TeamViewer Security

Overview, Architecture and Encryption

Please note that the information may not always be up-to-date and are non-binding.

Contents

TeamViewer: The Company and Software 4
About TeamViewer 4
Fundamentals of TeamViewer Security 4
Quality Management 4
Information Security and Compliance 5
Data Centers and Backbone 5
References 5
Security Posture 6
Security Basics 6
Product and Services Overview 7
Components 7
Clients 7
Management Console 7
Teamviewer Intelligence Suite 7
Security Features and Benefits 12
Main Use Cases 12
Secure Attended Access 12
Secure Unattended Access 12
Client Enrollment/Assignment: 13
Connection Authentication and Device Access Control 13
Block- and Allowlist 13
Access Control for Incoming and Outgoing Connections 14
Conditional Access 14
Bring your Own Certificate (BYOC) for connection authentication 15
Random Password for Connections 15
Account Authentication 16
Single Sign-On (SSO) 16
Two-Factor Authentication for Account Login (TFA/MFA) 16
Trusted Devices 16
Additional Security Features 16
Security Center 16
Device Policy 16
Black Screen / Privacy Screen 17
Auditability: Event Logging 17
SCIM System for Cross Domain Identity Management provisioning 17

Mobile SDK 17
Security Key Redirection 17
LDAPS (Local Domain Admin Password Solution) integration 17
Chat 18
Data Handling and Encryption 18
Account Data Protection 18
Encryption 19
Development Process 20
Our Secure Software Development Lifecycle (S-SDLC) 20
Security Testing and Composition Analysis (SCA) 20
Penetration Testing 20
Code Signing 20
Software Bill of Materials (SBOM) 20
Product Security Incident Response Team (PSIRT) 21
Vulnerability Disclosure Program (VDP) 21
Bug Bounty Program 21
Security Bulletins 22
Certified Numbering Authority (CNA) 22
Internal Vulnerability management timeframes 22
Hosting and Infrastructure 23
Definitions 24

Material Revision

Date	Autor	Version	Change Object
02/2022	Product Security	1.0	
03/2024	Product Security	1.1	
08/2025	Product Security	1.2	Added content
03/2026	Customer Trust and Security	1.3	Added and updated content

TeamViewer: The Company and Software

About TeamViewer

TeamViewer is a leading global technology company that provides a connectivity platform to remotely access, control, manage, monitor, and repair devices of any kind – from laptops and mobile phones to industrial machines and robots. Although TeamViewer is free of charge for private use, it has around 630,000 subscribers and enables companies of all sizes and from all industries to digitalize their business-critical processes through seamless connectivity. Against the backdrop of global megatrends like device proliferation, automation and new work, TeamViewer proactively shapes digital transformation and continuously innovates in the fields of Augmented Reality, Internet of Things and Artificial Intelligence.

Since the company's foundation in 2005, TeamViewer's software has been installed on more than 2.5 billion devices around the world. The company is headquartered in Goppingen, Germany, and employs more than 1,400 people globally.

Fundamentals of TeamViewer Security

Our customers provide spontaneous support over the internet, accessing unattended computers and devices (e.g. providing remote support for servers) and host online meetings. Depending on the configuration, TeamViewer can be used to remotely control the mouse and keyboard of another computer or device in real time, as though you were accessing it in person.

If an administrator logs in to a remote computer or device, that person will be granted administrator rights to that computer or device as well. 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 devices are safe. Your security is our highest priority: users only trust secure solutions and we're fully committed to providing secure solutions to sustain long-term business success.

Quality Management

Security management is inconceivable without an established quality management system. TeamViewer GmbH 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.

Information Security and Compliance

TeamViewer deploys industry leading cyber security resources both internally and externally. Absolutely no expenses are spared as 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 any threat.

TeamViewer annually conducts external audits against various compliance frameworks, such as ISO 27001, HIPPA Hi-Tech, SOC2 Type2/SOC3, CSA STAR level 2, TISAX, and ISO 9001. Additional information can be found in our Compliance Portal at https://compliance.teamviewer.com/

Data Centers and Backbone

To provide the best possible security and availability of TeamViewer services, all TeamViewer servers are located in data centers which are compliant with ISO 27001, leveraging multi-redundant carrier connections and redundant power supplies. Furthermore, only industry-grade hardware is used and all servers that store sensitive data are located in Germany or Austria.

Being ISO 27001-certified means that personal access control, video camera surveillance, motion detectors, 24/7 monitoring, and on-site security personnel ensure access to the data center is only granted to authorized persons, guaranteeing the best possible hardware and data security. There is also a detailed identification check at the single point-of-entry of the data centers. Additionally, TeamViewer's Information Security Management System (ISMS) itself is ISO 27001 certified.

References

Leading global enterprises across industries — such as financial services, healthcare, government, and other sectors with highly sensitive data — leverage TeamViewer for secure remote access and support, customer engagement, IoT, and industrial augmented reality solutions.

To see how your peers have used TeamViewer in their organizations, explore our customer success stories, which are available on our website at teamviewer.com/customers.

Security Posture

TeamViewer works to create a smarter working world through leading edge remote connectivity. These users provide spontaneous support over the internet, accessing unattended computers (e.g., providing remote support for servers) and host online meetings. Depending on the configuration, TeamViewer can be used to remotely control the mouse and keyboard of another computer or other devices in real time, as though you were accessing it in person. 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're fully committed to providing secure solutions to sustain long-term business success. We work diligently to ensure our solutions are the most secure on the market and are in alignment with the latest security and data privacy standards.

Security Basics

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

- Our Golden Security Rules: https://community.teamviewer.com/English/kb/articles/108694-golden-security-rules
- Properly configure Unattended Access: https://community.teamviewer.com/English/kb/articles/108689-set-up-unattended-access
- TeamViewer Security Handbook at https://community.teamviewer.com/English/kb/security-handbook
- Tensor Hardening Guide: https://teamviewer.scene7.com/is/content/teamviewergmbh/teamviewer/central-image-hub/pdf/en/teamviewer-security-technical-overview-en.pdf
- For further information, please refer to the TeamViewer Trust Center at : https://www.teamviewer.com/en/trust-center/

Product and Services Overview

Components

Clients

TeamViewer Remote and TeamViewer Tensor Clients

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

TeamViewer Web Client

TeamViewer has worked to provide a modern and web first approach to our solution. Our web client uses HTML5 to provide a secure remote access platform on the web without the need to download a native application. This works to combine the functionality of both the former classic desktop client and the Management Console into a unified view that simplifies the usability of the product into a single view for the technicians. This can also be useful for organizations that are working with immutable systems where installed/portable software is prohibitive.

Management Console

The TeamViewer (Classic) Management Console is a web-based platform for user management, connection reporting, and managing Computers and Devices.

It is hosted in ISO 27001-certified, HIPAA compliant data centers. All data transfers are using TLS (Transport Layer Security) encryption, the standard for secure Internet network connections. Sensitive data is stored AES 256-bit encrypted. It uses the same encryption and authentication mechanisms as those described for TeamViewer accounts.

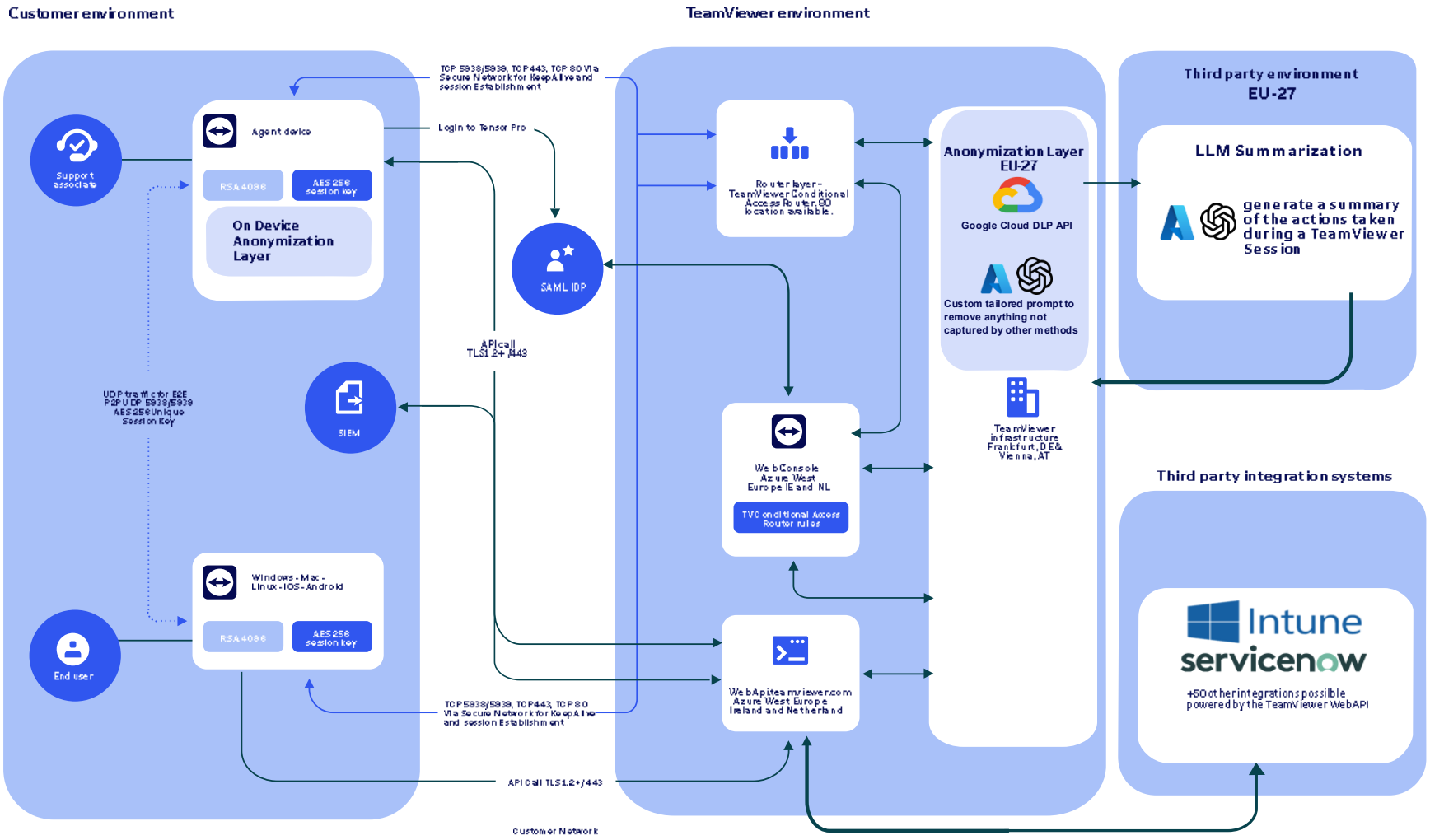
Teamviewer Intelligence Suite

Our products offer several features which are utilizing AI capabilities (e.g., TeamViewer Intelligence with Session Insights and CoPilot). These features are disabled by default, are opt in, and very clear on what data goes where and has specific terms of use, so that you the customer are able to make an informed decision about the functionality and the data.

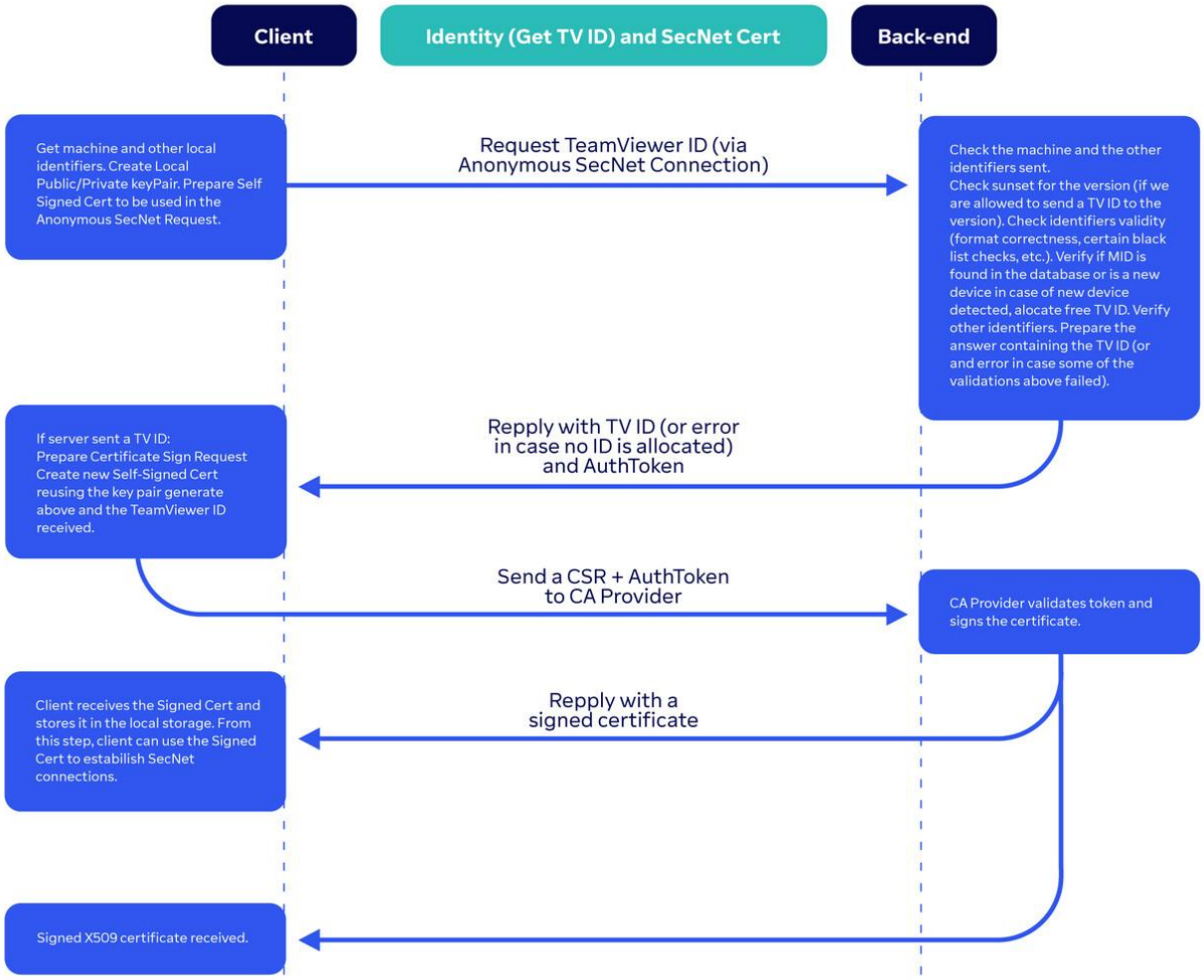
TeamViewer has added AI session insights, where we are able to generate a summary and transcription of your support sessions, this helps with knowledge capture and documentation of issues, that slow down agents and are a burden to helping people. These insights are able to be included in various integrations exposing the data into other systems of record further automating the backend boring work, while letting the human work through the actual problems. This data can also help to audit the sessions where event logging cannot fully capture the details of other actions on the system.

TeamViewer also has added in our remote management the ability to leverage AI to assist in script generation to help automate the boring and repetitive tasks that admins face.

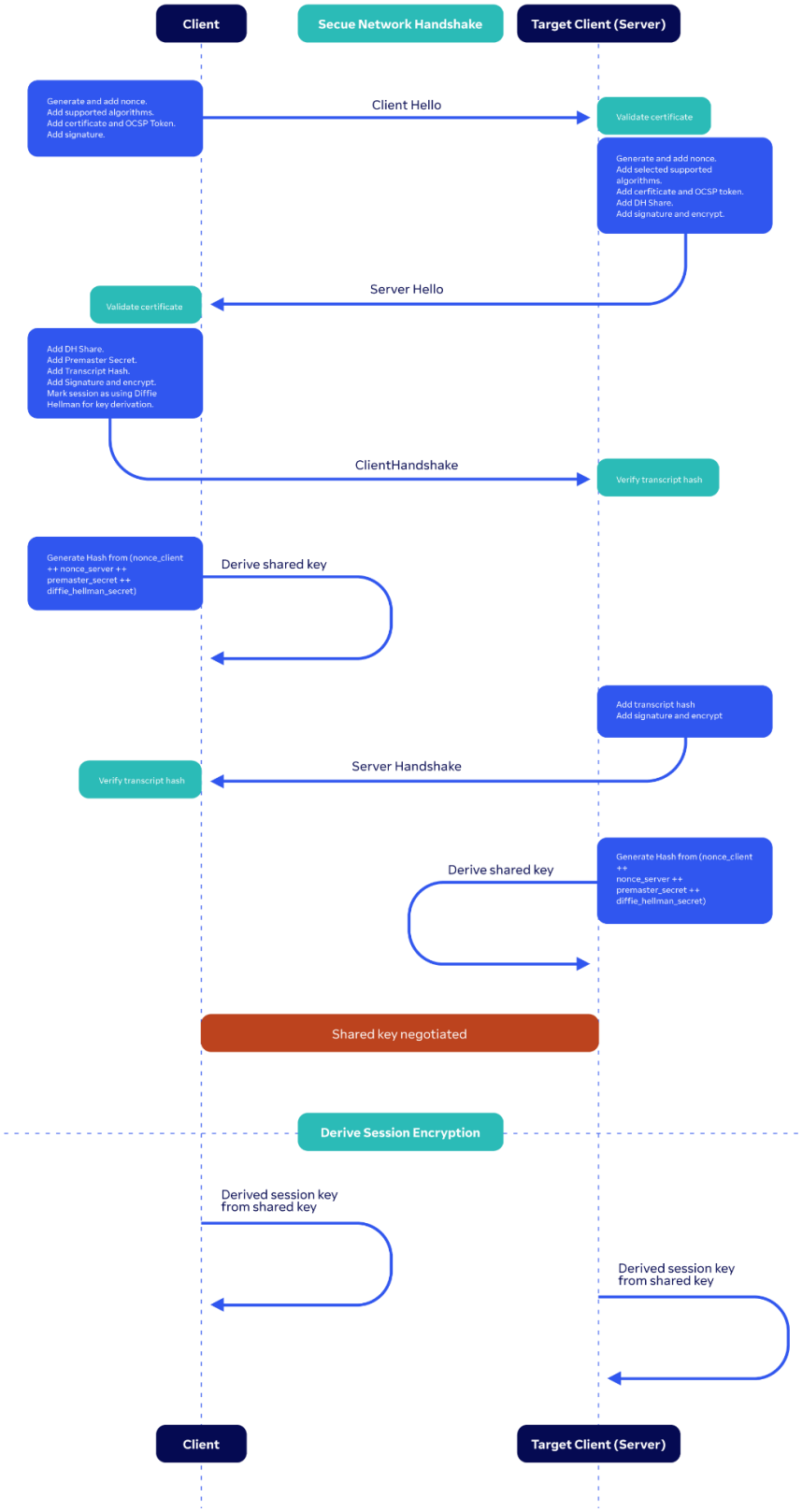
For more information, please see our knowledge base articles: https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-remote/remote-control/generate-session-summaries-with-session-insights/


Customer environment
TeamViewer environment
Third party environment
EU-27
TCP 5938/5939, TCP 443, TCP 80 Via Secure Network for KeepAlive and session Establishment
Login to Tensor Pro
Support associate
Agent device
RSA 4096
AES 256 session key
On Device Anonymization Layer
SAML IDP
Router layer - TeamViewer Conditional Access Router, 80 location available.
Anonymization Layer EU-27
Google Cloud DLP API
Custom tailored prompt to remove anything not captured by other methods
LLM Summarization
generate a summary of the actions taken during a TeamViewer Session
API call TLS1.2+ /443
UDP traffic for E2E P2P UDP 5938/5939 AES 256 Unique Session Key
SIEM
TeamViewer infrastructure Frankfurt, DE & Vienna, AT
Web Console Azure West Europe IE and NL
TVC onditional Access Router rules
Third party integration systems
Windows - Mac - Linux - IOS - Android
RSA 4096
AES 256 session key
End user
Web Api.teamviewer.com Azure West Europe Ireland and Netherland
Intune
servicenow
+50 other integrations possible powered by the TeamViewer WebAPI
TCP 5938/5939, TCP 443, TCP 80 Via Secure Network for KeepAlive and session Establishment
API call TLS1.2+/443
Customer Network

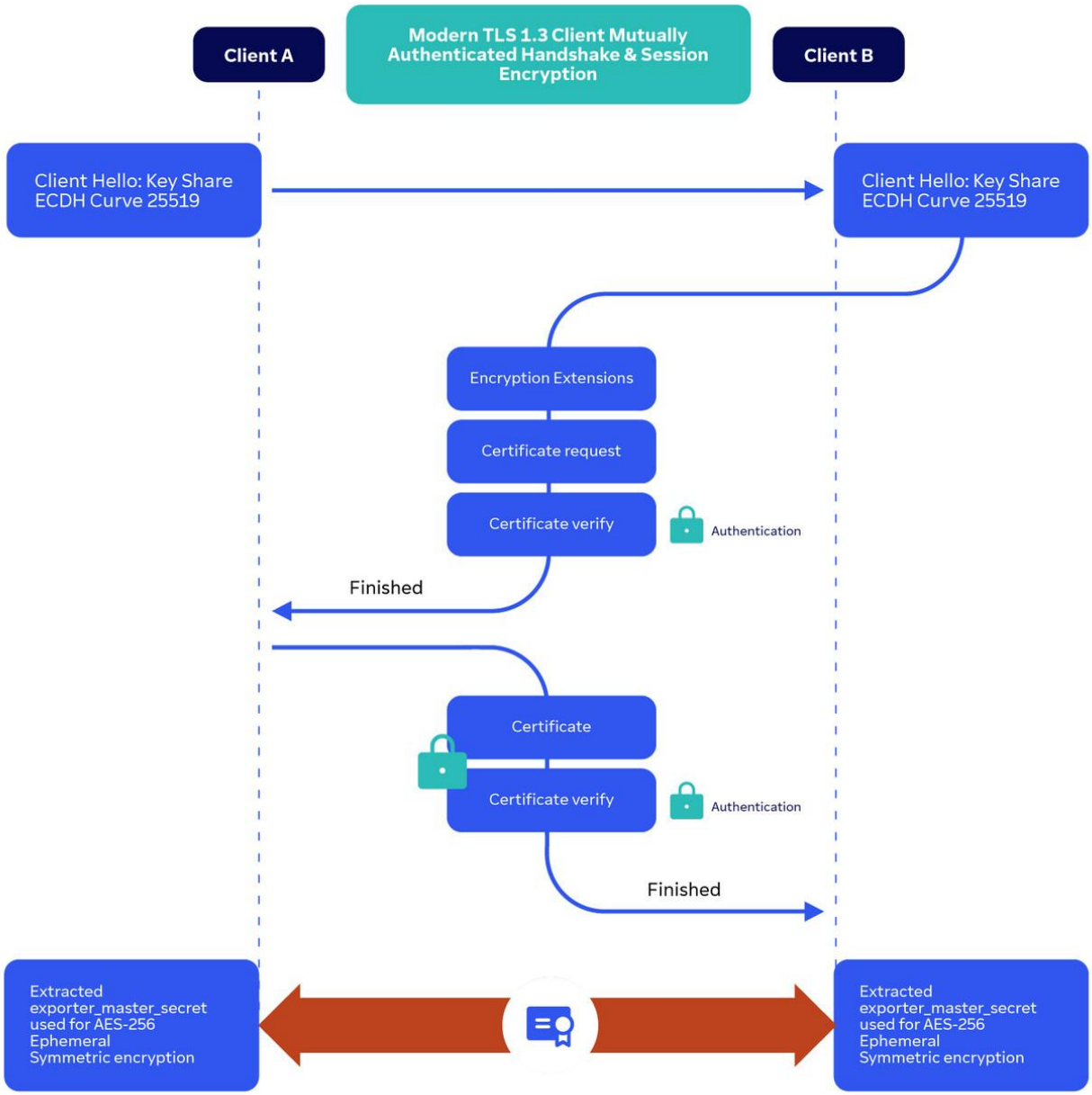
Session initialization diagram



Legacy Session Initialization Diagram (Secure Network Protocol) version <15.73 and other TeamViewer Backend Connections



Modern TLS1.3 Mutually Authenticated session Handshake Diagram (only for sessions as of today)>15.73



Security Features and Benefits

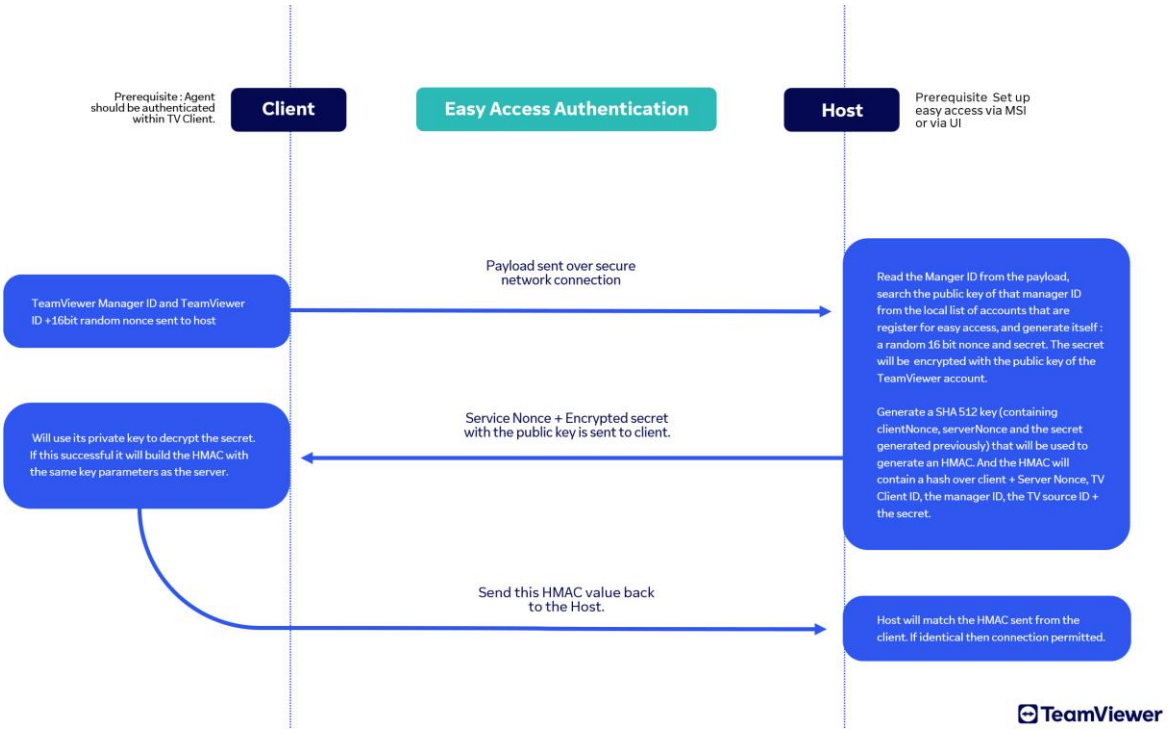
Main Use Cases

Secure Attended Access

To accomplish secure attended access, we leverage our feature called *Session Codes*, that uses public key cryptography to identify, authenticate and authorize users for accessing devices and combine it with the *Access Control* feature. With the 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 and the *Access Control* feature implements provides just in time approvals by the user on the device to secure attended support sessions.

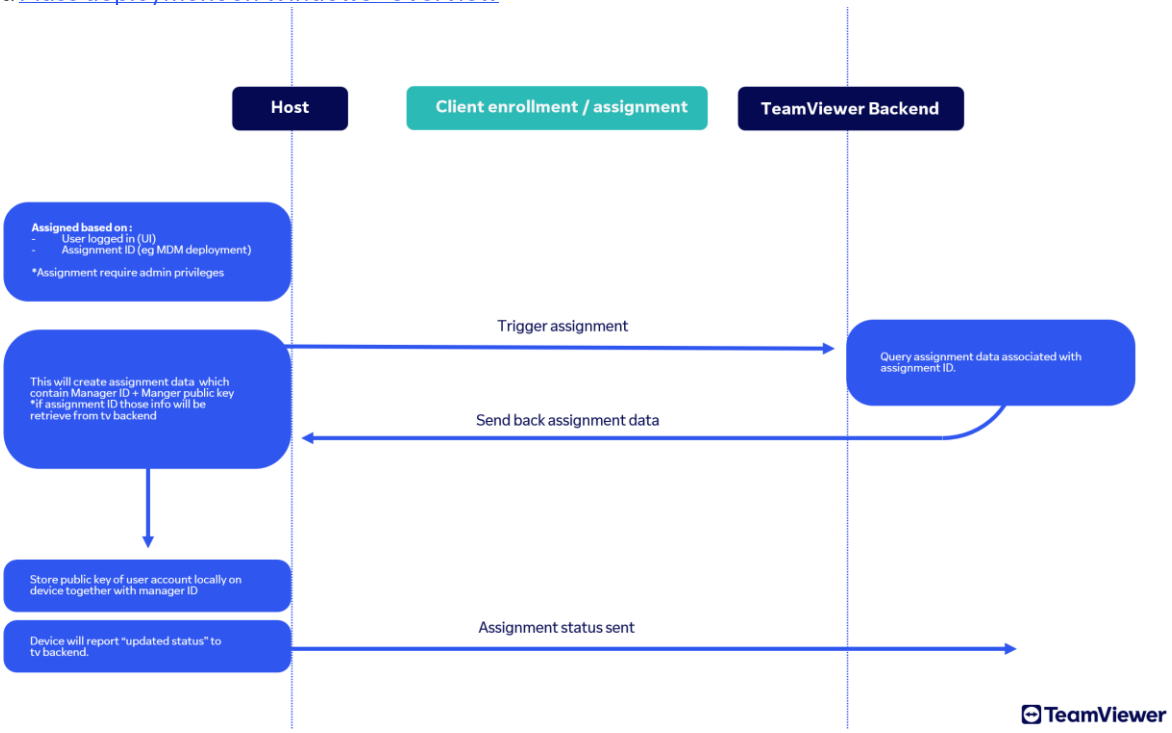
Secure Unattended Access

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 the *Easy Access* permission on a device, they will be able to connect to the device without a password but instead using strong public key cryptography. Using this connection method instead of the personal password for device connections, there is no risk of unauthorized access using exposed or stolen device passwords. Easy access is built on top of the already robust TeamViewer Account, commonly supported by SSO, and often in addition to our Conditional access for the access control we have a scalable, robust, authentication mechanism for unattended access. In addition, the features *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.



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 via MDM for efficiency and consistency. The process ensures that device assignments are authenticated, verified, and securely exchanged between the host and the TeamViewer backend, maintaining assignment integrity and alignment between local device data and backend records. TeamViewer has made progress in offering offline assignment, where we cache the assignment information until the device is able to come online to the TeamViewer network for deployments in unstable or disconnected environments helping to ensure your deployment completes more successfully on the first attempt. Further information for TeamViewer rollout: Mass deployment on Windows - Overview



Connection Authentication and Device Access Control

Block- and Allowlist

Especially when TeamViewer is used for unattended computer or device, maintenance and support (i.e., no connection partner is at the remote computer or device to accept incoming connection requests), Allowlist adds more security. Adding TeamViewer IDs or accounts to your Allowlist enables you to limit the number of people who can access specified machines to the explicit named IDs or accounts or company profiles. Moreover, even if a password is lost or compromised, unauthorized third parties still won't be able to access the device. The restrictions can either be made to allow only specific TeamViewer IDs or TeamViewer accounts or whole TeamViewer company profiles to access the devices remotely. Allowlist can be managed using the Policies described in the "Management Console" section.

The Blocklist lets you prevent certain partners or devices from establishing a connection to your computer or device. TeamViewer accounts or TeamViewer IDs on the Blocklists **can't connect** to your computer or device, but anyone else who is able to authenticate via password or other methods would be granted access to the device. Usually, an Allowlist is what you would be looking for in the majority of use-cases.

Note: *You will still be able to set up outgoing TeamViewer sessions with partners on the Blocklist.*
For more information, please refer to our knowledge base article at Block and allowlist

Two-Factor Authentication for Connections (TFA/MFA)

TeamViewer also supports Two-Factor Authentication for Connections (as well as for the account itself) using push notifications for approvals. When enabled, connections to a computer or device need to be approved using a push notification sent to specific mobile devices. Features can be enhanced and scaled with Conditional Access. Indeed, the rules can be enforced to multiple destinations. Finally, with Conditional access, the connection approval is made on account level rather than device level. For more information, please refer to our knowledge base article at https://community.teamviewer.com/English/kb/articles/110225-two-factor-authentication-for-connections

Access Control for Incoming and Outgoing Connections

You can individually configure the connection modes of TeamViewer. For instance, you can configure your remote support or meeting computer or device, so no incoming connections are possible, limiting file transfer, controlling screen recording. Limiting functionality to those features actually needed also means reducing systems exposure.

Conditional Access

TeamViewer Tensor has addon functionality for more granular controls over connections and connection routing with a dedicated connection router. For more information, please refer to our knowledge base article at https://community.teamviewer.com/English/kb/articles/108699-conditional-access

Bring your Own Certificate (BYOC) for connection authentication

TeamViewer Tensor has enabled "bring your own certificate" (BYOC) capabilities for our customers who would like to use their own certificates for managing connections with a greater level of granularity. The BYOC feature enables TeamViewer users to use their own certificates to authenticate the devices involved in a TeamViewer connection. This is independent of and always in addition to the authentication of the TeamViewer certificates. TeamViewer installations can be configured to require custom certificate authentication for incoming connection, outgoing connections, or both. When custom certificate authentication is required, the connection can only succeed if the other side has a private key for a certificate signed by the configured certification authority. This is an effective way to restrict TeamViewer connections to a specific set of devices. For more information, please refer to our knowledge base article at Bring your own certificate

- TeamViewer Tensor has introduced a functionality to allow enterprise customers to import their own certificate for use in the product in parallel to the TeamViewer managed certificates.
- Customers can import their certificates via the Windows trust store or using certificate files. Once this step is done only connections are possible where the customer certificate is present. This can also be managed to restrict all, restrict only incoming or restrict only outgoing.
- Using BYOC requires a single certificate authority (CA) to sign the certificates of all devices that need to authenticate themselves. All devices that require certificate authentication from other devices must have access to the CA certificate. All devices that want to authenticate themselves to other devices must have access to a certificate signed by the CA, the matching private key, and all intermediate certificates (if any).
- There is also a set of Certificate Revocation Lists (CRL's) that are supported by the BYOC feature. However, there may be some performance penalties as depending on the CRL configuration it may take longer to verify if the certs are still valid.
- TeamViewer supports X.509, PEM, and other certificate formats supported by OpenSSL, except for muti-cert files like PFX. Certificates and their private keys can be imported either from files or from the Windows certificate trust store.

Random Password for Connections

For spontaneous customer support, TeamViewer and TeamViewer QuickSupport generate a random password that can be changed at any time. If your connection partners or support requesters share their password with you, you can connect to their computers by entering their ID and password. Depending on the settings, TeamViewer generates a new password after it restarts, after the session (recommended and the new default setting), or when manually requested. TeamViewer QuickSupport should be configured to always generate a new password when it's launched or when users request it.

When using TeamViewer for unattended remote support (e.g. accessing and maintaining servers), we strongly recommend the following:

- Set up Easy Access for password-less access to provide secure unattended support: https://community.teamviewer.com/English/kb/articles/108689-set-up-unattended-access
- Restrict access to the device: https://community.teamviewer.com/English/kb/articles/108687-restrict-access
- Combined with two-factor authentication, using these security features will help ensure only authorized people can access specified devices.
- See also the sections about "Secure Unattended Access" and "Secure Attended Access" above.

Account Authentication

Single Sign-On (SSO)

TeamViewer Tensor offers support for Single Sign-On (SSO) using the SAML 2.0 protocol. The supported Identity Providers (IDP) include Entra ID, Okta, Centrify, G-suite, and OneLogin. As of this year we added support for organizations to lockout the creation of manual account creation for given SSO domains, this increases the security of the given domains, to push users into the established procurement procedures of their company For more information, please refer to our knowledge base article at https://community.teamviewer.com/English/kb/articles/108708-single-sign-on

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

TeamViewer supports Two-Factor Authentication (also called MFA – Multi Factor Authentication) using time-based one-time codes (TOTP) codes to secure access to their TeamViewer accounts. We strongly recommend enabling this feature for all TeamViewer accounts. In addition to both username and password, the user must enter a code in order to authenticate. This code is only valid for a short period of time, generated via the time-based one-time password (TOTP) algorithm. Through two-factor authentication and limiting access by means of adding devices to the Allowlist, TeamViewer assists you to meet the certifications requirements for standards such as HIPAA and PCI certification requirements. For more information, please refer to our knowledge base article at Two-factor authentication for your account

Trusted Devices

If you do not set up two-factor authentication, Trusted Devices is configured by default for your account. As a preventive measure to ensure your account's security, you must manually authorize new devices or browsers when signing in to access your TeamViewer account from them for the first time. As part of the authorization process, an email is sent to your email address associated with your TeamViewer account. Without adding a device, browser, or IP to your Trusted Devices, you can t log in. This protects your account from others trying to log in as they would need access to your email inbox as well to authorize the login.

Learn more about Trusted Devices and Managing Trusted Devices in the TeamViewer Knowledge Base:

1. Trusted Devices: Trusted Devices
2. Trust Management for Trusted Devices: Trust Management for Trusted Devices
3. Trusted Devices push notifications Trust devices via push notification

Additional Security Features

Security Center

We have identified that customers want to ensure their configuration is secure, but are not able to quickly and efficiently able to. To help customers meet their compliance and regulatory requirements, we have provided simple and easy to implement checks that allow admins to quickly ensure they are in line with recommended best practices for remote access solutions. We are constantly evaluating new criteria to provide further insights to provide even further visibility and simple resolutions to make a quick and efficient impact on the customers remote access security configurations.

Device Policy

TeamViewer offers a multitude of policies for managed devices that cover block and allow listing, access control, updates, for example allowing complete control of the deployed agents in their environments. For more information, please refer to our knowledge base article at Policies

Black Screen / Privacy Screen

TeamViewer offers for all licensed customers a privacy screen when working on remote systems to cover use cases such as restricting administrative tasks from standard users, or system snooping for systems that are being used for remote work. For more information, please refer to our knowledge base article at TeamViewer Black Screen

Auditability: Event Logging

TeamViewer Tensor has additional event logging that can be enabled further granularity and the ability to export this information programmatically through our Event log API. For more information, please refer to our knowledge base article at https://community.teamviewer.com/English/kb/articles/108707-auditability

SCIM System for Cross Domain Identity Management provisioning

TeamViewer has enabled SCIM API to enable syncing of users and user groups from cloud providers such as Entra ID and Okta. For more information, please see the relevant links to the knowledge base article. For more information, please refer to our knowledge base article at Microsoft Entra ID Integration - SCIM Configuration

Mobile SDK

TeamViewer offers an addon solution for customers that need to support their own mobile apps they have deployed with greater control over the screen data and workflows, that help overcome some objections to yet another app for supporting customers by embedding the TeamViewer functionality into their own mobile application. For more information, please refer to our knowledge base article at TeamViewer Mobile Software Development Kit (SDK)

Security Key Redirection

TeamViewer Tensor in helping support organizations on their journey to password-less authentication to allow local hardware tokens, PIV/FIDO to be present on remote systems to facilitate authentication. For more information, please refer to our knowledge base article at Security key redirection

LDAPS (Local Domain Admin Password Solution) integration

With TeamViewer Tensor we sought to integrate with the Microsoft LAPS solution as means to help support our customers in more easily leveraging their management secrets while servicing the devices . LAPS integration helps IT admins securely retrieve and inject local admin credentials during remote support sessions. This integration ensures elevated access without compromising security or exposing passwords. It works by connecting TeamViewer to Microsoft Entra ID and Intune, allowing password injection and optional rotation directly from within a TeamViewer session.

Security-related information

- Passwords are injected securely as keystrokes and never pass through the TeamViewer backend.
- The integration uses **PKCE** for secure token exchange.
- All password requests are made from a supporters device to your Intune tenant. Passwords are never transferred through TeamViewer's cloud infrastructure.

Chat

Chat messages and their history are end-to-end encrypted, stored in the TeamViewer account using RSA/AES as described in the "TeamViewer Account" section. Only participants in a chatroom or 1:1 chat can access the messages and history.

Data Handling and Encryption

Account Data Protection

TeamViewer accounts are hosted on dedicated TeamViewer servers. For information on access control, please refer to the "Data Center and Backbone" section. For authentication, the Secure Remote Password protocol (SRP) version 6 is used. This protocol combines the advantages of conventional ways of password storage. We do not store any information on our servers that could be used by an unauthorized third party to authenticate as the given account. Additionally, passwords are never stored on our servers during authentication. Rather, TeamViewer uses a unique verification process, valid for a single authentication run only, which can't be reused again.

Data stored in the account — such as passwords, keys, and chat logs — are encrypted using a combination of RSA and AES, where the root key for the encryption is derived from the user's password. This ensures that anyone without password can't access the data stored in the account. Accounts are encrypted using a combination of RSA and AES, where the root key for the encryption is derived from the user's password. This ensures that anyone without password can't access the data stored in the account.

There are two types of stored account data:

- Type 1 is accessible by TeamViewer for Data Processing purposes (email address, display name/username, status etc.). TeamViewer needs to have access to this basic data to fulfill our service. In addition, certain parts of this data are used for product improvement or bug detection. This data is pseudonymized. See C.5 product improvement of the Data Processing Agreement (DPA). Last but not least: TeamViewer processes this data for marketing (in product marketing) purposes. Users can easily opt-out of in-product marketing messages from version 15.8. Further information can be found at In-product marketing messages

- Type 2 is not accessible by TeamViewer since it is considered sensitive customer data (passwords, chat, authentication keys, assignments, API Token etc.)

Encryption

TeamViewer protects all 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. This approach provides a level of protection comparable to widely deployed HTTPS/TLS implementations and is considered secure by current cryptographic standards.

Starting with TeamViewer version 15.73 and later, session authentication and attestation leverage mutually authenticated TLS 1.3, which introduces Perfect Forward Secrecy (PFS) through modern Diffie-Hellman key exchange mechanisms. After the secure handshake, session data continues to be protected using AES-256-GCM encryption.

During the connection establishment, both 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 any sensitive data.

Importantly, private keys never leave the client device, ensuring that neither TeamViewer routing servers nor any intermediary systems can decrypt the end-to-end encrypted session traffic.

Remote session traffic between endpoints is protected using end-to-end encryption, ensuring that only the communicating devices can decrypt the transmitted date

While the TLS 1.3 handshake is now used for session authentication and attestation, some communication with TeamViewer backend services continues to rely on our proprietary protocol as part of an ongoing modernization effort.

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

Development Process

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 which also includes a hardened and audited software development pipeline. Most importantly we perform design, architecture and implementation reviews including attack surface analysis and threat modeling where identified risks are being prioritized and product security requirements are derived from. We also enforce code reviews, unit and integration tests and all code changes require code owners' approval. More information on our S-SDLC can be found at https://www.teamviewer.com/en/safety-first-last-and-always-the-seven-key-stages-of-secure-software-development/

Security Testing and Composition Analysis (SCA)

TeamViewer leverages industry leading tooling to perform software composition analysis, vulnerability management and dependency management of both opensource as well as third-party components. We perform static and dynamic application security testing (SAST/DAST) as part of our software development process and security reviews. There is also a significant and well segmented automation environment that is used to ensure our quality assurance can also be handled programmatically and in an automated fashion.

Penetration Testing

Both TeamViewer infrastructure and the TeamViewer software are subject to penetration testing. TeamViewer conducts multiple external white and black/grey box tests of all products annually. The tests are performed by independent companies, specialized in security testing. TeamViewer has partnered with multiple class leading testing firms, such as Blaze, Recurity, Securitum, YesWeHack,and XMCO.

Code Signing

All our software is signed via DigiCert Code Signing. Consequently, the publisher of the software is always readily identifiable. If the software has been changed afterward, the digital signature automatically becomes invalid. Code Signing allows for endpoint security tools to actively validate if the software is genuine and our software uses this as a self-check mechanism to validate only genuine copies can run, if this check fails the software will exit. This allows for programmatic protection and alerting for our customers. Build in anti-tampering, the software itself does have the ability to self-check on start the certificate and signature validity of all its components and it fails to run if inconsistencies are found.

Software Bill of Materials (SBOM)

TeamViewer maintains Software Bill of Materials (SBOM) information for its client software components as part of its 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 (NDA).
The SBOM includes information about third-party and open-source components used in the software, including relevant information. SBOMs are generated as part of the secure software development lifecycle (SSDLC) and are maintained through automated build processes within our CI/CD and DevSecOps activities.
SBOMs are updated in alignment with product release cycles, ensuring that the information reflects the components included in each software update.
To support customer tooling and vulnerability management processes, SBOMs can be provided in commonly used industry formats such as SPDX or CycloneDX, depending on the customer's preferred format.
At this time, SBOM availability is limited to TeamViewer client software. SBOMs for the TeamViewer SaaS platform and backend services are currently not provided.
Direct integration of SBOM data into customer systems or automated distribution mechanisms is not currently supported

Product Security Incident Response Team (PSIRT)

TeamViewer works diligently to identify and mitigate security vulnerabilities in our products. Our Product Security Incident Response Team (PSIRT) follows the Forum of Incident Response and Security Teams (FIRST) PSIRT Services Framework and Maturity Model and a continuous review ensures our processes are well defined and established. TeamViewer is a member of the Forum of Incident Response and Security Teams (FIRST) member and our Computer Security Incident Response Team (CSIRT) and our Product Security Incident Response (PSIRT) can be contacted via the published contact methods at https://www.first.org/members/teams/teamviewer_sirt and https://www.teamviewer.com/.well-known/security.txt



A high-level overview of our Product Security Incident Response adoption.

Vulnerability Disclosure Program (VDP)

Every customer, user, researcher, partner and any other person that interacts with TeamViewer's products and services is encouraged to report identified vulnerabilities and errors they identify in our products and services. These help us support responsible disclosure for products and services that are outside of the scope of the bug bounty program and to make our products safer for everyone Issues can be reported at https://vdp.teamviewer.com/ and https://teamviewer.com/.well-known/security.txt

Bug Bounty Program

TeamViewer has multiple public and private bug bounty programs to engage with a large community of security researchers and recognize them for their responsible disclose of findings to TeamViewer. TeamViewer currently has 4 programs in active hunting with one open to public enrollment. Since founding our BBP, TeamViewer ahs awarded 134,450€ in bounties. In 2025 TeamViewer awarded 49,060€ in bounties. Our average bounty reward is 695€. Our largest bounty paid was 4500€. Lastly our program has an average response time of 18 hours. The Bug Bounty program can be found at https://www.teamviewer.com/en/special/bug-bounty-program/

Security Bulletins

TeamViewer publishes security bulletins which include details about the nature of the vulnerabilities which have been addressed, their severity, versions which are affected, the versions where the issue has been solved and potential mitigations and workarounds for cases where updates cannot be easily applied. TeamViewer follows industry standard remediation timelines internally based on CVSS severity scoring to ensure timely resolution of security issues. The security bulletins can be found at https://www.teamviewer.com/en/trust-center/security-bulletins/

Each issue is categorized by severity:

- **Critical**: Major risk (e.g., remote code execution). Immediate update required.
- **Important**: Significant threat (e.g., easy privilege escalation). Prompt update advised.
- **Moderate**: Limited impact under specific conditions. Update when possible.
- **Low**: Minor or hard-to-exploit issues. Update in the next regular cycle.

Follow our recommendations to ensure your security posture stays strong. For these bulletins TeamViewer is leveraging the CVSS 3.0 scale as of today, we are also evaluating CVSS 4.0 but we are wanting to keep the ratings on the same standard for all published bulletins.

NOTICE: Due to our compliance in accordance with GDPR we are unable to automatically enroll you in such email-based notifications. Customers must self-register for emails here and are able to select the relevant services they wish to be notified about.

Certified Numbering Authority (CNA)

TeamViewer is a CNA for Common Vulnerabilities and Exposures (CVE) issuances against all TeamViewer products. This is a key measure of accurate risk assessment of all CVE's that may be issued against TeamViewer products. TeamViewer works diligently to partner with researchers and organizations to correctly report and disclose issues as a CNA. TeamViewer demonstrates mature vendor vulnerability management practices, and this highlights our commitment to cybersecurity to all our customers.

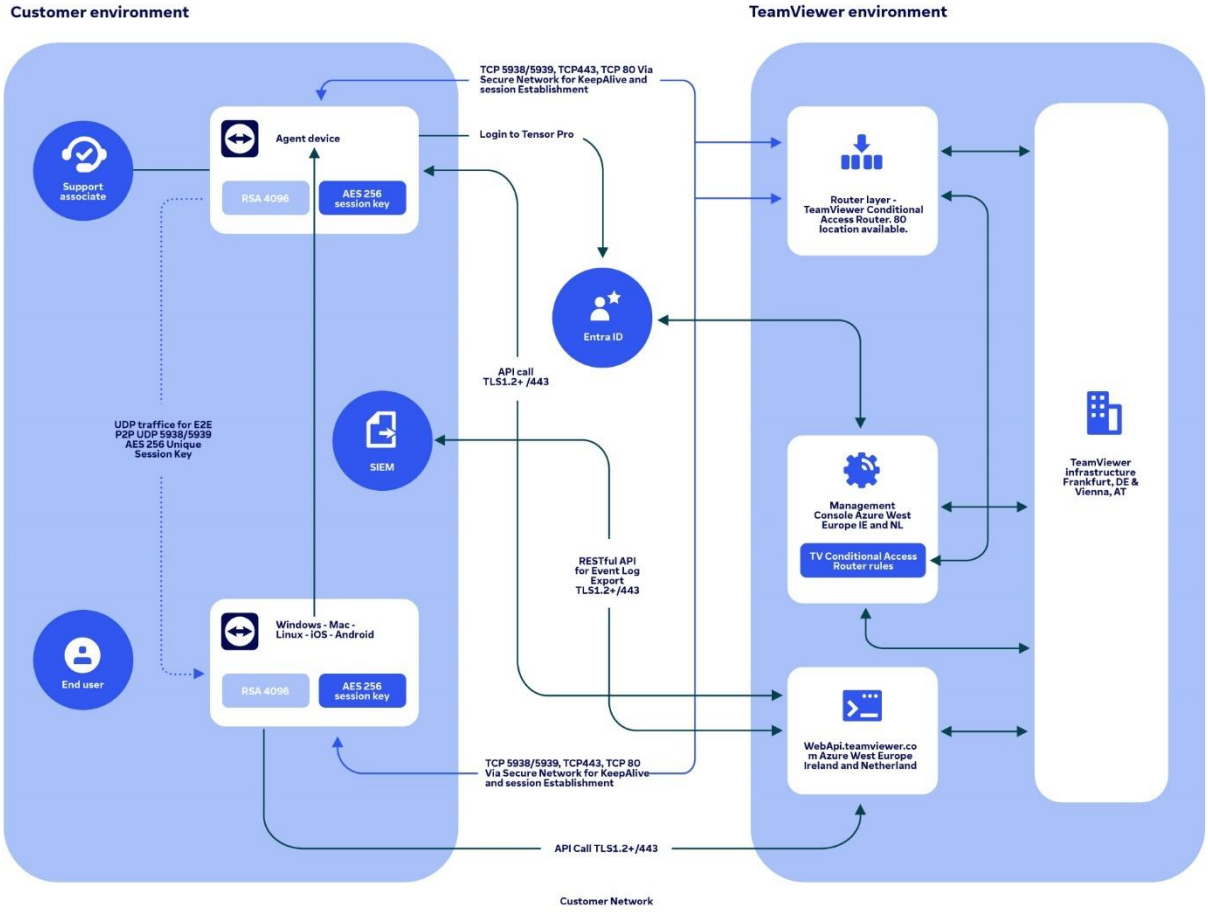
Internal Vulnerability management timeframes

TeamViewer has an internal vulnerability management program and in alignment with our CNA status and our VDP/BBP programs we maintain the internal guidelines for remediation timeframes in accordance with industry best practices.

Severity	Company / Product SLA
Critical – exploited (KEV/CRA)	Immediate (hotfix)
Critical – not yet exploited	≤ 14 days
High	≤ 14 days
Medium	≤ 3 months
Low	≤ 9 months

NOTICE: These timelines are represented here as for information guidance for our customers on our internal processes. These are not subject to any binding terms and conditions as this document is considered non-binding. Furthermore, these timelines are not subject to any customer SLA terms and conditions. For the protection of our customers, TeamViewer doesn't disclose or discuss security issues until our investigation is complete and any necessary updates are generally available

Hosting and Infrastructure



The TeamViewer production environment is a purely cloud-based infrastructure hosted in data centers provided by third parties. TeamViewer has access control measures in place to prevent unauthorized access to data processing equipment where personal data is stored or processed. To provide the best possible security and availability of TeamViewer services, all TeamViewer servers are located in data centers that are compliant with ISO 27001, leveraging multi-redundant carrier connections and redundant power supplies. Furthermore, only industry-grade hardware is used and all servers that store sensitive data are in EU zone. (Germany, Netherlands and Austria). Being ISO 27001-certified means that personal access control, video camera surveillance, motion detectors, 24/7 monitoring, and on-site security personnel ensure access to the data center is only granted to authorized persons, guaranteeing the best possible hardware and data security. There is also a detailed identification check at the single point-of-entry of the data centers. For more details about the IAAS providers we leverage as a part of the service please see our sub processor list as annex 3 of our DPA.

Definitions

Secure Remote Password Protocol is a secure password-based authentication and key-exchange protocol. It solves the problem of authenticating clients to servers securely, in cases where the user of the client software must memorize a small secret (like a password) and carries no other secret information, and where the server carries a *verifier* for each user, which allows it to authenticate the client but which, if compromised, would not allow the attacker to impersonate the client. In addition, SRP exchanges a cryptographically strong secret as a byproduct of successful authentication, which enables the two parties to communicate securely.

RSA - *Rivest, R.; Shamir, A.; Adleman, L.* is a public-key cryptosystem, one of the oldest, that is widely used for secure data transmission. The acronym "RSA" comes from the surnames of Ron Rivest, Adi Shamir and Leonard Adleman, who publicly described the algorithm in 1977.

AES - The block cipher AES (Advanced Encryption Standard) is a worldwide standard and one of the most popular cryptographic primitives. Designed in 1997

SSO - Web application single sign-on (SSO) solutions leverage the Secure Assertion Markup Language (SAML) to securely authenticate user access to cloud-based apps. As web applications emerged in the early 2000s, they were difficult to manage directly with traditional LDAP-based infrastructure or Microsoft Active Directory.

SAML 2.0 - The Security Assertion Markup Language (SAML) defines the syntax and processing semantics of assertions made about a subject by a system entity. In the course of making, or relying upon such assertions, SAML system entities may use other protocols to communicate either regarding an assertion itself, or the subject of an assertion. This specification defines both the structure of SAML assertions, and an associated set of protocols, in addition to the processing rules involved in managing a SAML system.

Zero knowledge account recovery - The Zero Knowledge Account Recovery acts as another layer of security for this process as the reset process requires you to enter the unique 64 characters Zero Knowledge Account Recovery Code for your account to prove your identity. Important to note is that this happens without any intervention and knowledge of the TeamViewer infrastructure.

HTTPS - Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP, the protocol over which data is sent between your browser and the website that you are connected to. The 'S' at the end of HTTPS stands for 'Secure'. It means all communications between your browser and the website are encrypted. HTTPS is often used to protect highly confidential online transactions like online banking and online shopping order forms.

TLS1.2 - TLS, a.k.a., SSL (Secure Sockets Layer), establishes a private end- to-end connection, optionally including strong mutual authentication, using a variety of cryptosystems. Initially, a handshake phase uses three subprotocols to set up a record layer, authenticate endpoints, set parameters, as well as report errors.

TLS 1.3 TLS allows client/server applications to communicate over the Internet in a way that is designed to prevent eavesdropping, tampering, and message forgery.

Perfect Forward Secrecy (PFS) - is a feature of specific key-agreement protocols that gives assurances that session keys will not be compromised even if long-term secrets used in the session key exchange are compromised

Windows Registry - is a hierarchical database that stores low-level settings for the Microsoft Windows operating system and for applications that opt to use the registry.

MAC address - is a unique identifier assigned to a network interface controller for use as a network address in communications within a network segment.

Ephemeral keys - A cryptographic key that is generated for each execution of a key-establishment process and that meets other requirements of the key type (e.g., unique to each message or session).

Certificate Authority (CA) - In cryptography, a certificate authority or certification authority is an entity that stores, signs, and issues digital certificates.

Windows Trust Store - A trust store is a collection of root certificates that are trusted by default and are maintained by the companies that make operating systems and web browsers, such as Apple, Microsoft, Mozilla, and Google.

Certificate Revocation Lists (CRL's) - a list of digital certificates that have been revoked by the issuing certificate authority (CA) before their scheduled expiration date and should no longer be trusted.

X.509 - In cryptography, X.509 is an International Telecommunication Union (ITU) standard defining the format of public key certificates.

Privacy-Enhanced Mail (**PEM**) - is a de facto file format for storing and sending cryptographic keys, certificates, and other data, based on a set of 1993 IETF standards defining "privacy-enhanced mail."

OpenSSL - is a software library for applications that provide secure communications over computer networks against eavesdropping, and identify the party at the other end.

PFX - In cryptography, **PKCS #12** defines an archive file format for storing many cryptography objects as a single file. It is commonly used to bundle a private key with its X.509 certificate or to bundle all the members of a chain of trust. The filename extension for PKCS #12 files is `.p12` or `.pfx`.

Cipher - a cipher (or cypher) is an algorithm for performing encryption or decryption—a series of well-defined steps that can be followed as a procedure.

Secure Hash Algorithm (SHA) - also known as SHA, are a family of cryptographic functions designed to keep data secured. It works by transforming the data using a hash function: an algorithm that consists of bitwise operations, modular additions, and compression functions. The hash function then produces a fixed-size string that looks nothing like the original. These algorithms are designed to be one-way functions, meaning that once they're transformed into their respective hash values, it's virtually impossible to transform them back into the original data. A few algorithms of interest are SHA-1, SHA-2, and SHA-3, each of which was successively designed with increasingly stronger encryption in response to hacker attacks. SHA-0, for instance, is now obsolete due to the widely exposed vulnerabilities.

HTML5 - (Hypertext Markup Language 5) is a markup language used for structuring and presenting content on the World Wide Web. It is the fifth and final major HTML version that is a World Wide Web Consortium (W3C) recommendation.

GDPR - General Data Protection Regulation (Regulation (EU) 2016/679, abbreviated GDPR) is a European Union regulation on information privacy in the European Union (EU) and the European Economic Area (EEA). The GDPR is an important component of EU privacy law and human rights law, in particular Article 8(1) of the Charter of Fundamental Rights of the European Union. It also governs the transfer of personal data outside the EU and EEA. The GDPR's goals are to enhance individuals' control and rights over their personal information and to simplify the regulations for international business.[1] It supersedes the Data Protection Directive 95/46/EC and, among other things, simplifies the terminology.

S-SDLC - A Secure SDLC requires adding security testing at each software development stage, from design, to development, to deployment and beyond. Examples include designing applications to ensure that your architecture will be secure, as well as including security risk factors as part of the initial planning phase.

SAST - **Static application security testing** (**SAST**) is used to secure software by reviewing the source code of the software to identify sources of vulnerabilities. Although the process of statically analyzing the source code has existed as long as computers have existed, the technique spread to security in the late 90s and the first public discussion of SQL injection in 1998 when Web applications integrated new technologies like JavaScript and Flash.

DAST - A dynamic application security testing (DAST) is a non-functional testing process where one can assess an application using certain techniques and the result of such testing process covers security weaknesses and vulnerabilities present in an application. This testing process can be carried out either in a manual way or by using automated tools. Manual assessment of an application involves more human intervention to identify the security flaws which might slip from an automated tool. Usually business logic errors, race condition checks, and certain zero-day vulnerabilities can only be identified using manual assessments.

SCA – Software Composition Analysis is the process of identifying and managing the open-source and third-party components used in software development. The goal of SCA is to identify potential security vulnerabilities, licensing issues, or outdated components in the software being developed or used.

VDP - A vulnerability disclosure program offers a secure channel for researchers to report security issues and vulnerabilities, and typically includes a framework for intake, triage, and workflows for remediation.

Bug Bounty Program - A bug bounty program is a deal offered by many websites, organizations, and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to security exploits and vulnerabilities.

ISO 27001:2022 - ISO/IEC 27001 is an international standard to manage information security. The standard was originally published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in 2005, revised in 2013, and again most recently in 2022. There are also numerous recognized national variants of the standard. It details requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) – the aim of which is to help organizations make the information assets they hold more secure. Organizations that meet the standard's requirements can choose to be certified by an accredited certification body following successful completion of an audit. The effectiveness of the ISO/IEC 27001 certification process and the overall standard has been addressed in a large-scale study conducted in 2020.

HIPPA Hi-Tech – A-LIGN ASSURANCE's examination of the controls of TeamViewer was limited to the HIPAA/HITECH requirements and related control activities specified by the management of TeamViewer and did not encompass all aspects of TeamViewer's operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105, AT-C 205 and AT-C 315

SOC2 Type2 - System and Organization Controls (SOC) for Service Organizations are internal control reports created by the American Institute of Certified Public Accountants (AICPA). They're intended to examine services provided by a service organization so that end users can assess and address the risk associated with an outsourced service.

SOC3 - System and Organization Controls (SOC) for Service Organizations are internal control reports created by the American Institute of Certified Public Accountants (AICPA). They're intended to examine services provided by a service organization so that end users can assess and address the risk associated with an outsourced service.

SOC 3 for Service Organizations: Trust Services Criteria for General Use Report is a short, publicly facing summary of the SOC 2 Type 2 attestation report for users who need assurances about service organization's controls but don't need a full SOC 2 report or aren't eligible under SOC 2 to receive one. Because SOC 3 reports are general use reports, they can be freely distributed.

TISAX - Trusted Information Security Assessment Exchange is an assessment and exchange mechanism for the information security of enterprises, developed by the ENX Association and published by the Verband der Automobilindustrie. TISAX concerns the secure processing of information from business partners, the protection of prototypes and data protection in accordance with the General Data Protection Regulation (GDPR) for potential business transactions between automobile manufacturers and their service providers or suppliers. The VDA established TISAX in 2017 together with the ENX Association.

ISO 9001 - ISO 9001 is based on the plan-do-check-act methodology and provides a process-oriented approach to documenting and reviewing the structure, responsibilities, and procedures required to achieve effective quality management in an organization.

PSIRT – (Product Security Incident Response Team) is an entity within an organization which, at its core, focuses on the identification, assessment and disposition of the risks associated with security vulnerabilities within the products, including offerings, solutions, components and/or services which an organization produces and/or sells.

CNA (Certified Naming Authority) - CNAs are vendor, researcher, open source, CERT, hosted service, and bug bounty provider organizations authorized by the CVE Program to assign CVE IDs to vulnerabilities and publish CVE Records within their own specific scopes of coverage.

IDP (identity provider) - An identity provider is a system entity that creates, maintains, and manages identity information for principals and provides authentication services to relying on applications within a federation or distributed network.

SCIM (System for Cross-domain Identity Management) - is a standard for automating the exchange of user identity information between identity domains, or IT systems.

API (Application Programming Interface) - is a way for two or more computer programs to communicate with each other. It is a type of software interface, offering a service to other pieces of software.

SDK (software Development Kit) - is a collection of software development tools in one installable package. They facilitate the creation of applications by having a compiler, debugger and sometimes a software framework.

PIV (Personal Identity Verification) - is intended to help you understand the purpose and uses of a PIV credential at your organization. This PIV 101 focuses on using PIV credentials for logical access such as authenticating to networks or applications or digitally signing and encrypting.

FIDO - FIDO protocols use standard public key cryptography techniques to provide stronger authentication. During registration with an online service, the user's client device creates a new key pair. It retains the private key and registers the public key with the online service. Authentication is done by the client device proving possession of the private key to the service by signing a challenge.