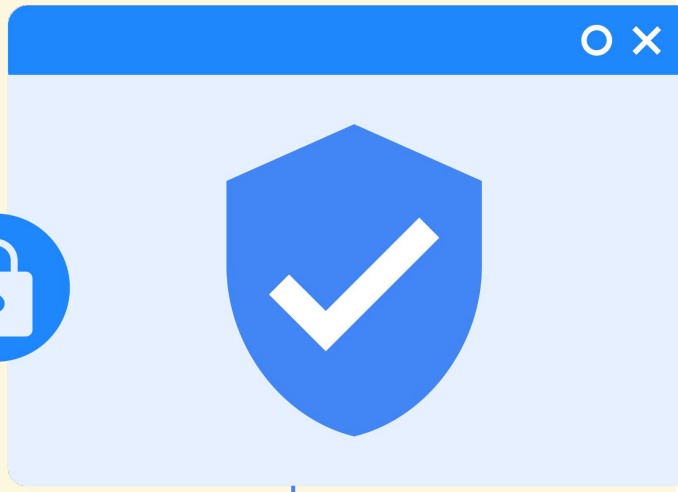
chromeOS

Deploying ChromeOS for Better Security Outcomes



88% of data breach incidents are caused by employee mistakes.[1]

It took businesses **13% longer** to bounce back from a ransomware attack between 2021 and 2022.[2]

chromeOS

How do ransomware attacks happen?

Employee error is responsible for the majority of ransomware attacks.

In a recent IDC survey,[3] companies said that their latest ransomware incident that blocked access to systems or data was caused by:

- 9% were insider threat (malicious insider)[2]
- 14% were malware stored on peripheral devices or removable media inserted into a system[2]
- 15% clicked on a malicious URL from a phishing email[2]
- 18% opened a malicious attachment in a phishing email[2]
- 11% were unable to determine the source of the initial compromise[2]
- 15% were supply chain attacks including SolarWinds, PC Cleaner, or Kaseya[2]
- 17% were drive-by compromises: malicious adversaries gained access over the normal course of internet browsing[2]

1. Just Why Are So Many Cyber Breaches Due to Human Error?, Security today, 30 July, 2022
2. IDC's Future Enterprise Resiliency and Spending Survey, Wave 7, August 2022; n = 829; Data weighted by country GDP (500+ employees)
3. IDC Use Case Brief, sponsored by Google ChromeOS, Deploying ChromeOS for Better Security Outcomes, doc #US50058623, March 2023

chromeOS

Decrease how often and how many security incidents happen

ChromeOS not only improves your security and compliance but also decreases the severity of attacks that land.

1 in 3
respondents said security was a top reason for choosing ChromeOS.[4]

Organizations using ChromeOS reported:

29%
less risk of security incidents.[4]

24%
less frequent security attacks.[4]

Faster OS / application updates[4]

More efficient incident management[4]

Faster security updating and patching[4]

Reduced frequency of reimaging[4]

4. IDC Use Case Brief, sponsored by Google ChromeOS, Deploying ChromeOS for Better Security Outcomes, doc #US50058623, March 2023

chromeOS

Tap into the power of ChromeOS

Secure your fleet

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

Protect your business against potential threats

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 happens, Password Alert Policy requires users to change a password when it's used with an unauthorized site.

Ransomware

- Low on-device data footprint limits the data that can be held at ransom.
- Read-only OS stops executables and malicious apps from running locally.
- If an attack happens, Verified Boot confirms the system is unmodified at boot up.

Malware

- Per-permission based blocklisting controls which extensions can be accessed.
- Managed Google Play allows curation by user group and policy configuration by app.
- If an attack happens, sandboxing limits the attack surface.

Get started today and protect your business with the secure, compliant, and modern ChromeOS.