chromeOS

SHI

ChromeOS has never had a reported ransomware attack

With the global shift to remote and hybrid work, ransomware crimes have skyrocketed. Ransomware encrypts data, making it inaccessible to users and posing costly threats to organizations across industries.

In the first half of 2022, there were an estimated **236.1 million** ransomware attacks globally.[1]

The average cost of a ransomware attack is **$4.54 million**, not including the cost of a ransom payment, which averages $812,360.[2]

93% of ransomware is Windows-based executables.[3]

ChromeOS is a cloud-first platform that provides protection against ransomware by default. **In fact, there have been no reported ransomware attacks ever on any business, education, or consumer ChromeOS device.**

ChromeOS has built-in and proactive security features to fight ransomware

Data and files are automatically backed up to the cloud and recoverable: ChromeOS is a cloud-first platform, which significantly limits the amount of data stored on the device that is susceptible to ransomware. All user data is backed up to the cloud. If ransomware bypasses ChromeOS security measures, your user data and files can be easily restored almost instantly.

Executables are blocked: Executable files, which can harbor ransomware, cannot run on ChromeOS. ChromeOS only runs curated apps from the Google Play store that have been scanned for malware.

Read-only OS: System files are kept in a separate partition to ensure the OS cannot be modified by apps or extensions and is thereby inaccessible to ransomware.

Google Safe Browsing: Google Safe Browsing is a proactive measure that warns users before attempting to navigate to dangerous sites or before downloading dangerous files.

Automatic updates: ChromeOS updates regularly and automatically in the background, providing continuous protection from threats.

Verified boot: If an attack does prevail, Verified boot confirms the OS has not been tampered with, and if it has, it reverts to a previous version of the OS.

[1] AAG-IT, 2022 [2] Lexology, 2022 [3] AAG-IT, 2022