SCC

Smarter technology for all

Lenovo

Improve security by loosening control

4 steps to protecting the new global workspace.

Remote working is here to stay

The makeup of today's workforce has changed radically. While it spans some five generations, the majority of workers are digital natives, Millennials and Gen Z born from the 1980s to early 2000s.

The new generations of digital-savvy employees expect a very different work style. The workplace is now where you choose to work, not where you go to work. And for that you need technology that allows you to communicate and collaborate, seamlessly and effortlessly, wherever you want.

This move from office workplace to remote working has been underway for some time. IDC forecast that nearly 75% of the total US workforce would be mobile workers by the end of 2020.

That was before recent events, which has resulted in 72% of companies either encouraging or requiring their employees to work remotely, according to our survey[1].

And that also means it is here for the long-term, with 77% of employees feeling that companies will be more open to remote working once things return to normal.

So with remote working a permanent feature, now is the time to invest in the systems and methods to make the most of the new way of working.

IT challenges of remote working

As the majority of people now have to work remotely, there is a rush to make sure that the systems are in place to let them do so, efficiently and effectively. While there are far better tools for remote work than ever before, they are not suited to all.

Windows 10

The best devices in the world run Windows 10 Pro.

[1] Lenovo internal research, March 2020

There are some workers who use proprietary legacy software or use special tools, such as plotters or high-volume scanners. But IT teams need to be aware of a number of key issues when preparing the business for remote working.

New risks of unauthorized access to PCs and data

When you open remote access ports be careful not to increase the security risk and other consequences. Ransomware attackers are looking for such open ports. Make sure you configure the firewall to restrict remote traffic to known sources.

Demands on IT to deliver support for remote workers

IT service desks are under pressure as they face more calls for help from remote users but can't simply 'drop by' to fix problems. Wait times and time-to-repair are growing as remote support tools need to be added or activated.

Better protection from phishing scams and user error

Email is likely to remain the main means of communication for remote employees. It's a fact that's not gone unnoticed by hackers who are using messages about current events as bait to fool people into clicking on links in malware. The message needs to be reinforced with employees that not all email is as innocent as it may appear. Companies should, as a minimum, insist that all remote-working employees use an antivirus tool on any machine connecting to the corporate network.

Need to secure devices on potentially risky remote networks

Remote working at scale presents a major security challenge. The network edge now encompasses all remote networks–from out-of-office locations to home networks. Where possible, IT teams need to know that those networks are properly set up and secure.

Where company devices are being used, what processes are used to help prevent physical access to valuable company data? If personal devices are being used, what protection is there for preventing computer viruses and malware reaching the core network?

Meeting the threat from this growing device sprawl may mean patching and securing remote endpoints.

Using a VPN to access the corporate network may also help security. But be careful that the sudden growth in traffic doesn't slow performance and cause service interruptions.

Make sure IT is in control

One of the key perils in remote working is the same as the office—human error. Wherever they work, your people will make mistakes. They might click something they shouldn't, send sensitive information to the wrong person or disable protections that get in their way. Most mistakes will be unintentional, some are not. So when it comes to securing the new global workspace, IT has to think differently.

4 steps for IT to safeguard remote working:

1 Ensure remote access doesn't increase risk

The first line of defense is PCs themselves. With security hard-wired in, there are new ways of protecting endpoints from attack, including:

- **Encryption**—self-encrypting drives protect data at rest against loss or theft.
- **Infrared cameras**—for security features like biometric authentication or presence detection to raise alerts in the event of being shoulder-surfed.
- **Virtualization**—creating a virtual desktop infrastructure does offer greater security.
- **Self-healing BIOS**—that automatically restores a computer's basic input/output system (BIOS) to a previously working version if it's attacked or corrupted.
- **WiFi security**—detects and analyses, in real-time, threats from unsafe wireless networks.
- **Tamper switches**—which prevent systems booting up if there's evidence of unauthorized access.

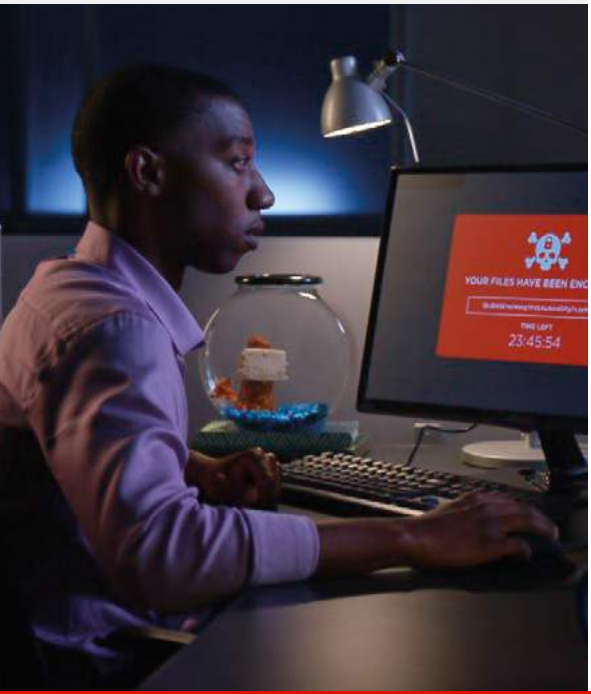
2 Increase endpoint protection

Protect devices wherever they are, in or out of the network. Typically, it can take one minute to detect an attack, 10 minutes to respond and up to an hour to remediate, which may have to include some sort of human intervention. The new breed of endpoint protection solutions has artificial intelligence (AI) on the device, which protects against known and unknown threats in real time.

Strengthen security factors for remote access

Add two-factor authentication (2FA) as an additional layer of protection. If users connect to the network through a VPN make sure you are running the latest version of the software on all machines. If you have a security information and event management (SIEM) logging solution, be aware you will have to change the way it is configured.

You can no longer simply block different locations as users may be coming in from anywhere. If you use the cloud, you may have to check that users working remotely have access to the appropriate bandwidth for the work they need to do and videoconferencing.



3 Allow for inevitable human error

Avoid potential employee mistakes that can make your business vulnerable, such as the non-compliant user.

They might switch off the anti-malware software without thinking, or they may simply be unaware that they and their devices aren't secure.

- **Look for the weakest link**—endpoint detection finds and automatically remediates PCs that are not in line with company policies.
- **Critical means later**—no need to delay vital updates, they can be delivered and applied automatically.
- **Malware isn't the end**—even if an employee clicks on a link to a phishing or other attack, it need not be terminal. Sandboxing can keep malicious files isolated so they cause no damage.

Highlight potential traps
It's easier for hackers to target individuals working remotely, so it's important to educate employees on potential scams. Warn users not to click on unsolicited emails and to only use official websites. Create a central online site where users can go for information about known problems, including links to national and international security alert systems.

Update acceptable use policies
This will help to cover your people's personal devices.

4 Think security first

New technologies create different risks. The customer service app that has just been launched is storing confidential information that can be hacked. And hackers are getting cleverer about the way they do it. The malicious minded are harnessing AI to mount co-ordinated strikes that are more powerful than anything before.

Old technology is unlikely to help. You need to have security built-in from the start of any new project or you will end up in security debt. Trying to retrofit security is ten times more expensive and not always successful.

The best way to fight the new is with the new. In particular, the way to combat evolving, AI-based threats is through even more advanced AI and machine learning solutions for intrusion detection and threat remediation.

Find out more

To find out how to secure the future of remote working in your business:

Visit: **www.lenovo.com/remoteworking**

Or email: online@scc.com