chrome enterprise

Keep your business safe in a cloud world

Organisations are spending a great deal to improve their security with products that claim to fend off hacks, espionage and vulnerability. But despite their efforts, the number of breaches continues to increase.

In 2019, the security information market is forecast to **increase by 8.7% to $124 billion**[1]

In parallel, the number of large, targeted breaches in the US is **growing by over 27%** per year[2]

While these threats may be growing in volume and sophistication, the types of attacks are already familiar to us: primarily malware, ransomware and phishing. Evidently, the traditional approach to security is no longer effective, and it's time to look for a new solution to an old problem.

Take a unique approach to endpoint security with Chrome Enterprise

Multi-layered device security

Each layer of a Chromebook works together to provide unique security benefits.

- Encrypt user data
- Prevent OS tampering
- Reduce on-device data footprint
- Regularly patch and update
- Deter user negligence

Isolated and managed apps

Make sure that harmful apps are kept out of users' hands.

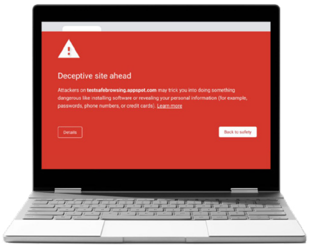
- Limit the attack surface with sandboxing
- Enforce access policies
- Secure multiple ecosystems, including Chrome Web Store, Google Play, web and native Linux apps

Data
App & Browser
OS
Firmware

[1] Ponemon and Accenture, 2017; [2] Gartner, 2018

chrome enterprise

Protect your enterprise against familiar threats with Chrome Enterprise and the power of Google Cloud



Deceptive site ahead

Attackers on **testsafebrowsing.appspot.com** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards). Learn more

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 an attack prevails: Password alert policy requires that users change a password when its used on an unauthorised site.

Ransomware

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

Read-only OS prevents executables from running locally.

If an attack prevails: Verified boot confirms the system is unmodified at boot-up.

Malicious apps

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

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

If an attack prevails: Sandboxing limits the attack to the surface.

Why Chromebooks don’t require antivirus

Read-only; installed apps and extensions can’t modify OS.

Sandboxing isolates any attack to a limited surface.

Verified Boot prevents the boot-up of tampered device.

Review process required for all extensions and apps.

Why Chromebook updates are so effective

No downtime; updates take place in the background while users work.

Two versions of OS on a device means that one can be used while the other is updated.

Update applies on reboot taking a matter of seconds to complete.

Learn more about Chrome Enterprise security:
cloud.google.com/chrome-enterprise/security