Proactive endpoint protection starts here

Capitalize on the advantages of cloud-based architectures for security — including fewer assets on endpoints, a smaller attack surface, and simple, fast updates.

Use case

Endpoint protection is the greatest challenge facing today's IT professionals. Securing an enterprise feels like a moving target when attacks continuously evolve. And as more and more users access their devices on the go, tools and processes designed for corporate networks are becoming less and less effective.

Now is the time to transition out of defense mode. A proactive security mindset rethinks the traditional endpoint model with cloud computing. On a central cloud platform, it's easier to track and update software. Monitoring information assets when they're stored and shared in the cloud rather than on vulnerable endpoints has innumerable security advantages as well.

Lenovo and Google Chrome OS help organizations optimize their approach to digital security.

68% of organizations have experienced one or more endpoint attacks that compromised data or IT infrastructure.[1]

Situation and challenges

Time-strapped IT
Teams expend tremendous effort managing hundreds of distributed devices.

User error
Users accidentally visit malicious sites, download unknown apps, or prevent software updates.

Data in danger
Traditional endpoints store intellectual property, personal information, and user credentials that can make or break a business if exposed.

Poorly enforced boundaries between processes
A single compromised software module can give attackers access to the entire system and the corporate network.

chrome OS

Smarter technology for all

Lenovo

An enterprise cloud solution

Chrome OS is Google's business-focused solution for Chrome devices, the Chrome browser, and Chrome OS. Chrome OS offers cloud-first tools, integrations with third-party products, and 24/7 support for IT administrators.

Security scenarios

The threat	The scene	The proactive block	The win
Ransomware	A Chromebook user clicks on a link to download a file, and malicious code attempts to encrypt all data and files on the device.	Sandboxing technology limits threats to a single application or Chrome browser tab to keep the rest of the OS secure and prevents malicious apps or websites from installing malware.	The actions of the code are contained within a single process sandbox. The user sees a prompt that they can't run the file, and the attack is halted before it can reach any user data.
Rootkit	A cybercriminal gains access to a Chromebook and obtains super-user privileges. They remount the root partition read-write directly, then add a rootkit in the form of a kernel module.	Verified boot ensures the firmware and OS haven't been tampered with or corrupted in any way after a reboot, reverting to a previous version of the OS if so.	On the next reboot, the signature of that part of the root partition doesn't match the expected signature. The boot process stops and the device reboots using the backup image of the firmware and OS. The cybercriminal can no longer use the rootkit to control the device.
Phishers	A manager receives a plausible email from the CEO to wire $20,000 to a new supplier immediately in order to lock in a supply of a component that's in very short supply.	Google Safe Browsing enables warnings to appear automatically when users attempt to navigate to dangerous sites that might contain malware or download malicious files.	When the employee clicks on a link in the email to the new vendor's website, they receive a warning that the site is deceptive and are invited to click a "Back to Safety" link on the warning screen.
Snoopers	A CEO and CFO are going overseas to negotiate a critical deal. If their strategy sessions are overheard by the other party, it could be costly.	IT can temporarily disable Bluetooth and block the Chrome web applications and browser extensions that could access the microphone and camera on their Chromebooks.	With a ThinkPad® C13 Yoga Chromebook Enterprise, the CEO and CFO also use physical and biometric security features like a webcam privacy shutter and touch fingerprint reader to ensure business assets remain safe throughout the trip.

chrome OS

Smarter technology for all

Lenovo

Secure by design, from the get-go

Lenovo's ThinkPad® C13 Yoga Chromebook Enterprise provides an unbeatable security combination of Lenovo's ThinkShield built-in security suite and Chrome OS.

Learn more at www.lenovo.com/Chrome-OS-Enterprise

Source

1 Ponemon Institute, "The Third Annual Study on the State of Endpoint Security Risk," 2020

chrome OS

Smarter technology for all

Lenovo