chromeOS

SHI

The most secure OS out of the box[1]

8 reasons why ChromeOS beats the competition

It's official – ChromeOS is the most secure operating system out of the box when compared to Windows 11 and macOS. That's according to a recent competitive analysis report by security research firm, Atredis Partners.

As ChromeOS is built on the Zero Trust philosophy, no user or device is automatically trusted. Everything from your login attempts to the files you want to download are verified to be secure – every single time. Let's take a look at 8 key claims validated by the report that show how ChromeOS secures users, data, and devices at every level.[2]

1

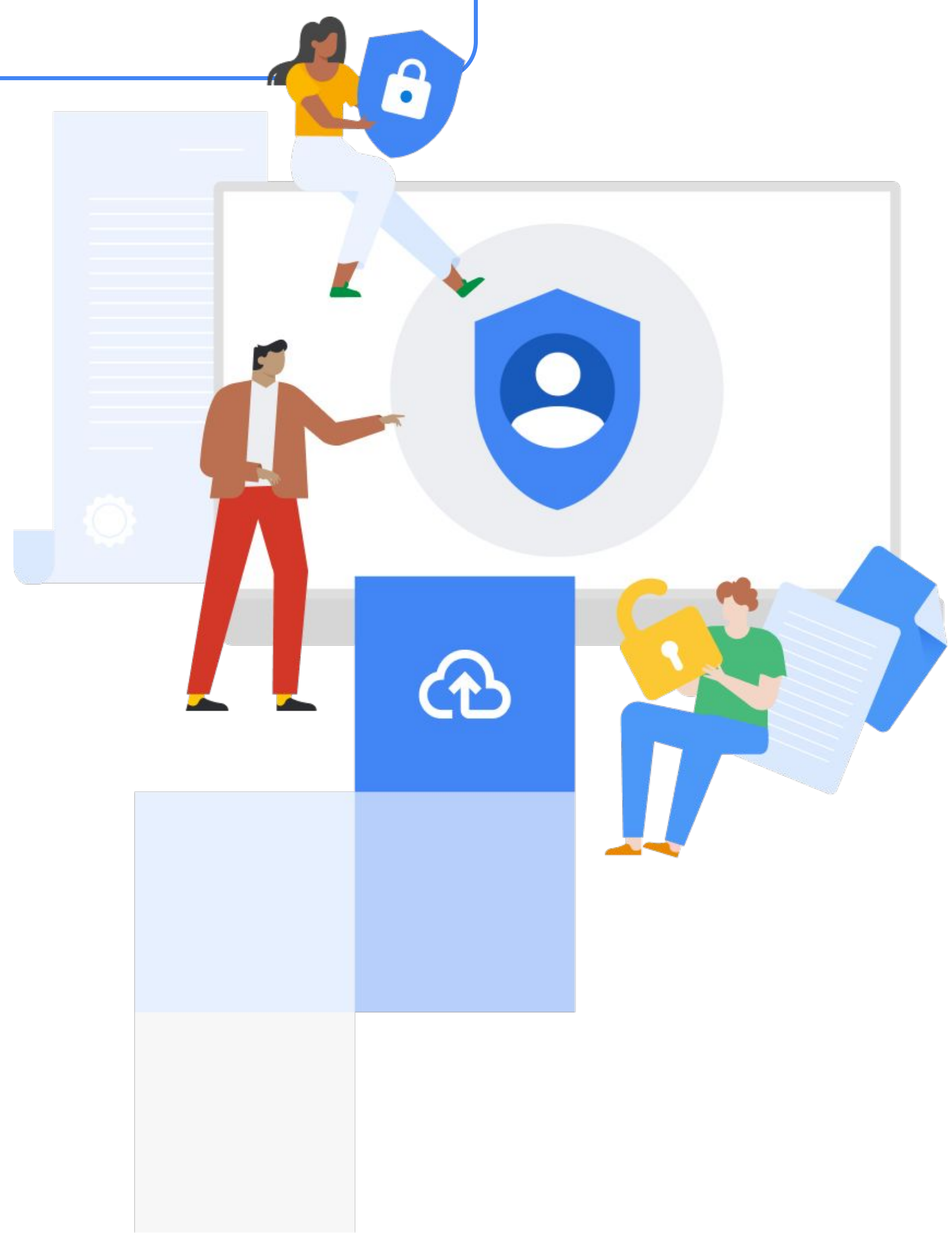
"ChromeOS devices start up secure every time"

ChromeOS has never had a reported virus or ransomware attack.[3]

ChromeOS checks for any changes to its firmware with Verified Boot every time a device powers up, which is a higher default security standard than macOS and Windows 11. If unfamiliar code is detected, ChromeOS automatically reverts to a previous version, keeping your device safe.[2]

chromeOS

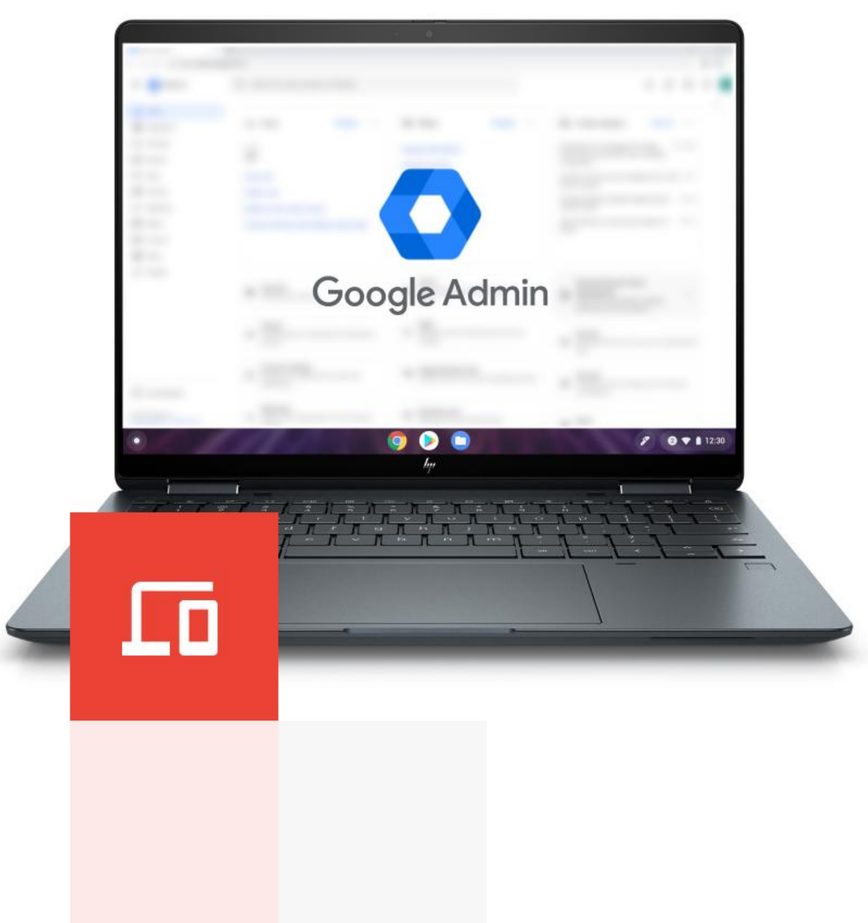
2 “User data is encrypted by default”



ChromeOS is the only operating system designed to prevent users from gaining access to other users’ data by default.

All data stored on the disk is encrypted with a unique set of credentials for each user, while guest user data is deleted immediately upon logout, making ChromeOS an ideal operating system for shared devices. Operating systems like Windows 11 and macOS have to be specially configured to support encryption, and administrators can still gain access to others’ data.[2]

3 “There are no admin users in ChromeOS”



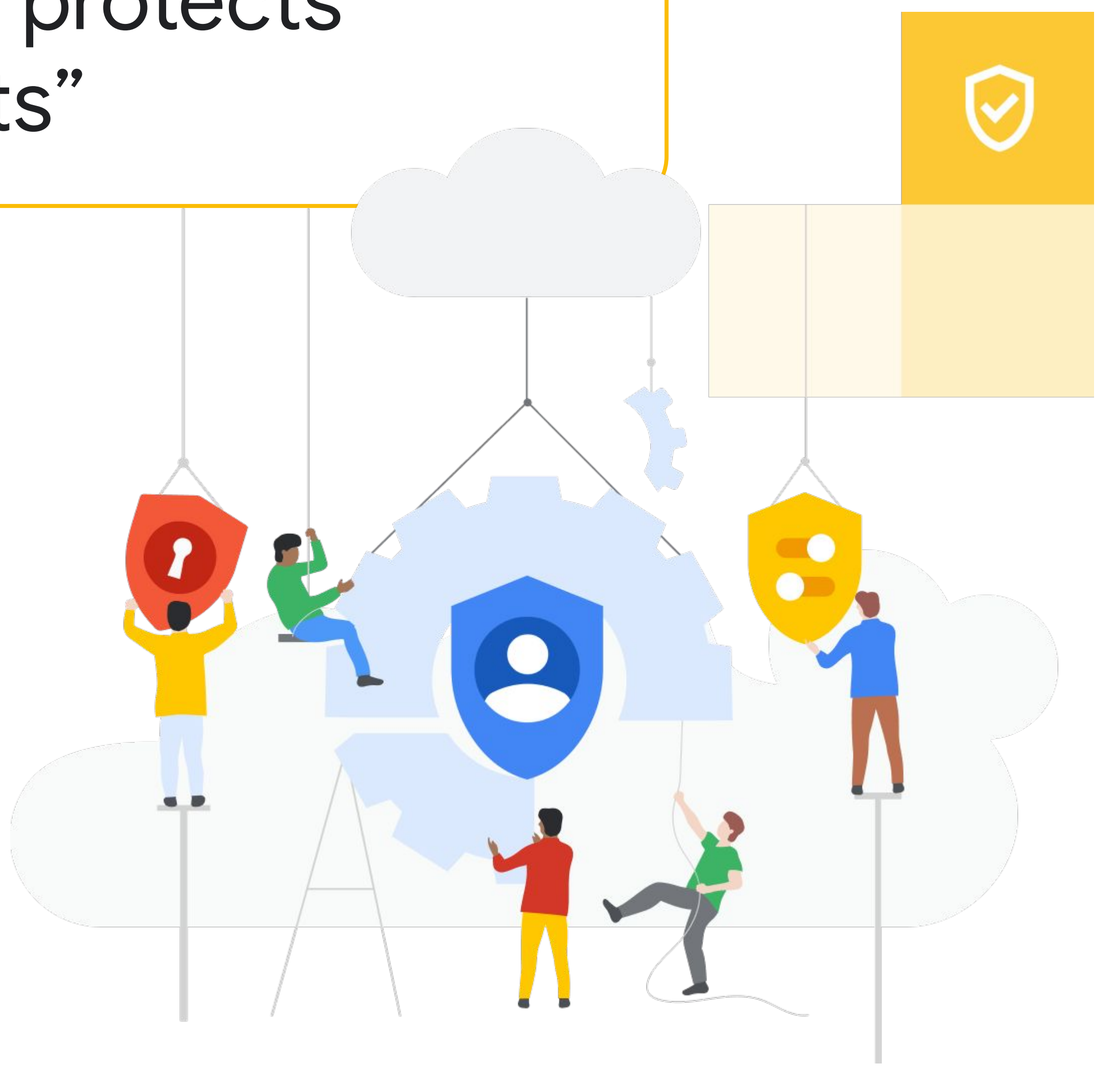
While macOS and Windows 11 allow administrator users to install software, create users, and make other changes that may compromise data, ChromeOS has a more secure approach.

There are no root or admin-level user types in ChromeOS, reducing the opportunities to exploit the system. Although users can make limited system changes in Developer Mode, it doesn't grant the same privileges as an admin user, ensuring that the ChromeOS attack surface is smaller than other systems.[2]

chromeOS

4

“ChromeOS automatically protects users against online threats”

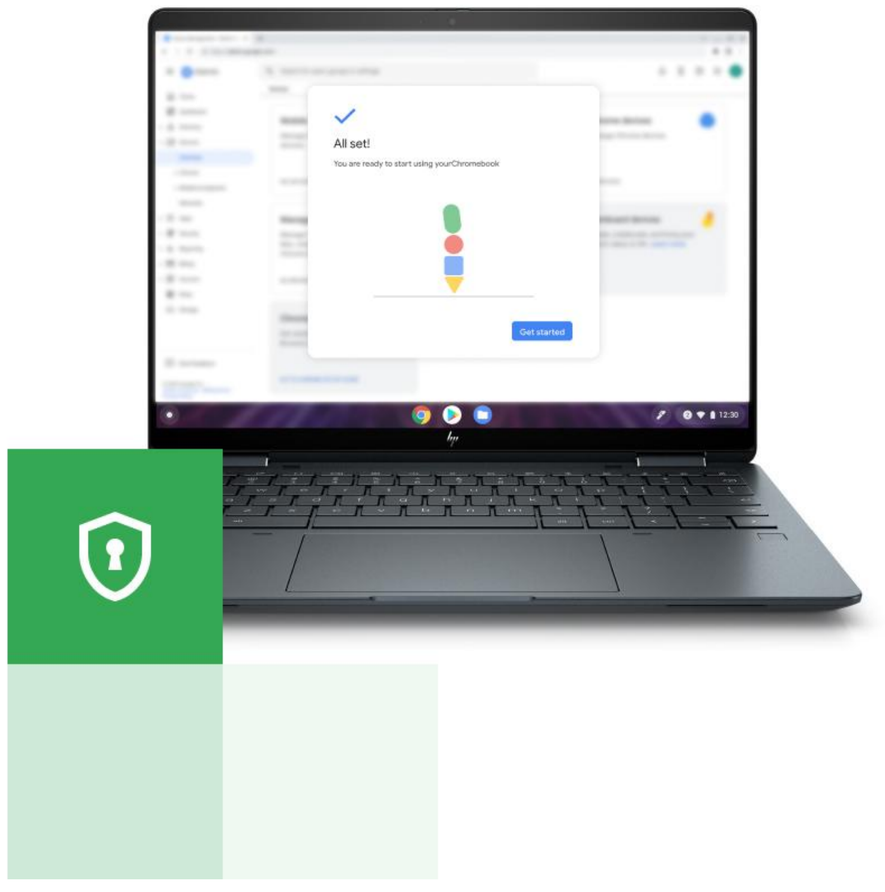


ChromeOS uses sandboxing at the system, application, and browser levels to ensure threats targeting your data are quickly contained and neutralized.

The built-in Safe Browsing feature in Chrome browser automatically protects more than 5 billion users every day by isolating each web page so it can’t affect other tabs, apps, or anything else on your device. Unlike macOS and Windows 11, the entire ChromeOS system architecture is segmented, and integral system files are completely isolated. Even if you access a malicious app or file, it can’t infiltrate your device’s firmware.[2]

5

“Education and enterprise organizations can lock down what users are able to access”

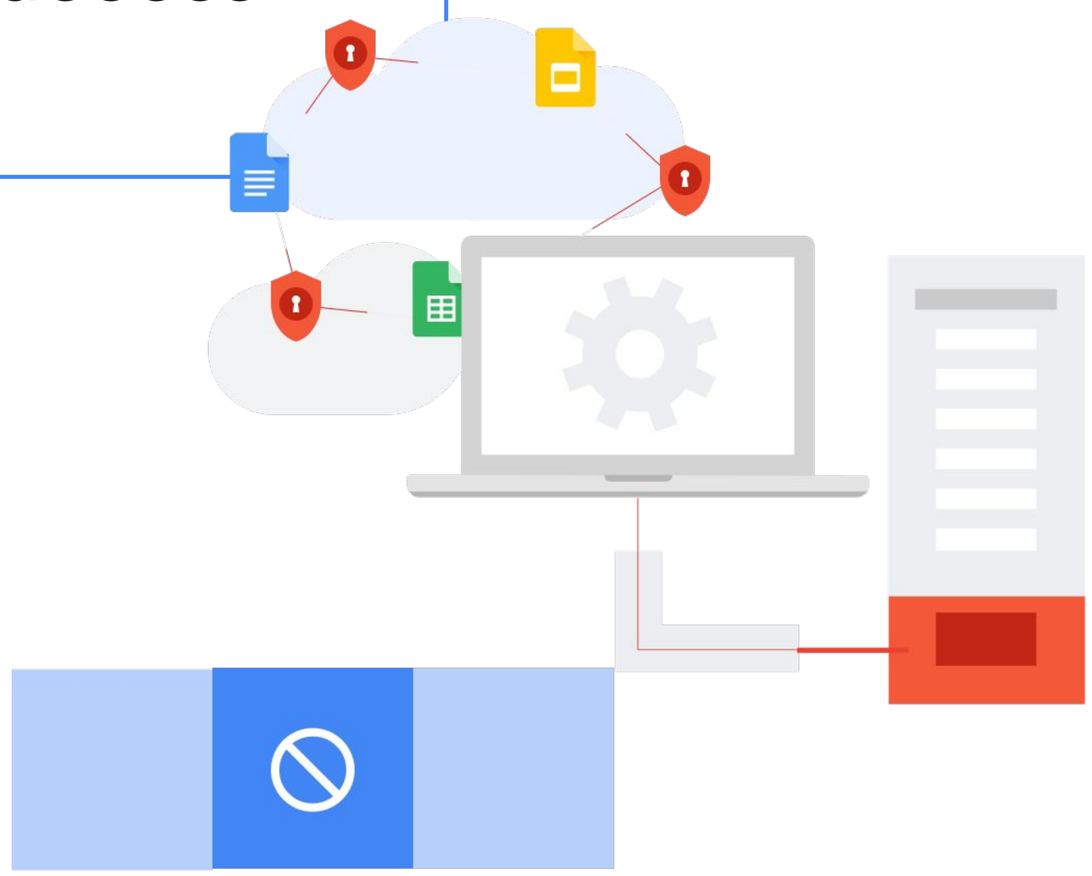


Chromebooks are used by 50 million students and teachers every day. ChromeOS supports their use cases by making it easy to restrict specific apps and websites.

The Google Admin console allows you to set policies for what web content and extensions users can access, as well as choose which sites are permitted to run JavaScript, set cookies, load images, and more. On macOS and Windows 11, it is much easier to bypass controls even if restrictions are set up.[2]

chromeOS

6 “Attackers can’t remotely access ChromeOS devices”

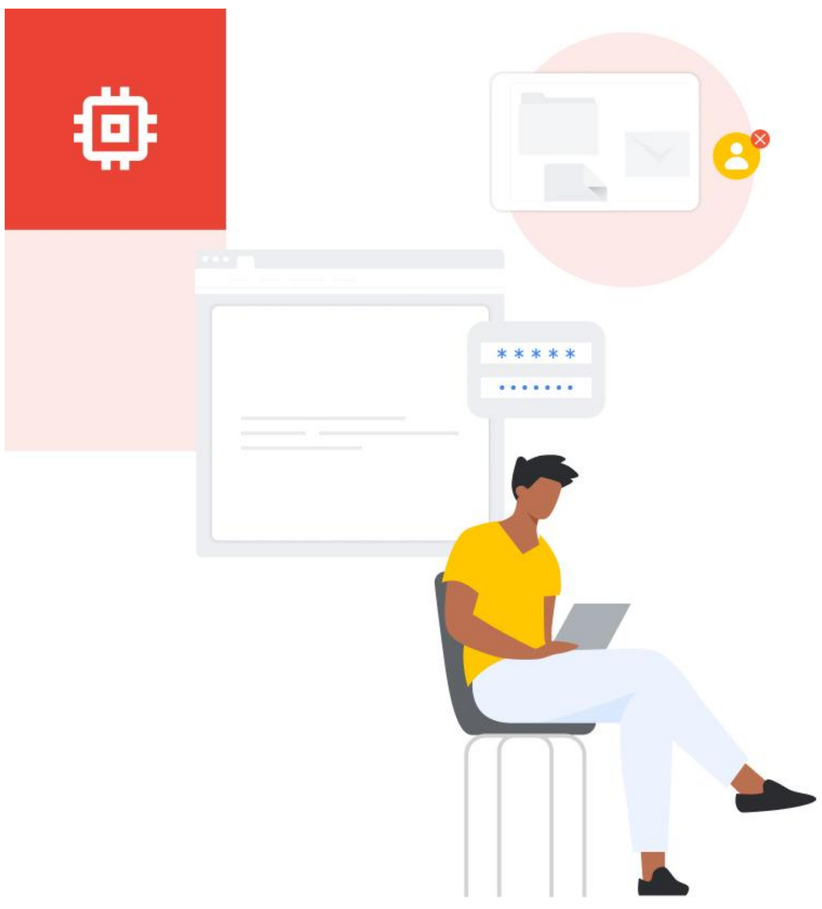


ChromeOS has a smaller remote access attack surface by design.

Using an innovative firewall defense system, ChromeOS prevents criminals from using service discovery protocols to poison requests and coerce systems into connecting to resources they control. While macOS and Windows 11 also use firewall defenses, they are ultimately less effective. Both are susceptible to poisoning via protocols that are not permitted by the ChromeOS firewall.[2]

“Due to default behavior, the abundance of configuration options, and the ability for applications to modify behavior, ChromeOS emerges as the most effective solution at limiting remote attack surface.” [2]

7 “The Google Security Chip thwarts attacks”



If an attacker wants to gain access to your data, they need physical access to your ChromeOS device, and even then it’s a difficult task.

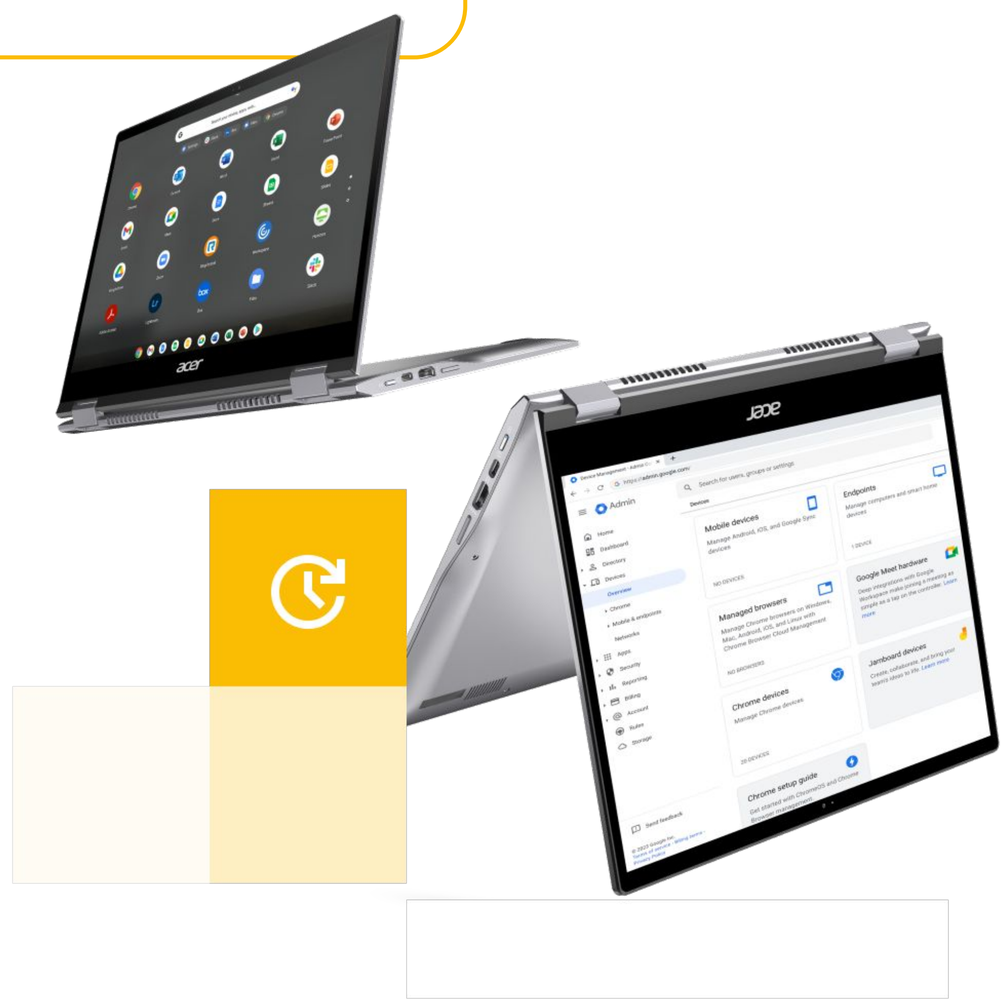
The Google Secure Microcontroller (H1) supports many security features throughout ChromeOS, including protecting encryption keys and local data. Even brute force attacks – when an attacker tries millions of combinations of passwords or pin codes in an attempt to log in – are prevented by the chip.[2]

8

“Automatic updates mean you always have the latest protection”

Regular updates are critical to data security. However, updates on some operating systems can be time-consuming and unnecessarily complicated.

Users are sometimes required to accept new terms of service or re-enter their password on macOS. And Windows 11 will only update automatically if you manually configure it to do so. ChromeOS updates run automatically in the background by default and notify the user if a system reboot is required. Since ChromeOS is purpose-built to be highly integrated, a system update will update all components at once.[2]



Your employees shouldn’t have to be IT security experts to work safely on the web.

ChromeOS has an advanced, default security infrastructure built around Zero Trust principles that ensures every device is ready to go out of the box, and that your organization will spend less time and money configuring additional security measures.

Read the full analysis from Atredis Partners here.

[Contact our experts](#) to learn how ChromeOS can meet the unique needs of your enterprise while offering a more secure experience out of the box than competing systems.[2]

chromeOS

[1] When contrasted with macOS and Windows 11, ChromeOS offers the most secure experience.
[2] A commissioned study conducted by Atredis Partners on behalf of Google, “Google ChromeOS Security Competitive Analysis Report”, April, 2024.
[3] As of May 2024, there has been no evidence of any documented, successful virus attack or ransomware attack on ChromeOS. Data based on ChromeOS monitoring of various national and internal databases.