chrome OS

Getech
Partner Services

Secure your fleet with Chrome OS

Companies face unprecedented levels of IP, data, and identity sprawl beyond the enterprise firewall. Every endpoint is an entry into businesses and human error on the inside is a constant risk.

Take control of your security with built-in, intelligent security, granular policy controls, and automatic updates for continuous protection from Chrome OS. Safeguard users and data against ransomware, malware, and phishing threats with a read-only OS and encrypted devices. Each layer of Chrome OS's vertically integrated stack reinforces security, while system-wide automatic updates future-proof your protection.

In 2020, the global cyber security market was **valued at $167 billion**[1]

In 2020, data breaches exposed **over 36 billion records**[2]

Protect your business against phishing, ransomware, and malware threats with Chrome OS

Phishing

Google Safe Browsing warns users of malicious sites before navigating to them.

Security keys and 2SV help prevent hackers from using stolen passwords.

If attack prevails, Password Alert Policy requires users to change a password when its used with an unauthorized site.

Ransomware

Low on-device data footprint limits the data that can be held at ransom.

Read-only OS prevents executables and malicious apps from running locally.

If attack prevails, Verified boot confirms the system is unmodified at boot up.

Malware

Per-permission based blocklisting controls what extensions can be accessed.

Managed Google Play facilitates curation by user group and policy configuration by app.

If attack prevails, sandboxing limits attack surface.

[1]Grand View Research, 2021; [2] RiskBased Security, 2020

chrome OS

Ransomware, malware, and phishing protection

Read-only OS: System files are kept in a separate partition to ensure the OS cannot be modified by apps or extensions and is thereby inaccessible to ransomware.

Blocked executables: Executable files, which can harbor malicious threats, cannot run on Chrome OS. Chrome OS only runs curated apps from the Google Play store that have been scanned for malware.

Encrypted hardware: Chrome OS devices are encrypted by default with a unique key, making it difficult for attackers to read user data.This encryption cannot be disabled.

Verified boot: Verified boot ensures the firmware and operating system have not been tampered with or corrupted in any way after a reboot. If it has been, it reverts to a previous version of the OS.

Sandboxing and site isolation: Sandboxing and site isolation limit threats to a single application or tab to keep the rest of the OS secure.

Remote and central management

Management policies: Centrally manage and set Chrome OS devices with over 500 policies, including parameters around sign-on and authentication.

Curated apps and extensions: Block users from installing specific apps and extensions based on permissions required to run. Prevent users from downloading malicious apps and extensions with the managed Chrome Web Store, Google Play Store, and Google Play Protect.

Ephemeral mode (wipe user data on log-out): Set devices to automatically wipe all data and settings after a user logs out.

Lost or stolen prevention (remote disablement and powerwash): Remotely disable or wipe devices if they are lost or stolen and post a message that lets the finder know where to return it.

Manage remote access and single sign-on: Create settings for remote access and SAML-based single sign-on (SSO) so users can access network and web applications with the right balance of security and convenience.

Reporting: Reports are available to show informative data, such as the latest version of the operating system and auto update expiration dates of your fleet.

Automatic updates to keep your fleet secure

Consistent, frequent, and fast updates: Chrome OS firmware and feature updates occur every six weeks, far more frequently than other majority systems. Updates apply on reboot, taking only seconds to complete.

Lower support costs: With Chrome OS, there's no need for costly manual patching or routine updates of the operating system.

No downtime or disruption: Updates happen automatically in the background while users work. Two versions of the OS means that one can be used while the other gets updated, keeping data secure and employees productive.

Manufacturer consistency: All Chrome OS devices, regardless of manufacturer, get the same updates.

→ Learn more about Chrome OS Security: https://chromeenterprise.google/os/security