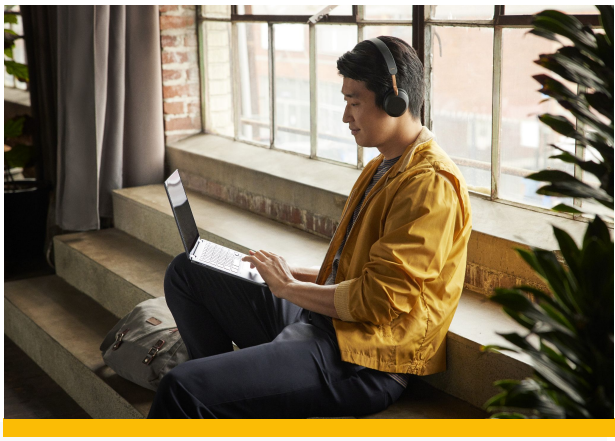
chromeOS

Schützen Sie Ihre Geräte mit ChromeOS



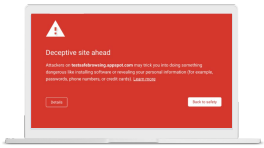
In Unternehmen gibt es immer mehr IP-Adressen, Daten und Identitäten jenseits der Firewall. Jeder Endpunkt stellt ein potenzielles Einfallstor in das Unternehmensnetzwerk dar und Fehler der Mitarbeiter sind ein konstantes Risiko.

Sorgen Sie mit den integrierten intelligenten Sicherheitsfunktionen, detaillierten Richtlinienkontrollen und automatischen Updates von ChromeOS für kontinuierlichen Schutz. Dank schreibgeschütztem Betriebssystem und verschlüsselten Geräten sind Nutzer und Daten vor Ransomware-, Malware- und Phishingangriffen geschützt. Jede Ebene des vertikal integrierten Stacks von ChromeOS schafft zusätzliche Sicherheit und mit den automatischen Updates für das gesamte System brauchen Sie sich auch in Zukunft keine Sorgen zu machen.

2020 wurde der weltweite Cybersicherheitsmarkt **auf 167 Milliarden $ geschätzt**.[1]

2020 wurden bei Datenpannen **mehr als 36 Milliarden Datensätze offengelegt**.[2]

Schützen Sie Ihr Unternehmen mit ChromeOS vor Phishing-, Ransomware- und Malwareangriffen



Phishing

Google Safe Browsing warnt Nutzer vor schädlichen Websites, bevor sie diese öffnen.

Sicherheitsschlüssel und die Bestätigung in zwei Schritten verhindern, dass Hacker gestohlene Passwörter nutzen können.

Im Falle eines Angriffs werden die Nutzer gemäß der Richtlinie für Passwort-Warnungen aufgefordert, ihr Passwort zu ändern, wenn es auf nicht autorisierten Websites verwendet wird.

Ransomware

Durch das geringe Datenvolumen auf dem Gerät können weniger Daten von Ransomware erfasst werden.

Das schreibgeschützte Betriebssystem verhindert, dass schädliche ausführbare Dateien lokal ausgeführt werden.

Im Falle eines Angriffs wird mit dem verifizierten Bootmodus bestätigt, dass das System beim Start unverändert ist.

Malware

Auf Berechtigungen basierende Sperrlisten legen fest, auf welche Erweiterungen zugegriffen werden darf.

Der Managed Play Store erleichtert die Zusammenstellung nach Nutzergruppen und die Richtlinienkonfiguration nach App.

Im Falle eines Angriffs wird durch Sandboxing die Angriffsfläche begrenzt.

[1] Grand View Research, 2021; [2] RiskBased Security, 2020

chromeOS

Schutz vor Ransomware-, Malware- und Phishingangriffen

Schreibgeschütztes Betriebssystem: Die Systemdateien befinden sich in einer separaten Partition, damit das Betriebssystem nicht von Apps oder Erweiterungen verändert werden kann. Damit ist es auch vor Ransomware geschützt.

Blockierung ausführbarer Dateien: Ausführbare Dateien, die Bedrohungen enthalten können, werden unter ChromeOS blockiert. Es werden nur ausgewählte Apps aus dem Google Play Store ausgeführt, die vorher auf Malware geprüft wurden.

Verschlüsselte Hardware: ChromeOS-Geräte werden standardmäßig mit einem eindeutigen Schlüssel verschlüsselt, um Angreifern den Zugriff auf Nutzerdaten zu erschweren. Die Verschlüsselung kann nicht deaktiviert werden.

Verifizierter Bootmodus: Mit dem verifizierten Bootmodus wird nach einem Neustart bestätigt, dass Firmware und Betriebssystem nicht manipuliert oder beschädigt wurden. Sollte dies doch der Fall sein, wird das Gerät auf eine vorherige Betriebssystemversion zurückgesetzt.

Sandboxing und Website-Isolierung: Durch Sandboxing und die Website-Isolierung lassen sich Bedrohungen auf eine Anwendung oder einen Tab beschränken, sodass der Rest des Betriebssystems weiterhin sicher ist.

Zentrale Remoteverwaltung

Richtlinien für die Verwaltung: Es stehen über 500 Richtlinien für die zentrale Verwaltung und Einrichtung von ChromeOS-Geräten zu Verfügung, einschließlich Parametern für die Anmeldung und Authentifizierung.

Ausgewählte Apps und Erweiterungen: Legen Sie Ausführungsberechtigungen fest, um sicherzustellen, dass Nutzer bestimmte Apps und Erweiterungen nicht installieren. Mit einem verwalteten Chrome Web Store, dem Managed Play Store und Google Play Protect können Sie außerdem verhindern, dass Nutzer schädliche Apps und Erweiterungen herunterladen.

Flüchtiger Modus (Löschung von Nutzerdaten bei der Abmeldung): Damit legen Sie fest, dass alle Daten und Einstellungen automatisch gelöscht werden, wenn sich ein Nutzer abmeldet.

Schutz bei Verlust und Diebstahl (Deaktivierung aus der Ferne und Powerwash): Es ist möglich, verloren gegangene oder gestohlene Geräte aus der Ferne zu deaktivieren oder deren Daten zu löschen. Außerdem können Sie eine Nachricht mit einer Rückgabeadresse eingeben.

Remotezugriff und Einmalanmeldung (SSO): Legen Sie Einstellungen für den Remotezugriff und die SAML-Einmalanmeldung fest, sodass Nutzer einfach auf das Netzwerk und Webanwendungen zugreifen können, aber trotzdem die nötige Sicherheit gewährleistet ist.

Berichterstellung: Es sind Berichte mit informativen Daten verfügbar, zum Beispiel der aktuellen Version des Betriebssystems und dem Enddatum der automatischen Updates für die Geräte.

Automatische Updates für zuverlässigeren Geräteschutz

Konsistente, regelmäßige und schnelle Updates: Die ChromeOS-Firmware und -Funktionen werden alle sechs Wochen aktualisiert. Das ist wesentlich häufiger als bei den meisten anderen Systemen. Updates werden innerhalb von Sekunden beim Neustart des Geräts eingespielt.

Geringere Supportkosten: Bei ChromeOS fallen keine kostspieligen manuellen Patches oder Routineupdates des Betriebssystems an.

Keine Ausfallzeiten oder Störungen: Updates werden im Hintergrund installiert, während die Nutzer weiterarbeiten. Da es zwei Versionen des Betriebssystems gibt, ist eine weiterhin verfügbar, wenn die andere aktualisiert wird. So sind die Daten geschützt und die Mitarbeiter können produktiv arbeiten.

Herstellerunabhängig: Auf allen ChromeOS-Geräten werden unabhängig vom Hersteller die gleichen Updates installiert.

→ Weitere Informationen zur ChromeOS-Sicherheit finden Sie unter: https://chromeenterprise.google/os/security

© 2021 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA