



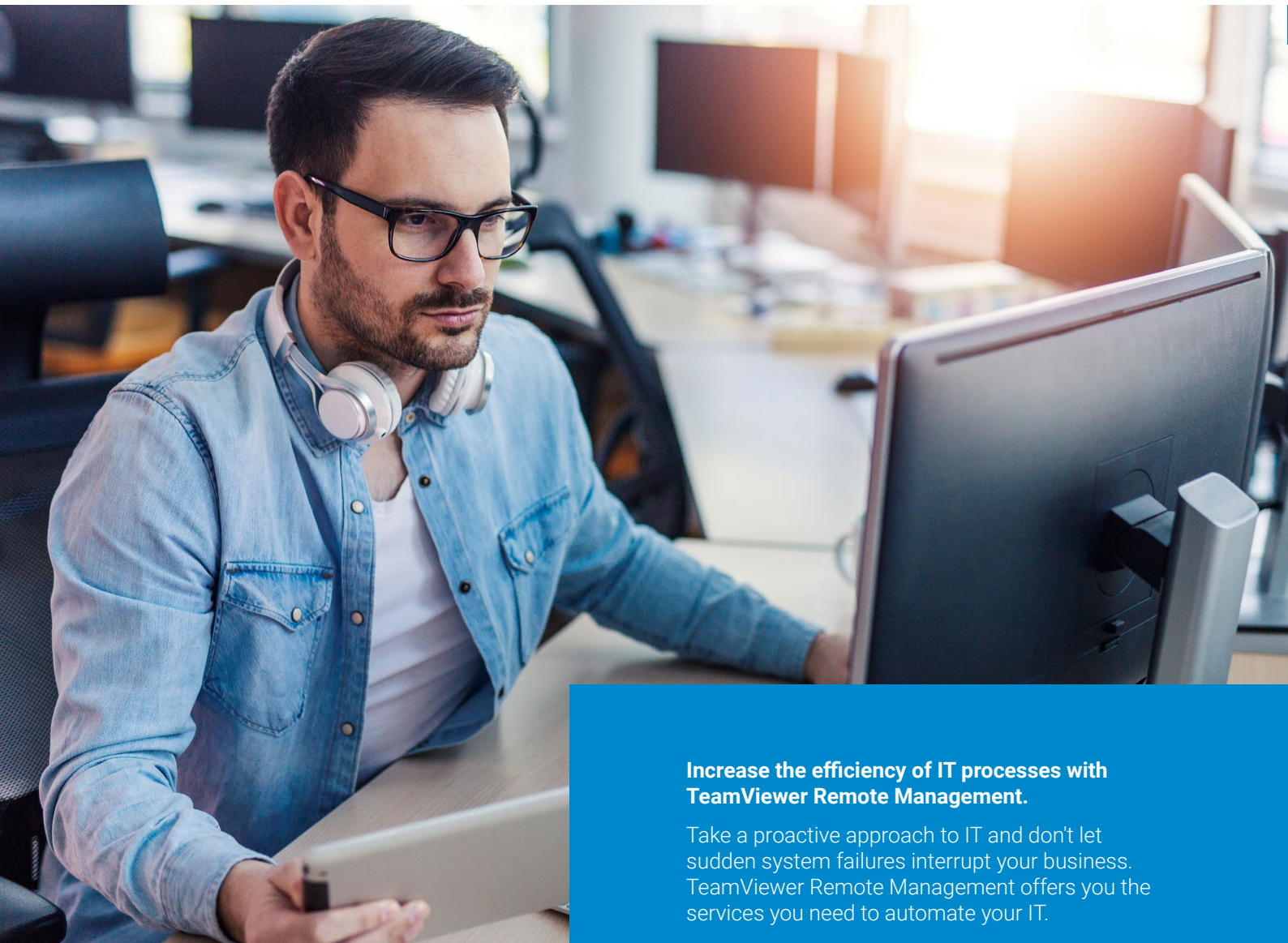
**TeamViewer**  
Remote Management



# Your Professional IT Management Platform

Manage IT Proactively with TeamViewer Remote Management

# Take Control of Your IT Infrastructure



IT monitoring and protection  
from within the TeamViewer  
console.

**Increase the efficiency of IT processes with  
TeamViewer Remote Management.**

Take a proactive approach to IT and don't let sudden system failures interrupt your business. TeamViewer Remote Management offers you the services you need to automate your IT.

**Better together: TeamViewer Remote Management  
is seamlessly integrated with TeamViewer.**

Fully integrated into your TeamViewer console, TeamViewer Remote Management informs you of existing and potential risks in your IT infrastructure, giving you the opportunity to intervene remotely and prevent problems before they occur.

# Get the Right Services For Your IT Management



---

---

---

---

---

---

---

---



# Device and Network Monitoring

Monitor critical aspects of your devices.



**TeamViewer Monitoring provides early recognition of problems in your IT infrastructure and warns you immediately.**

Define individual monitoring policies to inform you of disk health, CPU usage, online status of computers, printer toner levels, and much more.

Be proactive with your IT administration tasks and avoid time-consuming, costly outages and data loss with TeamViewer Monitoring.



## Faster Reaction Time

Individually define acceptable limits and receive a notification when these are reached.



## Significantly Fewer Outages

Reduce unplanned downtime by performing preventive maintenance when you receive notifications that limits are being reached.



## Save Money

Proactively maintaining your systems enables you to reduce the frequency of expensive outages and prevent potential data loss.

## Remote Task Manager

Up your support game – provide your clients with a faster, less intrusive, and more seamless experience.

View and manage all running processes and services on your devices remotely from a centralized dashboard with the built-in Remote Task Manager.

Start and stop processes and services remotely, without first establishing a remote connection.

## Remote Scripting

Automate complex tasks on one device or all of them.

Deploy scripts immediately or on a convenient schedule for you and your users.

Proactive scripts can run when certain events are detected or thresholds are reached.

# Identify Problems Early and React at a Moment's Notice

TeamViewer Monitoring continually keeps track of the critical aspects of your Windows, macOS, Linux, and network devices – like printers and routers – and alerts you immediately, so you can act quickly and efficiently.

## Online Status

Get alerts when devices go offline, triggered by predefined rules for offline status duration.

## CPU Usage

Set a limit and receive alerts when the threshold is exceeded for a longer period.

## System Update

Be informed of all available updates and see if users have deactivated automatic Windows updates.

## Processes

Get alerts when predefined processes are started, ended, or both.

## Disk Health

Get alerts as soon as one of your devices reports a S.M.A.R.T. error, allowing you to react quickly and avoid data loss.

## Disk Space

Get notified as soon as the disk space on devices falls below a defined limit.

## Windows Services

Get alerts when certain Windows services stop or after a consecutive number of attempts.

## Event Logs

Get notified when certain events are recognized in the event logs of your devices.

## Firewall

A deactivated firewall represents a substantial risk to your IT security. If the firewall is deactivated, you'll receive an immediate notification.

## Status of Antivirus Software

Monitoring alerts you the second antivirus software is detected to be inactive or out of date.

## Network Adapter Traffic

Set minimum and maximum thresholds for incoming outgoing traffic and get alerts if the traffic is not within those limits.

## Memory Usage

Work in an environment free from the issues and outages caused by pushing the memory to the limit.

## Learn more about

[Remote Device Monitoring](#)

[Network Device Monitoring](#)



# Asset Management

Gain instant visibility into your IT systems by automatically itemizing and tracking your deployed hardware and software.

TeamViewer Asset Management provides overviews of the operational hardware and software assets in your organization.

With just a few clicks, get essential information about your inventory in a centralized dashboard – seamlessly integrated with TeamViewer.



## Inventory Tracking

From the number of keyboards in use to an overview of specific software versions, with TeamViewer Asset Management, you will never lose track of your IT inventory.

### Hardware

Capture your operational hardware in a comprehensive inventory report in seconds.

- ✓ Type
- ✓ Name
- ✓ Details
- ✓ Manufacturer

### Software

Check whether users have installed inappropriate software in your infrastructure, or if your licenses fully account for actual software use.

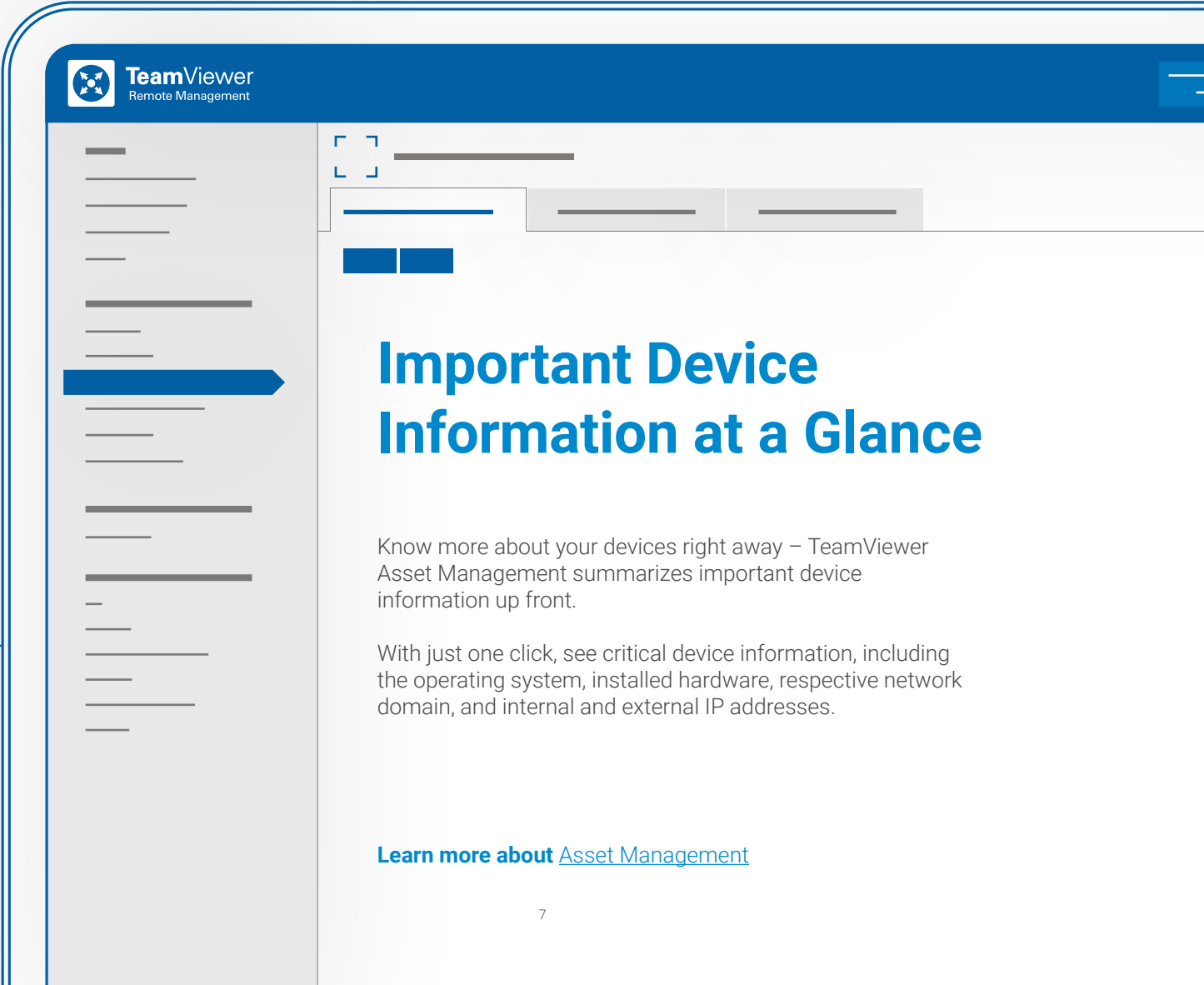
- ✓ Version
- ✓ Change date

Generate comprehensive reports on all your devices' configurations.

### Inventory Reporting

With TeamViewer Asset Management, you can generate comprehensive reports about your hardware and software. In seconds, you'll have a complete inventory report, or a customized report focused on specific data.

Export the information to a CSV file for other applications.



# Patch Management

Protect your devices with timely, automatic patching for Windows and third-party applications.



Many security incidents can be traced back to an inadequate patching strategy. Save time with automation and keep your operating systems and applications current.

One unpatched endpoint can put your entire IT infrastructure at risk. Patch Management from TeamViewer Remote Management (included in the TeamViewer Monitoring and Asset Management license) automatically detects potential vulnerabilities in operating systems and third-party applications. Patches are automatically deployed from the world's leading patch database.



### More Secure Data

Keep your devices up-to-date and protected, mitigating the risks of data breaches due to malware or ransomware that cost companies millions of dollars every year.



### More Efficient IT

Reallocate the time you would normally spend on manually patching to other high-value projects.



### Higher Productivity

Automated patching means employees are no longer interrupted during the day, while devices are still patched in a timely manner.

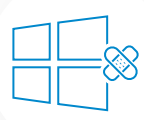


### Increased Compliance


Easily prove data security compliance and other regulatory requirements.

# Patching That Fits Your Needs


TeamViewer Patch Management gives you the power and flexibility to patch how you want, when you want, while still having visibility into the process.




**Patch Windows**  
Deploy Windows updates from a central location.




**Convenient Dashboard**  
See the patch status of every device immediately.




**Patch Third-Party Applications**  
Patch vulnerable applications with the leading patch database.



**Automation**  
Automatically identify and deploy patches on your schedule.

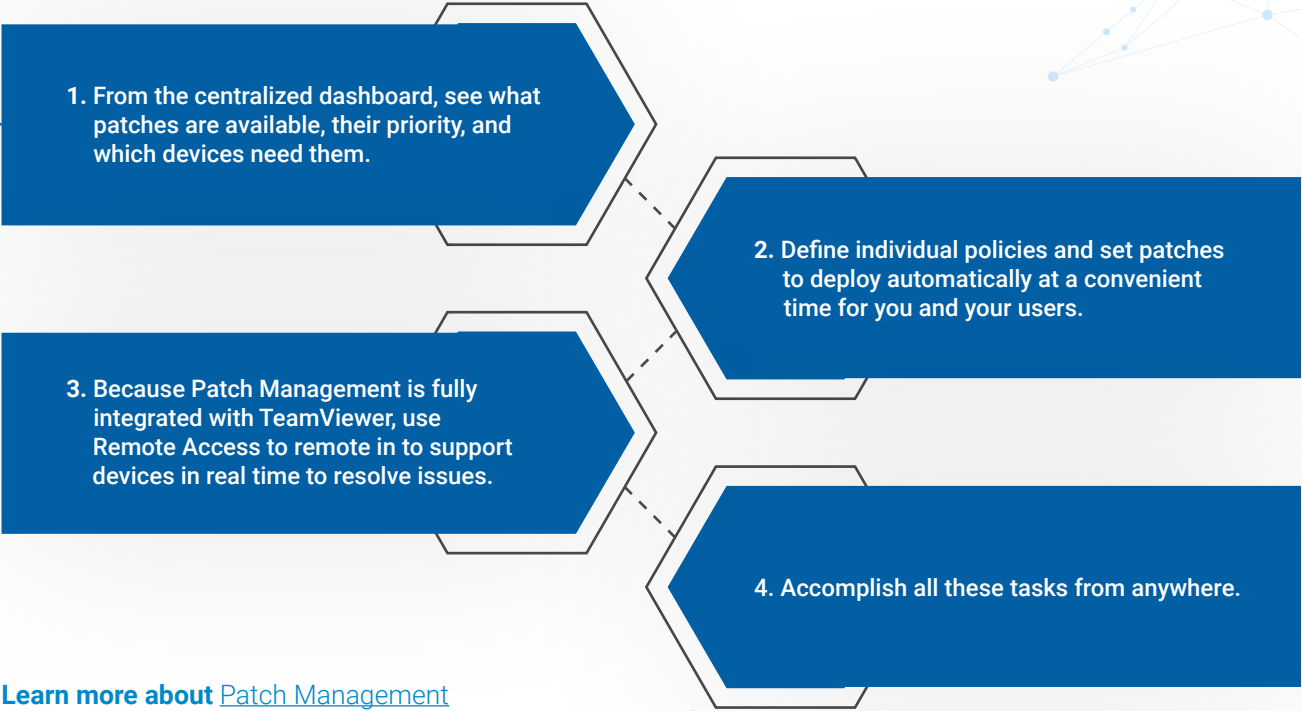


**Fully Integrated**  
Deploy patches from the same TeamViewer console you already know.



**Custom Policies**  
Define individual policies to meet your users' needs.

# See How Easy Patching Can Be

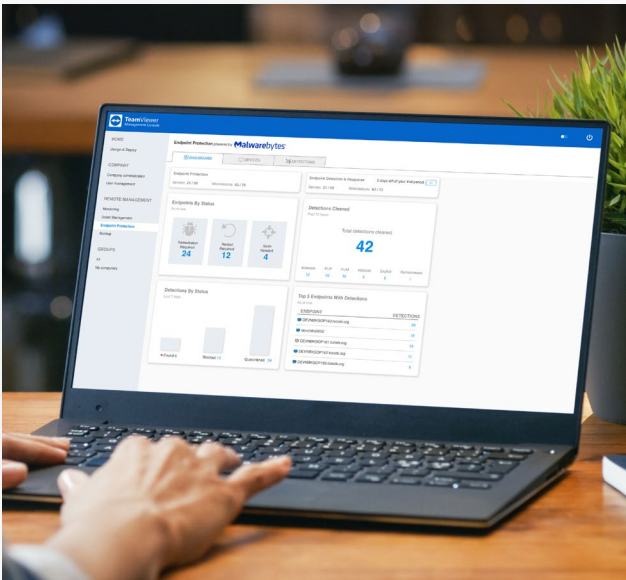


[Learn more about Patch Management](#)



# Endpoint Protection

Advanced cyber defense for forward-thinking organizations, powered by Malwarebytes, fully integrated with TeamViewer.



**Predictive threat detection and proactive threat blocking against viruses, trojans, and ransomware for zero-day threat prevention.**

There has never been a greater need for a unified, holistic approach to endpoint protection that's strong enough to stop advanced attacks and agile enough to adapt to the ever-changing cyber threat landscape.

Malwarebytes Endpoint Protection offers cloud-based malware protection and remediation with predictive threat detection, zero-day threat blocking, and integrated end-to-end protection — easily managed and scaled for SMBs and enterprises.

## Proactive Solutions Against Cyber Threats



### 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.



### Zero-Day Threat Prevention

Prevent zero-day malware attacks with signatureless payload analysis and anomaly detection.



### One-and-Done Remediation

Thoroughly and permanently remove both the infection and any artifacts for “one-and-done” remediation.



### Unified “Smart” Threat Detection

Behavioral monitoring and machine learning generate “smarter” threat discovery rates with fewer false positives across all layers: web, memory, application, and files.



### Centralized Scanning and Remediation

Automate scanning and remediation across a single department or thousands of devices at a time with just a few clicks — all from a centralized cloud console.

# Intelligent Protection



### 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.



### Easy Scalability

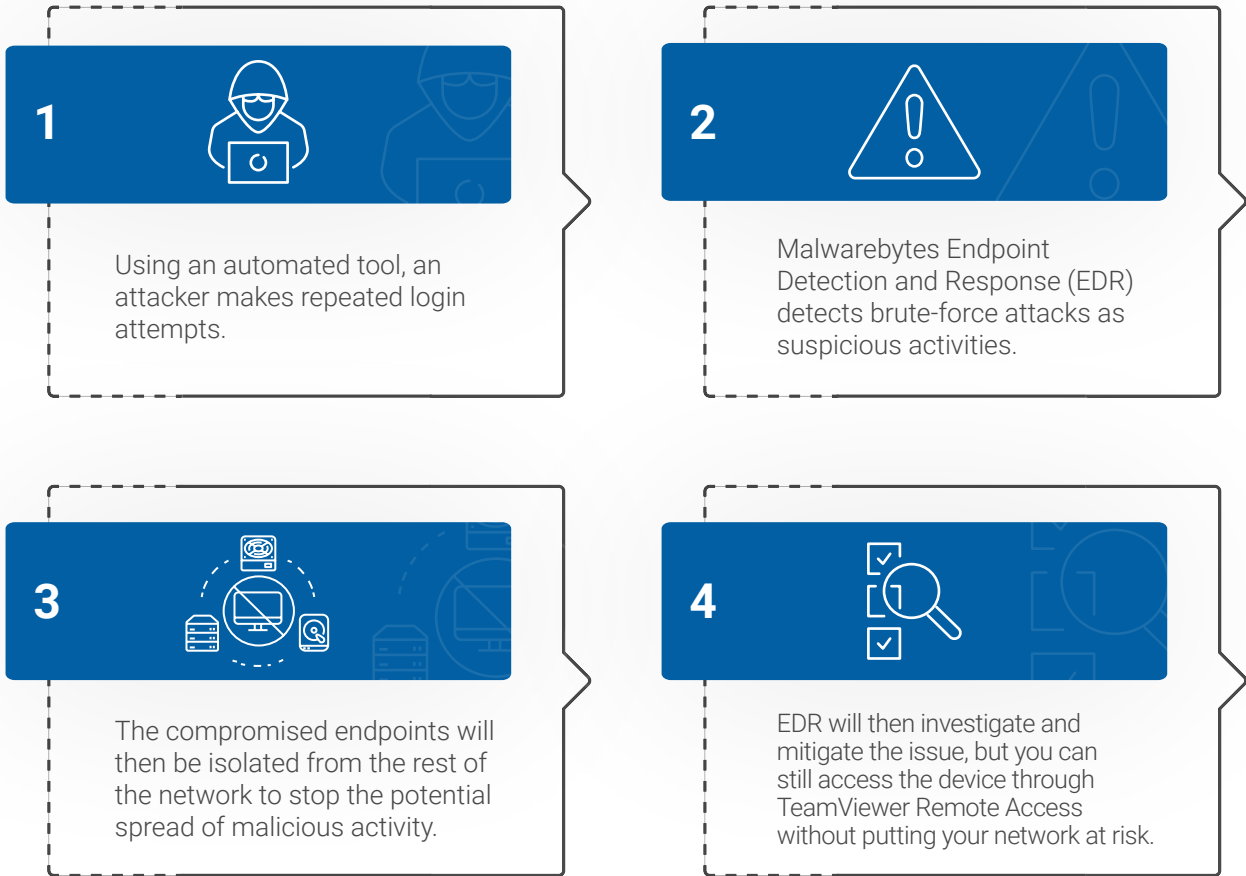
Our cloud-based solution scales to support organizations of all sizes, with quick remote deployment through TeamViewer — customizable to serve individual departments, enabling you to efficiently detect complex threats and provide fast, consistent responses.



### Script-Free Simplicity

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

## How Endpoint Detection and Response Stops Brute-Force Attacks



[Learn more about Malwarebytes Endpoint Protection](#)

# Backup

Access your backed up data from anywhere, anytime.

Seamlessly integrated with TeamViewer, TeamViewer Backup provides simple and reliable endpoint data backup protection.

Deployed and activated remotely in seconds, your or your customers' data will be stored securely in the cloud. Maintain peace of mind knowing your data is stored safely and – in case disaster strikes – always available for remote recovery.



## Endpoint Backup

Automatically back up data and files stored on devices to the cloud.



## The Cloud

Store your data safely in the cloud, available whenever it's needed.



## Remote Deployment

Have a backup running in less than a minute with just a few clicks.



## Remote Restore

Restore your files from anywhere, at any time, to your local or remote device.



## Unlimited Endpoints

Your TeamViewer Backup storage will automatically be allocated across all your devices.

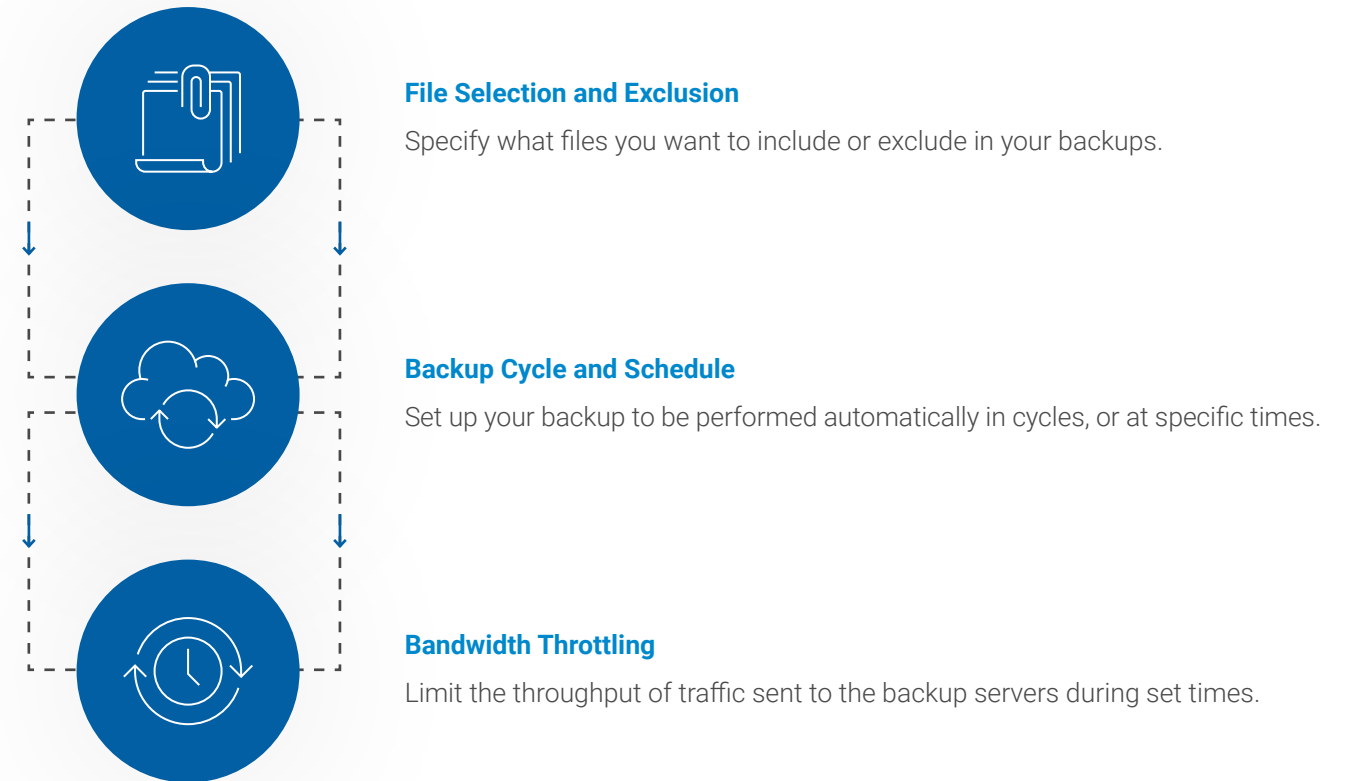


## Scalability

Purchase additional storage at any time.

# Individual Backup Policies

Whether managing one device, whole departments, or different customers, offer a backup plan that suits everyone best.



# Backup With the Highest Security Standards

We take the security of your stored data seriously. Maintaining the highest security standards is our top priority.

- Client-side, military-level **256-AES encryption** prior to data transfer
- SSL encrypted end-to-end data transfer
- Data storage on **256-AES encrypted Amazon AWS S3 servers**
- Data center locations:
  - EMEA: Frankfurt, Paris, London, Dublin, Stockholm
  - AMERICAS: Virginia (US), Montreal (CAN)
  - APAC: Sydney, Tokyo, Mumbai, Seoul, Singapore
- **ISO/IEC 27001:2005 Certification** for information security management systems
- Redundant data storage



[Learn more about Endpoint Backup](#)

# Web Monitoring

Ensure your website performance is optimized for every visitor, every time.

Your website is supposed to engage visitors and attract them to your business, but it can just as easily turn them off and send them to your competitors. In addition to how it looks and what it says, how well your website works has a lot to do with how well your business succeeds.

Websites need to be tested on a regular basis to make sure they are operating properly. But, regular, manual testing can be costly and complicated. When you use TeamViewer Web Monitoring, your website's availability and speed are automatically tested at customized intervals from dozens of locations around the world. If problems arise, you are alerted so issues can be fixed before an outage results in lost revenue.



## Avoid Lost Revenue

Provide the best possible website experience for every visitor, customer, and prospect.



## Improve Website Performance

Identify bottlenecks and suboptimal components.



## Identify Attacks Faster

Receive an alert if availability is threatened because of an outside attack.



## Rank Higher on Search Engines

Avoid website performance penalties and increase your SEO ranking and website presence on search engine results pages (SERP).

# Website Monitoring, Simplified

TeamViewer Web Monitoring helps you maintain a fast, stable website, no matter where you or your visitors may be.

## Uptime Monitoring

Websites can be down for a variety of reasons, including:

- Server Overload
- Hacker Attacks
- Data Center Problems
- Problems with Website Code
- Problems with Internet Service Providers

Uptime Monitoring alerts you when and where your website isn't available, so you can get it up and running as soon as possible.

## Page Load Monitoring

While 40 percent of consumers abandon websites that take more than three seconds to load, every second matters if you don't want to lose potential customers.

With Page Load Monitoring, get alerts if your website exceeds a load time threshold, continuously monitored by over 30 worldwide locations.

Find the individual elements and bottlenecks that are slowing down your website.

## Transaction Monitoring

Automated transaction monitoring can help you avoid lost revenue due to failed web shop sales, customer logins, or other transactions. How? By providing complete visibility into:

1. Whether or not transactions are working
2. Where the failures or slowdowns are occurring
3. The cost-effectiveness of your website performance
4. The operational status of third-party components

[Learn more about Web Monitoring](#)



# TeamViewer Takes Your Data Protection Seriously



As a German company, we're dedicated to meeting the European security standards and compliance requirements. Our solutions have layers of built-in security protocols to keep your data secure and private. While TeamViewer provides background security through encryption, code signing, two-factor authentication, and more, we also offer other helpful functions to maintain security during your everyday work.

## TeamViewer Security



### The TeamViewer ID

The TeamViewer ID is unique to your device, which is generated automatically and checked before each session.



### The Highest Security Standards Worldwide

Our main data center meets the ISO 27001 industrial security standards.



### Protection from Brute-Force Attacks

With TeamViewer, the time between failed login attempts is increased exponentially and is reset only when the correct password is entered. Remote access devices or connection partners are also protected from other attacks.



### The TeamViewer Password

TeamViewer automatically generates a new dynamic session password after each TeamViewer service restart. But there is also an optional setting which allows a password to be set dynamically after each session. This password is alphanumeric as standard, and consists of six characters, which means that there are more than 2.1 billion possible combinations.



### Secure Remote Password (SRP)

TeamViewer uses the SRP protocol for authentication and password encryption. So the password is never sent over the internet, even encrypted, and is therefore optimally protected from outside access. Passwords also receive back-end encryption.



### Encryption

All interactions through TeamViewer, including file transfers, VPN, chat, etc., are protected by end-to-end encryption with a RSA 4096 public/private key exchange.



### Conditional Access\*

With Conditional Access, you can enforce remote access rules in order to prevent unauthorized activity and adjust the security guidelines.



### Two-Factor Authentication

In this case, login takes place using a new unique code, which is generated each time by an algorithm and supplied from a mobile device.

\*Available with TeamViewer Tensor™. Terms and conditions apply.

## TeamViewer Sessions

### Session Setup and Connection

When setting up a session, TeamViewer selects the optimal type of connection. In 70 percent of cases, after the handshake through our master server (even behind standard gateways, NAT routers, and firewalls), data connection is by UDP or TCP. The other connections are made through our high-redundancy router network by TCP or HTTP tunnelling. That means you don't have to open any ports in order to work with TeamViewer.

### Encryption and Authentication

TeamViewer connections are made through fully secured data channels, which are set up by 4096 RSA public/private key exchange with 256-bit AES encryption. This technology is also applied in the same way for https/SSL and is considered completely safe by today's standards. Since the private key never leaves the client computer, this technology ensures that no intermediate computers connected on the internet can decrypt the data stream. This also applies to TeamViewer routers. As operator of the main data center, not even TeamViewer can read the encrypted data traffic.

## Compliance and Data Protection

### Trusted Devices

Trusted Devices ensures that authentication is requested the first time a new device attempts to log in to an existing TeamViewer account.

### Data Integrity

Data Integrity provides protection from cyber criminals: The system checks continuously for any unusual behavior on a user account and, if this is detected, generates an automatic password reset.

### Allow List/Block List

This function provides special protection if TeamViewer is installed on computers which are being maintained while unsupervised. The Allow List is used to decide which clients are allowed access. The Block List is used to decide which TeamViewer IDs and accounts are blocked or denied access.

### ISO/IEC 27001

Our main data center is certified to ISO/IEC 27001 standard. This represents the international standard for security management and controls.

### ISO 9001:2015

TeamViewer is also ISO 9001:2015 certified for Quality Management Systems (QMS).

### General Data Protection Regulation (GDPR)

On May 25, 2018, the European General Data Protection Regulation (GDPR) came into effect, reflecting the importance of data protection in our increasingly digital world. TeamViewer is a global organization, and for us, it is important that the personal information of our customers and our own people is handled in accordance with GDPR. To learn more about TeamViewer's commitment to data privacy and the GDPR, visit our [Trust Center](#).

### HIPAA, HITECH, and SOC2 Certified

TeamViewer received HIPAA, HITECH, and SOC2 certification from A-LIGN, a U.S. nationwide security and compliance provider. While HIPAA and HITECH are crucial for health care organizations to ensure the confidentiality and security of sensitive data and protected health information (PHI), SOC2 is an essential reporting framework for service provider organizations to establish a means to report on non-financial internal controls, so that their clients get a better understanding of the enforcement of the five Trusted Service Principles (TSP).





**TeamViewer**  
Remote Management

## Questions?

For more information, call us toll-free at **+ 49-7161-60692-50**  
or connect with us at [teamviewer.com/support](https://www.teamviewer.com/support).

TeamViewer Germany GmbH  
Bahnhofplatz 2  
D-73033 Göppingen  
Germany

## 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 1,300 people in offices across Europe, the US, and Asia Pacific.

## Stay Connected



[www.teamviewer.com](https://www.teamviewer.com)