chromeOS

Ein sicheres Betriebssystem – sofort einsatzbereit

8 Gründe, weshalb ChromeOS besser als vergleichbare Betriebssysteme abschneidet

Laut einer kürzlich erschienenen Wettbewerbsanalyse von Atredis Partners, einem Unternehmen im Bereich der Sicherheitsforschung, bietet ChromeOS sofortigen Schutz.

ChromeOS liegt das Zero-Trust-Prinzip zugrunde, laut dem Nutzer und Geräte niemals automatisch als vertrauenswürdig eingestuft werden sollten. Egal, ob Anmeldeversuche oder Nutzeranfragen zum Herunterladen von Dateien – alles wird jedes Mal verifiziert, um für mehr Sicherheit zu sorgen. Sehen wir uns die 8 Claims genauer an, die in dem Bericht validiert wurden und zeigen, wie ChromeOS auf allen Ebenen für mehr Sicherheit für Nutzer, Daten und Geräte sorgt.[1]

1

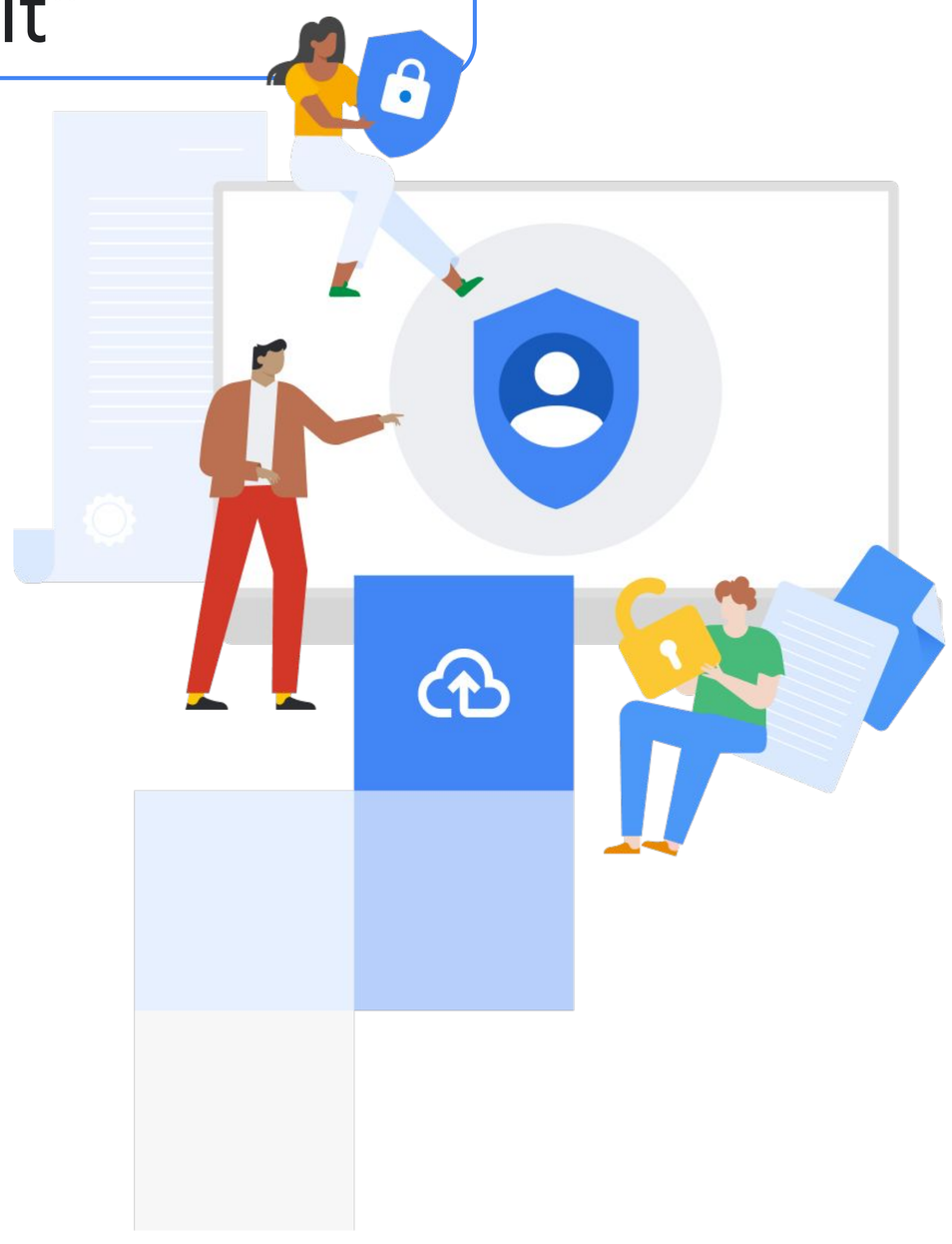
„ChromeOS-Geräte sind bei jedem Start sicher“

Bisher wurde noch nie ein erfolgreicher Virus- oder Ransomware-Angriff auf ChromeOS gemeldet.[2]

ChromeOS sucht bei jedem Gerätestart im verifizierten Bootmodus nach Änderungen an der Firmware und hat damit bessere standardmäßige Sicherheitsfunktionen als macOS und Windows 11. Sollte unbekannter Code gefunden werden, wird ChromeOS automatisch auf eine frühere Version zurückgesetzt, um das Gerät zu schützen.[1]

chromeOS

2 „Nutzerdaten werden standardmäßig verschlüsselt“



ChromeOS ist das einzige Betriebssystem, das standardmäßig verhindert, dass Nutzer auf die Daten anderer zugreifen können.

Alle auf der Festplatte gespeicherten Daten werden mit individuellen Anmeldedaten für jeden Nutzer verschlüsselt und Daten von Gastnutzern werden sofort nach dem Abmelden gelöscht. Daher ist ChromeOS ein ideales Betriebssystem für gemeinsam verwendete Geräte. Betriebssysteme wie Windows 11 und macOS müssen erst konfiguriert werden, damit eine Verschlüsselung möglich ist, und Administratoren haben auch danach Zugriff auf die Daten anderer Nutzer.[1]

3 „Bei ChromeOS gibt es keine Nutzer mit Administratorberechtigungen“

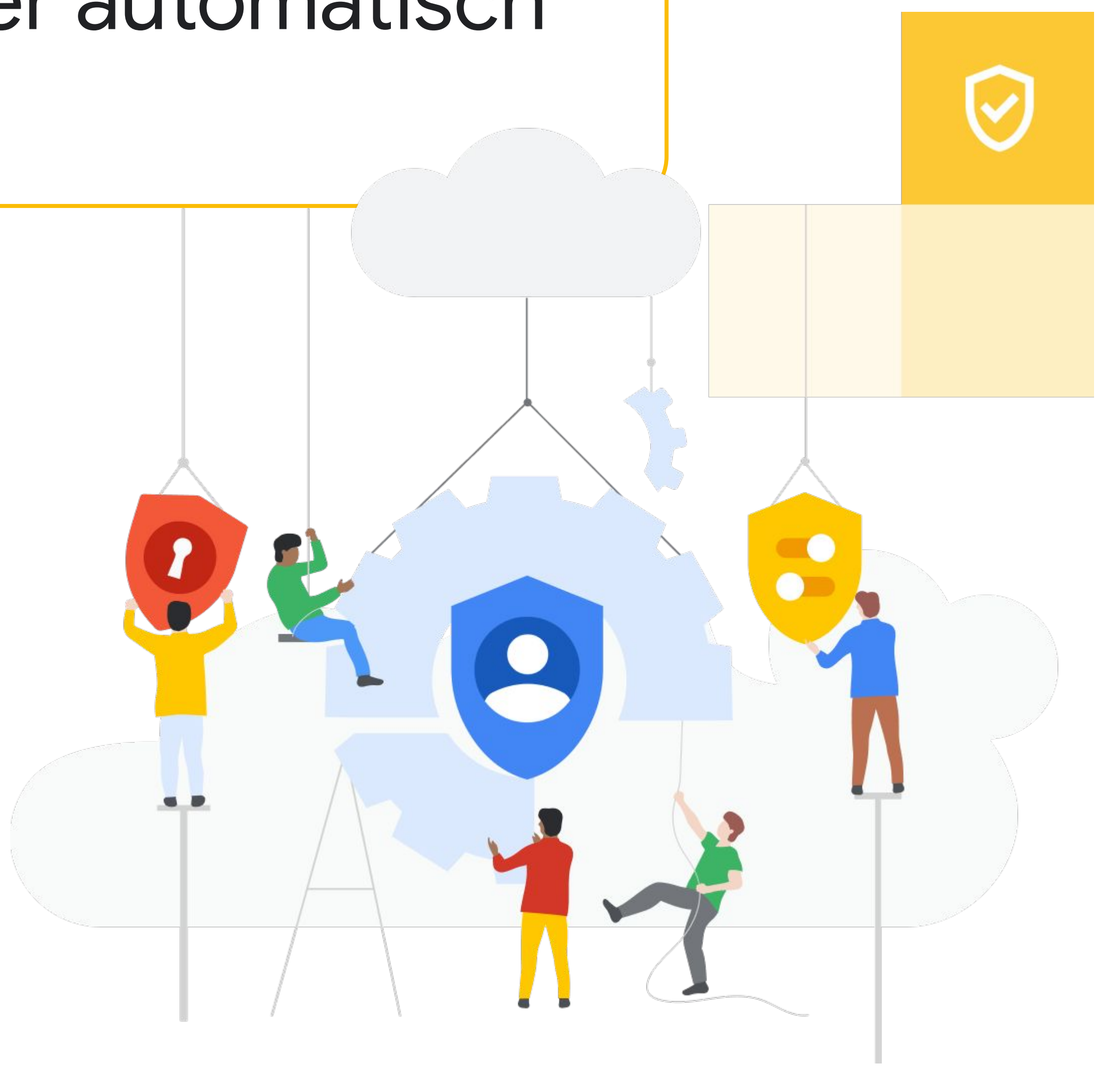
Unter macOS und Windows 11 dürfen Nutzer mit Administratorberechtigungen Software installieren, Nutzerprofile erstellen und andere Änderungen vornehmen, allerdings können dadurch aber Daten beschädigt werden. ChromeOS hingegen stützt sich auf einen strikteren Sicherheitsansatz.

Bei ChromeOS gibt es keine Root-Nutzer oder Nutzer mit Administratorberechtigungen und damit auch weniger Möglichkeiten, das System zu kompromittieren. Nutzer können zwar im Entwicklermodus bestimmte Systemänderungen vornehmen, haben aber nicht so umfangreiche Berechtigungen wie ein Nutzer mit Administratorberechtigungen. Dadurch ist die Angriffsfläche von ChromeOS kleiner als bei anderen Systemen.[1]

chromeOS

4

„ChromeOS schützt Nutzer automatisch vor Onlinebedrohungen“

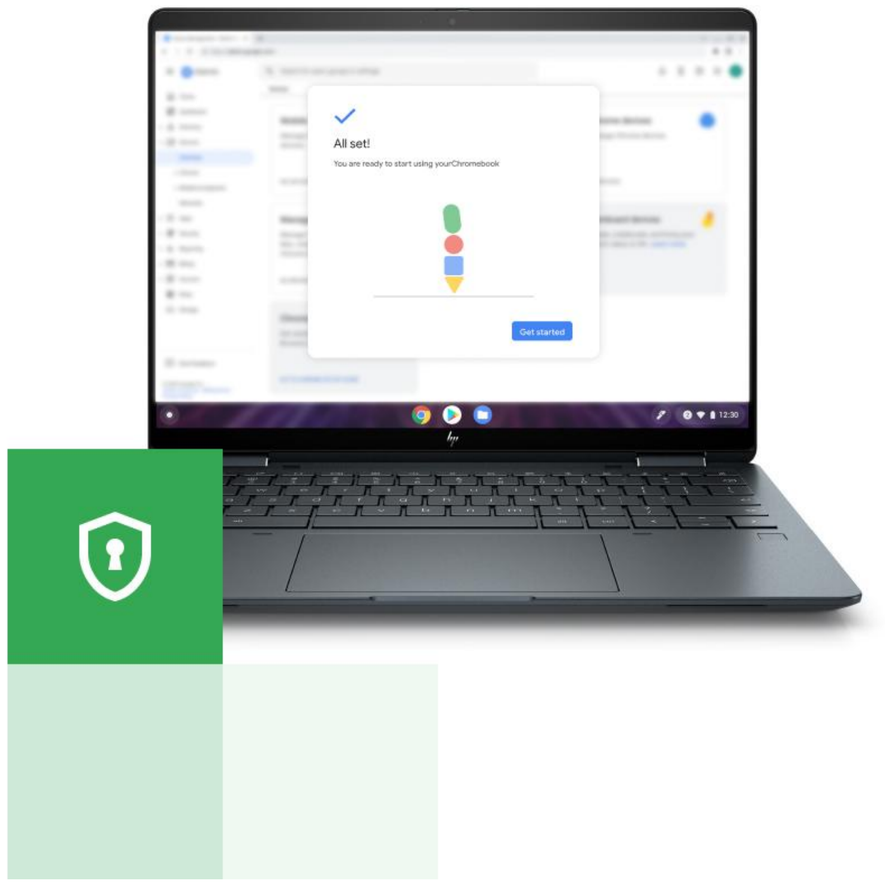


ChromeOS verwendet die Sandbox-Technologie auf System-, Anwendungs- und Browserebene, sodass Bedrohungen schnell eingedämmt und unschädlich gemacht werden können.

Die in den Chrome-Browser integrierte Funktion „Safe Browsing“ schützt automatisch mehr als 5 Milliarden Nutzer pro Tag, da jede Webseite isoliert wird. So können Bedrohungen nicht auf andere Tabs, Anwendungen oder sonstige Inhalte auf dem Gerät übergreifen. Im Gegensatz zu macOS und Windows 11 ist bei ChromeOS die gesamte Systemarchitektur segmentiert und wichtige Systemdateien sind vollständig isoliert. Falls Sie also versehentlich eine schädliche Anwendung oder Datei öffnen, kann diese dann nicht die Firmware des Geräts infiltrieren.[1]

5

„Bildungseinrichtungen und Unternehmen können Zugriffsrechte von Nutzern einschränken“



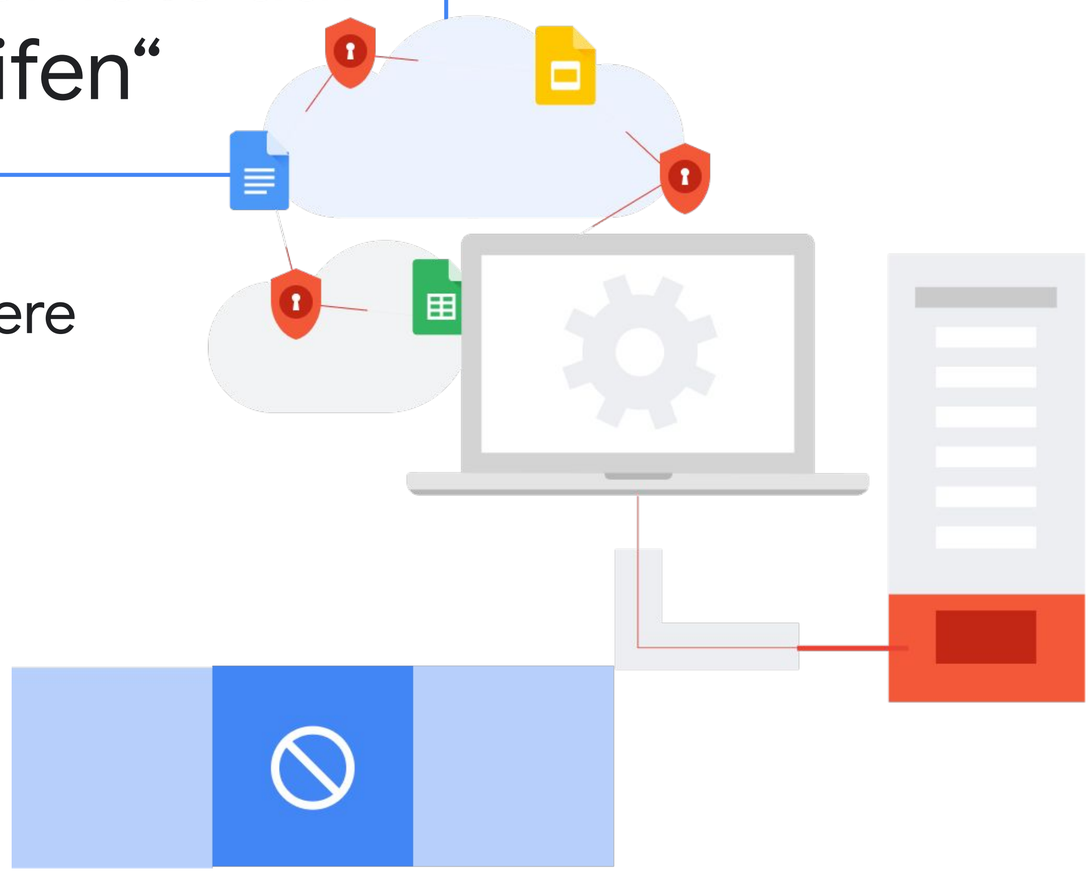
Chromebooks werden jeden Tag von 50 Millionen Schülern, Studenten und Lehrkräften genutzt. ChromeOS sorgt bei diesen Anwendungsfällen für mehr Sicherheit, da der Zugriff auf bestimmte Anwendungen und Websites problemlos eingeschränkt werden kann.

In der Admin-Konsole können Sie Richtlinien für den Zugriff auf Webinhalte und Erweiterungen einrichten und festlegen, welche Websites beispielsweise JavaScript ausführen, Cookies setzen und Bilder laden dürfen. Unter macOS und Windows 11 können Sicherheitsfunktionen viel einfacher umgangen werden, selbst wenn Einschränkungen festgelegt wurden.[1]

chromeOS

6

„Angreifer können nicht remote auf ChromeOS-Geräte zugreifen“



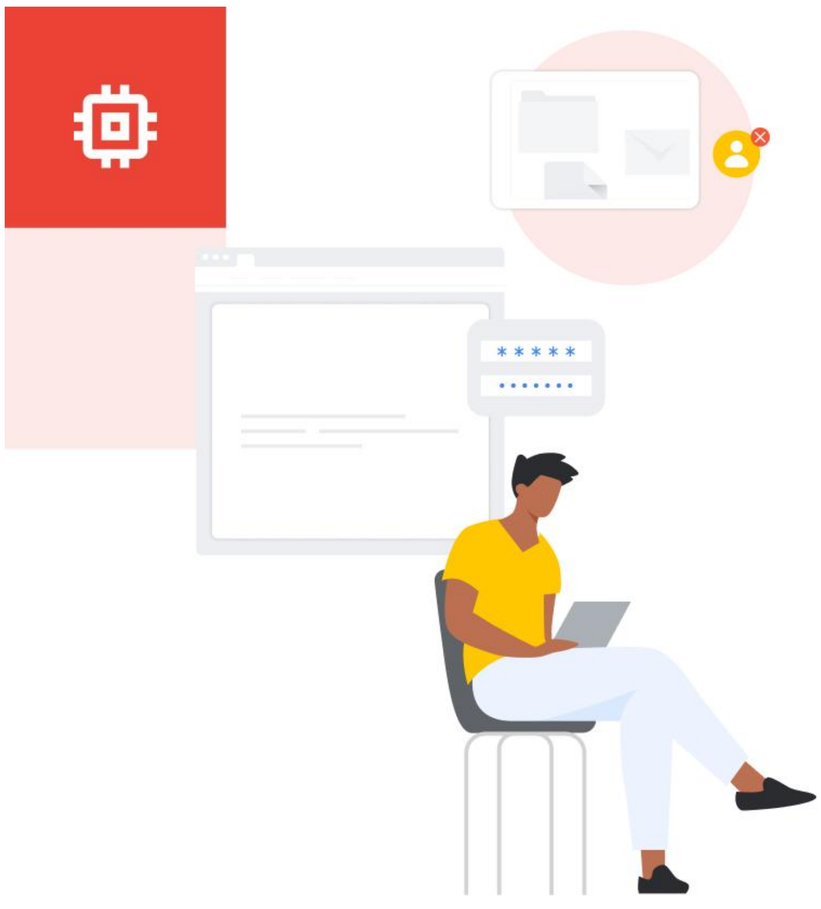
ChromeOS bietet grundsätzlich eine kleinere Angriffsfläche für den Remote-Zugriff.

Mithilfe eines innovativen Abwehrsystems auf Firewallebene verhindert ChromeOS, dass Cyberkriminelle Protokolle zur Erkennung von Diensten ausnutzen, um Anfragen zu fälschen und Systeme mit von ihnen kontrollierten Ressourcen zu verbinden. Unter macOS und Windows 11 gibt es zwar auch Abwehrfunktionen auf Firewallebene, doch diese sind weniger effektiv. Beide Betriebssysteme sind anfällig für Poisoning-Angriffe über Protokolle, die auf der ChromeOS-Firewall nicht zulässig sind.[1]

„Aufgrund des Standardverhaltens, der Vielzahl an Konfigurationsoptionen und der Möglichkeit, dass Anwendungen ihr Verhalten anpassen, ist ChromeOS die effektivste Lösung zur Reduzierung der Angriffsfläche für den Remote-Zugriff.“ [2]

7

„Der Sicherheitschip von Google kann Angriffe verhindern“

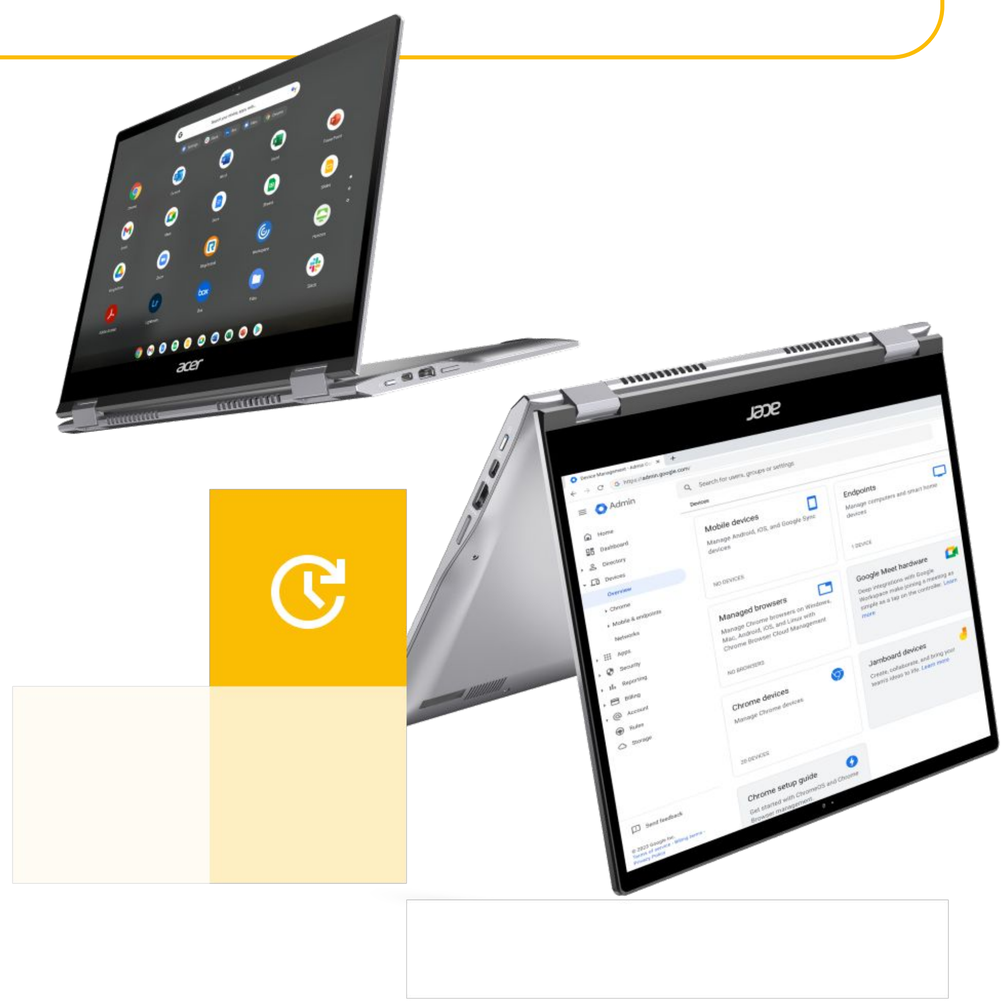


Ein Angreifer kann Ihre Daten nur abrufen oder stehlen, wenn er sich zuerst physischen Zugriff auf Ihr ChromeOS-Gerät verschafft hat – und selbst dann ist es nicht einfach.

Der Google H1-Chip ist ein Sicherheitsmikrocontroller und unterstützt viele Sicherheitsfunktionen in ChromeOS, zum Beispiel den Schutz von Verschlüsselungsschlüsseln und lokal gespeicherten Daten. Selbst Brute-Force-Angriffe, bei denen Angreifer Millionen Kombinationen von Passwörtern oder PINs ausprobieren, um sich auf einem Gerät anzumelden, werden vom Chip verhindert.[1]

8

„Dank automatischer Updates sind die Sicherheits-funktionen immer auf dem neuesten Stand“



Regelmäßige Updates sorgen für mehr Datensicherheit. Doch bei einigen Betriebssystemen ist die Installation von Updates äußerst zeitaufwendig und unnötig kompliziert.

Unter macOS müssen Nutzer manchmal neue Nutzungsbedingungen akzeptieren oder ihr Passwort neu eingeben. Unter Windows 11 müssen automatische Updates erst manuell konfiguriert werden. ChromeOS-Updates hingegen werden standardmäßig automatisch im Hintergrund ausgeführt und die Nutzer werden benachrichtigt, falls das System neu gestartet werden muss. Da ChromeOS auf eine nahtlose Integration ausgelegt ist, werden bei einem Systemupdate alle Komponenten gleichzeitig aktualisiert.[1]

Ihre Mitarbeiter sollten kein IT-Fachwissen benötigen, um sicher im Web arbeiten zu können

ChromeOS bietet standardmäßig eine erweiterte Sicherheitsinfrastruktur auf Grundlage der Zero-Trust-Prinzipien, sodass jedes Gerät sofort einsatzbereit ist. So spart Ihr Unternehmen Zeit und Geld, da keine aufwendigen Konfigurationen zusätzlicher Sicherheitsmaßnahmen notwendig sind.

Die vollständige Analyse von Atredis Partners können Sie hier lesen.

Wenn Sie wissen möchten, wie ChromeOS die Anforderungen Ihres Unternehmens erfüllen kann, kontaktieren Sie unsere Experten.

chromeOS

[1] Eine von Atredis Partners im Auftrag von Google durchgeführte Studie zur Sicherheit von ChromeOS im Vergleich zu anderen Betriebssystemen namens Google ChromeOS Security Competitive Analysis Report, April 2024.
[2] Bis Mai 2024 wurde kein erfolgreicher Virus- oder Ransomware-Angriff auf ChromeOS dokumentiert. Diese Erkenntnisse basieren auf Daten zu ChromeOS aus verschiedenen nationalen und internen Datenbanken.