

TeamViewer Remote Management



TeamViewer Remote Management

Monitoring & Asset Management	
Remotely monitor, track and patch your endpoints with TeamViewer.	Device-based License (per endpoint device). Starting from 5 endpoint devices. Endpoint device is any internet-capable computing device (e.g., desktops, notebooks, tablets, smartphones; examples not exhaustive and subject to the operating system requirements) designated by Customer to use the Services, regardless if in the effective use or not. The number of endpoint devices is subject to order.
Remote Device Monitoring Proactive device monitoring (CPU, memory usage, online status, etc.)	✓
Network Device Monitoring Detect and monitor network devices such as routers, switches, scan for all connected devices on a network.	✓
Asset Management Track deployed hardware, installed software, and selected device information from one single location.	✓
Patch Management Eliminate vulnerabilities caused by outdated software by detecting and patching software that is no longer up to date.	✓
Remote Task Manager Remotely manage processes and services without establishing a remote session.	✓
Device Checks	✓
Policies Set up policies and monitor aspects such as CPU usage, memory usage, running processes, and perform maintenance on time.	✓
Instant Alerting	✓

Endpoint Protection (EPP)	
Protect your devices against malicious software (powered by Malwarebytes Endpoint Protection solution)	Device-based License (per endpoint device). Starting from 5 endpoint devices.
Security Policies	✓
Endpoint Scans	✓
Automatic Updates	✓
Endpoint Detection and Response (EDR)	
Identify malicious and suspicious threats, respond and remediate immediately (powered by Malwarebytes Endpoint Detection and Response solution)	Device-based License (per endpoint device). Starting from 5 endpoint devices.
Security Policies	✓
Endpoint Scans	✓
Automatic Updates	✓
Active Ransomware Protection Prevent untrusted applications from modifying files in your protected folders	✓
Managed Threat Hunting Identify threats and empower your threat response with 24x7x365 service for alert prioritization and step-by- step guided remediation.	✓
Managed Detection and Response Protect your organization with managed 24x7x365 threat monitoring, investigation, and remediation by Malwarebytes' expert MDR analysts.	✓
Backup	
Securely backup your files and folders to the cloud.	Capacity-based License (per frontend gigabytes). Starting from 50 GB.
Individual Backup Policies	✓
Backup Endpoints	✓
Flexible Data Retention	✓
Device Monitoring	
Remotely monitor your endpoints with TeamViewer.	Device-based License (per endpoint device). Starting from 5 endpoint devices.

Remote Device Monitoring Proactive device monitoring (CPU, memory usage, online status, etc.)	✓
Remote Task Manager Remotely manage processes and services without establishing a remote session.	✓
Device Checks	✓
Policies Set up policies and monitor aspects such as CPU usage, memory usage, running processes, and perform maintenance on time.	✓
Instant Alerting Instant alerting on monitored aspects.	✓
Task Automation Create condition-based rules, which respond to specific system events, and time-based rules, automating actions at set intervals.	✓
Remote Scripting Execute scripts on remote devices without initiating a TeamViewer remote session.	✓
Asset Management & Discovery	
Remotely track and patch your endpoints with TeamViewer	Device-based License (per endpoint device). Starting from 5 endpoint devices.
Asset Management Track deployed hardware, installed software, and selected device information from one single location.	✓
Asset Discovery Automatically scan the network to identify and report all connected assets, providing a comprehensive inventory of devices within the environment	✓
Patch Management Eliminate vulnerabilities caused by outdated software by detecting and patching software that is no longer up to date.	✓
Vulnerability Management Identify, prioritize, and patch vulnerabilities quickly, focusing on high-risk CVEs to secure IT environments	✓
Software Deployment Remotely deploy and manage software across devices, ensuring up-to-date applications	✓

	MDM Essential	MDM Advanced	MDM Enterprise
	Simplify and secure mobile device setup and management, enhance productivity of your mobile workforce. Device-based License (per endpoint device). Starting from 5 endpoint devices.	Device-based License (per endpoint device). Starting from 5 endpoint devices.	Device-based License (per endpoint device). Starting from 5 endpoint devices.
Mobile Device Management (MDM)			
Device Enrollment Simplified mobile device enrollment for administrators to establish control and manage devices	✓	✓	✓
Configuration Management Manage device settings like Wi-Fi, email, VPN, and other organizational parameters	✓	✓	✓
Policy Enforcement Create and enforce policies for device security, settings, and user restrictions	✓	✓	✓
Security Controls Implement measures like password enforcement, remote lock, and data wipe to protect sensitive information	✓	✓	✓
Application Management Distribute and manage business apps with user-specific access and permissions	✓	✓	✓
Reporting Monitor compliance, track inventory, and analyze device usage with reporting tools	✓	✓	✓
Zero Touch Deployment Automate mobile device onboarding without manual setup	✗	✓	✓
Remote Support Enable remote troubleshooting with screen sharing, OTA updates, and configurations	✗	✓	✓
Compliance Monitoring Ensure devices adhere to organizational policies and regulations	✗	✓	✓
Content Management and Collaboration Securely distribute and manage files while enabling collaboration via platforms like SharePoint and Google Drive	✗	✗	✓

Enhanced Security Controls Use two-factor authentication, push notifications, encryption, and certificate-based authentication for robust security	✗	✗	✓
Secure Productivity Secure web browsing through secure tunneling, protecting both data-in-motion and data-at-rest	✗	✗	✓
Secure Connectivity Enable per-app VPN access to corporate resources without user intervention	✗	✗	✓
Integration and Ecosystem Support Seamlessly integrate MDM with enterprise systems like Salesforce for automated workflows	✗	✗	✓
Scalability Support large-scale deployments with high availability for uninterrupted device management	✗	✗	✓

Definitions

Unless otherwise stipulated herein below, capitalised terms in the Product Description shall have the same meaning as defined in the [TeamViewer EULA](#).

Named User License: Access to and use of the Product is exclusively granted and bound to the specific individuals designated by Customer (each a licensed User). Group or shared logins are strictly prohibited. Re-assignment is limited to two (2) times per User per calendar year.

Capacity-based License: The usage right granted to Customer as well as the calculation of license fees are based on the capacity of resources used, such as the amount of data processed or stored.

Credit-based License: This model uses AI credits as the primary licensed unit. AI credits are consumed in accordance with the applicable AI Credit Consumption Policy available at <https://www.teamviewer.com/en/legal/ai-terms/>. Where applicable, the license provides a monthly allocation of AI credits at no additional cost, as specified in the Contract; these credits are non-transferable and expire at the end of each calendar month. Additional AI credits are available as an annual subscription Add-On, co-termed to the main license; these annual subscription credits reset upon renewal, and any unused credits expire and do not roll over to the subsequent term.

Device-based License: The right to access and use the Services is designated and tied to specific computing devices (each a licensed device) as licensed units. The license fee is determined based on the total number of licensed devices. Customer is responsible for the management and control of remote connection access to its licensed devices. The total number of licensed devices is defined in the Contract or the Product Description, and may be increased by additional order or in-product purchase. Unless otherwise stipulated in the Contract or in the Product Description, the number of remote connections to/from the licensed devices is not contractually limited; however, such use is subject to fair-use principles and may not materially degrade performance, circumvent technical safeguards, or impose unreasonable demand on the Service infrastructure.

Endpoint-based License: The right to access and use the Services is designated to specific managed targets ("Endpoints"), regardless of whether a TeamViewer software component (e. g. client, agent) is installed on them. Endpoints may include physical devices, virtual systems, or network services that are reachable through supported access mechanisms (e.g., via an Agentless Access Gateway). The license fee is determined based on the total number of designated Endpoints, including any required access components such as Gateways. Customer is responsible for the management and control of remote access to its licensed Endpoints.

Add-On: Add-On refers to: i) additional licenced units (e. g. Users, Endpoints, etc.) purchased to extend the scope of License; ii) specific features and/or functionalities of the Product that may be activated by purchasing an additional Add-On License. Unless otherwise stipulated in the Contract, Add-On(s) will be added and co-termed to the existing Subscription License.

Channel: A Channel represents one active remote connection under the License. Within a single Channel, a User can open multiple sessions in separate tabs. The total number of Channels determines how many Users can connect simultaneously.

Managed Devices: A Managed Device refers to a computing device (e. g. desktops, notebooks, tablets, smartphones, workstations, servers, point-of-sale terminals, printers or handhelds; examples not exhaustive and subject to the operating system requirements) assigned to a specific TeamViewer account or company profile, and centrally manageable in the TeamViewer Management Console. Under the Device-based License model, each Managed Device designated by Customer to use the Services counts as one licensed device, whether actively used or not.

Multitenancy: Multitenancy enables a primary managing entity ("Primary Tenant"), such as a parent corporation or service provider, to centrally manage, oversee, and govern multiple logically isolated, self-contained software environments (each a "Tenant") associated with or dedicated to various legal entities or business units (e.g., subsidiaries, customers or partners; each a "Managed Client") from a single, secure interface.

Multitenancy is provided strictly as a technical management feature and shall not be construed as a permit to share, split, sub-license, or redistribute the Primary Tenant's license among Managed Clients or any other third parties, and each Managed Client must possess and maintain its own independent license to use the Product, unless such permit explicitly provided by the Contract.

Integration refers to the application that integrates the respective TeamViewer Product as embedded function of a third party solution or platform and enables Customer to use the TeamViewer Product via such third party platform or solution, for which Customer also needs additional license from the third party provider.

User: A User is a natural person identified by a personalized login and designated by the Customer to use the applicable TeamViewer Product within the scope of the acquired License. Each User must, at all times during the designation, meet the requirements of an Authorized User as defined in the EULA. For multi-user licenses, at least one User must be designated as a company administrator to manage Users in the TeamViewer Management Console on the Customer's behalf. Under the Named-User License model, each designated User counts as one licensed user.

Light User/Tensor Licensed User: A Light User is a Licensed User with limited amount of connections under the TeamViewer Tensor license. Each Light User is allowed to establish up to the maximum amount of connections as set out in the Contract or, in case no amount is stipulated, up to 20 connections within a calendar month.

Unlimited: When used in reference to the licensed items such as Users, user accounts (Seats), or sessions, "unlimited" (or "no limitation") means there is no contractual cap imposed on the number of such licensed items under the applicable License type, unless otherwise stated in the Contract. Nevertheless, such use remains subject to the technical limitations of the Service, which currently supports e. g. approximately 10,000 Seats without additional scaling. "Unlimited" is further subject to fair-use principles and does not permit any activity that materially degrades performance, circumvents technical safeguards, or imposes unreasonable demand on the Service infrastructure.