TeamViewer allows administrators to individually configure the connection modes and permissions available during remote sessions. For example, remote support or meeting devices can be configured so that incoming connections are restricted or disabled, file transfer capabilities are limited, screen recording is controlled, or other session features are managed according to organizational requirements.

Applying the principle of least privilege, organizations can limit functionality to only those features required for a specific use case. Reducing unnecessary capabilities helps minimize system exposure, supports compliance requirements, and provides additional control over how remote sessions are conducted.

Combined with policies, Conditional Access, Allowlists, and other TeamViewer security controls, access control settings help organizations enforce secure and consistent remote access configurations across their environments.

## 5.4.4 Conditional Access

TeamViewer Tensor provides Conditional Access, a centralized security capability designed to enforce a zero-trust approach to remote connectivity. By default, access can be restricted unless explicitly permitted through administrator-defined policies and rules.

### 5.4.4.1 TeamViewer Managed Conditional Access

Conditional Access enables organizations to define and enforce access controls based on users, groups, devices, managed device groups, and other organizational requirements. Policies can be configured to support specific operational and security needs, including approval-based access workflows, scheduled access windows, time-based restrictions, and granular authorization controls for remote connections.

By centralizing access decisions, Conditional Access helps organizations ensure that remote access is only granted to authorized users and devices under approved conditions. This provides an additional layer of protection beyond traditional authentication mechanisms and supports governance, compliance, and operational security requirements.

When combined with *Single Sign-On (SSO)*, *Multi-Factor Authentication (MFA)*, *Bring Your Own Certificate (BYOC)*, audit logging, device policies, and role-based access controls, Conditional Access helps organizations implement a comprehensive zero-trust remote access strategy based on the principle of "never trust, always verify."

For more information, please refer to the TeamViewer Knowledge Base article: [Conditional Access](#)

### 5.4.4.2 Hybrid Conditional Access (for Segmented and Security-Sensitive Environments)

For organizations operating highly segmented or security-sensitive environments, Conditional Access can be further extended through Hybrid Conditional Access, which enables policy enforcement and controlled access into isolated OT and industrial networks while maintaining network segmentation and centralized governance.

Hybrid Conditional Access extends TeamViewer's zero-trust access model into environments where organizations require local policy enforcement and additional control over how remote access traffic enters sensitive networks. By combining centralized identity-based access controls with on-premises enforcement, Hybrid Conditional Access enables organizations to maintain governance, visibility, and security controls while supporting network segmentation and regulatory requirements.

Hybrid Conditional Access can be deployed on-premises and acts as a controlled enforcement point for remote access traffic. This architecture allows organizations to continue leveraging TeamViewer authentication, authorization, auditing, and access control capabilities while maintaining greater control over network boundaries and access paths.

A common use case for Hybrid Conditional Access is highly segmented industrial and operational technology (OT) environments, where direct internet connectivity for critical assets is restricted or prohibited. Hybrid Conditional Access requires only a restricted outbound control-plane connection to the TeamViewer service for policy synchronization and access validation. Access policies are enforced locally while the policy rules remain centrally managed. This architecture helps preserve network segmentation, maintain centralized governance, and provide controlled access into isolated environments without requiring unrestricted connectivity between sensitive networks and external services.

By combining centralized policy management with local enforcement, Hybrid Conditional Access supports secure remote access across a wide range of enterprise, critical infrastructure, and industrial environments while helping organizations meet security, compliance, and operational requirements.

For more information, please refer to the TeamViewer Knowledge Base article: [Hybrid Conditional Access](#)

### 5.4.5 Bring Your Own Certificate (BYOC) for Connection Authentication

TeamViewer Tensor supports Bring Your Own Certificate (BYOC) capabilities for organizations that require additional control over connection authentication. BYOC enables customers to use their own certificates to authenticate devices participating in TeamViewer connections, in addition to the standard TeamViewer certificate-based authentication mechanisms.

TeamViewer installations can be configured to require customer certificate authentication for incoming connections, outgoing connections, or both. When certificate authentication is required, a connection can only be established if the communicating device presents a valid certificate issued by the configured Certification Authority (CA). This provides an additional layer of trust validation and can be used to restrict TeamViewer connections to a defined set of managed devices.

BYOC can be particularly valuable for organizations with strict security, compliance, or regulatory requirements that want to align TeamViewer access controls with their existing Public Key Infrastructure (PKI).

Key considerations include:

- Customers can import certificates through the Windows Certificate Trust Store or by using supported certificate files, depending on the deployment model.
- BYOC requires a trusted Certification Authority (CA) that issues certificates to all devices participating in certificate-based authentication.
- Devices that require certificate validation must have access to the relevant CA certificate and any required intermediate certificates.
- Devices authenticating themselves must possess a valid certificate, the corresponding private key, and any required intermediate certificates.
- Certificate Revocation Lists (CRLs) are supported and can be used to validate certificate status. Depending on the CRL configuration, additional validation checks may affect connection establishment times.
- TeamViewer supports X.509, PEM, and other certificate formats supported by OpenSSL. Certificates and private keys can be imported from supported certificate files or from the Windows Certificate Trust Store.
- BYOC authentication operates in addition to TeamViewer's built-in certificate validation and does not replace the standard TeamViewer trust model.

For more information, please refer to the TeamViewer Knowledge Base article: [Bring your own certificate](#)

#### 5.4.6 Random Password for Connections

For spontaneous customer support, TeamViewer and TeamViewer QuickSupport generate a random password that can be changed at any time. If a connection partner or support requester shares their password with a supporter, the supporter can connect to the device by entering the corresponding TeamViewer ID and password. Depending on the configured settings, TeamViewer can generate a new password after application restart, after a completed session, or when manually requested. TeamViewer QuickSupport should be configured to generate a new password when launched or when requested by the user.

For unattended remote access scenarios, TeamViewer recommends using Easy Access as the preferred password-less authentication method. Easy Access leverages TeamViewer account-based authentication and can be combined with Single Sign-On (SSO), Multi-Factor Authentication (MFA), Conditional Access, device policies, and Allowlist controls to provide a more secure and scalable access model.

To further strengthen security, organizations should restrict access to managed devices using the available access-control mechanisms and apply the principle of least privilege wherever possible. When combined with MFA and other TeamViewer security controls, these measures help ensure that only authorized users can access designated devices. For additional guidance, please refer to the sections [Secure Unattended Access](#), [Secure Attended Access](#), and the relevant TeamViewer Knowledge Base articles on [Easy Access](#) and [access restrictions](#).

## 5.5 Account Authentication

### 5.5.1 Single Sign-On (SSO)

TeamViewer Tensor and eligible TeamViewer ONE packages support Single Sign-On (SSO) using the SAML 2.0 protocol. Supported Identity Providers (IdPs) include Microsoft Entra ID, Okta, Centrify, Google Workspace (G Suite), and OneLogin, among others supported through SAML 2.0 integration. SSO enables organizations to integrate TeamViewer authentication with their existing identity and access management infrastructure, helping to centralize user lifecycle management, strengthen access controls, and align authentication processes with corporate security policies. In addition, TeamViewer supports controls that allow organizations to restrict or prevent manual account creation for approved SSO domains. This helps ensure that users authenticate through the organization's established identity provider and procurement processes, reducing the risk of unmanaged accounts and strengthening governance over user access. When combined with Multi-Factor Authentication (MFA), Conditional Access, SCIM provisioning, and role-based access controls, SSO helps organizations implement a consistent and scalable identity security strategy across their TeamViewer environment. For more information, please refer to the TeamViewer Knowledge Base article: [Single Sign-On \(SSO\)](#)

### 5.5.2 Two-Factor Authentication for Account Login (TFA/MFA)

TeamViewer supports Two-Factor Authentication, also referred to as Multi-Factor Authentication (MFA), using time-based one-time password (TOTP) codes to help protect TeamViewer accounts from unauthorized access. TeamViewer strongly recommends enabling this feature for all TeamViewer accounts.

When TFA/MFA is enabled, users must provide a second authentication factor in addition to their username and password. This second factor is a security code generated by an authenticator application using the time-based one-time password algorithm and is valid only for a short period of time.

TFA/MFA strengthens account security and can support customer governance, audit readiness, and compliance efforts when combined with other security controls such as Single Sign-On (SSO), Conditional Access, device policies, Allowlists, and least-privilege access management. As with all security controls, compliance impact depends on the customer's overall configuration, operating environment, and applicable regulatory requirements.

For more information, please refer to the TeamViewer Knowledge Base article: [Two-factor authentication for your account](#)

### 5.5.3 Trusted Devices

If two-factor authentication is not configured for a TeamViewer account, Trusted Devices provides an additional layer of account protection. As a preventive security measure, users must authorize new devices or browsers when signing in to access their TeamViewer account for the first time.

As part of the authorization process, an email is sent to the email address associated with the TeamViewer account. Without adding the device, browser, or IP address to Trusted Devices, the user cannot complete the login. This helps protect the account from unauthorized login attempts because an attacker would also need access to the associated email inbox to authorize the new device or browser.

Depending on the available configuration, users may be able to authorize a specific device, trust an IP address, or grant one-time trust. Trusted Devices can also be managed through the relevant TeamViewer account and management interfaces. Where supported, trusted device authorization may also be completed via push notification using the TeamViewer Remote Control app.

For more information, please refer to the TeamViewer Knowledge Base articles:

- [Trusted Devices](#)
- [Trust Management for Trusted Devices](#)
- [Trust devices via push notification](#)

## 5.6 Additional Security Features

### 5.6.1 Security Center

Customers want to ensure that their TeamViewer configuration is secure, aligned with recommended best practices, and easy to review. The Security Center provides administrators with a centralized view of security-relevant configuration areas, including checks, recommendations, visual indicators, and guidance to help identify opportunities for improvement across their TeamViewer environment.

Security Center recommendations are designed to help administrators quickly validate important remote access security settings and take appropriate remediation actions where available. This can support internal governance, audit preparation, and compliance readiness by making security configuration gaps easier to identify, prioritize, and address.

TeamViewer continuously evaluates additional criteria and recommendations to provide further visibility, practical guidance, and simple resolution paths for customer remote access security configurations. Availability of specific Security Center checks, indicators, reports, and remediation actions may depend on the applicable license, product configuration, and enabled features.

## 5.6.2 Device Policy and Unified Policies

TeamViewer provides policy-based administration for managed devices, enabling administrators to configure and enforce security, connection behavior, update, and management settings across their environment. Policies help organizations centrally manage deployed TeamViewer agents and apply consistent security and operational standards across managed devices.

In TeamViewer ONE, Unified Policies provide a single, streamlined policy model for supported settings. Instead of managing separate policy types for different modules, administrators can create one policy and assign it to device groups. Unified Policies currently include TeamViewer settings and Patch Management settings where licensed, helping reduce setup effort and ongoing administration.

Unified Policies are designed for group-based assignment and inheritance. Policies are assigned to device groups, and devices within those groups inherit the applicable policy from the group level, provided the device and group configuration supports inheritance. This enables organizations to standardize configuration, access behavior, patching preferences, and operational settings across distributed environments while reducing manual device-level administration.

This policy-driven model supports centralized governance across TeamViewer ONE environments. By managing settings through groups and inherited policies, administrators can apply consistent security and operational requirements at scale, simplify policy maintenance, and align endpoint configuration with organizational governance requirements.

Availability of specific policy sections, settings, inheritance behavior, assignment options, and Patch Management policy capabilities depends on the applicable TeamViewer ONE package, enabled features, device platform, and product documentation.

For more information, please refer to the TeamViewer Knowledge Base articles:

- [Policies](#)
- [Unified policies in TeamViewer ONE](#)

### Applicability of the following TeamViewer ONE sections

The following sections on endpoint management, Digital Employee Experience (DEX) and Automations apply only to customers using the relevant TeamViewer ONE packages, add-ons and enabled capabilities. They do not apply to customers using TeamViewer Tensor as a standalone product.

## 5.6.3 Endpoint Management and Security in TeamViewer ONE

TeamViewer ONE extends secure remote connectivity with endpoint management and security capabilities that help administrators maintain visibility, consistency, and control across managed devices. Depending on the licensed package and enabled add-ons, capabilities can include device and system health monitoring, asset inventory and discovery, patch management, software deployment, mobile device management, remote monitoring and management, endpoint protection and detection/response add-ons, backup add-ons, and related endpoint security capabilities. The TeamViewer ONE includes capabilities such as device and system health monitoring, Asset & Patch Management, Digital Employee Experience endpoint insights, remediation and automation, device policies, and add-on endpoint protection capabilities.

These capabilities help administrators monitor endpoint health, performance, patch status, software inventory, configuration state, and operational risks across distributed environments. TeamViewer ONE is positioned as a platform that brings together Digital Employee Experience, endpoint management, and secure remote connectivity, enabling earlier detection of issues, AI-driven workflows, and operational remediation from a unified platform.

From a security and governance perspective, endpoint management capabilities help organizations apply consistent configuration standards, prioritize remediation activities, reduce exposure from outdated software or misconfigurations, and support compliance readiness through endpoint visibility and reporting. The TeamViewer ONE platform specifically references patching, updates, configuration management, vulnerability and misconfiguration scanning, and strengthening the security posture of distributed environments.

TeamViewer ONE endpoint management and security capabilities are designed to complement TeamViewer’s secure remote connectivity foundation. Together, remote access, endpoint visibility, patching, software deployment, policy enforcement, automation, and reporting help organizations move from reactive support toward more proactive and governed endpoint operations.

Availability of specific endpoint management, security, monitoring, patching, deployment, remediation, reporting, and add-on capabilities depends on the applicable TeamViewer ONE package, device platform, configuration, region, and product documentation.

#### 5.6.4 Digital Employee Experience (DEX) and Digital Workplace Controls

TeamViewer ONE includes Digital Employee Experience (DEX) capabilities that provide visibility into endpoint and user experience signals across managed environments. These capabilities can help administrators identify performance, reliability, responsiveness, application, network, operating system, and failure patterns that may affect users, devices, or business operations. DEX Insights as processing device-level experience signals related to performance, reliability, responsiveness, and failures across devices, operating systems, applications, and networks.

From a security and governance perspective, DEX is an observability and control layer that supports earlier detection, prioritization, and remediation of operational issues. DEX capabilities help IT teams detect experience degradations early, understand impact, and prioritize remediation while maintaining controls for access, data protection, and secure processing.

Access to DEX insights, dashboards, reports, AI-supported outputs, and remediation capabilities should be governed through defined roles, permissions, tenant boundaries, and administrative controls. TeamViewer DEX AI documentation describes admin-controlled rollout and access through Admin Settings, permissions, policies, and/or RBAC/ABAC controls, as well as role-based visibility for insights and dashboards.

Where applicable, TeamViewer DEX and TeamViewer ONE Enterprise capabilities apply data protection and governance measures such as data minimization, anonymization where applicable, encryption in transit and at rest, tenant-scoped controls, and controlled access to reporting and analytics outputs. TeamViewer’s DEX AI security stance also states that DEX AI data is protected using encryption in transit and at rest and that DEX reporting access is governed through RBAC/ABAC and tenant-scoped data boundaries.

Where DEX insights are used together with automation, scripting, or AI-supported remediation capabilities, execution remains subject to the applicable permissions, workflow controls, review or approval mechanisms where supported, signing or execution tracking where applicable, and administrative oversight. The DEX AI security stance describes DEX Hub as a governed automation library where AI can generate script drafts but does not execute them automatically, with access and execution governed through role-based controls and automation workflows.

Availability of DEX telemetry, analytics, reporting, AI-supported insights, remediation workflows, auditability, and governance controls depends on the applicable TeamViewer ONE package, enabled features, region, configuration, and contractual terms.

## 5.6.5 Automations in TeamViewer ONE

Automations in TeamViewer ONE help administrators proactively monitor managed devices and respond to operational issues at scale using governed workflows. An automation can include a trigger, optional preconditions, one or more checks, and a remediation action. When configured conditions are met, TeamViewer ONE evaluates the assigned devices and, where supported, executes the defined remediation action.

Automations are deployed through policies, enabling administrators to centrally control which devices or device groups receive a given automation. When an automation is associated with a policy, devices assigned to that policy inherit the configured automation settings. This policy-based deployment model helps ensure consistent behavior across device groups, reduces administrative effort, and supports scalable rollout, update, and modification of automation workflows from a central location.

TeamViewer ONE automations are managed centrally. Administrators can create, update, enable, disable, duplicate, delete, and review automations, as well as assign or modify policies as operational requirements change. The Automations management screen also provides configuration and usage information such as automation name, assigned policy, supported operating systems, execution count, last modification date, and the user who most recently updated the automation.

Automations use the same permission model as Policies, helping organizations align automation management with existing administrative controls. The TeamViewer ONE Automations documentation lists Manage Policies as the required permission and states that Automations use the same permission model as Policies.

To support monitoring and traceability, administrators can review execution history where supported. Failed automation executions can be reviewed in the History Log, allowing administrators to inspect execution details and identify the cause of failures.

Where automations use script-based or AI-generated remediation content, such content should be governed through the applicable script library, permissions, review, signing or approval mechanisms where supported, and execution tracking controls. TeamViewer ONE Automations documentation states that detection logic and fixes can be created using AI-generated scripts, saved to the Script Library, and selected during automation configuration where applicable; the DEX AI security stance also describes script signing, approval, and execution tracking as governance controls for automation workflows.

Availability of automations, supported triggers, checks, remediation actions, execution details, script-based workflows, AI-generated script usage, and history information depends on the applicable TeamViewer ONE package, enabled features, device platform, and product documentation.

For more information, please refer to the TeamViewer Knowledge Base article: [Automations in TeamViewer ONE](#)

## 5.6.6 Black Screen / Privacy Screen

TeamViewer offers licensed customers a Black Screen / Privacy Screen capability when working on remote systems. This feature helps protect privacy during remote sessions by hiding the content of the remote screen and, where supported, disabling input on the remote computer while the remote session is active.

Typical use cases include restricting visibility of administrative tasks from local users, reducing the risk of screen observation in remote work scenarios, and supporting privacy controls during sensitive support or maintenance activities. Availability and behavior may depend on the operating system, TeamViewer version, license, and device configuration.

For more information, please refer to the TeamViewer Knowledge Base article: [TeamViewer Black Screen](#)

## 5.6.7 Traceability, Auditability and Session Recording

TeamViewer Tensor and eligible TeamViewer ONE capabilities provide auditability, traceability, reporting, and session-recording capabilities that help organizations maintain visibility into administrative actions, remote access activity, operational workflows, and security-relevant events. These capabilities can support governance, forensic investigations, compliance activities, internal controls, and operational oversight.

From an audit and compliance perspective, TeamViewer enables organizations to establish traceability across remote access sessions, administrative activities, policy changes, automation workflows, AI-supported activities, and other supported platform operations. Depending on the licensed package and enabled features, administrators can access event logs, connection reports, session records, automation histories, and other audit artifacts.

### 5.6.7.1 Event Logging

Event logging helps organizations understand who performed relevant actions, what changed, when an activity occurred, and which systems, devices, or settings were affected. Depending on the licensed package and enabled features, logs may include remote session activity, Management Console actions, user administration activities, policy changes, device management activities, automation execution details, and security-relevant configuration events.

Access to event logs should be restricted to authorized administrators with appropriate permissions. Where supported, event data can be filtered, exported, downloaded, or retrieved programmatically through the TeamViewer Event Log API to support governance, SIEM integration, compliance reporting, and security monitoring workflows.

For more information, please refer to the TeamViewer Knowledge Base article: [Auditability / Event Log](#)

### 5.6.7.2 Connection Reporting

Connection Reports provide visibility into remote access activity across the TeamViewer environment. Depending on the licensed package and enabled features, reports may include information such as participants, devices involved, connection timestamps, session duration, session type, and associated organizational context. These reports help organizations maintain accountability for remote access activities and support internal audit and compliance requirements. For more information, please refer to the TeamViewer Knowledge Base article: [Connection reports](#)

### 5.6.7.3 Session Recording and Retention

Where supported and enabled by the customer, as this feature is not enabled by default, TeamViewer provides session-recording capabilities that allow organizations to retain recordings of remote support and remote access sessions for review, quality assurance, training, investigative, and compliance purposes. Session recordings can be stored according to the organization's operational and compliance requirements. TeamViewer does not store these session recordings, but rather we enable customers to be in full control of their data through either on device, local network shares, or through SFTP upload to a customer's own cloud.

For customers requiring centralized storage and retention outside the TeamViewer platform, TeamViewer supports integration with customer-managed storage locations, including supported SFTP-based storage repositories where applicable. This enables organizations to align session-retention processes with existing governance, archival, and evidentiary requirements.

For more information, please refer to the TeamViewer Knowledge Base article: [Record a remote session](#)

### 5.6.7.4 AI and Tia Auditability

AI-supported capabilities, including TeamViewer Intelligent Agent (Tia), are designed to operate within governed access controls and administrative permissions. Where supported, organizations can review information related to AI-assisted activities, generated outputs, troubleshooting requests, reporting activities, and operational interactions through the applicable logging and audit mechanisms.

Access to AI-related functionality remains governed through administrative permissions, policies, role-based access controls, tenant boundaries, and applicable audit capabilities, helping organizations maintain oversight of AI-supported workflows and activities.

For more information, please refer to the TeamViewer Knowledge Base article: [SCIM System for Cross-Domain Identity Management Provisioning](#)

TeamViewer supports SCIM API capabilities to synchronize users and user groups from cloud identity providers such as Microsoft Entra ID and Okta. This supports centralized identity lifecycle management and helps customers keep TeamViewer user access aligned with their identity governance processes.

SCIM-based provisioning helps administrators create, update, and deactivate users through their identity provider and keep TeamViewer user and group information aligned with approved corporate identity sources. When combined with Single Sign-On (SSO), role-based access controls, and regular access reviews, SCIM can help reduce manual administration and support consistent access governance across the TeamViewer environment.

For more information, please refer to the TeamViewer Knowledge Base article: [Microsoft Entra ID Integration – SCIM Configuration](#)

## 5.6.8 Mobile SDK

TeamViewer offers a Mobile Software Development Kit (SDK) add-on for customers that need to embed TeamViewer remote support capabilities into their own mobile applications. This enables organizations to support users directly within their own app experience, where supported, while maintaining greater control over the support workflow and the screen data exposed during the session.

The Mobile SDK can help customers provide in-app support without requiring users to switch to a separate support application. Depending on the platform, license, and implementation, supported capabilities may include screen sharing, remote control for supported Android scenarios, mouse interactions, and file transfer from the SDK to the supporter.

The SDK is designed so that support access is limited to the customer's application context rather than the entire mobile device, helping protect user privacy during mobile support scenarios. Availability, supported features, and implementation responsibilities depend on the applicable license, platform, and SDK documentation.

For more information, please refer to the TeamViewer Knowledge Base article: [TeamViewer Mobile Software Development Kit \(SDK\)](#)

### 5.6.9 Security Key Redirection

TeamViewer supports organizations on their journey toward password-less and phishing-resistant authentication by enabling Security Key Redirection where supported. This allows a local hardware security key or smartcard, such as FIDO-based security keys or PIV-compatible credentials, to be redirected through a TeamViewer session so that it can be recognized by the remote computer as if it were locally attached.

This is currently not supported means of authentication for the TeamViewer Account directly, if you have single sign on enabled this may be possible through the supported features of your identity provider of choice.

Security Key Redirection can support remote authentication use cases such as web authentication, Windows logon, or privileged tasks requiring elevated authentication, depending on the customer environment, operating system, device configuration, and supported security key type.

This capability helps organizations extend strong hardware-backed authentication into remote support and administration workflows while reducing reliance on passwords. Availability depends on the applicable TeamViewer Tensor license, supported platform, installed components, and configuration requirements.

For more information, please refer to the TeamViewer Knowledge Base article: [Security key redirection](#)

### 5.6.10 Agentless Access for Operational Technology (OT)

TeamViewer supports Agentless Access capabilities designed for operational technology (OT), industrial control systems, and legacy environments where software installation on target systems is not possible or desirable.

Agentless Access enables secure access to assets such as PLCs, HMIs, industrial servers, network appliances, and legacy systems without requiring a TeamViewer Host installation on the target endpoint.

The solution supports a zero-trust approach through controlled point-to-point access mechanisms and protocol isolation. Depending on the deployment scenario, supported access methods can include protocols such as VNC, SSH, and other native industrial or administrative protocols.

Access remains governed by TeamViewer authentication, authorization, auditing, and policy controls, helping organizations maintain secure remote operations while preserving network segmentation and reducing exposure of sensitive OT assets.

## TeamViewer Tensor OT – Secure Remote Access Architecture

Zero-trust remote access into segmented OT environments with Hybrid Conditional Access and Agentless Access

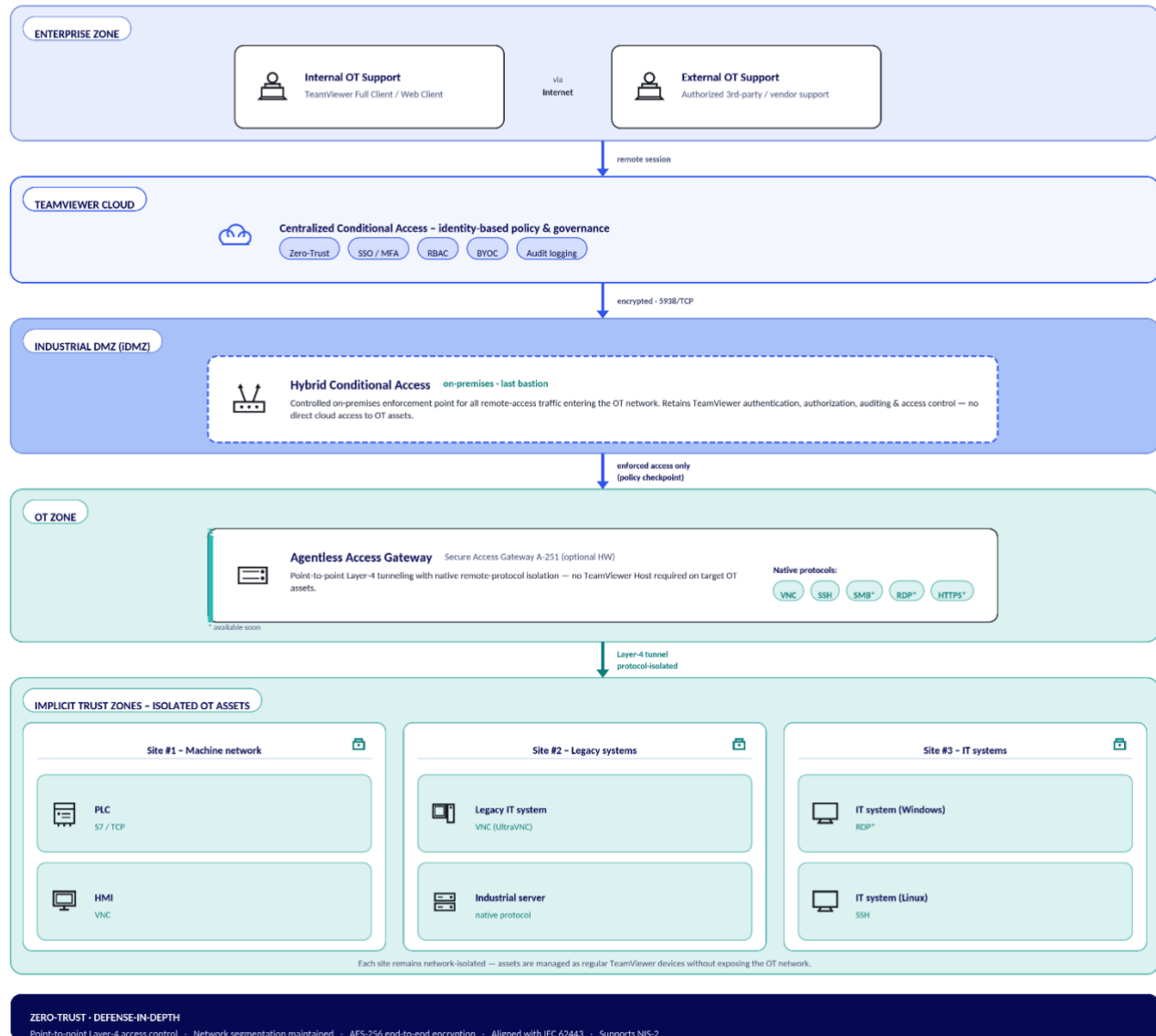


Figure 4: TeamViewer Tensor OT Architecture with Hybrid Conditional Access and Agentless Access

Example deployment showing how TeamViewer enables zero-trust remote access into segmented OT environments using Hybrid Conditional Access and Agentless Access Gateways while maintaining network isolation and centralized policy enforcement.

### 5.6.11 LAPS Integration

TeamViewer integrates with Microsoft Windows LAPS to help customers securely leverage managed local administrator credentials during remote support scenarios. LAPS integration helps IT administrators retrieve and inject local administrator credentials during remote support sessions, supporting elevated access without exposing passwords to the supporter.

The integration works by connecting TeamViewer to Microsoft Entra ID and Microsoft Intune, allowing password injection and optional password rotation directly from within a TeamViewer session, where supported by the customer configuration. This can help organizations support privileged access workflows while reducing manual password handling and improving control over local administrator credentials.

Security-related information:

- Passwords are injected securely as keystrokes and do not pass through the TeamViewer backend.
- The integration uses PKCE for secure token exchange.
- Password requests are made from the supporter's device to the customer's Intune tenant. Passwords are not transferred through TeamViewer cloud infrastructure.

For more information, please refer to the TeamViewer Knowledge Base article: [Getting started with the Windows LAPS integration](#)

### 5.6.12 Chat

Chat messages and chat history are end-to-end encrypted and stored in the TeamViewer account using RSA/AES as described in the Account Data Protection section of this document. Only participants in a chatroom or one-to-one chat can access the messages and history.

Chat content is considered sensitive customer data according to the account data protection model described in this document.

## 6 Architecture

### 6.1 ONE platform architecture

Existing TeamViewer remote session architecture diagrams remain relevant for TeamViewer Remote and TeamViewer Tensor remote session establishment, including the TeamViewer network, certificate-based client verification, and encrypted session traffic. TeamViewer ONE is as an integrated platform layer that combines these remote connectivity capabilities with DEX, endpoint management, automation, reporting, AI, and enterprise integrations.

TeamViewer ONE is a layered model: endpoint/client layer, remote connectivity layer, management and policy layer, DEX telemetry and analytics layer, automation and remediation layer, AI services layer, identity and access management layer, integration layer, and reporting layer. Each layer should be controlled by tenant scope, administrative permissions, secure authentication, encryption, monitoring, and auditability where applicable.

- **Endpoint/client layer:** TeamViewer clients, hosts, managed devices, mobile devices, and supported endpoint agents collect or process only the data needed for the configured feature. For supported Tia troubleshooting scenarios, the locally installed TeamViewer Automation Client provides diagnostic information through its local integration with the TeamViewer Remote Client. Tia-related communication continues to use the TeamViewer Remote Client infrastructure rather than establishing a separate remote-access channel.
- **Connectivity layer:** Remote sessions are authenticated, authorized, and encrypted using TeamViewer connection mechanisms described in this document.
- **Management and policy layer:** Administrators manage users, devices, access rules, policies, automations, and feature rollout centrally.
- **DEX and endpoint telemetry layer:** TeamViewer ONE and DEX capabilities process endpoint signals, performance data, reliability signals, application and network experience data, and user feedback where configured.
- **Automation layer:** Automations evaluate configured triggers, preconditions and checks, then execute defined remediation actions through policy-controlled workflows.
- **AI layer:** AI-supported workflows use defined inputs and controlled processing boundaries, with customer controls for rollout, access, permissions, and feature availability. Tia troubleshooting requests are processed within defined permissions and controlled processing boundaries, with diagnostic collection performed through the locally integrated Automation Client where supported.
- **Integration layer:** Integrations with ITSM, endpoint management, identity, security, and reporting tools should maintain correct identity, permissions and audit integrity.

## 6.2 Session Initialization

The following diagram provides a high-level view of how a TeamViewer remote session is initialized before secure session communication is established. During this process, the TeamViewer client communicates with TeamViewer backend services to validate local identifiers, request or confirm the TeamViewer ID, exchange authentication information, and obtain signed certificate material used for subsequent secure TeamViewer network communication.

This initialization flow establishes the identity and certificate basis for remote session establishment. It complements the access-control mechanisms described in the previous sections, such as attended and unattended access, Conditional Access, BYOC, MFA/TFA, device policies, and allowlist controls. The cryptographic protection of session traffic, including mutually authenticated TLS 1.3 for supported session flows, Perfect Forward Secrecy, and AES-256-GCM session encryption, is described in the Encryption section of this document.

The following diagram provides a simplified conceptual overview. It does not represent all service components, processing activities, hosting regions, or deployment variations

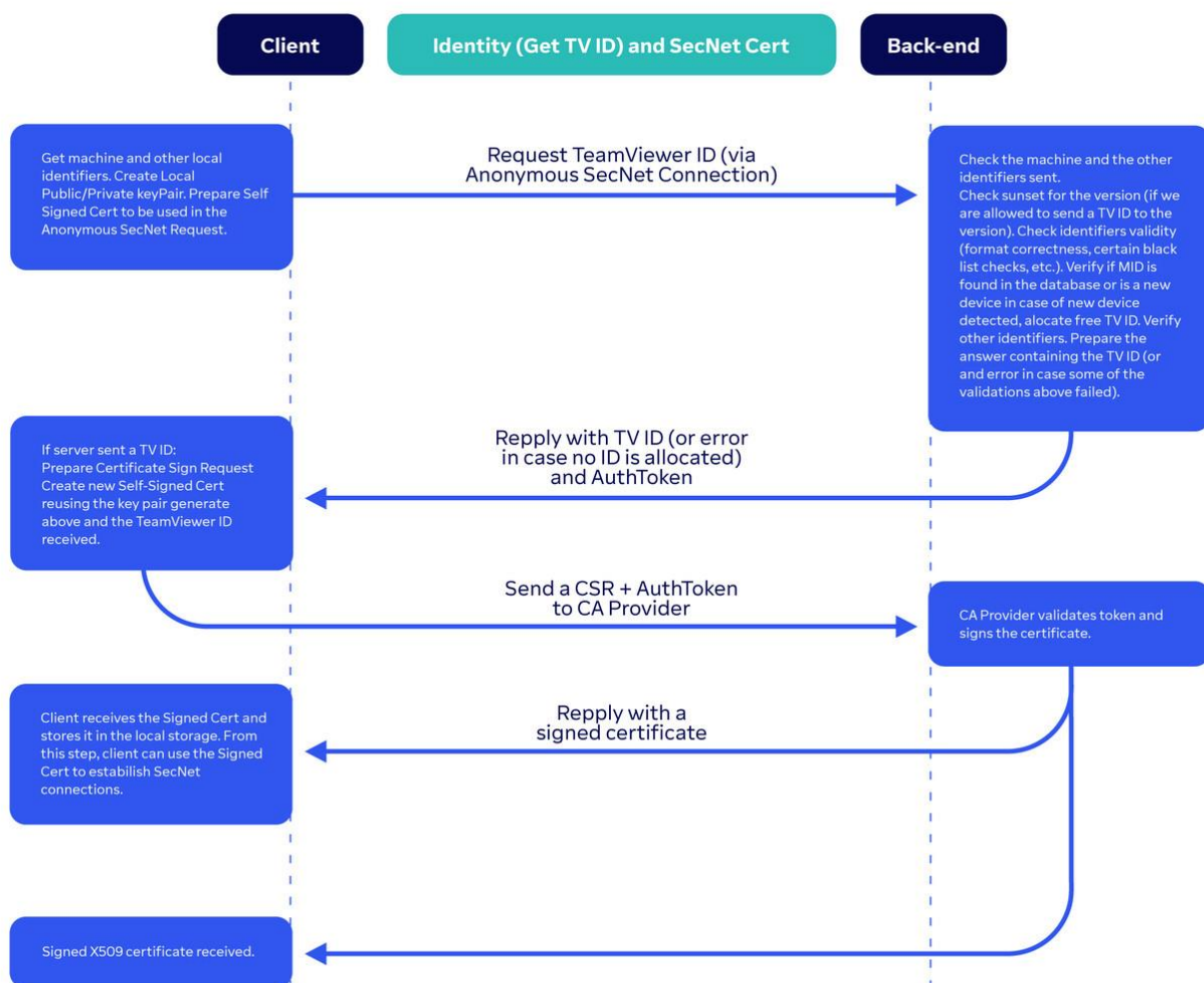


Figure 5: TeamViewer Remote Session Initialization and Certificate Issuance Flow

## 6.3 Modern TLS 1.3 Mutually Authenticated Session Handshake

TeamViewer uses a modern mutually authenticated TLS 1.3 handshake for supported remote-session flows in TeamViewer version 15.73 and later. This handshake builds on the session initialization process described above and establishes the cryptographic foundation for secure communication between the participating endpoints. During this process, the communicating clients exchange key-share information, verify certificate material, and establish session-specific encryption keys before protected session traffic is transmitted.

Mutually authenticated TLS 1.3 enables both endpoints to authenticate the session context and supports Perfect Forward Secrecy through modern Diffie-Hellman key exchange mechanisms. After the secure handshake is completed, session data is protected using AES-256-GCM encryption. Private keys remain on the client device and are not available to TeamViewer routing servers or intermediary systems, helping ensure that end-to-end encrypted session traffic can only be decrypted by the communicating endpoints.

The diagram below illustrates the high-level TLS 1.3 handshake and session encryption flow for supported current remote sessions. Legacy compatibility and selected backend connection scenarios that rely on TeamViewer protocol components are described separately in the following section.

The following diagram provides a simplified conceptual overview. It does not represent all service components, processing activities, hosting regions, or deployment variations

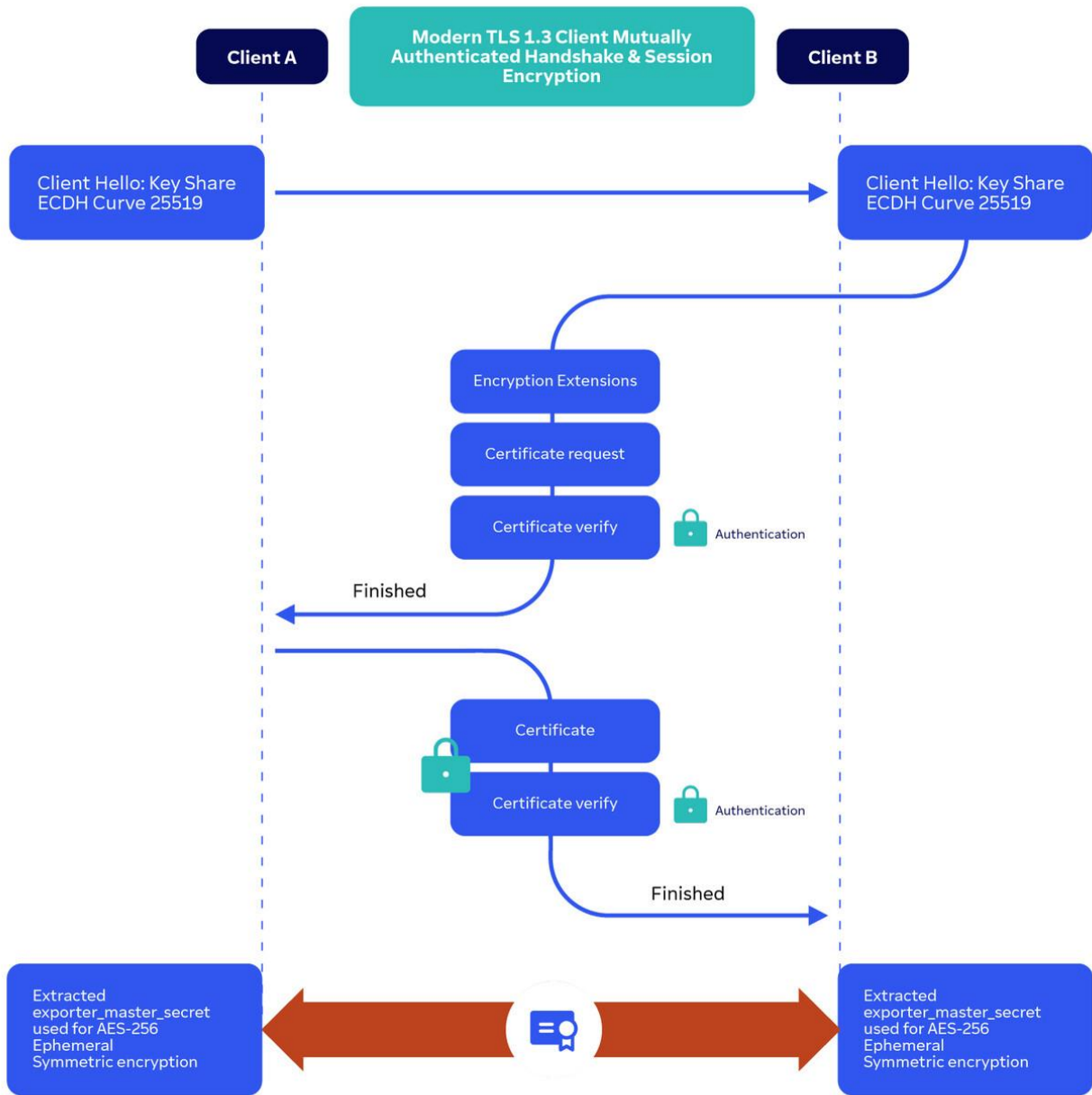


Figure 6: Modern TLS 1.3 Mutually Authenticated Session Handshake Flow

## 6.4 Legacy Secure Network Protocol and Backend Connection Flows

The following diagram illustrates the legacy Secure Network Protocol session establishment flow used for TeamViewer versions prior to 15.73 and for selected TeamViewer backend connection scenarios. It is included to provide architectural and compatibility context for environments where TeamViewer protocol components are still used.

In this flow, the participating clients complete a Secure Network Protocol handshake, negotiate shared key material, and derive session encryption used to protect the communication between endpoints. For legacy protocol versions, TeamViewer uses RSA-4096 public key exchange combined with AES-256 session encryption. TeamViewer's encryption documentation also states that private keys are generated on the client side and do not leave the client, while session keys are generated during the handshake, are ephemeral, and are not retained after the session ends.

This legacy flow should be understood as a compatibility and selected backend communication model rather than the primary current remote-session handshake. For supported current remote-session flows, TeamViewer uses mutually authenticated TLS 1.3 for session authentication and attestation, with Perfect Forward Secrecy and AES-256-GCM session encryption as described in the previous section. The Encryption section summarizes the cryptographic protections used across both modern and legacy connection models.

The following diagram provides a simplified conceptual overview. It does not represent all service components, processing activities, hosting regions, or deployment variations.

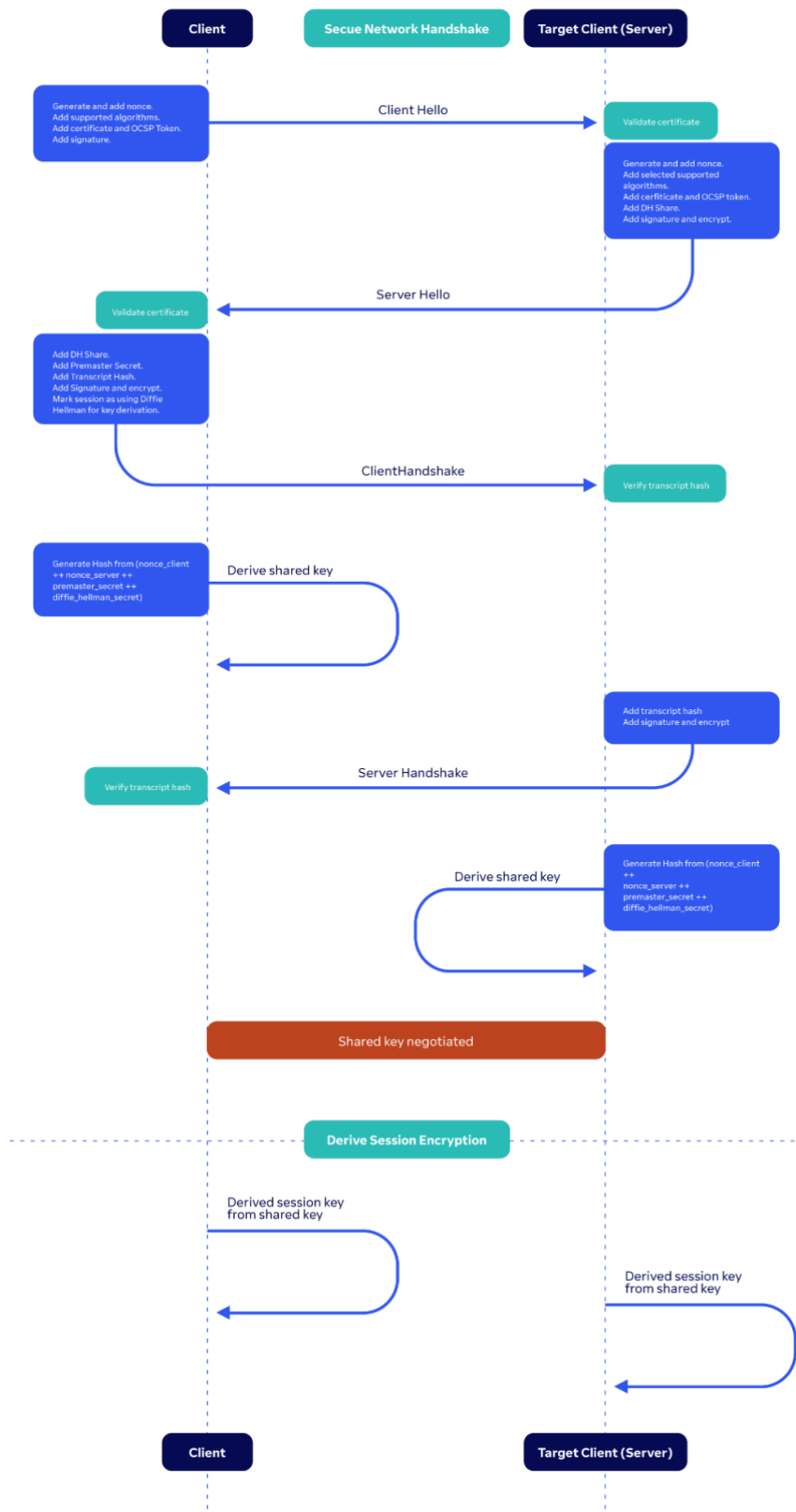


Figure 7: Legacy Secure Network Protocol Session Initialization and Backend Connection Flow

## 7 Encryption and Data Protection

TeamViewer remote session traffic is protected through end-to-end encryption. Private keys remain on the communicating endpoints and are never available to TeamViewer routing servers or intermediary systems. As a result, TeamViewer cannot decrypt remote session content transmitted between participating endpoints. Only the communicating devices can decrypt remote session traffic.

If you're looking for further specifics on encryption, there is documentation that's available under NDA just like our Pentest Executive Summaries and SOC2 reports.

**Scope boundary:** This statement applies to remote session content and remote session traffic. Account information, licensing information, administrative configuration, audit records, telemetry, reporting data, endpoint management data, and DEX operational data are processed according to the service-specific data handling models described elsewhere in this document.

### 7.1 Account Data Protection

TeamViewer accounts are hosted on dedicated TeamViewer backend infrastructure. For information on hosting, infrastructure access controls, and operational safeguards, please refer to the Data Centers and Backbone section of this document.

For authentication, TeamViewer uses the Secure Remote Password protocol (SRP) version 6. TeamViewer does not store information on its servers that could be used by an unauthorized third party to authenticate as the given account. Passwords are not stored on TeamViewer servers during authentication. Instead, TeamViewer uses a unique verification process that is valid for a single authentication run only and cannot be reused.

Data stored in the account, such as passwords, keys, and chat logs, is encrypted using a combination of RSA and AES, where the root key for encryption is derived from the user's password. This helps ensure that anyone without the password cannot access sensitive data stored in the account.

### 7.2 Encryption

TeamViewer protects remote session traffic using strong, industry-standard cryptographic mechanisms. Connections are secured through a combination of asymmetric key exchange and symmetric session encryption.

For legacy protocol versions, TeamViewer uses RSA-4096 public key exchange combined with AES-256 session encryption. Starting with TeamViewer version 15.73 and later, supported remote-session flows use mutually authenticated TLS 1.3 for session authentication and attestation. This introduces Perfect Forward Secrecy (PFS) through modern Diffie-Hellman key exchange mechanisms. After the secure handshake, session data is protected using AES-256 encryption.

During connection establishment, communicating clients verify each other's identity using certificates issued by the TeamViewer master cluster. This ensures that endpoints can authenticate the TeamViewer infrastructure before exchanging sensitive data. Private keys never leave the client device, ensuring that neither TeamViewer routing servers nor intermediary systems can decrypt end-to-end encrypted remote session traffic.

Remote session traffic between endpoints is protected using end-to-end encryption, ensuring that only the communicating devices can decrypt transmitted session data. While TLS 1.3 handshake modernization is used for supported remote-session authentication and attestation, some communication with TeamViewer backend services continues to rely on TeamViewer protocol components as part of ongoing modernization efforts.

Additional technical documentation, including details about supported cipher suites and cryptographic implementations, can be made available to customers under mutual non-disclosure agreements (NDA).

The architecture diagrams in Chapter 6 illustrate the *Modern TLS 1.3 Mutually Authenticated Session Handshake Flow* and the *Legacy Secure Network Protocol Session Initialization and Backend Connection Flow*.

### 7.3 TeamViewer ONE, DEX and AI Data Handling

This section applies to customers using TeamViewer ONE and the relevant enabled capabilities. Customers using TeamViewer Tensor without TeamViewer ONE are not affected by DEX, endpoint-management, Patch Management, Automation, DEX Hub, DEX Insights or other TeamViewer ONE-specific data-processing controls described below.

For TeamViewer ONE, data handling depends on the configured capabilities, purchased package, enabled features, region, and contractual terms. Remote connectivity follows the remote-session encryption and account protection model described above. Endpoint management, DEX, automation, reporting, and AI-enabled capabilities process the data needed to deliver the selected capability, such as device health, performance, reliability, responsiveness, application, network, configuration, automation, and support-session data.



TeamViewer AI applies shared security and data-handling principles across supported product environments. Administrators control rollout, access, permissions, policies, and feature availability. AI workflows are designed to process only the data needed for the specific capability, with privacy protections such as minimization and anonymization applied where applicable. Data is protected in transit and at rest, supported by controlled key management and secure processing boundaries. Customer data processed by TeamViewer AI features is not used to train TeamViewer AI models, as described in the applicable TeamViewer AI security resources.

For Session Insights and Tia in TeamViewer Remote, Tensor, and TeamViewer ONE, session documentation and troubleshooting workflows use defined inputs and controlled processing. Tia provides guided troubleshooting and does not autonomously execute remediation actions, install software, or modify endpoint configurations. For supported troubleshooting scenarios, the TeamViewer Automation Client may collect limited diagnostic information from the endpoint based on the active troubleshooting request. The Automation Client is locally integrated with the TeamViewer Remote Client, and communications associated with Tia troubleshooting continue to use the TeamViewer Remote Client infrastructure. Tia may also use user-triggered screenshots, in-session conversation context, and permission-based Session Insights visibility. The troubleshooting workflow is not intended to collect personal documents, communication content, keystrokes, or general user activity data.

For TeamViewer DEX and TeamViewer ONE Enterprise AI capabilities, DEX Insights may process device-level experience signals from endpoints and connected systems, including performance, reliability, responsiveness, and failure signals. DEX Hub can store and manage automation content such as scripts and packs for review, reuse, and governed execution. Tia Reporting uses tenant-scoped data models, governed reporting access, RBAC for feature access, ABAC for data-level filtering, tenant-specific schemas, filtered views, and scoped session tokens to help ensure that users access only authorized data.

Additional information regarding TeamViewer AI security, architecture, data handling, governance controls, and processing workflows is available in dedicated TeamViewer AI security resources published through the TeamViewer Trust Center and related TeamViewer AI security documentation. These resources provide detailed architecture diagrams and explanations for TeamViewer AI capabilities, including Session Insights, Tia, AI-assisted scripting, DEX Intelligence Insights, DEX Hub, and Tia Reporting. They also describe relevant administrative controls, data protection mechanisms, encryption, tenant isolation, auditability, anonymization and minimization measures, and AI service boundaries.

Customers who require a deeper technical understanding of TeamViewer AI security and data processing can refer to the following resources:

- [TeamViewer AI security, privacy, and customer control](#)
- [TeamViewer AI Security, Control, and Data Handling for TeamViewer Remote, Tensor, and TeamViewer ONE](#)
- [TeamViewer AI Security, Control, and Data Handling for TeamViewer DEX and TeamViewer ONE Enterprise](#)

These documents include detailed architecture diagrams and security explanations that complement the high-level overview provided in this document. Product availability, feature scope, processing details, and controls may vary depending on the applicable product environment, license, configuration, region, and contractual terms.

## 8 Secure Development and Product Security

### 8.1 Our Secure Software Development Lifecycle (S-SDLC)

TeamViewer follows a strict Secure Software Development Life Cycle (S-SDLC) throughout all phases of our products' lifecycle, including a hardened and audited software development pipeline. Security activities are embedded across the development process, including requirements review, design and architecture review, implementation review, verification, release, and response activities.

TeamViewer performs design, architecture, and implementation reviews, including attack surface analysis and threat modeling, where identified risks are prioritized and product security requirements are derived. TeamViewer also enforces code reviews, unit and integration tests, and code owner approval for code changes.

For additional background, TeamViewer's [public S-SDLC material](#) includes secure development as a holistic framework covering security training, requirements, design, implementation, verification, release, and response.

### 8.2 Security Testing and Composition Analysis (SCA)

TeamViewer leverages established tooling to perform Software Composition Analysis (SCA), vulnerability management, and dependency management for open-source and third-party components. Static and dynamic application security testing (SAST/DAST) are performed as part of the software development process and security reviews.

A segmented automation environment supports quality assurance programmatically and in an automated fashion. These activities help identify security vulnerabilities, outdated dependencies, and potential supply chain risks during the development and verification process. TeamViewer's public S-SDLC material also describes SCA and static code analysis as part of verification and dependency risk management.

### 8.3 Penetration Testing

Both TeamViewer infrastructure and TeamViewer software are subject to penetration testing. TeamViewer's infrastructure and products are subject to risk-based penetration testing. Independent security specialists perform external testing using appropriate white-box, grey-box or black-box approaches depending on the scope and objectives of the assessment. Tests are performed by independent companies specialized in security testing.

### 8.4 Code Signing

TeamViewer software is digitally signed, allowing customers to verify the identity of the software publisher and the integrity of the software. Any unauthorized modification of the software after signing will invalidate the digital signature.

Code signing allows endpoint security tools to validate whether the software is genuine. TeamViewer software also uses code-signing validation as a self-check mechanism to help ensure that only genuine copies can run. If this validation check fails, the software exits. This helps protect against tampering and supports customer endpoint security controls.

## 8.5 Software Bill of Materials (SBOM)

TeamViewer maintains Software Bill of Materials (SBOM) information for client software components as part of secure software development and software supply chain security practices. SBOM documentation can be made available to customers upon request and subject to a mutual non-disclosure agreement (MNDA).

SBOMs may include information about relevant open-source and third-party components used in TeamViewer client software. SBOMs are updated in alignment with product release cycles and can be provided in common industry formats such as SPDX or CycloneDX, depending on customer preference and available scope.

Availability may be limited by product and component scope. SBOM information for SaaS platform components, backend services, or third-party hosted services may not be available in the same format unless otherwise agreed or documented.

## 8.6 Product Security Incident Response Team (PSIRT)

TeamViewer works diligently to identify and mitigate security vulnerabilities in its products. TeamViewer's Product Security Incident Response Team (PSIRT) coordinates product vulnerability handling activities, including vulnerability intake, validation, risk and impact assessment, remediation coordination, verification, CVE assignment where applicable, security communications, and disclosure.

TeamViewer's product security response practices are aligned with recognized product security incident response approaches, including the FIRST PSIRT Services Framework and Maturity Model. TeamViewer is also represented through its [FIRST-listed TeamViewer SIRT](#); the FIRST entry identifies TeamViewer SIRT as a member since July 21, 2021 and lists [psirt@teamviewer.com](mailto:psirt@teamviewer.com) as the Product Security contact channel.

External parties can use TeamViewer's published reporting channels, including [TeamViewer's Vulnerability Disclosure Program](#), the public security.txt file (<https://www.teamviewer.com/.well-known/security.txt>), and the contact addresses.

## 8.7 Vulnerability Disclosure Program (VDP)

Every customer, user, researcher, partner, and any other person that interacts with TeamViewer products and services is encouraged to report identified vulnerabilities and errors. Responsible disclosure helps TeamViewer analyze, coordinate, and address potential security issues in a structured and transparent manner.

[TeamViewer's Vulnerability Disclosure Program](#) provides a public channel for submitting vulnerability reports. The VDP states that TeamViewer values contributions from the security community and is committed to maintaining a transparent and collaborative disclosure process.

Issues can be reported through the TeamViewer Vulnerability Disclosure Program: <https://vdp.teamviewer.com/>

## 8.8 Bug Bounty Program

TeamViewer cooperates with security researchers through a crowdsourced security program. The Bug Bounty Program complements TeamViewer's secure development practices, automated security testing, code reviews, vulnerability scanning, penetration testing, and responsible disclosure activities.

TeamViewer's public Bug Bounty Program is operated through YesWeHack. It is designed to motivate security researchers and ethical hackers to identify qualifying security vulnerabilities in defined in-scope TeamViewer products and services. Scope, eligibility, reward levels, and program rules are governed by the applicable program terms and TeamViewer public security guidance.

For more information, please refer to the TeamViewer Bug Bounty Program: <https://www.teamviewer.com/en/resources/trust-center/bug-bounty-program/>

## 8.9 Security Bulletins

TeamViewer publishes security bulletins for relevant product security information. Security bulletins may include information about the nature of addressed vulnerabilities, affected products or versions, assigned CVEs where applicable, severity, priority, fixed versions, mitigations, and workarounds where relevant. Customers can review published bulletins through the TeamViewer Trust Center. TeamViewer's public Security Bulletins page states that bulletins are ranked with priority levels from Low to Critical, and the page provides a subscription option so customers can receive bulletins directly via email.

Each issue is categorized by priority:

- **Critical:** A critical priority is assigned to an issue that affects a core TeamViewer function or service and could have a critical impact on the customer's security posture, such as a remote code execution vulnerability in the wild. Customers should closely follow TeamViewer communications and implement advised measures, which may include an immediate client update.
- **Important:** An important priority is assigned to an issue that could significantly impair the customer's security posture, such as an easily reproducible privilege escalation vulnerability. Customers should implement all advised measures promptly, which may include an immediate client update.
- **Moderate:** A moderate priority is assigned to an issue that could impair local security posture only under specific circumstances. Customers should implement advised measures and update at the earliest convenience.
- **Low:** A low priority is assigned to an issue that is unlikely to be reproduced and requires privileged local access to be exploited. Customers should implement advised measures, typically during the next regular update cycle. This category may also include general security-related announcements.

TeamViewer uses CVSS-based scoring where applicable and publishes CVSS values in security bulletins when relevant. TeamViewer's Bug Bounty page states that security experts review reports and determine scores in accordance with the CVSS 3 evaluation scheme, and the VDP submission form also uses CVSS3 scoring fields. Customers can find TeamViewer Security Bulletins here: [Security](#)

**Note:** Customers must self-register for bulletin notifications and select relevant services where supported. TeamViewer does not automatically enroll customers in email-based notifications due to compliance with privacy regulations.

## 8.10 Certified Numbering Authority (CNA)

TeamViewer is [authorized by the CVE Program as a CVE Numbering Authority \(CNA\)](#). This supports standardized vulnerability identification, coordinated disclosure, and accurate reporting of vulnerabilities affecting TeamViewer products.

As a CNA, TeamViewer can assign CVE IDs where applicable and publish relevant vulnerability information through the appropriate CVE and security advisory processes.

## 8.11 Internal Product Vulnerability Management Timeframes

TeamViewer maintains internal vulnerability management processes to assess, prioritize, and remediate vulnerabilities. Timeframes and processes depend on vulnerability severity, exploitability, affected product, compensating controls, technical complexity, and applicable customer commitments.

The following internal target timeframes provide customer-facing guidance on TeamViewer's vulnerability management approach:

| Severity                       | Internal Target Timeframe |
|--------------------------------|---------------------------|
| Critical – exploited (KEV/CRA) | Immediate (hotfix)        |
| Critical – not yet exploited   | ≤ 14 days                 |
| High                           | ≤ 14 days                 |
| Medium                         | ≤ 3 months                |
| Low                            | ≤ 6 months                |

**Notice:** These timeframes are provided for informational transparency regarding TeamViewer's internal vulnerability management process. They are non-binding and do not create contractual commitments, customer-specific SLAs, or service-level obligations. Actual handling may depend on exploitability, affected product, affected version, technical complexity, compensating controls, customer impact, and applicable legal or contractual requirements.

For the protection of customers, TeamViewer generally does not disclose or discuss security issues publicly until investigation is complete and any necessary updates, mitigations, or advisories are available or coordinated through the responsible disclosure process.



Figure 8: High-level product vulnerability response lifecycle

## 9 Hosting and Infrastructure

### 9.1 Hosting and Infrastructure Overview

**TeamViewer Remote** and **TeamViewer Tensor** provide secure remote connectivity services, including routing, authentication, authorization, access control, and session management for attended and unattended remote access.

**TeamViewer ONE** builds on this foundation by adding cloud-based IT operations and Digital Employee Experience (DEX) capabilities, including endpoint management, security monitoring, telemetry collection, analytics, reporting, automation, dashboards, enterprise integrations, and AI-supported insights. TeamViewer operates a combination of TeamViewer-managed infrastructure and cloud services to support these offerings. Infrastructure and data-processing details, including hosting locations, sub processors, retention periods, and service configurations, vary by product, feature, customer region, and contractual arrangements.

**Remote/Tensor** primarily facilitate secure remote connectivity and access. **TeamViewer ONE/DEX** additionally process endpoint telemetry and operational data to deliver device management, experience monitoring, analytics, automation, reporting, and AI-supported capabilities such as insights, anomaly detection, and workflow assistance. TeamViewer implements Technical and Organizational Measures (TOMs), including physical and logical access controls, system and transfer safeguards, availability and resilience measures, incident response processes, and privacy-by-design principles. Further details regarding infrastructure, hosting, sub processors, and data protection controls are available through TeamViewer's Trust Center, Data Processing Agreement, and related compliance documentation.

For further documentation please reference our [DPA Annexes](#), [sub processor list](#), [product description](#), and contract for authoritative details. In particular, sub processor information should be reviewed through the applicable [DPA annex](#) or [sub processor list](#), as providers, regions, services, and sub processors may differ depending on product, feature, customer region, configuration, and contractual arrangements.

## 9.2 Cloud Providers, Sub-processors and Infrastructure Dependencies

TeamViewer uses a combination of TeamViewer-operated infrastructure and carefully selected cloud service providers to deliver remote connectivity, endpoint management, Digital Employee Experience (DEX), automation, AI-supported capabilities, reporting, and related platform services.

Infrastructure providers, hosting services, and approved sub-processors may vary depending on product, feature, region, and contractual arrangements. TeamViewer maintains and publishes approved [sub-processor information](#) through the applicable [Data Processing Agreement annexes](#) and [Trust Center resources](#).

Different TeamViewer services may process and retain different categories of information, including account data, audit logs, connection reports, session recordings, endpoint-management data, Digital Employee Experience (DEX) telemetry, reporting data, automation-related information, and AI-supported service data. The applicable retention model may vary between products and capabilities.

For capabilities such as session recording, audit logging, connection reporting, and integrations with customer-managed storage solutions, retention and archival practices may be configured or managed by the customer according to organizational, regulatory, contractual, and evidentiary requirements. Session recordings can also be exported or stored within customer-managed repositories where supported.

Authoritative information regarding data-retention periods, storage duration, deletion processes, service-specific retention behavior, and customer-configurable retention options is maintained through the applicable [product documentation](#), contractual documentation, [Data Processing Agreement \(DPA\)](#), [Privacy Notice](#), [Trust Center](#) resources, and [Compliance Portal](#) documentation. Retention requirements may differ between products, services, deployment models, and enabled capabilities.

Customers can review current sub-processor information, service providers, and processing scopes through the official TeamViewer compliance resources.

## 9.3 Network Connectivity Requirements

TeamViewer services are designed to operate within enterprise network environments while supporting a range of customer security, routing, and connectivity requirements. TeamViewer Remote product is designed as an outgoing protocol so that we reduce any extra firewall configurations, as outgoing traffic is normally allowed on a firewall and replied traffic to permitted outgoing traffic is normally already authorized and no additional rules are required.

Organizations can restrict communication to defined TeamViewer services through network allowlisting and firewall controls. TeamViewer provides publicly available guidance regarding required service endpoints, network destinations, ports, and communication requirements to help customers align TeamViewer deployments with corporate network security policies.

For environments that require outbound traffic routing, proxy-based routing, or controlled internet access, TeamViewer supports deployment scenarios that can operate through supported proxy configurations. Specific proxy requirements and supported deployment models depend on the applicable TeamViewer product and operating environment.

Customers operating highly regulated, segmented, or security-sensitive environments may further restrict connectivity through capabilities such as Conditional Access and Hybrid Conditional Access. These capabilities help organizations implement policy-based access controls while maintaining governance and visibility across remote access activities.

Detailed and continuously updated guidance regarding network requirements, allowlisting, proxy support, ports, endpoint connectivity, and deployment considerations is maintained through TeamViewer product documentation and the TeamViewer Knowledge Base.

## 9.4 Data Residency and Data Processing

Data residency and data processing are related but different concepts.

**Data residency** refers to the region in which customer data is hosted or stored for a particular TeamViewer service or component.

**Data processing** refers to the activities required to provide, operate, secure, maintain, and support the service. Depending on the service and configuration, processing may involve TeamViewer infrastructure and approved sub-processors.

For *TeamViewer Remote and Tensor*, customers can choose between TeamViewer's standard global infrastructure and, where applicable, regional offerings such as TeamViewer Tensor Regional Restricted Access (RRA) ([Configure TeamViewer Tensor US Regional Restricted Access within your TeamViewer environment](#)). Regional offerings are subject to the applicable product documentation and contractual terms.

For *TeamViewer ONE*, different service components may have different hosting and processing arrangements. The remote-connectivity, endpoint management, Digital Employee Experience (DEX), automation, reporting, integration, and AI capabilities may rely on different infrastructures, supporting services, or approved sub-processors depending on the enabled functionality.

Because hosting locations, sub-processors, service architectures, and regional offerings may evolve over time, customers should refer to the following documents for authoritative and current information:

- [DPA Annex 1 – Details of the Processing](#)
- [DPA Annex 2 – Technical and Organizational Measures \(TOMs\)](#)
- [DPA Annex 3 – Approved Sub-processors](#)
- [Applicable Product Descriptions](#)
- Customer contractual documentation and order forms

These documents provide the authoritative information regarding hosting arrangements, approved sub-processors, processing activities, and applicable regional offerings.

## 9.5 Business Continuity and Service Availability

TeamViewer designs and operates its services with a focus on availability, resilience, and business continuity. The platform leverages redundant infrastructure, resilient network connectivity, and operational monitoring capabilities to help maintain service availability and support continuity of critical business operations. TeamViewer's hosting environments are designed with redundancy across network connectivity, power infrastructure, and critical service components to reduce the risk of service disruption and support operational resilience.

TeamViewer maintains business continuity and disaster recovery processes as part of its broader Information Security Management System (ISMS) and operational governance framework. These processes are designed to support the continued delivery of services during disruptive events and to enable the recovery of affected systems, services, and supporting infrastructure where required. TeamViewer's Business Continuity Management (BCM) program is reviewed, tested, and updated at least annually to help ensure continued alignment with business requirements, operational risks, technology changes, and evolving threat scenarios. Business continuity and disaster recovery activities are supported by established governance processes, periodic testing activities, lessons-learned reviews, and continuous improvement initiatives intended to strengthen organizational resilience and recovery capabilities.

Operational resilience is further supported through security monitoring, incident management, vulnerability management, change management, backup processes where applicable, and the availability of dedicated operational and security response teams. TeamViewer's Security Operations Center (SOC), Computer Security Incident Response Team (CSIRT), and Product Security Incident Response Team (PSIRT) support the detection, management, and response to operational and security-related events across the environment.

To provide transparency regarding service availability and operational status, TeamViewer publishes service health and incident information through the TeamViewer Status Page. Where applicable, customers can review current service status, scheduled maintenance activities, and historical service events through this resource.

To provide transparency regarding service availability and operational status, TeamViewer publishes service health, maintenance, and incident information through the [TeamViewer Status Page](#). Customers can use the Status Page to review the current operational status of TeamViewer services, planned maintenance activities, historical service events, and incident communications. The Status Page serves as a central communication channel for service availability and operational-impact notifications.

Additional information regarding TeamViewer's Technical and Organizational Measures (TOMs), business continuity controls, disaster recovery measures, and operational safeguards can be found in the applicable [Data Processing Agreement \(DPA\)](#), [DPA Annexes](#), [Trust Center resources](#), and [Compliance Portal documentation](#).

## 9.6 Security Incident Management

TeamViewer maintains a structured security incident management capability designed to identify, assess, respond to, and communicate security incidents affecting TeamViewer services, systems, and products. Incident-management activities are supported through dedicated security and operational response functions, including the Security Operations Center (SOC), Computer Security Incident Response Team (CSIRT), and Product Security Incident Response Team (PSIRT).

Security incidents are managed through established processes that support detection, triage, investigation, containment, remediation, recovery, communication, and continuous improvement activities. Depending on the nature of the incident, additional internal stakeholders such as Legal, Privacy, Compliance, Infrastructure, Product Security, and Engineering teams may participate in response activities.

Where required by applicable contractual commitments, regulatory obligations, or data-protection requirements, TeamViewer provides customer notifications in accordance with the applicable agreements, including the Data Processing Agreement (DPA) and related contractual documentation. Customers should refer to their contractual documentation for authoritative notification obligations and timelines.

TeamViewer publishes relevant security communications through established customer communication channels, which may include the [TeamViewer Trust Center](#), [Security Bulletins](#), customer notifications, service communications, and the [TeamViewer Status Page](#).

TeamViewer Security Bulletins provide customers with information regarding relevant product-security matters, including vulnerabilities, fixed versions, mitigations, severity information, and associated CVEs where applicable. Customers may subscribe to bulletin notifications through the [TeamViewer Security Bulletin page](#).

## 10 Definitions

| Term                                     | Definition                                                                                                                                                                                                                              |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ABAC</b>                              | Attribute-Based Access Control. A method of controlling access based on attributes such as user, resource, action, context, tenant, or data scope.                                                                                      |
| <b>Access Control</b>                    | TeamViewer session-level controls that allow administrators to configure which connection modes and permissions are available during remote sessions.                                                                                   |
| <b>AES</b>                               | Advanced Encryption Standard. A symmetric encryption algorithm used to protect data.                                                                                                                                                    |
| <b>AES-256</b>                           | Advanced Encryption Standard using a 256-bit key.                                                                                                                                                                                       |
| <b>AES-256-GCM</b>                       | AES-256 using Galois/Counter Mode. A modern authenticated encryption mode used to protect session data after secure key establishment.                                                                                                  |
| <b>Agentless Access</b>                  | A TeamViewer capability for accessing supported OT, industrial, legacy, or network assets without installing a TeamViewer Host on the target endpoint.                                                                                  |
| <b>Agentless Access Gateway</b>          | A gateway component used in Agentless Access scenarios to enable controlled access to selected assets or protocols in segmented environments.                                                                                           |
| <b>AI-assisted scripting</b>             | A TeamViewer AI workflow that helps draft scripts from prompts and optional context, while execution remains governed by permissions and approved workflows.                                                                            |
| <b>AI-supported services</b>             | TeamViewer capabilities that use AI-assisted processing to support functions such as session documentation, troubleshooting, insights, scripting assistance, automation support, and reporting, depending on license and configuration. |
| <b>Allowlist</b>                         | A security control that restricts access to selected devices so that only explicitly authorized TeamViewer IDs, accounts, or company profiles can connect.                                                                              |
| <b>API</b>                               | Application Programming Interface. A defined interface that allows systems or applications to exchange data or integrate functionality.                                                                                                 |
| <b>Asset Management</b>                  | Endpoint management capability used to identify, inventory, and manage hardware and software assets.                                                                                                                                    |
| <b>Auditability / Event Logging</b>      | TeamViewer logging and reporting capabilities that help administrators review security-relevant actions, connection activity, administration actions, and other supported events.                                                       |
| <b>Automation</b>                        | A TeamViewer ONE workflow that evaluates configured triggers, preconditions, checks, and remediation actions to respond to operational issues where supported.                                                                          |
| <b>BYOC</b>                              | Bring Your Own Certificate. A feature that enables customers to use their own certificates to authenticate devices involved in TeamViewer connections, in addition to TeamViewer certificates.                                          |
| <b>CA / Certification Authority</b>      | An entity that issues digital certificates used to validate identities or certificate-based authentication chains.                                                                                                                      |
| <b>CCM</b>                               | Cloud Control Matrix                                                                                                                                                                                                                    |
| <b>Certificate Revocation List (CRL)</b> | A list used to identify certificates that have been revoked before their scheduled expiration date.                                                                                                                                     |

|                                        |                                                                                                                                                                                                  |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Client Enrollment / Assignment</b>  | The process of assigning a TeamViewer client or host to a TeamViewer account or company profile and synchronizing assignment information with the TeamViewer backend.                            |
| <b>CMDB</b>                            | Configuration Management Database. A repository used by IT organizations to track configuration items, assets, relationships, and service-management data.                                       |
| <b>CNA</b>                             | CVE Numbering Authority. An organization authorized by the CVE Program to assign CVE IDs and publish vulnerability information for products within its scope.                                    |
| <b>Code Signing</b>                    | A software integrity mechanism that digitally signs software so that the publisher can be identified and tampering can be detected.                                                              |
| <b>Conditional Access</b>              | A TeamViewer capability for enforcing granular remote connection and routing rules based on users, devices, groups, managed device groups, and policy conditions.                                |
| <b>Conditional Access Router</b>       | A TeamViewer routing and policy-enforcement component shown in the architecture view for applying Conditional Access decisions to connectivity flows.                                            |
| <b>CRA</b>                             | Cyber Resilience Act                                                                                                                                                                             |
| <b>CSA STAR</b>                        | Cloud Security Alliance Security, Trust, Assurance, and Risk framework. A cloud security assurance framework referenced in compliance contexts.                                                  |
| <b>CSIRT</b>                           | Computer Security Incident Response Team. A team responsible for coordinating response to cybersecurity incidents.                                                                               |
| <b>CVE</b>                             | Common Vulnerabilities and Exposures. A standardized identifier for publicly known cybersecurity vulnerabilities.                                                                                |
| <b>CVSS</b>                            | Common Vulnerability Scoring System. A scoring framework used to assess and communicate vulnerability severity.                                                                                  |
| <b>DAST</b>                            | Dynamic Application Security Testing. Security testing performed against a running application or service.                                                                                       |
| <b>Data Processing Agreement (DPA)</b> | A contractual document that describes data-processing roles, obligations, safeguards, and annexes such as sub processors and Technical and Organizational Measures.                              |
| <b>DEX</b>                             | Digital Employee Experience. Capabilities designed to provide visibility into endpoint and user experience signals across devices, applications, networks, operating systems, and user feedback. |
| <b>DEX Hub</b>                         | A TeamViewer DEX and TeamViewer ONE Enterprise capability for storing, managing, reviewing, reusing, and governing automation content such as scripts and packs.                                 |
| <b>DEX Insights</b>                    | TeamViewer DEX capability that processes endpoint experience signals such as performance, reliability, responsiveness, and failure signals to support operational insights.                      |
| <b>Digital Workplace</b>               | A technology environment that supports secure, managed, and optimized digital work across devices, applications, users, and IT services.                                                         |
| <b>DMZ</b>                             | Demilitarized Zone. A segmented network zone used to separate trusted internal networks from less trusted networks or external access paths.                                                     |

|                                        |                                                                                                                                                                                                                          |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Easy Access</b>                     | A TeamViewer unattended access method that enables password-less access for authorized users based on TeamViewer account-based authentication and permissions.                                                           |
| <b>End-to-end encryption</b>           | An encryption model where only the communicating endpoints can decrypt transmitted session data.                                                                                                                         |
| <b>Endpoint Management</b>             | Capabilities used to monitor, configure, patch, inventory, secure, and manage devices across an organization.                                                                                                            |
| <b>Event Log API</b>                   | An interface that allows supported event log information to be exported or retrieved programmatically for reporting, governance, SIEM, or compliance workflows.                                                          |
| <b>FIDO</b>                            | Fast Identity Online. A standard for phishing-resistant authentication using hardware-backed or platform-based authenticators.                                                                                           |
| <b>FIRST</b>                           | Forum of Incident Response and Security Teams. An international organization for incident response and security teams.                                                                                                   |
| <b>HCA / Hybrid Conditional Access</b> | Hybrid Conditional Access. A TeamViewer capability that extends Conditional Access with local enforcement for segmented or security-sensitive environments.                                                              |
| <b>HIPAA/HITECH</b>                    | U.S. healthcare privacy and security frameworks referenced in compliance contexts where applicable.                                                                                                                      |
| <b>HMI</b>                             | Human-Machine Interface. An industrial interface used by operators to monitor or control machines, processes, or industrial systems.                                                                                     |
| <b>iDMZ</b>                            | Industrial Demilitarized Zone. A segmented network zone commonly used to separate enterprise IT networks from OT or industrial networks.                                                                                 |
| <b>IdP</b>                             | Identity Provider. A system used to authenticate users and provide identity assertions to applications or services.                                                                                                      |
| <b>ISMS</b>                            | Information Security Management System. A structured management system for governing information security policies, controls, risks, and continuous improvement.                                                         |
| <b>ISO/IEC 27001</b>                   | An international standard for information security management systems.                                                                                                                                                   |
| <b>ISO 9001</b>                        | An international standard for quality management systems.                                                                                                                                                                |
| <b>ITSM</b>                            | IT Service Management. A set of processes and practices used to design, deliver, manage, support, and improve IT services throughout their lifecycle.                                                                    |
| <b>KEV</b>                             | Known Exploited Vulnerabilities. A term used in vulnerability management to identify vulnerabilities known to be actively exploited.                                                                                     |
| <b>LAPS</b>                            | Local Administrator Password Solution. In this document, Microsoft Windows LAPS integration supports secure retrieval and injection of managed local administrator credentials during supported remote support sessions. |
| <b>Layer 4 tunneling</b>               | A network tunneling approach operating at the transport layer, commonly associated with controlled access to selected TCP or UDP services.                                                                               |

|                                      |                                                                                                                                                                                      |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>MDM</b>                           | Mobile Device Management. Technology used to deploy, configure, secure, and manage mobile devices.                                                                                   |
| <b>MFA/TFA</b>                       | Multi-Factor Authentication / Two-Factor Authentication. An authentication method that requires an additional factor beyond username and password.                                   |
| <b>Microsoft Entra ID</b>            | Microsoft's cloud identity and access management service, formerly known as Azure Active Directory.                                                                                  |
| <b>Microsoft Intune</b>              | Microsoft endpoint management service used to manage devices, applications, and related policies.                                                                                    |
| <b>Mobile SDK</b>                    | TeamViewer Mobile Software Development Kit. An add-on that enables customers to embed supported TeamViewer remote support capabilities into their own mobile applications.           |
| <b>Mutual TLS / mTLS</b>             | A TLS configuration where both communicating parties authenticate each other using certificate-based mechanisms.                                                                     |
| <b>NDA</b>                           | Non-Disclosure Agreement. A legal agreement used to protect confidential information shared between parties.                                                                         |
| <b>OpenSSL</b>                       | An open-source cryptographic toolkit and library referenced in relation to supported certificate formats.                                                                            |
| <b>Operational Technology (OT)</b>   | Hardware and software used to monitor, control, or manage industrial processes, devices, machines, and physical operations.                                                          |
| <b>Patch Management</b>              | The process of identifying, deploying, and tracking software or operating system updates to reduce vulnerabilities and improve stability.                                            |
| <b>PEM</b>                           | Privacy-Enhanced Mail format. A common text-based format for certificates and cryptographic material.                                                                                |
| <b>Perfect Forward Secrecy (PFS)</b> | A property of key exchange protocols that helps protect past session keys even if long-term keys are later compromised.                                                              |
| <b>PIV</b>                           | Personal Identity Verification. A standard for smartcard-based identity credentials used in strong authentication scenarios.                                                         |
| <b>PKCE</b>                          | Proof Key for Code Exchange. A security extension for OAuth-based authorization flows that helps protect token exchange.                                                             |
| <b>PKI</b>                           | Public Key Infrastructure. A framework for issuing, managing, validating, and revoking digital certificates and public/private key pairs.                                            |
| <b>PLC</b>                           | Programmable Logic Controller. An industrial computer used to control machines or processes in OT environments.                                                                      |
| <b>PSIRT</b>                         | Product Security Incident Response Team. A team responsible for coordinating product vulnerability intake, validation, remediation, disclosure, and related security communications. |
| <b>RBAC</b>                          | Role-Based Access Control. A method of controlling access based on assigned user roles and permissions.                                                                              |
| <b>RDP</b>                           | Remote Desktop Protocol. A protocol commonly used for remote access to Windows systems.                                                                                              |

|                                 |                                                                                                                                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>RMM</b>                      | Remote Monitoring and Management. Capabilities used by IT teams to monitor, manage, and maintain devices remotely.                                                                      |
| <b>RSA-4096</b>                 | RSA public-key cryptography using a 4096-bit key size.                                                                                                                                  |
| <b>SAML 2.0</b>                 | Security Assertion Markup Language 2.0. A standard for exchanging authentication and authorization data between identity providers and service providers.                               |
| <b>SAST</b>                     | Static Application Security Testing. Security testing performed by analyzing source code, bytecode, or binaries without executing the application.                                      |
| <b>SBOM</b>                     | Software Bill of Materials. An inventory of software components, including relevant open-source and third-party components, used to support software supply chain transparency.         |
| <b>SCA</b>                      | Software Composition Analysis. A process and tooling category used to identify, track, and assess open-source and third-party software dependencies.                                    |
| <b>SCIM</b>                     | System for Cross-domain Identity Management. A standard for synchronizing user and group information between identity systems and applications.                                         |
| <b>Security Bulletins</b>       | TeamViewer publications that communicate relevant product security information such as affected versions, severity, fixed versions, mitigations, workarounds, or CVEs where applicable. |
| <b>Security Key Redirection</b> | A TeamViewer capability that allows supported local hardware security keys or smartcards to be redirected into a remote session for authentication scenarios.                           |
| <b>Session Insights</b>         | A TeamViewer AI capability that creates structured session summaries, action steps, and labels for support sessions where available.                                                    |
| <b>SIEM</b>                     | Security Information and Event Management. A security platform category used to collect, analyze, and correlate security events and logs.                                               |
| <b>SIRT</b>                     | Security Incident Response Team. A team responsible for coordinating security incident or vulnerability response activities.                                                            |
| <b>SOC</b>                      | Security Operations Center. A team or function that monitors, detects, analyzes, and responds to cybersecurity events.                                                                  |
| <b>SOC 2 / SOC 3</b>            | Independent assurance reports based on AICPA Trust Services Criteria, commonly used to assess controls relevant to security and other trust services categories.                        |
| <b>SPDX</b>                     | Software Package Data Exchange. A common industry format for software bill of materials information.                                                                                    |
| <b>SSH</b>                      | Secure Shell. A protocol commonly used for secure administrative access to systems and network devices.                                                                                 |
| <b>SRP v6</b>                   | Secure Remote Password protocol version 6. An authentication protocol used by TeamViewer account authentication to avoid storing reusable password material on TeamViewer servers.      |
| <b>SSO</b>                      | Single Sign-On. An authentication model that allows users to authenticate through an identity provider, commonly using SAML 2.0 in the TeamViewer context.                              |

|                                     |                                                                                                                                                                                                                                                                                                         |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>S-SDLC</b>                       | Secure Software Development Life Cycle. TeamViewer's secure development process covering security activities across requirements, design, implementation, verification, release, and response.                                                                                                          |
| <b>TeamViewer Automation Client</b> | An endpoint component used for supported TeamViewer ONE automation and Tia troubleshooting workflows. In supported Tia scenarios, it is locally integrated with the TeamViewer Remote Client to collect diagnostic information within the applicable permissions, configuration, and workflow controls. |
| <b>TeamViewer Host</b>              | A TeamViewer client component installed on a device to support remote access scenarios, including unattended access where configured.                                                                                                                                                                   |
| <b>TeamViewer ID</b>                | A TeamViewer identifier used to address or identify a TeamViewer client or device in connection workflows.                                                                                                                                                                                              |
| <b>TeamViewer ONE</b>               | TeamViewer's digital workplace platform that brings together secure remote connectivity, endpoint management, DEX, automation, analytics, reporting, and AI-supported capabilities.                                                                                                                     |
| <b>TeamViewer Remote</b>            | TeamViewer's remote connectivity product experience for remote support, remote access, and remote work use cases.                                                                                                                                                                                       |
| <b>TeamViewer Tensor</b>            | TeamViewer's enterprise remote connectivity platform with security, scalability, management, integrations, auditability, and access-control capabilities.                                                                                                                                               |
| <b>Tenant-scoped controls</b>       | Controls that limit data access, processing, reporting, or administrative visibility to the authorized customer tenant or permitted tenant context.                                                                                                                                                     |
| <b>Tia</b>                          | TeamViewer Intelligent Agent. A TeamViewer AI capability that provides guided troubleshooting based on defined inputs, permissions, controlled context, and supported diagnostic information collected through the applicable TeamViewer components                                                     |
| <b>Tia Reporting</b>                | A TeamViewer DEX and TeamViewer ONE Enterprise AI capability for governed natural-language reporting based on tenant-scoped DEX data models and access controls.                                                                                                                                        |
| <b>TISAX</b>                        | Trusted Information Security Assessment Exchange. An information security assessment framework commonly used in the automotive industry.                                                                                                                                                                |
| <b>TLS</b>                          | Transport Layer Security. A cryptographic protocol used to protect communications over a network.                                                                                                                                                                                                       |
| <b>TLS 1.3</b>                      | Version 1.3 of the Transport Layer Security protocol, used in the document to describe supported modern remote-session authentication and attestation flows.                                                                                                                                            |
| <b>TOMs</b>                         | Technical and Organizational Measures. Contractual and operational safeguards designed to protect personal data and systems.                                                                                                                                                                            |
| <b>TOTP</b>                         | Time-Based One-Time Password. A method for generating short-lived authentication codes used as an additional authentication factor.                                                                                                                                                                     |
| <b>Trusted Devices</b>              | A TeamViewer account protection mechanism that requires new devices, browsers, or IP addresses to be authorized before login when two-factor authentication is not configured.                                                                                                                          |
| <b>Unified Policies</b>             | TeamViewer ONE's policy model for centrally assigning supported settings to device groups, enabling group-based policy assignment and inheritance where supported.                                                                                                                                      |

|                   |                                                                                                                                                   |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>VDP</b>        | Vulnerability Disclosure Program. A public channel for reporting vulnerabilities and supporting coordinated vulnerability disclosure.             |
| <b>VNC</b>        | Virtual Network Computing. A protocol commonly used for remote screen access to systems.                                                          |
| <b>WebAPI</b>     | A web-based application programming interface used to integrate TeamViewer functionality or data with external systems where supported.           |
| <b>X.509</b>      | A standard format for public key certificates used in certificate-based authentication.                                                           |
| <b>YesWeHack</b>  | The crowdsourced security platform referenced for TeamViewer's public Bug Bounty Program.                                                         |
| <b>Zero Trust</b> | A security approach based on the principle "never trust, always verify," where access is explicitly verified and controlled before being granted. |

## 11 Public Source Links

The following public resources support the product and security information summarized in this document.

| Link title                                             | URL                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TeamViewer Trust Center                                | <a href="https://www.teamviewer.com/en/resources/trust-center/">https://www.teamviewer.com/en/resources/trust-center/</a>                                                                                                                                                                                   |
| TeamViewer Compliance Portal                           | <a href="https://compliance.teamviewer.com/">https://compliance.teamviewer.com/</a>                                                                                                                                                                                                                         |
| Industry-leading security                              | <a href="https://www.teamviewer.com/en/resources/trust-center/industry-leading-security/">https://www.teamviewer.com/en/resources/trust-center/industry-leading-security/</a>                                                                                                                               |
| Security Bulletins                                     | <a href="https://www.teamviewer.com/en/resources/trust-center/security-bulletins/">https://www.teamviewer.com/en/resources/trust-center/security-bulletins/</a>                                                                                                                                             |
| Data Processing Agreement (DPA)                        | <a href="https://www.teamviewer.com/en/legal/eula/?tab=dpa">https://www.teamviewer.com/en/legal/eula/?tab=dpa</a>                                                                                                                                                                                           |
| DPA Annexes Overview                                   | <a href="https://www.teamviewer.com/en/legal/dpa-annex/">https://www.teamviewer.com/en/legal/dpa-annex/</a>                                                                                                                                                                                                 |
| Annex 1 - Details of Data Processing                   | <a href="https://media.teamviewer.com/is/content/teamviewergmbh/teamviewer/central-image-hub/pdf/en/teamviewer-dpa-annex-1-details-of-processing-en.pdf">https://media.teamviewer.com/is/content/teamviewergmbh/teamviewer/central-image-hub/pdf/en/teamviewer-dpa-annex-1-details-of-processing-en.pdf</a> |
| Annex 2 – Technical and Organizational Measures (TOMs) | <a href="https://media.teamviewer.com/is/content/teamviewergmbh/teamviewer/central-image-hub/pdf/en/teamviewer-dpa-annex-2-tom-en.pdf">https://media.teamviewer.com/is/content/teamviewergmbh/teamviewer/central-image-hub/pdf/en/teamviewer-dpa-annex-2-tom-en.pdf</a>                                     |
| Annex 3 – Sub processor List                           | <a href="https://media.teamviewer.com/is/content/teamviewergmbh/teamviewer/central-image-hub/pdf/en/teamviewer-dpa-annex-3-subprocessor-list-en.pdf">https://media.teamviewer.com/is/content/teamviewergmbh/teamviewer/central-image-hub/pdf/en/teamviewer-dpa-annex-3-subprocessor-list-en.pdf</a>         |
| Product Descriptions                                   | <a href="https://www.teamviewer.com/en/legal/product-descriptions/">https://www.teamviewer.com/en/legal/product-descriptions/</a>                                                                                                                                                                           |
| TeamViewer ONE Product Description                     | <a href="https://www.teamviewer.com/en/legal/product-descriptions/teamviewer-one/">https://www.teamviewer.com/en/legal/product-descriptions/teamviewer-one/</a>                                                                                                                                             |
| Privacy Notice – Products                              | <a href="https://www.teamviewer.com/en/legal/privacy-and-cookies/?tab=products">https://www.teamviewer.com/en/legal/privacy-and-cookies/?tab=products</a>                                                                                                                                                   |
| TeamViewer Third-Party Terms                           | <a href="https://media.teamviewer.com/is/content/teamviewergmbh/teamviewer/central-image-hub/pdf/en/teamviewer-third-party-terms-en.pdf">https://media.teamviewer.com/is/content/teamviewergmbh/teamviewer/central-image-hub/pdf/en/teamviewer-third-party-terms-en.pdf</a>                                 |
| TeamViewer AI Terms                                    | <a href="https://www.teamviewer.com/legal/ai-terms/">https://www.teamviewer.com/legal/ai-terms/</a>                                                                                                                                                                                                         |
| TeamViewer EULA                                        | <a href="https://www.teamviewer.com/eula/">https://www.teamviewer.com/eula/</a>                                                                                                                                                                                                                             |
| TeamViewer ONE Platform Overview                       | <a href="https://www.teamviewer.com/en-us/platform/one/">https://www.teamviewer.com/en-us/platform/one/</a>                                                                                                                                                                                                 |
| TeamViewer ONE Features                                | <a href="https://www.teamviewer.com/en/platform/one/features/">https://www.teamviewer.com/en/platform/one/features/</a>                                                                                                                                                                                     |
| TeamViewer Management Console                          | <a href="https://login.teamviewer.com/LogOn">https://login.teamviewer.com/LogOn</a>                                                                                                                                                                                                                         |

|                                                              |                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>TeamViewer Web App</b>                                    | <a href="https://web.teamviewer.com/">https://web.teamviewer.com/</a>                                                                                                                                                                                                                                                   |
| <b>TeamViewer Customer Success Stories</b>                   | <a href="https://www.teamviewer.com/en/success-stories/">https://www.teamviewer.com/en/success-stories/</a>                                                                                                                                                                                                             |
| <b>TeamViewer Tensor</b>                                     | <a href="https://www.teamviewer.com/en-us/products/tensor/">https://www.teamviewer.com/en-us/products/tensor/</a>                                                                                                                                                                                                       |
| <b>TeamViewer Tensor Security Center</b>                     | <a href="https://www.teamviewer.com/en/products/tensor/features/security-center/">https://www.teamviewer.com/en/products/tensor/features/security-center/</a>                                                                                                                                                           |
| <b>Security Golden Rules Insight Article</b>                 | <a href="https://www.teamviewer.com/en/insights/the-security-golden-rules/">https://www.teamviewer.com/en/insights/the-security-golden-rules/</a>                                                                                                                                                                       |
| <b>TeamViewer Security Handbook</b>                          | <a href="https://community.teamviewer.com/English/kb/security-handbook">https://community.teamviewer.com/English/kb/security-handbook</a>                                                                                                                                                                               |
| <b>Product-Specific Hardening and Configuration Guidance</b> | <a href="https://compliance.teamviewer.com/tc/share/66d9d142bda480c94de31efc">https://compliance.teamviewer.com/tc/share/66d9d142bda480c94de31efc</a>                                                                                                                                                                   |
| <b>Best Practices for Secure Unattended Access</b>           | <a href="https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-classic/security/best-practices/best-practices-for-secure-unattended-access/">https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-classic/security/best-practices/best-practices-for-secure-unattended-access/</a>   |
| <b>Security Center</b>                                       | <a href="https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-remote/security/increase-your-security-posture-with-the-security-center/">https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-remote/security/increase-your-security-posture-with-the-security-center/</a>           |
| <b>Secure Attended Access</b>                                | <a href="https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-classic/remote-control/connection-methods/remote-control-via-attended-access/">https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-classic/remote-control/connection-methods/remote-control-via-attended-access/</a> |
| <b>Easy Access</b>                                           | <a href="https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-classic/remote-control/connection-methods/remote-control-via-easy-access/">https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-classic/remote-control/connection-methods/remote-control-via-easy-access/</a>         |
| <b>Provide Unattended Remote Support</b>                     | <a href="https://www.teamviewer.com/en-us/global/support/knowledge-base/teamviewer-remote/remote-control/provide-unattended-remote-support/">https://www.teamviewer.com/en-us/global/support/knowledge-base/teamviewer-remote/remote-control/provide-unattended-remote-support/</a>                                     |
| <b>Mass Deployment on Windows – Overview</b>                 | <a href="https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-remote/deployment/mass-deployment-on-windows-overview/">https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-remote/deployment/mass-deployment-on-windows-overview/</a>                                               |
| <b>Block and Allowlist</b>                                   | <a href="https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-remote/security/block-and-allowlist/">https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-remote/security/block-and-allowlist/</a>                                                                                   |
| <b>Two-Factor Authentication for Connections</b>             | <a href="https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-classic/security/security-features/two-factor-authentication-for-connections/">https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-classic/security/security-features/two-factor-authentication-for-connections/</a> |
| <b>Restrict Access</b>                                       | <a href="https://community.teamviewer.com/English/kb/articles/108687-restrict-access">https://community.teamviewer.com/English/kb/articles/108687-restrict-access</a>                                                                                                                                                   |
| <b>Conditional Access</b>                                    | <a href="https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-tensor-classic/security/conditional-access/">https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-tensor-classic/security/conditional-access/</a>                                                                     |
| <b>Hybrid Conditional Access</b>                             | <a href="https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-tensor/conditional-access/hybrid-conditional-access/">https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-tensor/conditional-access/hybrid-conditional-access/</a>                                                   |
| <b>Bring Your Own Certificate</b>                            | <a href="https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-tensor/security/bring-your-own-certificate/">https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-tensor/security/bring-your-own-certificate/</a>                                                                     |

|                                                     |                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Single Sign-On (SSO)                                | <a href="https://www.teamviewer.com/en-us/global/support/knowledge-base/teamviewer-tensor/sso/single-sign-on-sso/">https://www.teamviewer.com/en-us/global/support/knowledge-base/teamviewer-tensor/sso/single-sign-on-sso/</a>                                                                                                           |
| Single Sign-On for Microsoft Entra ID               | <a href="https://www.teamviewer.com/en-us/global/support/knowledge-base/teamviewer-tensor-classic/sso/single-sign-on-for-microsoft-entra-id/">https://www.teamviewer.com/en-us/global/support/knowledge-base/teamviewer-tensor-classic/sso/single-sign-on-for-microsoft-entra-id/</a>                                                     |
| Two-Factor Authentication for Account Login         | <a href="https://www.teamviewer.com/en-us/global/support/knowledge-base/teamviewer-classic/security/multi-factor-authentication/activate-two-factor-authentication/">https://www.teamviewer.com/en-us/global/support/knowledge-base/teamviewer-classic/security/multi-factor-authentication/activate-two-factor-authentication/</a>       |
| Trusted Devices                                     | <a href="https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-classic/security/trusted-devices/trusted-devices/">https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-classic/security/trusted-devices/trusted-devices/</a>                                                                           |
| Trust Management for Trusted Devices                | <a href="https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-classic/security/trusted-devices/trust-management-for-trusted-devices/">https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-classic/security/trusted-devices/trust-management-for-trusted-devices/</a>                                 |
| Trust Devices via Push Notification                 | <a href="https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-remote/security/trust-devices-via-push-notification/">https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-remote/security/trust-devices-via-push-notification/</a>                                                                     |
| Microsoft Entra ID Integration – SCIM Configuration | <a href="https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-tensor/integrations/microsoft-entra-id-integration-scim-configuration/">https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-tensor/integrations/microsoft-entra-id-integration-scim-configuration/</a>                                 |
| Okta Integration – SCIM Configuration               | <a href="https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-tensor/integrations/okta-integration-scim-configuration/">https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-tensor/integrations/okta-integration-scim-configuration/</a>                                                             |
| Policies                                            | <a href="https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-remote/devices/policies/">https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-remote/devices/policies/</a>                                                                                                                             |
| Policy Settings                                     | <a href="https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-remote/devices/policy-settings/">https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-remote/devices/policy-settings/</a>                                                                                                               |
| Unified Policies in TeamViewer ONE                  | <a href="https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-one/unified-policies-in-teamviewer-one/">https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-one/unified-policies-in-teamviewer-one/</a>                                                                                               |
| Unified Policy Migration Guide                      | <a href="https://www.teamviewer.com/en-us/global/support/knowledge-base/teamviewer-one/unified-policy-migration-guide/">https://www.teamviewer.com/en-us/global/support/knowledge-base/teamviewer-one/unified-policy-migration-guide/</a>                                                                                                 |
| Automation in TeamViewer ONE                        | <a href="https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-one/automations-in-teamviewer-one/">https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-one/automations-in-teamviewer-one/</a>                                                                                                         |
| TeamViewer Black Screen                             | <a href="https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-remote/security/teamviewer-black-screen/">https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-remote/security/teamviewer-black-screen/</a>                                                                                             |
| Auditability / Event Log                            | <a href="https://www.teamviewer.com/en-us/global/support/knowledge-base/teamviewer-tensor/security/auditability-event-log/">https://www.teamviewer.com/en-us/global/support/knowledge-base/teamviewer-tensor/security/auditability-event-log/</a>                                                                                         |
| Event Log API Documentation                         | <a href="https://webapi.teamviewer.com/api/v1/docs/index">https://webapi.teamviewer.com/api/v1/docs/index</a>                                                                                                                                                                                                                             |
| TeamViewer Mobile Software Development Kit (SDK)    | <a href="https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-classic/integrations/core-integrations/teamviewer-mobile-software-development-kit-sdk/">https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-classic/integrations/core-integrations/teamviewer-mobile-software-development-kit-sdk/</a> |
| Security Key Redirection                            | <a href="https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-tensor/security/security-key-redirection/">https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-tensor/security/security-key-redirection/</a>                                                                                           |
| Windows LAPS Integration                            | <a href="https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-tensor/integrations/getting-started-with-the-windows-laps-integration-in-teamviewer/">https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-tensor/integrations/getting-started-with-the-windows-laps-integration-in-teamviewer/</a>     |

|                                                                                                                  |                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Provide In-Session Chat Transcripts for Integrations</b>                                                      | <a href="https://www.teamviewer.com/en-us/global/support/knowledge-base/teamviewer-tensor/security/provide-in-session-chat-transcripts-for-integrations/">https://www.teamviewer.com/en-us/global/support/knowledge-base/teamviewer-tensor/security/provide-in-session-chat-transcripts-for-integrations/</a>                           |
| <b>TeamViewer AI Security, Privacy and Customer Control</b>                                                      | <a href="https://www.teamviewer.com/en-us/products/add-ons/ai/security/">https://www.teamviewer.com/en-us/products/add-ons/ai/security/</a>                                                                                                                                                                                             |
| <b>FAQ: AI Security and Privacy</b>                                                                              | <a href="https://www.teamviewer.com/en/products/add-ons/ai/security/fag/">https://www.teamviewer.com/en/products/add-ons/ai/security/fag/</a>                                                                                                                                                                                           |
| <b>TeamViewer AI for IT Support</b>                                                                              | <a href="https://www.teamviewer.com/en-us/platform/one/features/teamviewer-ai/">https://www.teamviewer.com/en-us/platform/one/features/teamviewer-ai/</a>                                                                                                                                                                               |
| <b>Tia – AI-Guided Troubleshooting</b>                                                                           | <a href="https://www.teamviewer.com/en-us/products/add-ons/ai/tia/">https://www.teamviewer.com/en-us/products/add-ons/ai/tia/</a>                                                                                                                                                                                                       |
| <b>Troubleshoot IT Issues with Tia</b>                                                                           | <a href="https://www.teamviewer.com/en-us/global/support/knowledge-base/teamviewer-remote/remote-control/troubleshoot-it-issues-with-tia/">https://www.teamviewer.com/en-us/global/support/knowledge-base/teamviewer-remote/remote-control/troubleshoot-it-issues-with-tia/</a>                                                         |
| <b>Generate Session Summaries with Session Insights</b>                                                          | <a href="https://www.teamviewer.com/en-us/global/support/knowledge-base/teamviewer-remote/remote-control/generate-session-summaries-with-session-insights/">https://www.teamviewer.com/en-us/global/support/knowledge-base/teamviewer-remote/remote-control/generate-session-summaries-with-session-insights/</a>                       |
| <b>AI Credit-Based Payment Model</b>                                                                             | <a href="https://www.teamviewer.com/en-us/global/support/knowledge-base/teamviewer-remote/licenses/licenses-and-features/ai-credit-based-payment-model/">https://www.teamviewer.com/en-us/global/support/knowledge-base/teamviewer-remote/licenses/licenses-and-features/ai-credit-based-payment-model/</a>                             |
| <b>AI Security Stance – TeamViewer Remote, Tensor and ONE</b>                                                    | <a href="https://media.teamviewer.com/is/content/teamviewergmbh/teamviewer/central-image-hub/pdf/en/teamviewer-ai-security-stance-datasheet-en.pdf">https://media.teamviewer.com/is/content/teamviewergmbh/teamviewer/central-image-hub/pdf/en/teamviewer-ai-security-stance-datasheet-en.pdf</a>                                       |
| <b>AI Security Stance – DEX and TeamViewer ONE Enterprise</b>                                                    | <a href="https://media.teamviewer.com/is/content/teamviewergmbh/teamviewer/central-image-hub/pdf/en/teamviewer-dex-one-enterprise-ai-security-stance-datasheet-en.pdf">https://media.teamviewer.com/is/content/teamviewergmbh/teamviewer/central-image-hub/pdf/en/teamviewer-dex-one-enterprise-ai-security-stance-datasheet-en.pdf</a> |
| <b>TeamViewer AI Security Resource – Trust Center Share</b>                                                      | <a href="https://compliance.teamviewer.com/tc/share/69bd62c2a5b97f40dd19cf8e">https://compliance.teamviewer.com/tc/share/69bd62c2a5b97f40dd19cf8e</a>                                                                                                                                                                                   |
| <b>TeamViewer AI Security, Control and Data Handling for TeamViewer Remote, Tensor and ONE</b>                   | <a href="https://compliance.teamviewer.com/tc/share/69bc20a5915f44b87d9a74e8">https://compliance.teamviewer.com/tc/share/69bc20a5915f44b87d9a74e8</a>                                                                                                                                                                                   |
| <b><u>TeamViewer AI Security, Control and Data Handling for TeamViewer DEX and TeamViewer ONE Enterprise</u></b> | <a href="https://compliance.teamviewer.com/tc/share/6a465876f60627ba71b4501b">https://compliance.teamviewer.com/tc/share/6a465876f60627ba71b4501b</a>                                                                                                                                                                                   |
| <b>Safety First, Last and Always: The Seven Key Stages of Secure Software Development</b>                        | <a href="https://www.teamviewer.com/en/insights/safety-first-last-and-always-the-seven-key-stages-of-secure-software-development/">https://www.teamviewer.com/en/insights/safety-first-last-and-always-the-seven-key-stages-of-secure-software-development/</a>                                                                         |
| <b>FIRST-listed TeamViewer SIRT</b>                                                                              | <a href="https://www.first.org/members/teams/teamviewer_sirt">https://www.first.org/members/teams/teamviewer_sirt</a>                                                                                                                                                                                                                   |
| <b>TeamViewer security.txt</b>                                                                                   | <a href="https://www.teamviewer.com/.well-known/security.txt">https://www.teamviewer.com/.well-known/security.txt</a>                                                                                                                                                                                                                   |
| <b>TeamViewer Vulnerability Disclosure Program</b>                                                               | <a href="https://vdp.teamviewer.com/">https://vdp.teamviewer.com/</a>                                                                                                                                                                                                                                                                   |

**TeamViewer Bug Bounty Program**

<https://www.teamviewer.com/en-us/resources/trust-center/bug-bounty-program/>

**YesWeHack TeamViewer Bug Bounty Program**

<https://yeswehack.com/programs/teamviewer-bounty-program>

**CVE Program – TeamViewer CNA Partner Page**

<https://www.cve.org/PartnerInformation/ListofPartners/partner/TeamViewer>

**TeamViewer Status Page**

<https://status.teamviewer.com/>

**Knowledgebase about AI capabilities in TeamViewer**

<https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-remote/teamviewer-ai/enable-tia-troubleshooting-in-teamviewer/>