Don’t trust anyone

Human error, privilege misuse, stolen credentials and social engineering account for three-quarters of all data breaches.

Up-to-date antivirus definitions can’t protect against those. Here’s how ChromeOS and Google Workspace can.

According to the Microsoft Digital Defence Report, data exfiltration doubled in the year to October 2023. Although most cyber attacks have a financial motivation — the theft of business-critical data or personal information such as employee bank details or student medical records — others can involve simple mistakes caused by your users to wreak unintentional chaos on your IT infrastructure.

Ransomware still accounts for a significant proportion of cyber attacks, holding steady at around a quarter of the overall threat landscape. Thankfully, there have been no reported ransomware or malware attacks on a ChromeOS device — ever — but there are many institutions in the UK still to adopt Google’s cloud-native operating system, leaving them at risk.

Proper cyber security means protecting the devices we all use. Even if your organisation is committed to keeping your endpoints on the thicker side of mobile thin clients, Google offers a vast array of features you can take advantage of to protect your users and data from online (and offline) security issues.

There have been no reported ransomware attacks on a ChromeOS device — ever

ChromeOS has 98% fewer vulnerabilities than Windows and no known live exploits

Gmail is the top-ranked email provider, blocking over 99.9% of cyber attacks

Google Workspace helps save up to 50% on cyber insurance premiums (At-Bay[1], 2023)

Risk	Reality	Google's resolution
Unmanaged endpoints	Unmanaged Windows devices account for up to 90% of breaches. (Microsoft[2], 2023)	Chrome Education Upgrade empowers IT admins to set over 600 policies tailored to the needs of their organisation, use cases or users at a group or individual level.
Lost or stolen devices	The more portable an asset is, the more it needs protection against loss or theft.	ChromeOS devices have several options to protect against data loss even after the event, such as forced re-enrolment, remote disable, restricted sign-in and ephemeral mode.
Weak passwords	Almost three-quarters of people who have tried to guess someone's password have been correct. (Beyond Identity[3], 2021)	Google Workspace allows admins to enforce password requirements, make users with weak passwords change them, set minimum character length and prevent reuse of common words and phrases.
Stolen credentials	Almost half of external breaches involve the use of stolen credentials.	Multi-factor authentication is enforced via the Google Admin console without the need for third-party apps. Context-aware Access can control criteria that must be met, such as location and WiFi network.
Social engineering	Phishing attacks account for 36% of all data breaches, with the UK representing the prominent target for attacks in Europe. (Proofpoint[4], 2023)	Gmail's suite of protections, including ML models powered by TensorFlow, automatically blocks more than 99.9% of spam, phishing and spoofing emails.
Malicious software	Downloading files from third-party websites and email attachments poses serious security concerns.	The National Cyber Security Centre expressly advises that apps and software should only downloaded from official marketplaces such as Google Play. Admins can also auto-install and pin apps their users need based on organisational units.
Email attachments	Email attachments are fundamentally flawed, causing data sprawl, multiplication of files and custody loss once sent.	Providing users with a cloud-based architecture such as Google Workspace encourages them to share assets via links or directly from apps like Google Drive rather than sending and receiving potentially harmful attachments.
Unauthorised file sharing	From accidentally sharing a file with the wrong email address to disgruntled employees selling sensitive information — access is a risk.	IT admins have access to a unified security dashboard to quickly identify files that have been shared outside their domain or triggered DLP rules and take action to neutralise organisation-wide security or privacy issues in seconds.
Outdated software	Downloaded applications need frequent patching as we uncover new vulnerabilities — this is also true for operating systems, virus definitions and hardware drivers.	IT admins can control updates for ChromeOS and applications, pinning Chrome versions as desired, so users always have access to the tested and trusted platforms they need.
Accidents and user error	1 in 5 cybersecurity breaches involve internal actors caused by carelessness, lack of awareness or simple human error. (Verizon[5], 2023)	ChromeOS devices benefit from process sandboxing, so if a user does inadvertently access a malicious website or application, the threat is automatically contained and removed when the tab or window is closed.
Privilege abuse	Restricting admin rights has seen a decline to 67% in 2023, impacting basic cyber hygiene policies. (UK Government[6], 2023)	IT admins can delegate a variety of limited administrator privileges to individuals within their organisation, so users only have the permissions they are required to have.
OS vulnerabilities	Windows 11 has 600 known vulnerabilities, including active public exploits as of February 2024. (SecurityScorecard[7], 2024)	ChromeOS receives automatic updates every four weeks and extra security patches every 2-3 weeks without disrupting users. Long-term Support channel is available for maximum stability.

[1] https://www.at-bay.com/ranking-email-security-solutions

[2] https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

[3] https://www.beyondidentity.com/blog/over-1000-americans-divulge-their-password-habits-survey

[4] https://www.proofpoint.com/uk/newsroom/press-releases/proofpoints-2023-state-phish-report-reveals-email-based-attacks-dominated

[5] https://www.verizon.com/business/resources/reports/dbir/

[6] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023

[7] https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-102217/Microsoft-Windows-11.html

Getech