

COMBATING ENDPOINT MANAGEMENT AND SECURITY CHALLENGES IN THE COVID-19 ERA

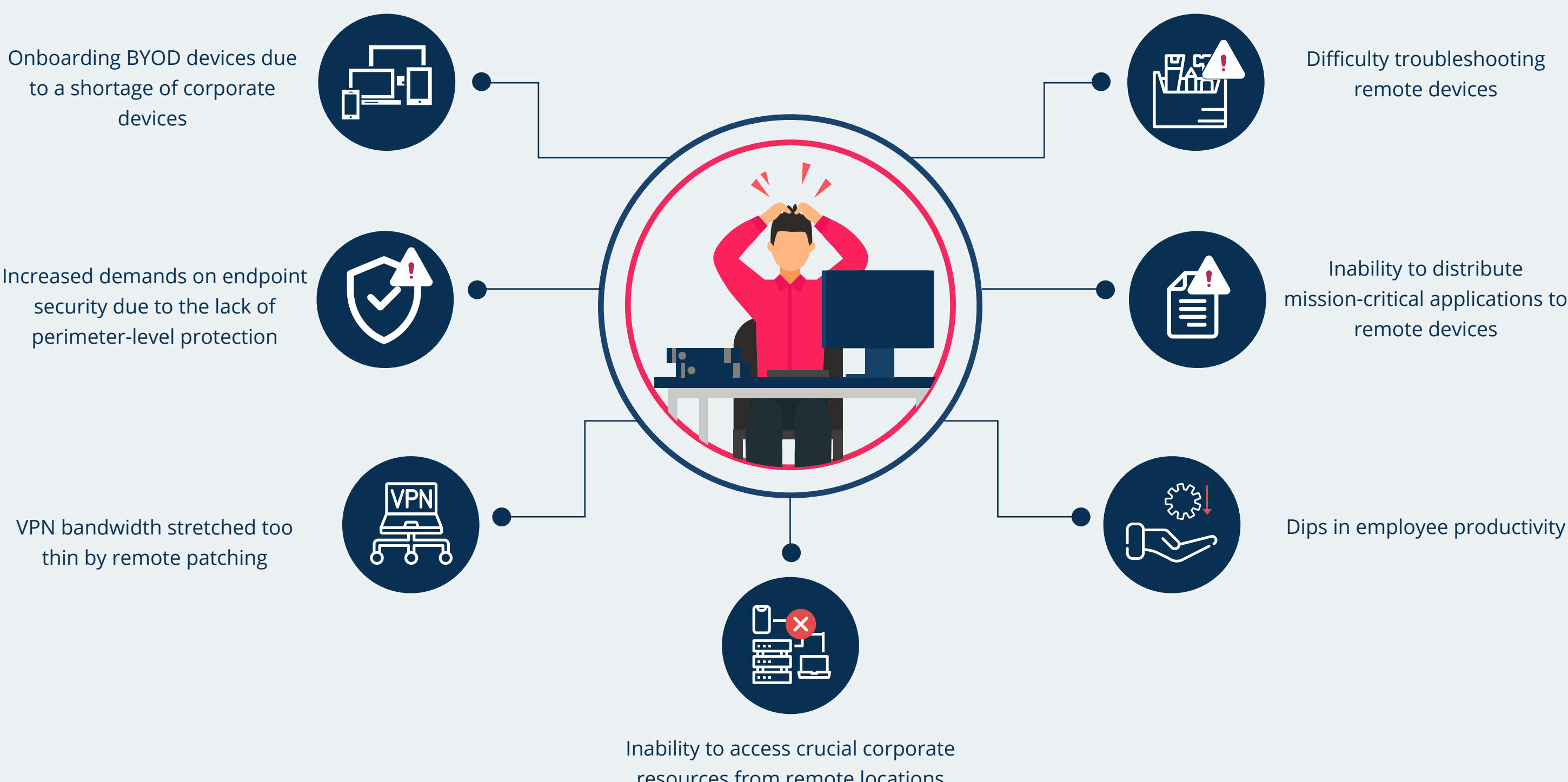


For the first time in the digital era, almost the entirety of the global workforce has shifted to a remote work model to diminish the spread of COVID-19. This unprecedented transition has not only opened up new avenues for security risks, but has also proven to be a challenge for facilitating endpoint management routines and enabling remote access to critical corporate resources.

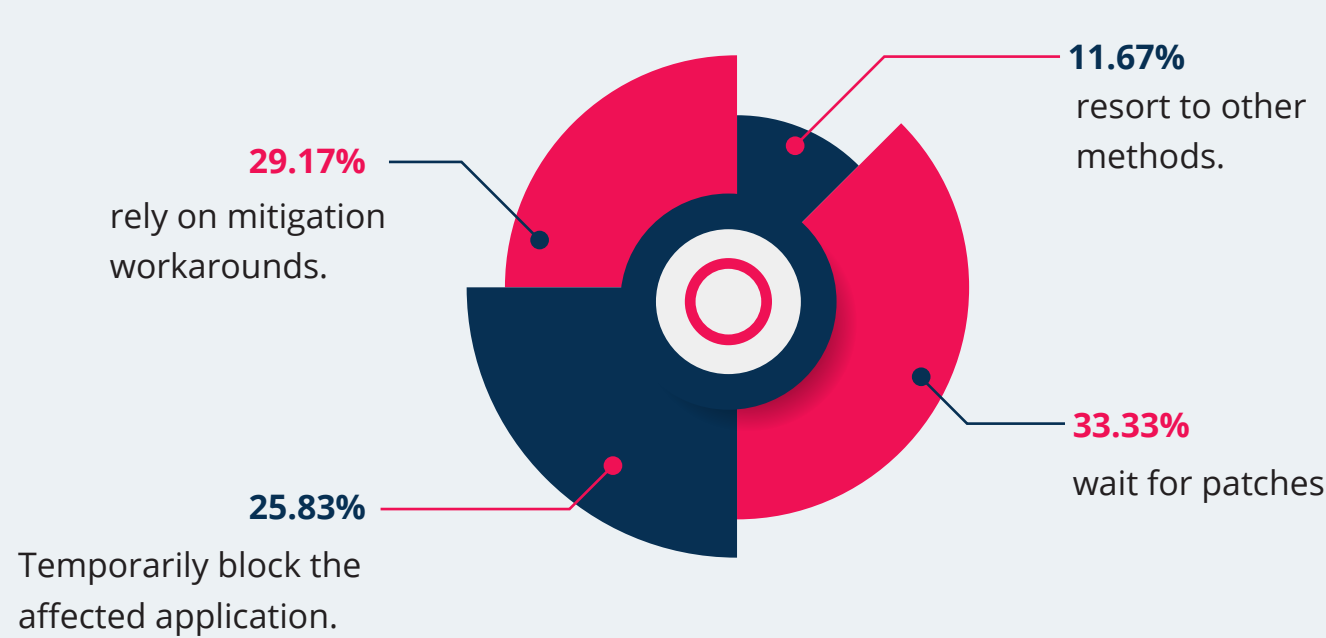
We polled infosec and IT professionals to study the impact of COVID-19 on IT, how they're currently adopting to the remote work scenario, and how to better prepare for the upcoming trends the new norm may bring about.

TOP REMOTE WORK CONCERNS

Among respondents, **47%** admitted that they're facing new challenges now that they're working remotely.



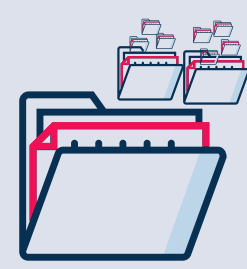
HERE'S HOW ORGANIZATIONS ARE RESPONDING TO ZERO-DAY VULNERABILITIES



More and more organizations are showing readiness to **temporarily block applications** with zero-day vulnerabilities due to increased exposure of endpoints to insecure internet connections.

REMOTE WORK PROMPTS GROWTH OF BYOD AND SELF-SERVICE PORTALS

15% of businesses don't have enough corporate laptops to facilitate remote work. As a result, there's been a surge in the usage of personal devices for work.



43% of surveyed organizations provide end users with a self-service portal to install licensed software needed to perform their daily routines.

73% of companies that require remote users to connect via VPN for vulnerability and patch scans have experienced bottlenecks and a significant drop in update deployment speeds.

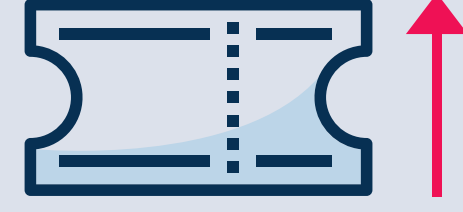


PATCHING COMPLEXITIES HAVE BEEN AMPLIFIED



48% of organizations had to grant remote users the flexibility to postpone patch deployments and subsequent reboots to prevent disruptions in productivity.

On average, IT admins now receive **25** help desk tickets a day. **43%** of respondents revealed that they receive more tickets while employees are working remotely.



IT FACES A STEEP INCREASE IN HELP DESK TICKETS



Most admins said they work an extra **2.5 hours** on average to resolve help desk tickets and troubleshoot issues.

46% of admins employed remote access tools for troubleshooting.

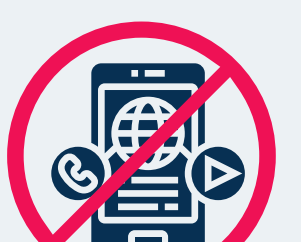


INCREASED SECURITY DEMANDS ON CORPORATE DEVICES DUE TO LACK OF PERIMETER PROTECTION

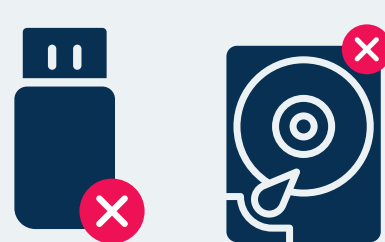
45% of respondents had to enforce restrictions, such as disk encryption, on users' corporate devices.



42% blacklisted social media and gaming applications as they can cause employees' productivity to decline while working remotely.



38% prevent untrustworthy devices from connecting to remote computers.



70% adopted endpoint-level browser security controls to restrict access to malicious web content in the absence of proxy servers or DNS filtering.



Just over three-quarters of respondents answered that their organization is an essential service that has to run despite the pandemic, but **26%** of them work with tools that aren't conducive to remote work. In light of the endpoint management changes brought on by remote work, investing in the right technology is in many ways more important than ever.

THE ULTIMATE HUB FOR IMPECCABLE REMOTE WORK

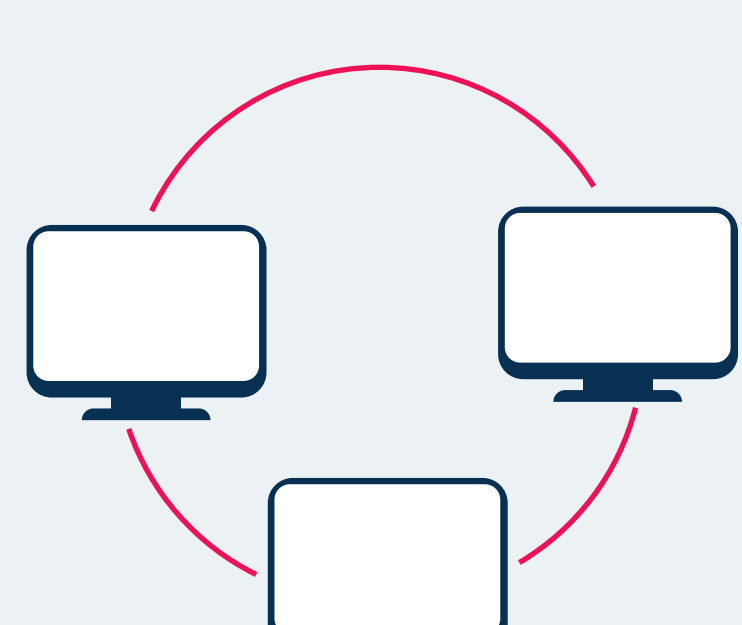
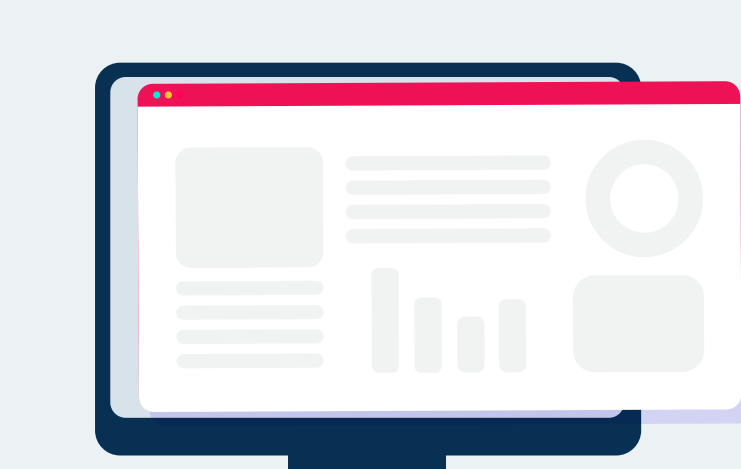
Whether it's a sudden shift towards remote work in response to the pandemic or keeping up with future trends, ManageEngine's unified endpoint management and security solutions are the go-to tools to empower your distributed workforce with safe and efficient working conditions. Our vast array of robust solutions offer:

- Remote monitoring and troubleshooting
- Zero Trust based application and device control
- BYOD and modern device management
- Corporate data containerization
- Remote OS and software deployment
- Web filtering and browser security
- Vulnerability and security configuration management
- Effortless access to corporate resources
- Remote patching without VPN constraints
- Seamless employee onboarding

HOW CAN OUR ENDPOINT MANAGEMENT AND SECURITY SOLUTIONS ENABLE UNINTERRUPTED REMOTE WORK?

WEB-BASED SOLUTIONS

All our solutions are web-based. A device with internet connectivity is all you need to gain a bird's-eye view of your global hybrid IT and conduct all your endpoint management and security tasks from anywhere, anytime.

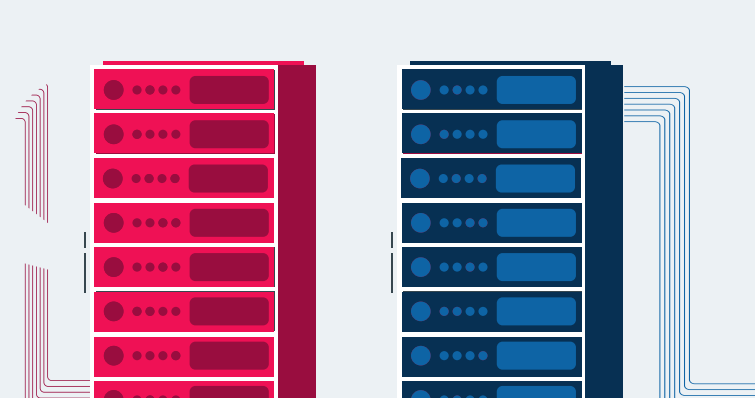


REMOTE CLIENT AGENTS

Concerned about endpoints plugging in to the network? Leverage our agent-based technology to perform uninterrupted endpoint management and security tasks across your distributed IT infrastructure without relying on VPN connectivity.

DISASTER MANAGEMENT

With the failover server option to take over in case the primary server fails, you can maintain business continuity and eliminate downtime.



SO, WHAT ARE YOU WAITING FOR? EQUIP YOURSELF WITH ALL THE ESSENTIALS FOR MANAGING AND SECURING YOUR REMOTE WORKFORCE.

Grab your gear