ManageEngine

The Endpoint endgame:

Essential security practices you need to thrive in a remote world

Table of Contents

Introduction

Digital transformation was inevitable. One way or the other we knew we had to embrace it. The pandemic ushered it in, almost overnight, and compelled us to work remotely. Though it's been more than a year, its ripple effects continue to linger. The pandemic required us to rethink the way we work and collaborate with our peers, establishing a benchmark for the future.

What We'll Cover in This White Paper

In this white paper we'll--

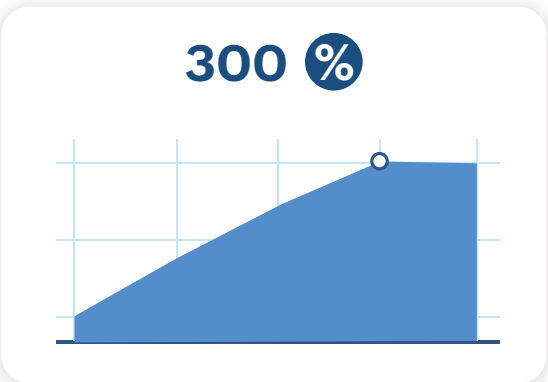
- Discover how and why organizations are finding it difficult to equip their remote or hybrid workforces to adjust to the new normal.
- Address the divide between your organization and your workforce.
- Learn how IT professionals are experiencing difficulties securing and managing end users and their devices across various remote locations.
- Reveal the key security measures that promote a productive end-user experience.

Remote work statistics

Let's run a few numbers and do a
quick reality check,
shall we?

Before 2020, remote work was reserved for a select few and generally not encouraged. Some individuals were willing to even take a pay cut in exchange for the option of working from home. Compare that to today; it's a completely different picture.

Rise in full-time remote workers

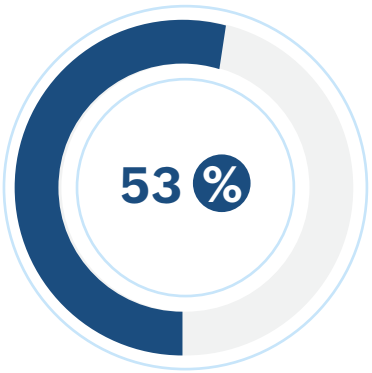


30 % of the workforce will be fully working from home.

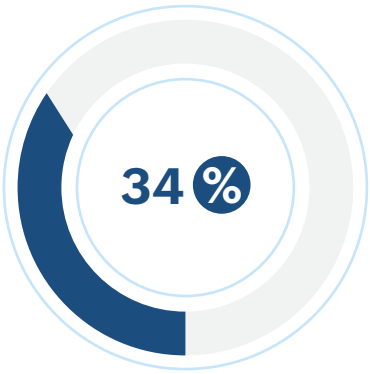
Remote work surged and it continues to do so. According to Forrester, the number of permanent, **full-time remote workers is expected to increase by 300 percent or more from pre-pandemic levels.** Global Workplace Analytics estimates that **by the end of 2021, around 30 percent of the workforce will be fully working from home.**

From an IT infrastructure point of view, the remote work explosion has not been easy to accommodate. Distributing laptops and setting up virtual private networks was often carried in haste and without much planning. Most organizations were left virtually stranded when forced to adopt remote work scenarios.

The 2020 Forrester survey also found that **53 percent** of IT decision makers felt that their infrastructure was not prepared to handle a heavy remote employee base. And even when they did, from an end-user perspective, things did not fare well. The inability to provide a conducive virtual environment negatively impacted the end-user experience. A 2020 Workforce Survey notes that only **34 percent** of its employees felt that their company did a good job of supporting and engaging remotely located employees.



53 percent of IT decision makers felt that their infrastructure was not prepared to handle a heavy remote employee base.



34 percent of its employees felt that their company did a good job of supporting and engaging remotely located employees.

To make things worse, the pandemic inflicted serious wounds on many organizations' revenues. On the business end of things, Forrester also found that over half of IT decision makers stated that their organization experienced a decrease in revenue.

What does all this mean?

It means organizations have to figure out a way to improve the end-user experience working with a tight budget and, at the same time, shield their diverse endpoints from external threats.

Overcoming the digital divide

Are you facing a digital divide or a digital rift?

Make sure it's not the latter.

Now that we've learned how the pandemic has flipped the way we work, let's talk about the impact of remote work on end users in your organization.

Before the pandemic, your end users were accustomed to working from the office. It's likely that your organization had a robust security policy in place, like a demilitarized zone (DMZ), antivirus solutions, a firewall, etc. to thwart external threats and attacks. Thanks to those industry grade-security layers, IT teams could feel reasonably confident they were protecting their network. Be it by delaying patches, or utilizing the generous network bandwidth to deploy apps and software, they could keep tabs on endpoints as long as you were maintained under a single roof.

However, with work-from-anywhere being the new norm, your end users and their devices are now spread across the virtual wilderness. End users are no longer inside your security perimeter, but outside the comfort zone. In most cases, a VPN is the only tether that connects users to your office when they have to access corporate data.

With inadequate infrastructure, rising security loopholes, and an ever shrinking budget, organizations are usually found asking these questions:

As a business owner:

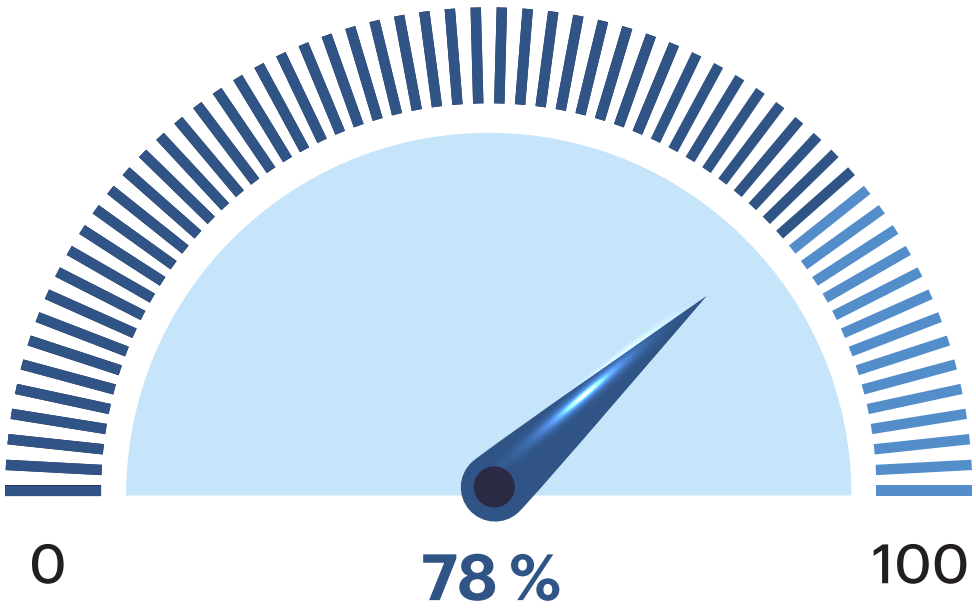
- How do I get the best out of my remote workforce?
- How can I adopt a hybrid work set up and make my business future-ready?
- How do I reduce operating costs and get my business lean?

As an IT manager:

- Should I prioritize end-user productivity over endpoint security?
- Is there a single silver bullet that addresses both endpoint management and endpoint security without costing too much?
- How do I make my existing IT infrastructure work and minimize downtime?

As an end user:

- How can I be more productive?
- How do I reach out for technical support and troubleshooting assistance if I run into an issue?
- How do I secure my devices against malware attacks and ransomware?



According to the World Economic Forum, **78 percent of business leaders think hybrid and home-working will have a negative impact on productivity.**

Endpoint security risks

Your endpoints are scattered in the wild. And are being preyed upon.

What will you do?

Unlike a conventional office set up, your end users don't have the luxury of a firewall or solutions to detect intruders and viruses. Threat actors and hackers are no longer interested in attacking your fortified IT enterprise. They're coming after your personal devices and home networks which are likely less secure.

The line between corporate and personal networks went from being blurred to being non-existent, elevating the dangers of unsecure network. In short, with digital transformation, COVID has changed the threat landscape.

According to Cybersecurity Ventures, by the end of 2021, a ransomware is expected to attack a business every 11 seconds. Supply chain attacks grew by 420 percent ever since we switched to remote work.Ransomware and phishing will remain primary risks in 2021.

Threat actors now attack your remote network in ways which have not been possible on corporate networks with your IT team monitoring endpoints. These attacks on your end-user devices, in the form of spyware, rogue, or hack tools have the potential to affect your corporate data leading to serious repercussions. It has already been estimated that cybercrime will cost the world $10.5 trillion annually by 2025, according to a recent report on **Cyberwarfare in the C-suite** from Cybersecurity Ventures.

To summarize, before the pandemic, there was excessive trust in only a single mode of security control. For example, after investing in an expensive security perimeter, organizations did not feel the need to invest in a viable browser security solution. Today, ensuring your remote workers don't end up downloading a shady extension is more important than an intrusion detection system in your office. Attackers are thriving because your end users are vulnerable. To make things worse, work-from-home users have limited IT support to remediate threats and vulnerabilities. The lack of endpoint security affects the way you manage end users and vice versa.

The need to ensure security environments for remote workers will continue for the foreseeable future. A **2020 Gartner survey** of company leaders found that 80 percent plan to allow employees to work remotely at least part of the time after the pandemic, and 47 percent will allow employees to work from home full-time.

Ways to enhance endpoint security

Well, here's what you can do.

5 security measures to bolster your endpoint management

Both management and security are key to building a resilient IT workforce. It is not possible to prioritize one over other.

Here are five security practices that will help you manage your endpoints and ensure a productive end-user experience

01 Secure your end user browsers.

One major aspect we overlook while securing your end user devices is the management of browsers. We monitor laptops, memory devices, and networks, but usually leave out internet browsers. According to a report by Sans Institute, 48 percent of threats entered organizations via web-based drive-by, or download. Here are a few common ways to thwart browser based attacks in your organization:

- Isolate the browsers deployed by your end users.
- Filter URLs.
- Restrict suspicious extensions and plug-ins.
- Track browsers and browser add-ons.
- Enforce security configurations and ensure compliance.

02 Shield your endpoints against unknown vulnerabilities and threats.

There are two types of vulnerabilities: known and unknown. Known vulnerabilities are well documented within the internet community. They can be located, identified, and understood. Unknown vulnerabilities show up as suspicious activities or abnormal traffic whose causes are difficult to pinpoint. Alerts for these vulnerabilities are generated by the IDP Series Profiler, or your firewall, or IDP security event logs in your product environment.

While known vulnerabilities can be addressed by conventional patches released by the vendors, fixing unknown vulnerabilities is tricky. According to a report by Skybox Security, there has been a 50 percent increase in mobile vulnerabilities.

Vulnerability management is an effective way to gain visibility on, assess, and remediate threats and unknown vulnerabilities from a single console. A vulnerability management solution includes implementation of the following practices:

- Scanning endpoints for vulnerabilities, assessing their threat level, and patching them regularly.
- Resolving security misconfigurations and hardening web servers from XSS, click jacking, and brute-force attacks.
- Identifying publicly disclosed and actively exploited vulnerabilities to patch them on higher priority.
- Preventing zero-day vulnerabilities by employing alternate fixes before patches are available.
- Monitoring ports in use and the processes running in them.

03 **Monitor and keep tabs** on end user devices.

One major aspect we overlook while securing your end user devices is the management of browsers. We monitor laptops, memory devices, and networks, but usually leave out internet browsers. According to a report by Sans Institute, 48 percent of threats entered organizations via web-based drive-by, or download. Here are a few common ways to thwart browser based attacks in your organization:

Device control is crucial when you want to manage the connections of external devices, like USB drives to an end user's machine. It can be any device that is connected to a laptop or computer. Device control lets you to:

- Control, block, and monitor USB and peripheral devices.
- Prevent data leak and theft.
- Limit data transfer rates.
- Set role-based access to files.
- Enable file shadowing to protect sensitive data.
- Grant temporary access to devices without compromising on security

04 Filter applications and software used by your end user devices.

Deploying software and apps used to be straightforward. Your IT team deployed it using a software tool, or enabled end users to access a set of approved software and applications from the enterprise app store. As an extended measure, your corporate network made sure that you didn't install any suspicious apps over the internet.

It's not possible to exercise the same level of control when end users are working from all corners of the world. Not only can end users gain unauthorized access, they are also more likely to fall prey to malicious apps. According to Netskope, 61 percent of all malware is now delivered via cloud applications.

To safeguard your organization from the increasing threat of unscrupulous applications, you can opt for an application control policy that lets you create lists of approved and denied apps and software that your end users can install. It acts as a filter for applications that your organization considers suspicious. You can gain complete control over what applications your end users use in the following ways:

- Deny malicious applications, allow trusted applications, and manage greylisted applications effortlessly.
- Create rule-based application lists to fine-tune application management.

- Achieve application-specific privileged access with endpoint privilege management.
- Curb cyberattack risks by blocking non-business applications and malicious executables.

05 **Encrypt your end user** devices and data.

Not encrypting your data and devices is like waiting for the inevitable. Sooner or later you will experience trouble unless you take proactive measures. You can secure your data on Windows systems by encrypting it with BitLocker.

With BitLocker Encryption, **you can:**

- Ensure data transfers are only completed on BitLocker-encrypted devices.
- Monitor the encryption status of endpoints from a single console.
- Keep endpoints with or without Trusted Platform Module (TPM) protection.

Conclusion

Your organization's management and security need to go hand in hand and unify at some point. Many organizations invest diligently in managing endpoints, without strengthening their security. Conversely, many organizations fortify their digital security but fail to tie loose ends in management, which often results in lower productivity and morale among their remote workforce. You need the best of both management and security.

A well managed network is a secure network, and a well secured network is the one that's well managed.

About **ManageEngine Desktop Central**

ManageEngine develops endpoint management and security tools for teams that are looking to adopt change and innovate fearlessly. Our Unified Endpoint Management solution automates tasks, delivers insights, and provides a reliable way to ensure management and security of your workforce. From a single dashboard, you're enabled to secure your organization by minimizing risks without affecting your agility. Work smarter, stay informed, and accelerate your operations without any obstacles.

www.manageengine.com/products/desktop-central/
sales@manageengine.com | +1-925-924-9500

References

- **Predictions 2021: Remote Work, Automation, And HR Tech Will Flourish** by Forrester
- **Business Technographics® Priorities And Journey COVID-19 Recontact Survey, 2020** by Forrester
- **Work-At-Home After Covid-19—Our Forecast** by Global Workplace Analytics
- **The Future of Jobs Report 2020** by World Economic Forum
- **Web Browser Insecurity** SANS Report

  2020 Vulnerability And Threat Trends by Skybox Security
- **Cloud and Threat** Report by Netskope
- **One Ransomware Victim Every 10 Seconds in 2020** by Info Security
- **State of the Software Supply Chain 2020 Report**
- **Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021** by Cybersecurity Ventures