Keep your business safe in a cloud world

Organizations are spending big 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

In parallel, the number of large, targeted breaches in the U.S. is growing by over 27% per year

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**

Ensure harmful apps are kept out of users’ hands.

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

¹ Ponemon and Accenture, 2017; ² Gartner, 2018
Protect your enterprise against familiar threats with Chrome Enterprise and the power of Google Cloud

### 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 from running locally.
- **If attack prevails: Verified boot** confirms the system is unmodified at boot up.

### Malicious apps

- **Per-permission based blacklisting** 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.

---

### 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 boot up of tampered device.
- **Review process** required for all extensions and apps.

---

### Why Chromebook updates are so effective

- **No downtime**: updates happen in the background while users work.
- **Two versions of OS** on device means one can be used while the other gets updated.
- **Update applies on reboot** taking a matter of seconds to complete.

---

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