TeamViewer | ThreatDown Powered by Malwarebytes

Endpoint Protection and Endpoint Detection & Response

System Requirements	
TeamViewer	Windows: TeamViewer 15.16, or higher macOS: TeamViewer 15.17, or higher
Operating Systems	Microsoft Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11, Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, 2022 MacOS Mojave, Catalina, Big Sur, Monterey, Ventura Linux: Endpoint Protection: Debian 9, Red Hat Enterprise Linux 7, Red Hat Enterprise Linux 8, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS, CentOS 7, SUSE Linux Enterprise Server 15 Endpoint Detection and Response: Red Hat Enterprise Linux 7, Red Hat Enterprise Linux 8, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS, CentOS 7, CentOS 8. 64-bit only. Linux Kernel version 3.10 or newer

Malware Protection & Detection	
Engine	ThreatDown
Malware Protection	✓
Zero-Day Exploit Protection	✓
Ransomware Protection	Additional EDR capability: Ransomware Rollback (up to 72h; Windows only)
Web Protection	✓
Rootkit Protection	✓
Trojan Protection	✓

Real-Time Protection	Every file is scanned for malicious software as soon as it is accessed.
Suspicious Activity Monitoring	✔
Compressed Folder Scanning (.zip, .rar, etc.)	Scan of compressed folders for potential threats.
Signature-less Anomaly Detection	Machine-learning and AI for predictive malware protection.
PUPs Detection & Removal	Detection and removal of potentially unwanted programs (PUPs).
PUMs Detection & Removal	Detection and removal of potentially unwanted modifications (PUMs).

Threat Response (EDR)	
Network Isolation	Limitation of device communications.
Process Isolation	Restriction of executable operations.
Desktop Isolation	Alerts end-users and temporarily blocks end-user access.
Automated Remediation	Automated and permanent removal of all subtle changes, artifacts, PUPs and PUMs.
Ransomware Rollback	Rollback of any files modified, deleted, or encrypted byransomware up to 72 hours after the infection.

Management & Scheduling	
Unlimited Policies	Granular definition of protection settings.
Scheduling	Scan scheduling with various degrees of thoroughness. Hourly (1 to 23 hours intervals) / Daily / Weekly
Device Grouping	Group devices and assign a safety policy and various scan schedules per group.
Thoroughness	Definition of scan thoroughness for each scan schedule. Threat Scan / Hyper Scan / Custom Scan
Scan Specifications	Automated and permanent removal of all subtle changes, artifacts, PUPs and PUMs.
Exclusions	Exclude drives, paths, files, or file types from being scanned.
Tray Icon Behavior	Show or hide the ThreatDown tray icon and allow or block user-initiated Threat Scans.
Role-based User Management	Definition of user roles and access to groups.

Central Management	
Remote Activation	Create and customize as many individual strategies as you need.
Bulk Activation	✓
Status Overview	✓
Alerts	✓

Managed Service Provider Benefits	
Individualization	Create and customize individual safety policies and scan schedules.
Central Management	View and manage your protected devices from the central TeamViewer dashboard.
Group View	Create device groups for different clients or departments.
Alerts	Set up notifications to be informed about all detected threats, or only if you need to take action.
Scalability	Stock up on endpoints at any time.
Automated Maintenance	✓
Free Updates	✓
TeamViewer Integration	Endpoint Protection and Endpoint Detection & Response are fully integrated into TeamViewer Remote.

TeamViewer **Remote**

The world's most trusted remote access and support platform, now better than ever.

- **Even more efficient:** Get started faster with better onboarding and an all-new connection process.
- **Even more secure:** Remain protected with two factor authentication, Expert information, and stronger authorization.
- **Even easier to use:** Stay in control with a refreshed design and unified access and support features.

What makes TeamViewer Remote **special**

Industry Leading Security
TeamViewer Remote offers built-in security features such as end-to-end 256-bit AES encryption and two-factor authentication to meet the highest security standards.

Cross-platform compatibility
Compared to its market competitors, TeamViewer Remote covers the widest range of devices and platforms.

Best performance
TeamViewer Remote provides the best possible connection, so you can benefit from high image quality and lightning-fast file transfers, even in low-bandwidth environments.

Get started right away

Experience firsthand how TeamViewer Remote can improve your work-flows, with a free, no-obligation 14-day business trial.
Request free business trial

TeamViewer

About TeamViewer

As a leading global technology company, TeamViewer offers a secure remote connectivity platform to access, control, manage, monitor, and support any device — across platforms — from anywhere. With more than 600,000 customers, TeamViewer is free for private, non-commercial use and has been installed on more than 2.5 billion devices. TeamViewer continuously innovates in the fields of Remote Connectivity, Augmented Reality, Internet of Things, and Digital Customer Engagement, enabling companies from all industries to digitally transform their business-critical processes through seamless connectivity.

Founded in 2005, and headquartered in Göppingen, Germany, TeamViewer is a publicly held company with approximately 1,400 global employees. TeamViewer AG (TMV) is listed at Frankfurt Stock Exchange and belongs to the MDAX.

www.teamviewer.com/support

TeamViewer Germany GmbH
Bahnhofsplatz 2 73033 Göppingen Germany
+49 (0) 7161 60692 50

TeamViewer US Inc.
5741 Rio Vista Dr Clearwater, FL 33760 USA
+1 800 638 0253 (Toll-Free)

Stay Connected

www.teamviewer.com