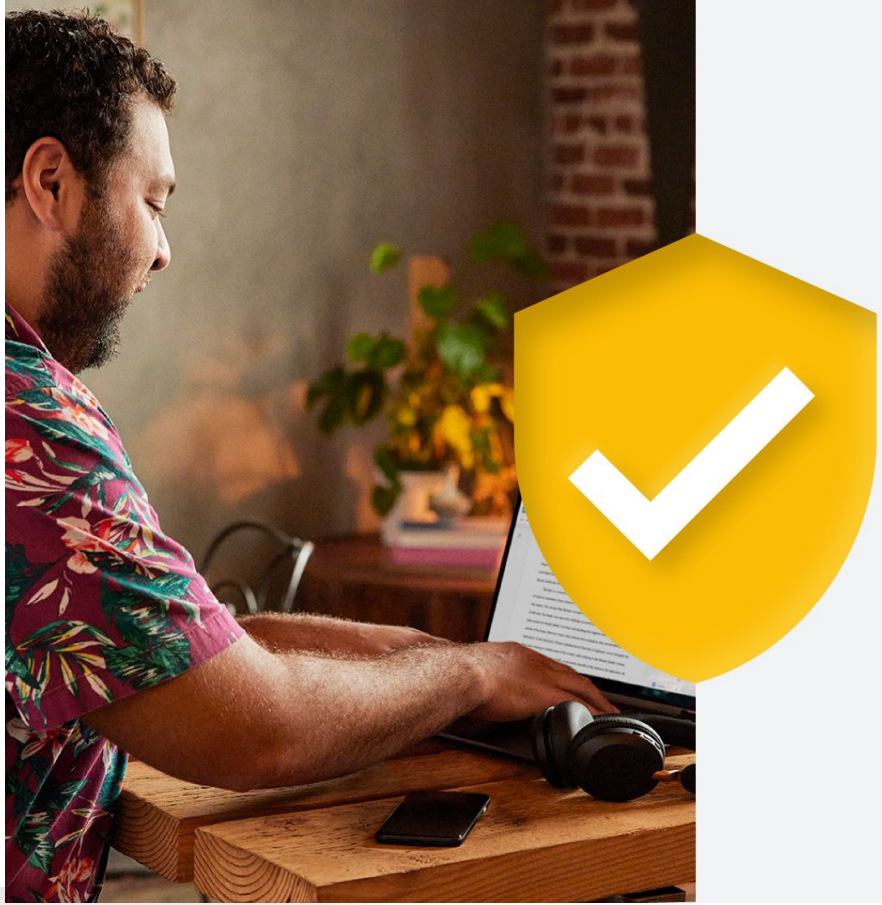
chrome OS SYNNEX

Chrome OS Security & Threat Prevention

Take control of your security with Chrome OS



Cybersecurity crimes are **growing & costly**

Malware

320%

increase in year-over-year reports in **global potentially unwanted applications (PAUs)**[1]

Ransomware

150%

Increase in **global ransomware** in 2020[2]

Phishing

75%

of organizations **experienced a phishing attack** in 2020[3]

chrome OS

Sources: [1] Verizon, 2021, [2] Cybersecurity Ventures, 2020, [3] Tessian, 2020

Employees and human error **put data at risk**

85%

of studied data breaches were **caused by human error**[1]

70%

of IT leaders say employees have **put data at risk accidentally** in the last 12 months[2]

chrome OS

Sources: [1] IBM & Ponemon Institute, 2020, [2] Egress & Opinion Matters, 2019

Factors when choosing an operating system to keep data secure

- Built-in protection from external threats
- Intelligent security to reduce employee negligence
- Customized policies for greater IT control
- Automatic updates for continuous protection

chrome OS

Rethink your approach to security

Chrome OS and browser are secure by design and prevent end users from falling hostage to harmful cybersecurity attacks and their consequences.

chrome OS

Take control of your security with Chrome OS

Built-in, proactive security

- No need for antivirus
- Read-only OS and no executables
- Active threat prevention

Granular, flexible policy controls

- 500+ policies in the Admin console
- Approve or block apps & extensions
- Granular reporting

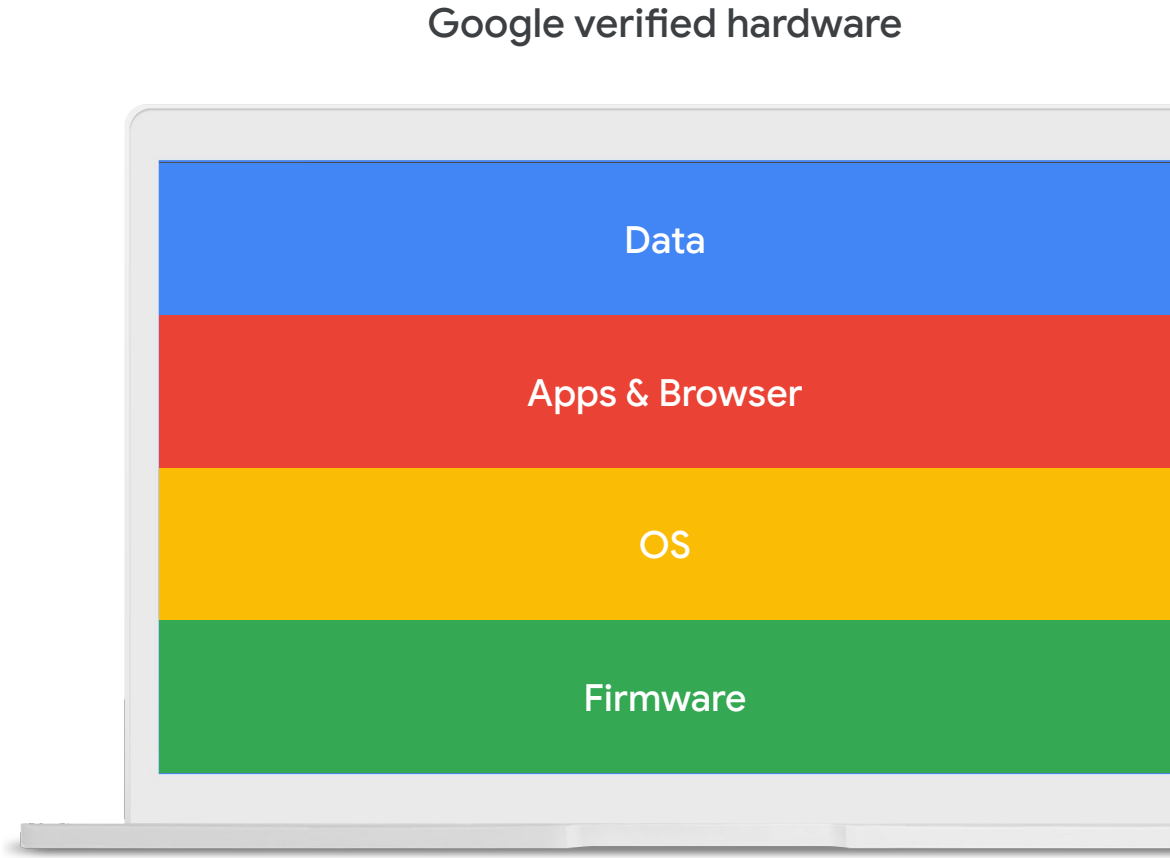
Continuous and automatic updates

- Consistent, frequent and ultrafast
- No downtime or disruption
- Lower support costs

chrome OS

Multi-layered OS architecture

The layers of Chrome OS work together to provide innovative security benefits. OEM manufacturers follow strict hardware requirements.



ZERO

reported ransomware attacks on Chrome OS ever

chrome OS

Source: Bitdefender, 2020

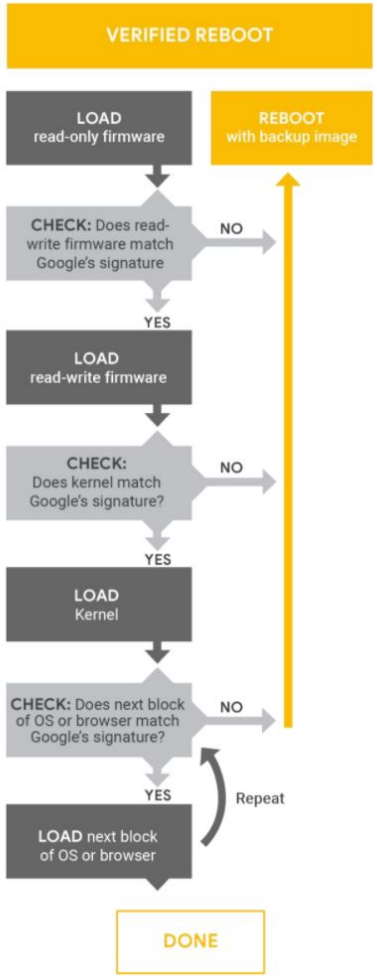
Built in and proactive security to deter negligence and limit attack surfaces

Read-only, tamper-proof operating system backed by Verified Boot

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

Verified boot:

- **Protects against dangerous attacks** by ensuring that the firmware and operating system have not been tampered with or corrupted in any way after a reboot.
- **Detects malware** and stops the reboot process when threats are identified. Reboots the device with a version of the writable firmware and operating system.
- **Enables employees** to avoid work required to remediate compromised firmware and files.



chrome OS

Hardware-backed protection

powered by the Titan C security chip

Continuous security

Designed and updated by Google so you're always protected from the most recent threats.

User protection

Protect from logins on remote devices, brute force attacks, and phishing scams.

System Integrity

Ensure the OS and encryption keys haven't been compromised and enforce policies remotely.

Data and settings encryption

All Chrome OS devices encrypt user data and settings. All data and settings are encrypted with a unique key, meaning that an attacker would always need both the user password and access to the security module. This makes it extremely difficult for attackers to read user data.

This encryption cannot be disabled, allowing colleagues to share loaner devices safely and adopt “Grab and Go” practices.

Blocked Executables

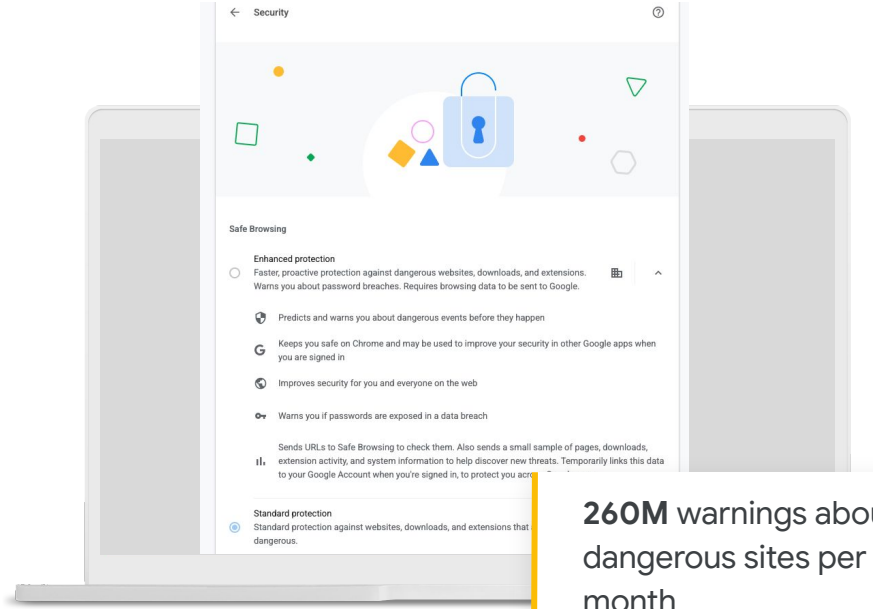
Chrome OS blocks executables from running: Malicious threats often hide in executable files that corrupt your data. These executable files cannot run on Chrome OS, which blocks apps from running that are not from the Google Play Store. .

Google Safe Browsing

Warns users before they attempt to navigate to dangerous sites or download malicious files.

Finds harmful and deceptive content/software by constantly scanning the web and classifying the danger.

Offers scalable and ultra fast support with input from Global Threat Intelligence and hundreds of Google Security Analysts and Engineers.



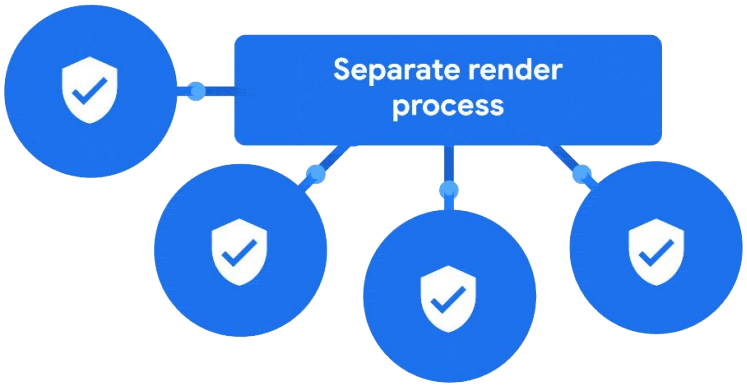
260M warnings about dangerous sites per month

chrome OS

Sandboxing and Site Isolation

Sandboxing limits all security threats to a single application or browser tab to keep the rest of the operating system secure.

Site isolation keeps all processes within each browser tab separating & stopping malicious sites from the rest of the OS.



HTTPS by Default

When a user types an address into the address bar without specifying the protocol, Chrome will attempt to navigate using https first, then fallback to http if https is not available.

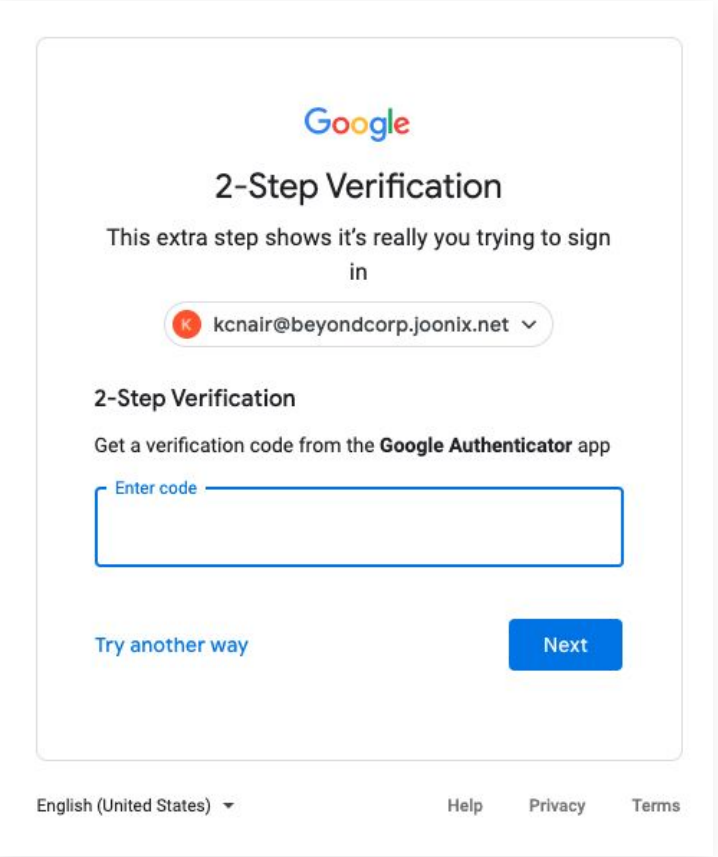
HTTPS by default improves **privacy and loading speed** for users visiting websites that support HTTPS.

Two-Factor Authentication and Single Sign-on (SSO)

Protect employees against phishing attacks by turning on two-factor authentication, which requires users to provide a password and authentication key/code when logging into their Google account.

Set parameters 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.

Enroll special user accounts into the Advanced Protection program, a free program from Google that proves 2FA in addition to other protections.



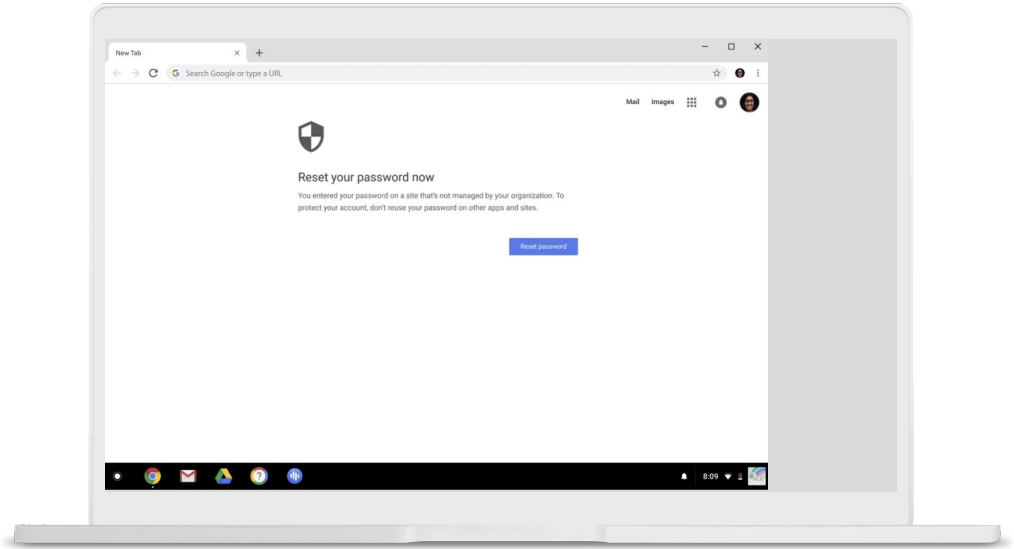
chrome OS

Password Alert Policy

Prevents password reuse by automatically prompting users to change their corporate password if they enter it on an untrusted website.

Protects the integrity of corporate Google and non-Google accounts.

Reduces the potential for a breach, lowering the risk of compliance penalties and fines.



chrome OS

Flexible, comprehensive policy controls

Flexible, comprehensive policy controls

Manage 500+ policies in the Google Admin console, including advanced security controls to protect your fleet.

Restrict apps & extensions:
Block or allow users from installing specific apps and extensions based on the name, category, or device permissions they require to run.

Block external storage devices:
Restrict the use of external storage devices such as USB flash drives and optical storage devices.

Ephemeral mode (wipe user data on log-out):
Set devices to automatically wipe all data and settings after a user logs out. Ephemeral mode makes it safer for shared and short-term users and kiosks.

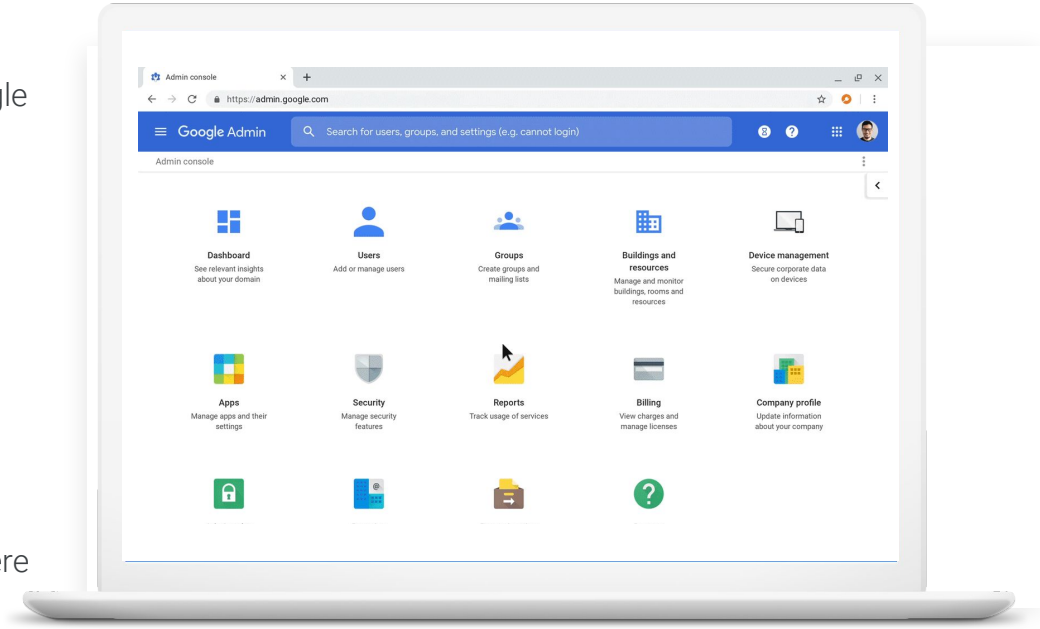
Flexible, comprehensive policy controls

Manage 500+ policies in the Google Admin console, including advanced security controls to protect your fleet.

Manage remote access and single sign-on (SSO):
Set parameters 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.

Deprovision devices:
Remotely deprovision devices and prevent them from accessing corporate resources.

Remote disablement and powerwash:
Remotely disable or wipe devices that have been lost or stolen and post a message that lets the finder know where to return them.



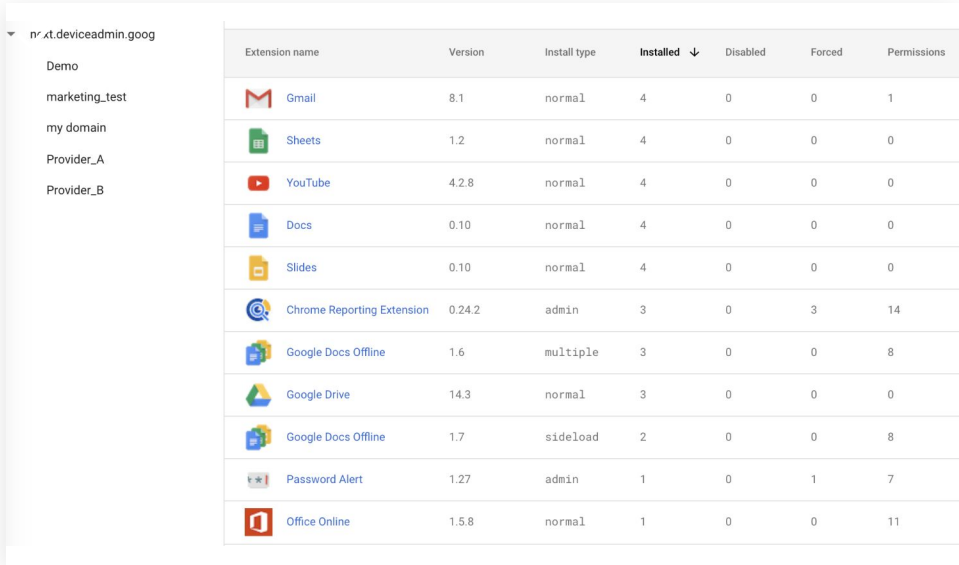
chrome OS

Granular Reporting

Extensions:
Get visibility into version, install type, and permissions around extensions

Version Report:
View all versions of Chrome in your fleet in a daily report

Auto Update Expiration Chrome Insights Report:
See how many Chrome OS devices in your fleet have reached their AUE dates or are expiring soon



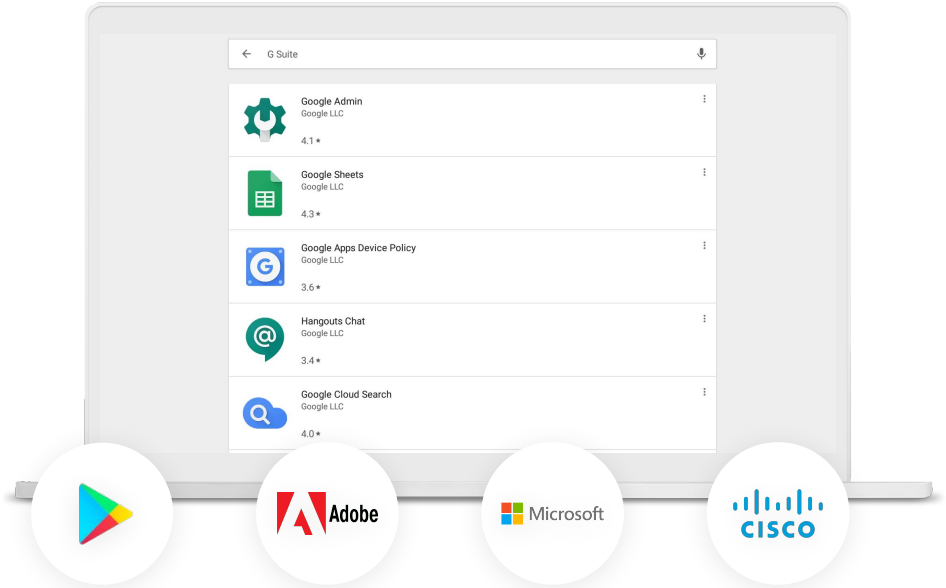
chrome OS

Managed Google Play Store with built in threat detection

Managed Google Play: Provide employees with a curated store containing secure, tested, and approved applications. This prevents users from downloading malicious or vulnerable applications.

Google Play Protect: Google Play Protect is the most widely deployed mobile threat protection in the world with 2B daily users. It continuously scans and verifies apps in the Google Play Store, identifying malware and uninstalling any malicious apps from affected devices.

Configure app-specific policies with managed configuration



Chrome Web Store

The Chrome Web Store:

- **Offers manual and automatic** extension reviews
- **Provides visible permissions** that show users and admins what's required to run the extension
- **Accepts Manifest V3 extensions** for stricter privacy and more control of your data

Inline Installs of extensions are disabled as of mid 2018.

Automatic updates for continuous protection

How Chrome OS automatic updates provide continuous protection

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

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

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

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

chrome OS

Why Chrome OS doesn't need third-party antivirus

- **Read-Only OS** does not allow installed apps and extensions to modify it
- **Sandboxing** isolates any attack to a limited surface
- **Verified Boot** prevents boot up of tampered devices
- **Review Process** is required for all extensions and apps
- **Low on-device footprint** means less data at risk of attack

Protection from Phishing Attacks

Common Attack

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.

chrome OS

Protection from Ransomware attacks

Common Attack

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

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

If attack prevails: Verified Boot confirms the system is unmodified or tampered at boot up.

chrome OS

Protection from Malicious Apps & Extensions

Common Attack

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

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

If attack prevails: Sandboxing and site isolation limit attack surfaces.

chrome OS

BeyondCorp Enterprise

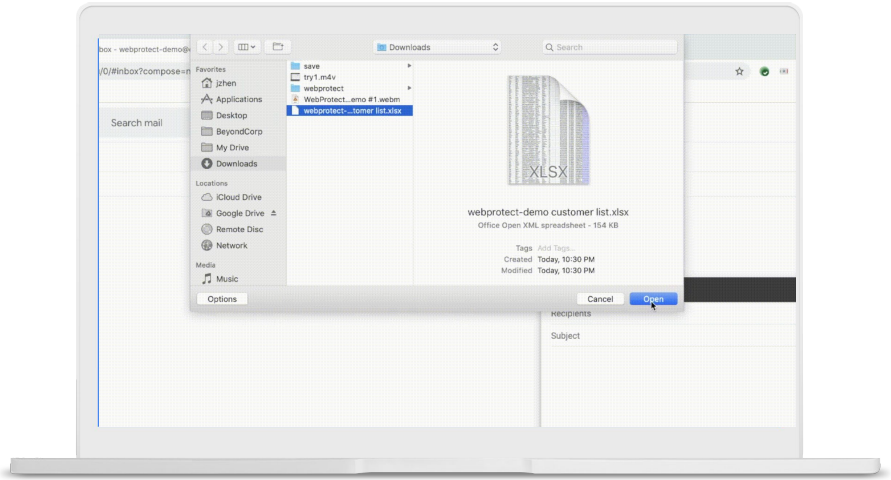
Advanced capabilities available in Chrome with BeyondCorp Enterprise

Real-Time Phishing and Malware Protections — Enhanced Safe Browsing and malware scanning reduces threat to your users

Sensitive Data Protection — Prevents both accidental and intentional exfiltration of company data

Visibility and Insights — Supports remediation efforts, compliance reporting, and overall security hardening efforts

Easy Configuration and Management — Apply security and data protection policies across Chrome, with built-in auto-updates



chrome OS

It’s time for a change

Rethink your security

chrome OS