TeamViewer | Malwarebytes

SOLUTION BRIEF

Advanced Cyber Defense Against Malware and Zero-Day Threats

Malwarebytes detects, identifies, blocks, and isolates malware to protect your endpoints from both known and advanced attacks.

Why Organizations Need Better Endpoint Protection

Endpoints are easy targets for cybercriminals. Their security doesn't receive as much attention as servers, leaving them more vulnerable to cyberattacks. The increasing number of remote workers and bring your own device (BYOD) policies have increased the number of endpoint devices in use and placed them further from IT, making them even more inviting.

Cybercriminals have learned how to launch advanced attacks that find vulnerabilities in endpoints, spread through a company's network, and cause damage that can cost sustantial sums of money to remediate.

Why So Many Endpoint Protection Solutions Are Ineffective at Detecting Advanced Threats

Traditional endpoint protection solutions only search computers for signatures of known malicious software (malware) and scan for algorithms that perform brute-force attacks.

But the greatest threat to endpoints today comes from new and unknown (advanced) attacks that have no signature to store or known algorithm to detect by scanning. These advanced attacks can be so new that anti-malware vendors don't know about them yet. Or, they may lurk for months or years without being recognized and then suddenly strike the moment they find a vulnerability: the "zero day."

Traditional malware solutions don't recognize new kinds of attacks. The only advanced attacks they can be sure of are those that have been used before and cataloged. Because they are uncertain about new attacks, they report a high percentage of false positives, sending IT hunting for threats that don't exist.

Meanwhile, the number of known threats grows every day, so databases of known threats get bigger and bigger with no end in sight. The heavy footprint of known malware databases and their demand on system resources slows the devices they are intended to protect.

Malwarebytes takes a different approach.

How Malwarebytes Works

Unlike traditional endpoint protection solutions, Malwarebytes has a lightweight footprint that doesn't slow down the endpoint. How?

Malwarebytes recognizes and catalogs "goodware" — properly signed code from known vendors — instead of "malware." When Malwarebytes analyzes code and matches it to known goodware, it allows whatever process the code is running to continue.

When code does not match known goodware, Malwarebytes isolates the code until it determines whether it is goodware or malware. Over time, machine learning enables Malwarebytes to become increasingly faster and incrementally more precise at making predictive malware verdicts.

Key Benefits

Fast Insights

Get insights faster with automated threat analysis and potential impact assessments, enabling CISOs to save time and alert executive leadership teams of potential risks quickly to mitigate issues and prevent escalated incidents.

High Performance

Using a single lightweight agent, quickly pinpoint and block malicious code from running without impacting device performance.

Script-Free Simplicity

Fight malware in a matter of clicks, not scripts, with comprehensive endpoint security features and automated capabilities.

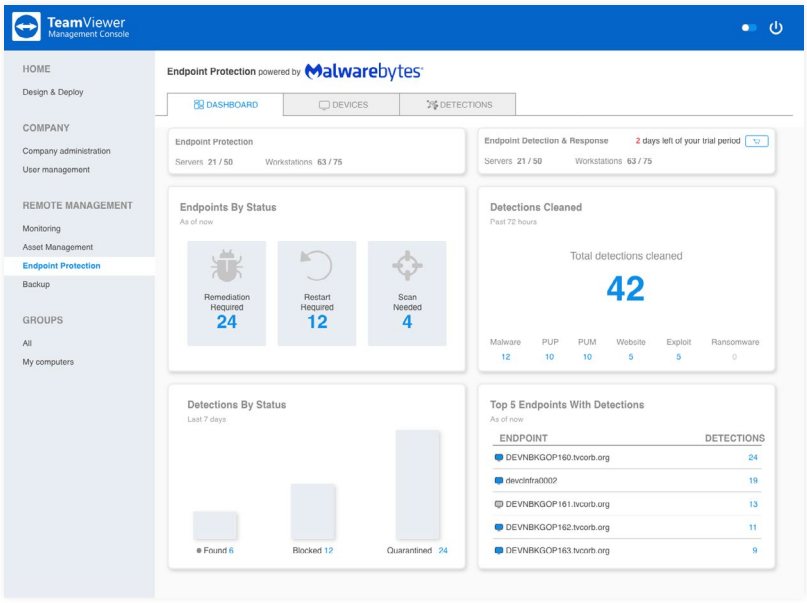

Figure 1: From within the TeamViewer Management Console, the Malwarebytes dashboard gives you a clickable overview of all malware activity in your IT infrastructure, how it's being handled, and which devices require attention.

Malwarebytes Endpoint Protection (EPP) and Malwarebytes Endpoint Detection and Response (EDR)

Both Malwarebytes Endpoint Protection and Endpoint Detection and Response can be mass deployed quickly and silently through TeamViewer, with no user disruption.

Malwarebytes Endpoint Protection

Malwarebytes Endpoint Protection provides cloud-based malware protection and remediation with precise threat detection, proactive threat blocking, and thorough remediation. EPP is fully scalable and easy to use for organizations of all sizes.

With its lightweight agent, Malwarebytes EPP is designed to keep endpoints operating at full speed, so you don't have to choose between protection and performance. And because Malwarebytes Endpoint Protection is a complete solution for spyware, ransomware, zero-day exploits, Trojans, and rootkits, you don't have to cobble together multiple tools to achieve your cyber security goals.

Malwarebytes Endpoint Detection and Response

Designed to meet the security needs of enterprises and mid-market businesses, Malwarebytes Endpoint Detection and Response provides all the functionality of Malwarebytes Endpoint Protection and adds several critical EDR capabilities:

- ✓ Granular isolation of threats for processes, networks, and Windows desktops
- ✓ Detailed threat information collection for analysis and investigation
- ✓ Guided threat hunting to search indicators of compromise (IOC)
- ✓ 72-hour ransomware rollback for Windows workstations, so you never have to pay a ransom, lose your data, or replace your endpoint due to ransomware attack
- ✓ Higher Remote Desktop Protocol protection to block brute-force login attempts
- ✓ Enterprise-class malware detection that employs machine learning for anomaly detection
- ✓ Low rate of false-positive alerts

Endpoint Detection and Response's low rate of false positives also helps keep enterprises from running afoul of personal information authorities that make organizations prove their alerts did not expose personal information or face fines for the presumed PI exposure.

Both Malwarebytes Endpoint Protection and Malwarebytes Endpoint Detection and Response work with any combination of Windows and MacOS desktops and laptops. Server protection is also available.

Better Together: Malwarebytes and TeamViewer

Malwarebytes advanced endpoint protection meets TeamViewer remote connectivity and ease of use.

Remote Endpoint Access

When Malwarebytes identifies a threat, you can remote in to the endpoint device with TeamViewer to check settings and status, and to take whatever action is needed to mitigate risk, — all from the same platform. Even when Endpoint Detection and Response isolates a compromised device to protect the network, you can still safely remote in with TeamViewer.

Integrated Dashboard

Ability to rapidly deploy, launch, and manage Malwarebytes from the same integrated TeamViewer dashboard used to securely monitor, patch, and remote in to endpoints, giving you an increased level of situational awareness.

Support Workers Anywhere

Simple and fast deployment of Malwarebytes to in-office, remote, hybrid-remote, and BYOD workforces of any size through TeamViewer.

Ready to Launch

Malwarebytes is integrated with your TeamViewer dashboard, ready to download and use with one click. No coding necessary.

Security

Data and Program Encryption

TeamViewer connections are secured by 4096 RSA private/public key exchange and AES 256-bit end-to-end session encryption. This technology is based on the same standards as https/SSL and meets today's standards for security. The key exchange also guarantees full client-to-client data protection. This means that even our routing servers can't read the data stream. All program files are secured using DigiCert code signing technology.

Key Features

Zero-Day Threat Prevention

By applying signatureless payload analysis and anomaly detection, proactively identify and block malware attempting to exploit hidden vulnerabilities in the operating systems and applications of your organization's endpoints, preventing zero-day attacks.

Unified "Smart" Threat Detection

Get more accurate, "smarter" threat discovery rates with fewer false positives by profiling threats across web, memory, application, and files with behavioral monitoring and machine learning.

Centralized Scanning and Remediation

Monitor and maintain the protection state of your devices by identifying threats and quarantining devices with automated scanning and remediation across a single department or thousands of devices at a time with just few clicks — all from a centralized cloud console.

Proactive Behavior-Based Blocking

With behavior-based analysis, get near real-time identification of malicious behavior and automatically block threats — one of the most proactive security features on the market today.

One-and-Done Remediation

Applying in-depth insights from the Linking Engine, thoroughly and permanently remove both the infection and any artifacts for "one-and-done" remediation.

Comprehensive Web Protection

Prevent users from accessing malicious sites, malvertising (malicious advertising), scammer networks, and suspicious links, as well as downloading unauthorized programs and making unapproved modifications.

Seamless Integration, Fast Deployment

Malwarebytes Endpoint Protection and Endpoint Detection and Response are completely integrated with TeamViewer, ready to deploy remotely — no complicated setup necessary.

Easy Scalability and Customization

Our cloud-based solution scales to support organizations of all sizes and is customizable to serve individual departments, enabling you to efficiently detect complex threats and provide fast, consistent responses.

License Overview

	Endpoint Protection	Endpoint Detection and Response
Windows or Mac desktops and laptops	✓	✓
Multi-Vector Protection Protection against all varieties of threats, including ransomware, malware, zero-day exploits, adware, and viruses. Levels of protection include: • Web • Application Hardening • Application Behavior • Exploit Mitigation • Payload Analysis • Anomaly Detection Machine Learning • Ransomware Mitigation	✓	✓
Remediation • Linking Engine Remediation Technology • Cleans Infected Device(s)	✓	✓
Installation and Management • Centralized Cloud Management • Security Policies • Endpoint Group Management • Deploys Easily from the Endpoint Protection Dashboard • Threat Visibility Dashboards • On-Demand and Scheduled Scans • On-Demand and Automated Reports • Email Notifications • SysLog Support	✓	✓
System-Specific Isolation Modes • Network • Process • Desktop	✗	✓
EDR Capabilities • Detect and Report Suspicious Activity • Granular Endpoint Isolation • Ransomware Rollback	✗	✓

Next Steps

See firsthand how Malwarebytes solutions work with a free, no-obligation 14-day trial.

Request Free Trial

Explore the Malwarebytes solutions, integrated with TeamViewer.

Learn More

Questions?

Call **800 638 0253 (Toll-free)**

Let's Connect

About TeamViewer

As a leading global remote connectivity platform, TeamViewer empowers users to connect anyone, anything, anywhere, anytime. The company offers secure remote access, support, control, and collaboration capabilities for online endpoints of any kind and supports businesses of all sizes to tap into their full digital potential. TeamViewer has been activated on approximately 2.5 billion devices, up to 45 million devices are online at the same time.

Founded in 2005 in Göppingen, Germany, TeamViewer is a publicly held company listed on the Frankfurt Stock Exchange, employing about 1,350 people in offices across Europe, the US, and Asia Pacific.

Stay Connected

www.teamviewer.com