

SPONSORED CONTENT | WHITE PAPER

# Safeguarding Security for Remote and Hybrid Environments

Organizations with remote and hybrid workers face increased security risks. But with the right approach and solutions, companies can effectively safeguard themselves.



CIO

@ 2023 TeamViewer Germany GmbH

SPONSORED BY

 **TeamViewer**

M

## **ORE THAN HALF OF FULL-TIME EMPLOYEES IN THE U.S.**

are remote-capable, and half of those are hybrid workers, [according to Gallup](#). With today's increased numbers of remote and hybrid workers, companies often face significant known and unknown security risks.

Businesses have changed their workplace structures to adapt to the extended enterprise, moving beyond the traditional enterprise perimeter to address new imperatives, such as cloud, remote users, applications, and the internet of things/operational technology (IoT/OT). This, in turn, has increased their overall attack surface, now extending to home devices and Wi-Fi networks.

These types of security risks are a critical problem in light of increasing cybersecurity attacks in recent years. One study showed [that the number of material breaches that companies across sectors suffered climbed by 20.5% from 2020 to 2021](#). Another study shows that [working from home increases cyberattack frequency by 238%](#).

Data breaches can be costly, both financially and when it comes to customer trust. The [average data breach cost rose](#) in 2022 to \$4.35 million, from \$4.24 million in 2021 and \$3.86 million in 2020. At the present growth rate, [damage from cyberattacks is predicted to reach \\$10.5 trillion annually by 2025](#).

IT, for its part, is often overwhelmed by the increasing need to support, manage, and maintain visibility into all of its company's connected remote and network devices. Without strong security measures, remote devices are at risk, whether they're company-issued or employee-owned.

"IT departments today are faced with heterogeneous and distributed IT environments that are the opposite of a standardized work setup in a fortified, access-controlled corporate environment," says Frank Ziarno, Vice President of Product Management at TeamViewer. "The use of unprotected Wi-Fi networks or leaving the laptop unattended for a brief moment may seem benign but can be fatal for an organization. To maintain a strong security posture, IT departments need to extend the same level of protection to remote devices as if those were back at HQ — through training and proper security solutions."

# The Top Security Challenges

Often, risks that start small can — and do — escalate, with serious impact if they are not addressed quickly. Here are the top four security risks that companies face as they embrace hybrid work:

## 1. Network and remote device vulnerabilities

Outdated anti-malware software is one of the most significant security threats when it comes to network and remote devices. Other potential issues include outdated operating systems, abnormal memory behavior, and disabled firewalls.

Outdated or unsupported software and antivirus solutions can expose organizations to serious risks, enabling hackers to easily gain control of systems and data. Although outdated antivirus software may still function in some capacity, it often cannot effectively handle and neutralize malware or security threats.

## 2. Cyberattacks

Endpoints such as computers and mobile devices are simply not protected the same way that servers are.

Cybercriminals recognize devices as vulnerable places to launch attacks through methods such as phishing, ransomware, and zero-day exploits — three of the most common and expensive types of attacks.

## 3. Data loss

Loss of data can happen in a variety of ways, including losing devices or leaving them behind. Often companies do not back up their devices, thinking that their anti-malware software provides sufficient protection. But data loss can also include:

- Cyberthieves' stealing devices from homes, offices, cars, and coffee shops
- Employees' accidentally deleting files from hard drives
- Natural disasters, such as floods and fires

Some companies rely on their employees to back up their endpoint devices. But that's a mistake. Employees may not be properly trained or motivated to do this. Relying on employees for this task also means that IT can't see backups that are supposed to be done on external hard drives. There's no way to ensure that backups exist.

## **4. Insufficient IT oversight**

Frequently, IT departments lack complete visibility into end user devices. IT can't easily tell if all remote and hybrid workers' devices are in good working order or how many are connected to the corporate network at any given time.

With insufficient oversight, devices that are vulnerable to cyberattacks do not get patched and operating systems and third-party software do not get updated. IT cannot efficiently perform spontaneous audits to find forbidden or potentially harmful software on the company network, identify unauthorized devices, or see the status of backups or gather critical device information without relying on end user input. The risk applies not only to the single endpoint but actually to the entire network.

## **Solutions That Work**

What's the answer? It's critical to start with a holistic, comprehensive view of all devices (regardless of format, manufacturer, and operating systems), including any devices owned by employees. Applications and tools that allow IT to remotely monitor and manage all networked devices can greatly improve IT efficiency and effectiveness.

"Cyber protection will always be an arms race," says Robert Haist, Chief Information Security Officer at TeamViewer. "Cyber attackers aren't standing still, and organizations must always stay one step ahead. A company's security strategy requires continuous attention, monitoring, and re-evaluation of tools, frameworks, and approaches. Gaining and maintaining deep insights into the entire distributed IT environment is a crucial first step in achieving a good and sustainable security posture. You can protect only what you know exists."

Here are four tactics to help avoid the security risks associated with remote and hybrid work:

### **1. Be more proactive with web monitoring.**

Without proactive web monitoring, browsing employees, whether intentionally or not, may access infected downloads as well as websites that have been compromised.

A good web monitoring solution uses servers around the world that regularly ping your website. If a response to the ping takes too long or the ping goes unanswered, that sets off an alert. With proactive web monitoring, IT is immediately informed of a threat or an outage. A good web monitoring tool should have:

- Automated scripts to keep important processes running flawlessly.
- Fast response times with notifications for quick resolutions.
- Reporting to get full analytics of performance for optimizations.

## 2. Retire your VPN.

Although a virtual private network (VPN) is the status quo solution for employee access to corporate systems, there are drawbacks. VPNs are complex, requiring extensive effort for setup and configuration. They also pose challenges in terms of scalability and security.

With a VPN, when users download files from the server to their own computer and make changes to documents locally before saving them back to the server, problems can occur.

Security-wise, nothing prevents remote workers from saving documents to their personal devices. What's more, VPNs can shut down for no apparent reason, leaving the connection between the server and the device unsecured.



### **3. Use a remote monitoring and management platform.**

With remote access, workers can directly access their office desktop, see a mirror image of what's happening on their in-office computer, and operate it from anywhere in the world.

All sessions and file transfers are protected by end-to-end encryption. Remote employees can work efficiently without any latency or delay in actions such as file transfer or download.

Unlike a VPN — which requires extensive setup and configuration and must be compatible with your router — cloud-based remote access solutions can be set up and scaled within minutes without requiring extensive maintenance.

Remote monitoring and management (RMM) platforms keep devices safe in three ways, and all from a single easy-to-use dashboard:

- Anti-malware software prevents and remediates cyberattacks.
- Patch management tools remove software vulnerabilities.
- Regularly scheduled device backup protection ensures that data is backed up to the cloud and available for restoration and recovery, even if cyberattacks succeed.

With remote monitoring and management platforms, IT can perform spontaneous audits to find harmful software on the company network; gather critical device information; and easily see the status of backups, software updates, and patches.

### **The Bottom Line**

The security risks associated with hybrid and remote work are very real. But with the right approach and solutions, companies can effectively safeguard themselves to help prevent future attacks and business disruptions.



Are you at risk? Take this short quiz to see which security risks from remote and hybrid work your company might currently be facing.

Yes No

Can you ensure that your connections are compliant with your access controls?

Yes No

Are you able to leverage your pre-existing roles in your tools?

Yes No

Do you have visibility into how often your tools are leveraged?

Yes No

Can you leverage centralized purchasing and delegated administration?

Yes No

Do you have access to sensitive systems managed by approval only?

Yes No

Are you able to trust that your users are really your users?

If you answered “No” to any of these questions, your company is at risk. [Contact an expert](#) today to talk about your company’s vulnerabilities.



CIO

SPONSORED BY

 TeamViewer