

# Chromebook and Google Workspace security

## Protect Chrome OS users from advanced threats

Chromebooks are an increasingly popular alternative to traditional Windows and macOS devices — particularly in schools and educational institutions — due to their affordability, ease of use, and integration with Google Workspace productivity tools.

### Chromebook users need stronger security

While Chrome OS may generally be considered more secure than other traditional operating systems, with built-in security features like automatic updates and sandboxing, Chromebook users are still vulnerable to a broad range of security risks. Potential threats include malicious browser extensions and websites, phishing attacks, Google account credential compromise, and more.

**Sophos provides layered protection against threats targeting Chromebook and Google Workspace users through a portfolio of integrated solutions, all deployed and managed through a single, cloud-based cybersecurity platform.**



Prevent Chromebook users from accessing malicious and inappropriate websites.



Identify unwanted browser extensions installed on Chromebooks.



Detect attempts to install dangerous Android Apps on Chromebooks.



Block email-borne attacks including phishing and business email compromise.



Detect, analyze, and neutralize threats targeting Google Workspace.



Sophos MDR experts investigate and respond to sophisticated threats on your behalf.

### Key features

- Protect against threats that Chrome OS security features miss, including malicious browser extensions and websites, dangerous Android apps, and more.
- Sophos' direct integration with Google Workspace enables rapid threat detection, investigation, and response.
- Auto-install a proprietary Chrome security extension for “agentless” security on Chromebooks.
- Manage your security in-house or benefit from a fully managed 24/7 detection and response services from the world's leading MDR provider.

## Threat: Inappropriate and malicious websites

Chromebooks offer Restricted Mode and Safe Search features to help mitigate risks from malicious websites. Still, they have known limitations, leaving your users at risk of accessing malicious and undesirable web content.

- ▶ **Solution:** Sophos offers a proprietary Chrome security extension<sup>1</sup> that blocks websites with malicious, undesirable, or illegal content — based on your organization's policies and powered by the latest threat intelligence from our expert research unit, Sophos X-Ops.

## Threat: Dangerous browser extensions

Chromebook users may unknowingly install harmful extensions from the Chrome Web Store or other sources that can steal data, inject ads, or perform other malicious actions. While Chrome OS provides basic protection from commodity malware, it can still be affected by more advanced threats introduced through malicious browser extensions or compromised websites.

- ▶ **Solution:** Sophos<sup>1</sup> identifies unwanted browser extensions on Chromebooks, enabling you to prevent their use by threat actors.

## Threat: Malicious Android apps

Chromebooks allow the use of Android apps from the Google Play Store, and users can also sideload apps from third-party app stores. While adding functionality, the ability to run Android apps can also introduce potential security risks, like providing access to sensitive data and exposing Chromebook devices to malicious software.

- ▶ **Solution:** Sophos detects attempts to install dangerous apps and prompts users to remove them<sup>1</sup>.

## Threat: Compromised Google account credentials

Chromebooks rely on Google accounts for login and provide access to all Google Workspace apps and services, such as Gmail, Google Drive, Google Docs, Google Sheets, Google Slides, and more. If an attacker gains access to a user's Google account credentials, they can access all associated data and services.

- ▶ **Solution:** Sophos integrates directly with Google Workspace, providing you with greater visibility into suspicious activity and the ability to detect and stop threats more effectively<sup>2</sup>.

## Threat: Phishing and business email compromise

Despite the device's built-in security features, Chromebook users are not immune to email-borne attacks. Attackers use deceptive emails or websites to trick users into revealing personal information or login credentials.

- ▶ **Solution:** Sophos integrates directly with Google Workspace to enhance your organization's email security posture and protect against a wide range of email-borne threats, including phishing and business email compromise<sup>3</sup>.

## Benefits

- ▶ Comprehensive security for Chromebooks and Google Workspace that extends beyond built-in tools.
- ▶ Easy to deploy: Simply install a Sophos Chrome extension and activate our API-based Google Workspace integration.
- ▶ Easy to manage: Protect your Chrome OS, Windows, macOS, and Linux devices from a unified cloud-based cybersecurity console.
- ▶ Peace-of-mind protection from a trusted cybersecurity leader. Sophos solutions protect over 600,000 organizations worldwide.
- ▶ Sleep easy with strong protection, delivered exactly how you want it. Let Sophos manage threat detection and response on your behalf.

## Advanced protection against threats targeting Google Workspace

Google Workspace includes some built-in security controls, but investigating, validating, and responding to threats can be challenging for under-resourced security teams. You need granular visibility across your entire IT environment to defend against active adversaries effectively.

### Sophos XDR: An open AI-native SecOps platform

Sophos Extended Detection and Response (XDR) correlates data from a broad ecosystem of products and technologies — **including Google Workspace** — providing full visibility across your applications, tools, and security components. By ingesting and analyzing security data from Google Workspace, analysts can rapidly identify and investigate potentially malicious activity, including:

- Suspicious Google Account logins.
- Activity associated with suspended user accounts.
- Anomalous changes to administrator settings.

Powerful generative AI tools make it easy for users of all skill levels to conduct threat investigations using the Sophos XDR platform.

Learn more at [sophos.com/xdr](https://sophos.com/xdr)

### Sophos MDR: 24/7 managed detection and response service

**Sophos Managed Detection and Response (MDR) is a fully managed service that provides 24/7/365 security monitoring across your entire IT environment.**

By analyzing security data from Chromebooks<sup>1</sup> and Google Workspace in the Sophos data lake, our experts investigate and respond to threats on your behalf, such as unauthorized Google Account access and malicious Gmail activity.

Sophos MDR analysts also identify previously unseen threats by monitoring network activity<sup>4</sup> for suspicious patterns, including malicious traffic from unmanaged systems, rogue assets, applications on Chromebook devices, and more.

Learn more at [sophos.com/mdr](https://sophos.com/mdr)

The screenshot displays the Sophos Threat Analysis Center (TAC) interface. The top navigation bar includes 'Dashboards', 'My Products', 'Threat Analysis Center', 'Alerts', and 'More'. The left sidebar shows the 'Threat Analysis Center' menu with sections for 'DETECT' (Dashboard, Cases, Detections), 'INVESTIGATE' (Investigations (Legacy), Search, Threat Graphs, Live Discover), and 'SETTINGS' (Integrations, Configured, Marketplace, Preferences). The 'Integrations' section is highlighted.

The main content area is titled 'Google Workspace' and includes a breadcrumb trail: 'Overview / Threat Analysis Center Dashboard / Integrations / Google Workspace'. It features the Google logo and a green checkmark indicating that Google Workspace is 'Included'. Below this, there are buttons for 'API' and 'Sophos XDR'. A 'Summary' box describes Google Workspace as a comprehensive suite of cloud-native productivity and collaboration tools that enhance organizational workflows and communication. It lists various tools like Gmail, Calendar, Meet, Chat, Drive, Docs, Sheets, Slides, Forms, Sites, and more, noting that these generate a spectrum of alerts pertaining to user activities, permissions, and data interactions within its environment. The Google Workspace API is identified as the data ingestion API.

Below the summary, there is a section titled 'Data Ingest (Security Alerts)' with an 'Add Configuration' button. It explains that Google Workspace can be configured to send security alerts to the Sophos Central platform via API. Received alerts are enriched and correlated into related groups, and some are escalated into cases.

The bottom section is titled 'Configured Google Workspace Integrations' and includes a search bar. Below the search bar is a table with columns for 'Name', 'Vendor', 'Connection Method', and 'Status'. The table is currently empty.

Sophos correlates security data from hundreds of tools and technologies, including Google Workspace.

## Simplify cybersecurity management

**Spend less time managing security for your Chromebook and Google Workspace users.**

Sophos Central is an adaptive AI-native cybersecurity platform that unifies all Sophos next-gen security solutions in a single cloud-based management console. It simplifies cybersecurity management, automates threat responses, and provides real-time insights, reducing administrative burden and enhancing overall security efficiency.

If it needs protecting, we can help you secure it: endpoints (including Chromebooks), servers, mobile devices, public cloud, firewalls, email, wireless, ZTNA, and more.

Learn more at [sophos.com/central](https://sophos.com/central)

To learn more about how Sophos delivers comprehensive cybersecurity for Chromebooks and Google Workspace, speak with a Sophos expert today.

1 Subscription: Sophos Intercept X for Mobile or Sophos Mobile Advanced

2 Subscription: Sophos XDR or Sophos MDR

3 Subscription: Sophos Email Advanced

4 Subscription: Sophos NDR

United Kingdom and Worldwide Sales

Tel: +44 (0)8447 671131

Email: [sales@sophos.com](mailto:sales@sophos.com)

North American Sales

Toll Free: 1-866-866-2802

Email: [nasales@sophos.com](mailto:nasales@sophos.com)

Australia and New Zealand Sales

Tel: +61 2 9409 9100

Email: [sales@sophos.com.au](mailto:sales@sophos.com.au)

Asia Sales

Tel: +65 62244168

Email: [salesasia@sophos.com](mailto:salesasia@sophos.com)