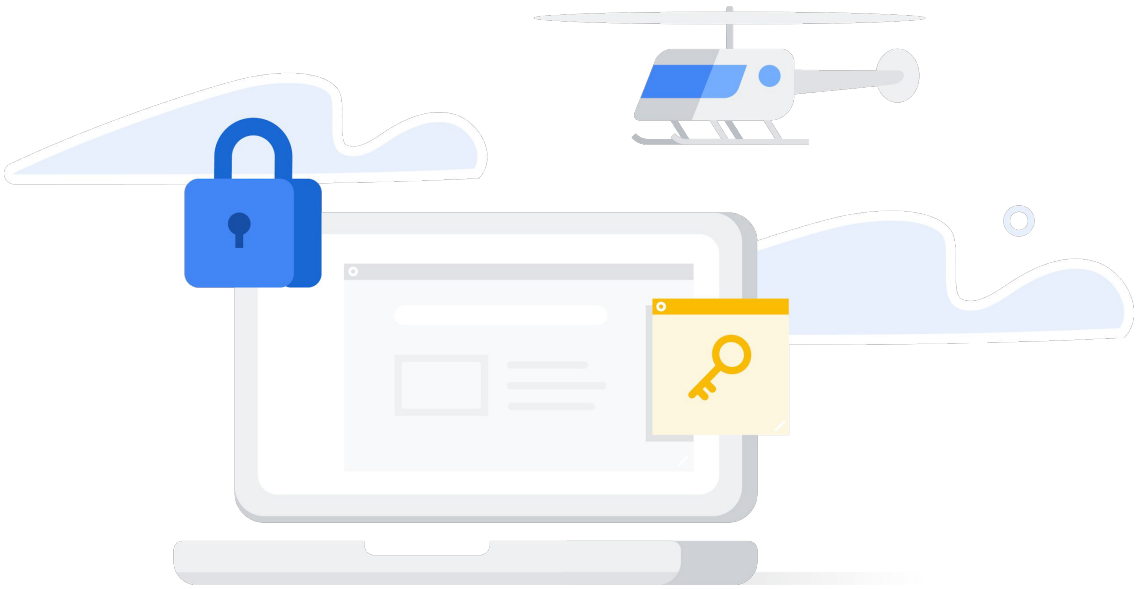
chrome enterprise

Browser sind die erste Abwehrlinie bei der Endpunktsicherheit

Die Sicherheitsstrategie Ihres Unternehmens verbessern – mit dem Chrome-Browser



Der Browser als strategisches Sicherheitstool

Viele Menschen unterschätzen ihren Browser – für sie ist er vor allem ein Portal, das ins Internet führt. Inzwischen haben sich Browser jedoch zu komplexen Plattformen entwickelt. Sie kompilieren und führen Skripts und Codes aus, bieten effektive Unterstützung bei der Internetrecherche und sorgen dafür, dass Nutzer durch das Web surfen und Apps verwenden können. Außerdem stellen sie immersive Umgebungen bereit, bei denen Text, Bilder, Audio, Video und virtuelle Umgebungen miteinander verschmelzen, und sorgen für eine nahtlose Integration zahlreicher Anwendungen und Erweiterungen.

Browser verfügen bereits über zahlreiche Funktionen, um die Netzwerk- und Endpunktsicherheit zu verbessern. Aufgrund ihrer einzigartigen Positionierung eignen sie sich optimal als strategische Sicherheitsebene in Unternehmen. Denn sie befinden sich genau dort, wo Internet, Nutzer und Anwendungen aufeinandertreffen. So bieten sie unter anderem die folgenden Vorteile:

Sie können mit Nutzern in Echtzeit interagieren und sie von riskanten Aktionen abhalten.

Über sie lassen sich nutzerzentrierte Sicherheitsrichtlinien auf Endpunkten erzwingen.

Sie können auf einfache Weise für Endpunktsicherheit sorgen – unabhängig vom Gerät und Betriebssystem.

Dieser Artikel beschreibt anhand von Beispielen mit Google Chrome, wie Browser diese drei Funktionen umsetzen.

Nutzer von riskanten Aktionen abhalten

Unternehmen haben Milliarden in leistungsstarke Sicherheitstools investiert, um Malware und Kompromittierungsindikatoren auf ihren Systemen und Netzwerken zu erkennen. Doch leider können Angreifer diese Tools umgehen, indem sie die größte Schwachstelle in der Unternehmenssicherheit ausnutzen – die Computer- und Smartphone-Nutzer selbst, darunter Mitarbeiter, Auftragnehmer, Kunden und Lieferanten.

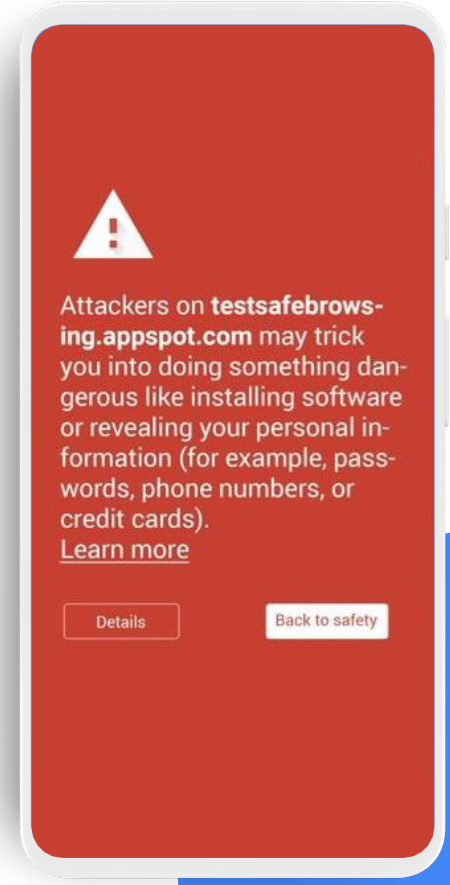
Heutzutage existieren sehr ausgeklügelte Phishing- und Social-Engineering-Angriffe. Sie verleiten die Nutzer zum Aufruf von Hacker-Websites, damit sie dort schädliche Dateien herunterladen. Oder sie bringen sie dazu, ihre Anmeldedaten einzugeben und Geld auf unbekannte Bankkonten zu überweisen. Sogar die besten Sicherheitsprogramme können gefährliche Aktionen wie diese nicht vollständig verhindern.

Browser können Nutzer vor Fehlern bewahren, indem sie sie von riskanten Aktionen abhalten. Chrome bietet hervorragende Beispiele für Funktionen, mit denen Nutzer auf mögliche Phishing- und Social-Engineering-Angriffe aufmerksam gemacht werden, und verweist sie auf angemessene Reaktionsmöglichkeiten.

Safe Browsing: Echtzeitschutz gegen Phishing und Schadsoftware

Die Funktion „Safe Browsing“ in Chrome bewahrt die Nutzer davor, infizierte oder schädliche Websites im Internet aufzurufen.

Dieser Google-Dienst prüft die Inhalte von Milliarden von Webseiten und erstellt eine Liste solcher, die nicht sicher sind. Diese Liste beinhaltet sowohl Hacker-Websites als auch Websites, die zwar legitim sind, jedoch gehackt wurden.
Google identifiziert diese Websites auf Grundlage von gefundener Malware, früheren Phishing- und Social-Engineering-Angriffen sowie Links oder Codes, die den Nutzer auf eine Angriffswebsite weiterleiten. Zusätzliche Indikatoren stellen z. B. Versuche dar, sich als eine andere, vertrauenswürdige Entität oder Website auszugeben, sowie Texte und Formulare, die den Nutzer dazu auffordern, Passwörter einzugeben, einen technischen Support anzurufen oder Software herunterzuladen. Der Safe Browsing-Dienst verzeichnet gegenwärtig über 21.000 Malware-Angriffs- und 1,8 Mio. Phishingwebsites. Jeden Tag versendet er mehr als 3 Mio. Warnmeldungen an Nutzer.



> Jedes Mal, wenn Nutzer eine Webseite aufrufen möchten, die in der Safe Browsing-Liste enthalten ist, zeigt der Browser eine Warnung an, in der das entsprechende Risiko beschrieben wird. Außerdem ist eine Schaltfläche vorhanden, mit welcher der Nutzer zur vorherigen, sicheren Website zurückkehren kann (siehe Abbildung 1). Im Jahr 2019 hat Chrome über eine Milliarde solcher Warnmeldungen angezeigt.

Safe Browsing ist standardmäßig aktiviert und aktualisiert die entsprechende Liste alle 30 Minuten mit neu entdeckten Malware- und Phishingwebsites. Wenn zusätzlich erweitertes Safe Browsing durch einen Administratoren oder Endnutzer aktiviert wird, prüft Chrome jede Webseite in Echtzeit. Diese Echtzeitprüfung schützt gegen Angriffe, bei denen im Minutentakt neue URLs erstellt werden, um Sicherheitstools zu umgehen, die konventionelle URL-Sperrlisten verwenden. IT-Teams können Safe Browsing über eine Richtlinie für ihr jeweiliges Unternehmen konfigurieren.

Analysen von Google haben gezeigt, dass der Schutz vor Phishing mithilfe dieser Funktion um 30–50 % steigt.

Safe Browsing schützt Nutzer außerdem vor schädlichen Erweiterungen und Schadsoftware. Wenn Chrome gestartet oder die Safe Browsing-Liste aktualisiert wird, scannt der Browser die installierten Erweiterungen und vergleicht sie mit denen, die Safe Browsing als missbräuchlich eingestuft hat. Bei Übereinstimmungen deaktiviert Chrome die betroffene Erweiterung, informiert den Nutzer und stellt gegebenenfalls Optionen zum Entfernen oder erneuten Aktivieren der Erweiterung bereit.

Auf ähnliche Weise gleicht Chrome Ihre Downloads mit einer Liste potenziell gefährlicher Dateitypen wie ausführbaren Dateien und häufig missbrauchten Dokumententypen ab. Wenn die Sicherheit der Datei nicht bestätigt werden kann, sendet Chrome die entsprechenden Informationen an Google-Server, um festzustellen, ob sie wirklich sicher ist. Ist die Antwort negativ, wird dem Nutzer eine Warnmeldung angezeigt.[1]

Das Aktivieren der Funktion „Erweitertes Safe Browsing“ erhöht dank Echtzeitdaten den Schutz vor schädlichen Websites und Downloads beträchtlich. Wenn ein Nutzer angemeldet ist, lässt sich über Chrome und andere verwendete Google-Apps wie Gmail und Drive das Sicherheitslevel weiter erhöhen. Sie erhalten beispielsweise einen umfassenden Überblick über die Bedrohungen im Internet und Angriffe auf das betroffene Google-Konto. Anders gesagt sorgt das erweiterte Safe Browsing dafür, dass Sie von der Intelligenz der hochmodernen Sicherheitstools von Google direkt über Ihren Browser profitieren können.

Safe Browsing schützt Nutzer außerdem bei der vielseitigen Verwendung der Google Suche, von Gmail-Konten und Android-Smartphones.

[1] Weitere Informationen zu Google Safe Browsing finden Sie im Google Transparenzbericht und im Whitepaper zum Datenschutz in Chrome.

Erweiterter Passwortschutz

Angreifer verwenden die Passwörter von Nutzern, um sich Zugriff auf Netzwerke, Anwendungen und Daten zu verschaffen. Das Problem ist besonders akut, da viele Menschen dasselbe Passwort für mehrere Konten verwenden und es selbst dann nicht ändern, wenn es gehackt wurde. Eine umfassende Studie zur Wiederverwendung von Passwörtern hat gezeigt, dass 52 % der Nutzer dasselbe Passwort für zwei oder mehr Konten nutzen oder jeweils nur minimale Änderungen vornehmen, sodass die Passwörter mithilfe von trainingsbasierten Algorithmen leicht vorhergesagt werden können. Darüber hinaus nutzen mehr als 70 % der Befragten dieselben Passwörter für mehr als ein Jahr weiter, nachdem diese durch Datenpannen offengelegt wurden; 40 % sogar für weitere drei Jahre.[2]

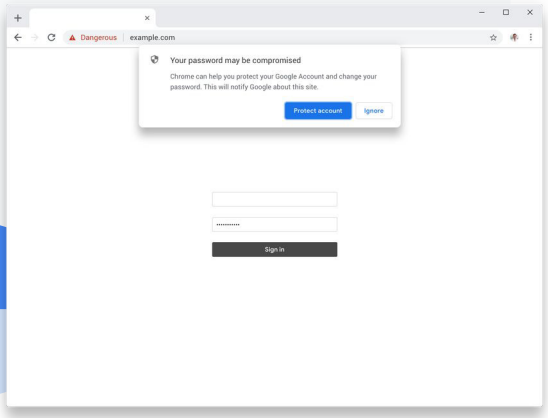
> Chrome verfügt über einige Funktionen, mit denen die Nutzer davon abgehalten werden sollen, dieselben Passwörter oder solche, die bei Datenpannen offengelegt worden sind, wiederzuverwenden.

Mit dem **präventiven Phishingschutz** werden Nutzer gewarnt, sobald sie ein Passwort, das im Passwortmanager von Chrome gespeichert ist, in eine Website eingeben, die unter Phishingverdacht steht. Dies verhindert, dass Angreifer in den Besitz geschäftlicher Anmeldedaten gelangen und diese dazu verwenden, in die Organisation einzudringen (oder sie an andere Angreifer zu verkaufen).

Die **Passwort-Warnung** ist eine für Unternehmen verfügbare Chrome-Richtlinie. Wenn Administratoren diese Funktion aktivieren, erkennt Chrome Nutzer, die ihre geschäftlichen Passwörter auf nicht zugelassenen Websites wiederverwenden. Die Nutzer werden daraufhin benachrichtigt, vor einem Richtlinienverstoß gewarnt und aufgefordert, ihr Passwort zu ändern (Abbildung 2).[3]

Endnutzer können außerdem den Sicherheitsstatus ihrer Passwörter sehen. Wenn Nutzer sich auf einer Website anmelden, werden sie durch den **Passwortcheck** vor einer möglichen Kompromittierung ihres Nutzernamens und Passworts gewarnt. Ihnen wird empfohlen, das Passwort für jedes Konto, bei dem es verwendet wurde, zu ändern.

Außerdem können Nutzer jederzeit einen Passwortcheck durchführen, um zu sehen, ob ihre Passwörter bei einer Datenpanne offengelegt worden sind, ein zu schwaches Sicherheitsniveau aufweisen oder für mehrere Konten verwendet werden (siehe Abbildung 3).



[2] „The Next Domino to Fall: Empirical Analysis of User Passwords across Online Services“, Chun Wang, Steve T.K. Jan, Hang Hu, Douglas Bossart, Gang Wang, Department of Computer Science, Virginia Tech: https://people.cs.vt.edu/gangwang/pass.pdf.
[3] Weitere Informationen zur Passwort-Warnung finden Sie in den FAQs zu „Admin Essentials: Protecting enterprise credentials with Password Alert and the Phishing prevention with Password Alert“.

Richtlinien auf allen Endpunkten erzwingen

Sicherheitsrichtlinien sind dazu da, Nutzer vor gefährlichen Handlungen wie dem Aufruf infizierter Websites oder dem Herunterladen und Installieren schädlicher Anwendungen aus Onlineshops zu bewahren. In beiden Fällen eignen sich Browser hervorragend, um diese Richtlinien auf den unterschiedlichen Endpunkten einheitlich zu erzwingen.

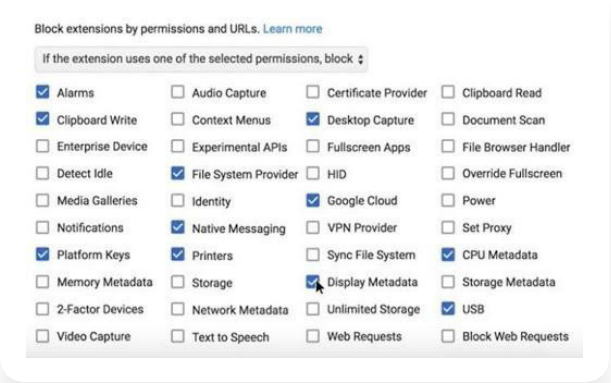
Einige Browser-Richtlinien lassen sich durch die Nutzer individuell festlegen. An dieser Stelle möchten wir jedoch auf Beispiele von Richtlinien eingehen, die zentral in der Chrome-Verwaltung über die Cloud oder über Gruppenrichtlinien konfiguriert und auf verwalteten Endpunkten mithilfe von Chrome erzwungen werden können. Die Chrome-Verwaltung über die Cloud hat den Vorteil, dass Richtlinien sowohl im Unternehmensnetzwerk als auch außerhalb davon erzwungen werden können. Dies eignet sich optimal für mobiles Arbeiten.

Zulassungs- und Sperrlisten für URLs

Mit Sperrlisten können Administratoren die Nutzer davon abhalten, gefährliche oder unangemessene URLs aufzurufen. Und mit Zulassungslisten lässt sich der Zugriff der Nutzer auf genehmigte URLs beschränken. Sperr- und Zulassungslisten können gezielt auf jedes Mitglied einer bestimmten Organisationseinheit oder Nutzergruppe angewendet werden.

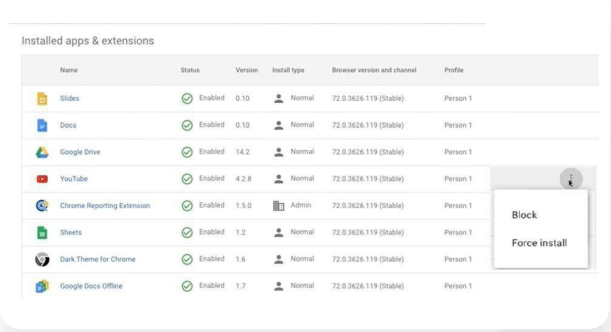
Anwendungen und Erweiterungen steuern

Herunterladbare Anwendungen und Erweiterungen spielen eine wichtige Rolle für die Nutzer. Sie verbessern die Funktionen des Browsers, stellen Anwendungsfunktionen bereit und ermöglichen den Zugriff auf Daten, Dokumente und Computerressourcen. Allerdings stellen sie auch ein Risiko dar, denn Angreifer können Nutzer dazu verleiten, vermeintlich nützliche Anwendungen herunterzuladen und zu installieren, die sich letztendlich als Schadsoftware herausstellen.



Die Chrome-Verwaltung über die Cloud ermöglicht es Administratoren, Sperrlisten bekannter gefährlicher Anwendungen und Erweiterungen zu erstellen und zu erzwingen. Sie können außerdem dafür sorgen, dass Nutzer ausschließlich Inhalte aus der Zulassungsliste herunterladen können.

Zusätzlich können Administratoren jede Anwendung oder Erweiterung blockieren, die bestimmte Berechtigungen fordert – so z. B. den Zugriff auf Drucker oder USB-Ports, das Kopieren von Daten in die Zwischenablage, Audio- und Videoaufnahmen sowie Webanfragen (siehe Abbildung 4). Solche Berechtigungen sind problematisch, wenn es sich um eine schädliche Erweiterung handelt.



Außerdem können Administratoren sehen, welche Anwendungen und Erweiterungen auf jedem verwalteten Endpunkt installiert sind. Sie können die Installation bestimmter Software auf allen verwalteten Endpunkten ihrer Organisation blockieren oder erzwingen (siehe Abbildung 5). Dadurch können sie die Ausführung von verdächtigen oder nicht-arbeitsbezogenen Anwendungen und Erweiterungen verhindern und sicherstellen, dass alle Systeme über die Software verfügen, die den sicherheitsbezogenen und betrieblichen Anforderungen des Unternehmens entspricht. Administratoren können zusätzliche Details in Bezug auf Erweiterungen über eine API exportieren, um weitere Analysen durchzuführen oder Sicherheits- und Complianceberichte anzufertigen.

Angriffsflächen reduzieren

Administratoren können den Missbrauch von Endpunkten durch schädliche Webanwendungen und Erweiterungen verhindern, indem sie beispielsweise den Zugriff auf Mikrofone, Kameras oder USB-Geräte blockieren oder die Ausführung von JavaScript verhindern.

Die Bestätigung in zwei Schritten erzwingen

Die Bestätigung in zwei Schritten schützt Systeme und Daten selbst dann, wenn Passwörter gehackt wurden. Mit Chrome können Administratoren die Nutzung der Bestätigung in zwei Schritten mithilfe einer Vielzahl von Authentifizierungsmethoden erzwingen – darunter die Eingabe von Codes, das Bestätigen einer Aufforderung auf dem Smartphone und das Anschließen eines physischen Sicherheitsschlüssels an den USB-Port des Laptops oder eines anderen Geräts.

Ältere Browser verwalten

Einige Nutzer benötigen weiterhin Zugriff auf ältere Webanwendungen mit Plug-ins und ActiveX-Technologien, die von aktuellen Browsergenerationen nicht unterstützt werden. Allerdings erhöht die Verwendung dieser veralteten Browser nicht nur das Risiko von Datenpannen und gehackten Endpunkten, sondern führt auch zu Problemen in Hinblick auf Leistung und Kompatibilität.

Die in Chrome integrierte Unterstützung älterer Browser reduziert diese Probleme auf ein Minimum und sorgt dafür, dass Nutzer weniger Zeit in unsicheren Browsern verbringen. Administratoren können anhand von Richtlinien festlegen, dass Nutzer Chrome verwenden müssen, um aktuelle Webanwendungen des Unternehmens sowie externe Websites aufzurufen. Außerdem können sie die Nutzung eines älteren Browsers auf bestimmte Anwendungen beschränken, die anders nicht funktionieren würden. So können Nutzer nahtlos zwischen den beiden Oberflächen hin- und herwechseln.

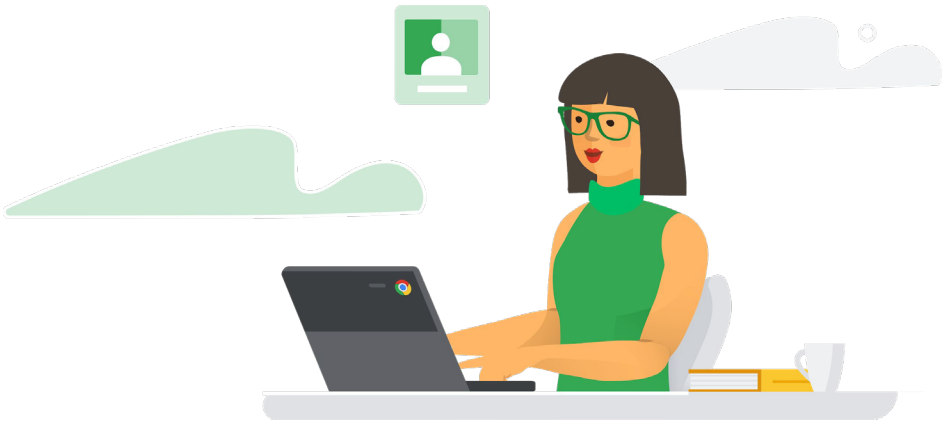
Privatsphäre und Datenschutz

Heutzutage werden viele Endpunkte mit anderen geteilt: Leihgeräte und temporäre Systeme für Gäste und Auftragnehmer, Kioske und andere öffentliche Geräte, temporäre Arbeitsstationen für mobile Mitarbeiter sowie Geräte, die auch außerhalb des Büros verwendet werden, z. B. von Freunden und Familienmitgliedern. In solchen Situationen ist es wichtig, dass Nutzer eines gemeinsam verwendeten Geräts die Aktivitäten des jeweils anderen nicht sehen können. Außerdem ist in vielen Fällen wünschenswert, dass alle Aufzeichnungen über diese Aktivitäten gelöscht werden, sobald ein Nutzer seine Sitzung beendet.

> Auf gemeinsam genutzten Systemen mit Chrome als Browser können Administratoren den Gastmodus und den flüchtigen Modus erzwingen. In beiden dieser Modi können Nutzer die Chrome-Profilinformationen anderer Nutzer weder sehen noch ändern.

Im Gastmodus starten die Nutzer mit einer leeren Benutzeroberfläche – ganz ohne Lesezeichen, aktivierte Anwendungen oder Erweiterungen. Am Ende der Sitzung werden alle Verlaufsinformationen wie besuchte URLs, im Cache gespeicherter Seitentext, Snapshots der besuchten Seiten, Aufzeichnungen der heruntergeladenen Dateien und IP-Adresse von Seiten, die auf den aufgerufenen Websites verlinkt waren, vom Browser gelöscht.

Im flüchtigen Modus können Nutzer die Chrome-Synchronisierung aktivieren, um auf ihre Lesezeichen (einschließlich geschäftlicher Lesezeichen), den Browserverlauf, Anwendungen und Erweiterungen, Intranetseiten und die Webmail des Unternehmens zuzugreifen und Funktionen wie Cloud-Richtlinien und die Passwortspeicherung zu verwenden. Am Ende der Sitzung werden all diese Browseraktivitäten – genau wie im Gastmodus – wieder gelöscht.



Die Sicherheit von Endpunkten auf allen Geräten und Betriebssystemen verwalten

Die Endpunktverwaltung bedeutet für IT- und Sicherheitsorganisationen eine Herausforderung. Traditionell erstellen Administratoren verschiedene Richtlinien und stellen unterschiedliche Agents für unterschiedliche Arten von Endpunkten bereit. Endpunkt-Sicherheitstools mit Updates und Patches versorgen zu müssen, ist eine mühselige Aufgabe. Werden diese Aktualisierungen jedoch vernachlässigt, setzt man die Endpunkte ungeschützt den neuesten Angriffen aus.

Im Gegensatz dazu können Administratoren mit Browsern wie Chrome eine Reihe von Richtlinien erstellen und sie für alle Endpunkte übernehmen. Auch die Nutzer profitieren davon, dass auf jedem ihrer Geräte die gleichen Richtlinien gelten.

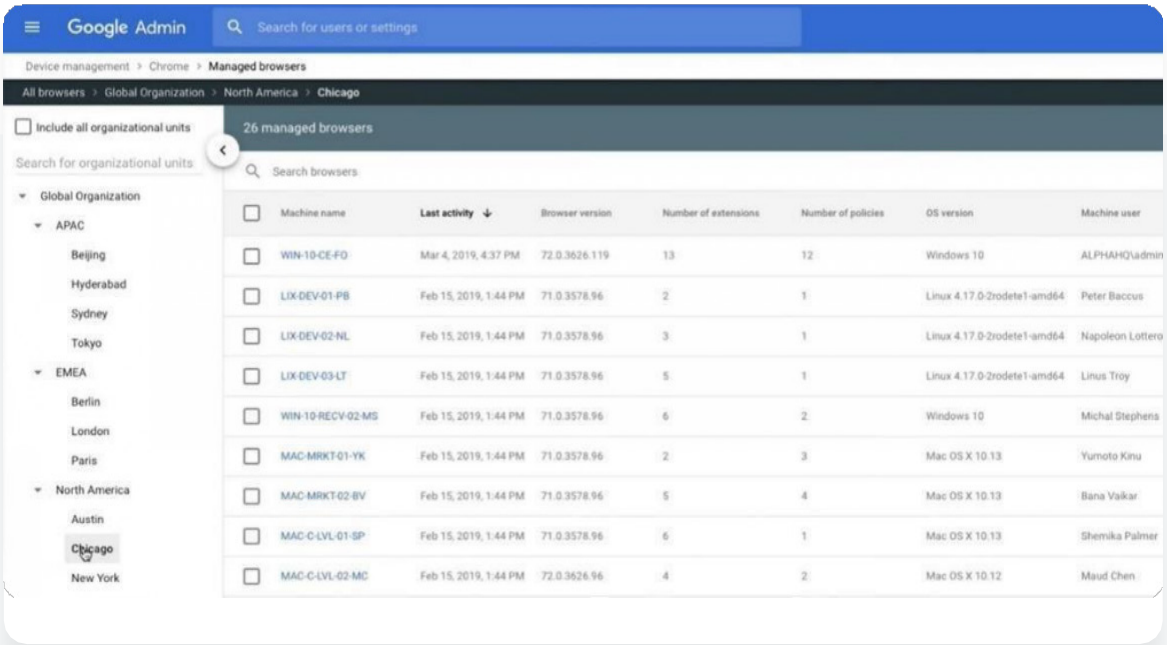
Ein Tool für alle Desktop-Betriebssysteme

Die Chrome-Verwaltung über die Cloud ermöglicht es Administratoren, Sicherheitsrichtlinien über eine einzige Konsole für Chrome-Browser auf Endpunkten mit den Betriebssystemen Windows, MacOS, Linux und Chrome festzulegen und zu verwalten.

> Angesichts der Vertraulichkeit unserer Daten ist ein verlässlicher Schutz ganz entscheidend. Mit Google Chrome können wir ihn an jedem Berührungspunkt, jedem Laptop und bei jedem Nutzer in unserer Organisation gewährleisten.“
>
> **Chief Technology Officer,**
> **The Climate Corporation**

Sichtbarkeit

Die Chrome-Verwaltung über die Cloud bietet einen zentralen Überblick über verwaltete Geräte der Organisation, darunter Informationen wie Betriebssysteme, Version des Chrome-Browsers, installierte Erweiterungen und die Anzahl erzwungener Richtlinien (siehe Abbildung 6).



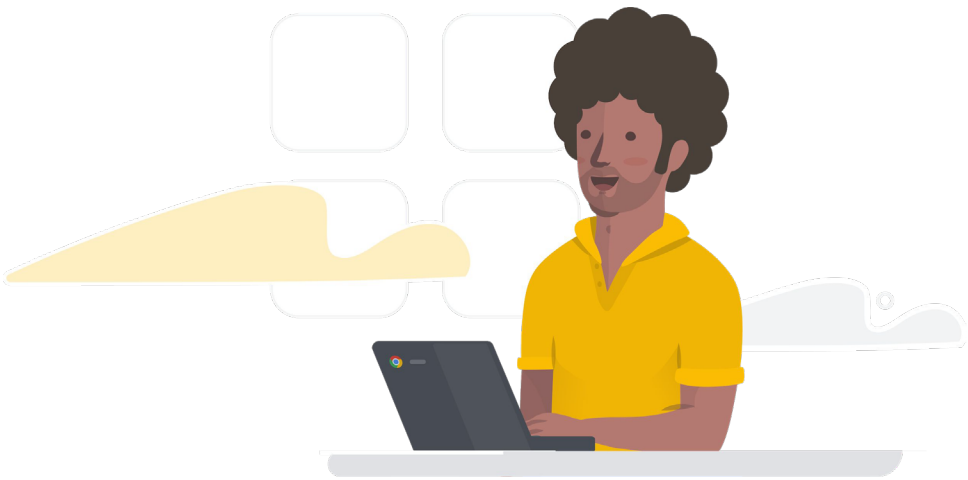
Mühelose Verwaltung

Die Chrome-Verwaltung über die Cloud ermöglicht es Administratoren, Hunderte von Richtlinien in Bezug auf Sicherheit, Erweiterungen, Zugriff, Inhalte, Aufrufbarkeit, Authentifizierung, Unterstützung älterer Browser, Netzwerkeinstellungen, Passwortverwaltung und Berichterstellung im Handumdrehen zu erstellen und zu implementieren.

Chrome-Browser können über Windows-Gruppenrichtlinien oder auf Mac über die Datei „Preferences“ (Einstellungen) registriert werden. Die Registrierung kann auch dadurch abgeschlossen werden, dass die entsprechende Datei direkt auf dem Computer ausgeführt wird. Richtlinien können basierend auf den Nutzerrollen angewandt werden, die in Active Directory definiert wurden, während Browser sich auf Grundlage von Standort, Gerätetyp und anderen Faktoren in Gruppen verwalten lassen. Administratoren müssen sich keine Gedanken darüber machen, Agents für alle Endpunkte bereitzustellen, denn aktualisierte Richtlinien werden automatisch an die Browser ausgegeben. So können Administratoren ausgewählte Browser-Verwaltungsaufgaben an IT-Experten in der Organisation auslagern.

Einbindung in andere Sicherheitstools

Die Chrome-Verwaltung über die Cloud lässt sich zusammen mit Ihren bestehenden Sicherheits- und Managementlösungen nutzen. Sie teilt Informationen über APIs mit Produkten wie VMware Workspace One, Intune, JAMF, SIEMs und anderen Sicherheitstools. Und für Organisationen, die traditionelle Windows-Managementtools bevorzugen, stehen Vorlagen für Gruppenrichtlinien zur Verfügung.



Sicherheit im Browser

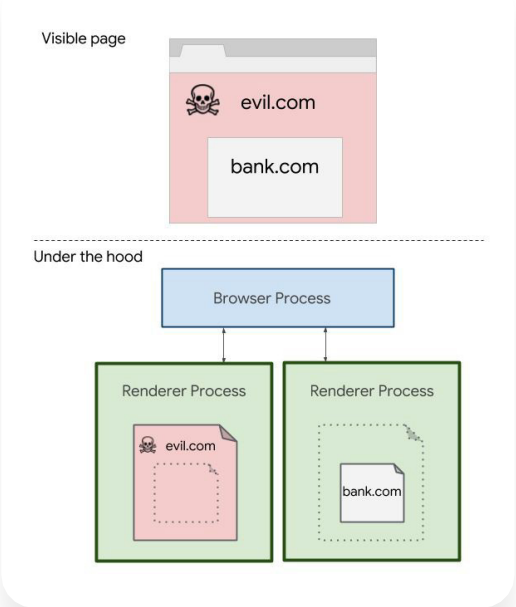
Damit Browser ein effektives Sicherheitstool sind, muss ihr eigener Schutz gewährleistet sein.

Sandbox-Funktionen und Website-Isolierung

Chrome setzt die Sandbox-Technologie ein. Anstatt die Arbeitslast als einen großen Browserprozess zu behandeln, teilt Chrome sie in mehrere separate Prozesse auf und schränkt deren Fähigkeit ein, aufeinander und auf andere Systemressourcen zuzugreifen. Jede Anwendung und Erweiterung läuft dabei in einem eigenen Prozess.

Wenn eine HTML-Seite beispielsweise mehrere JavaScripts enthält, erfolgen das HTML-Rendering und die Ausführung von JavaScript in jeweils eigenen, voneinander getrennten Prozessen. Chrome ändert die Zugriffstokens für die Prozesse, damit schädlicher Code weder andere Prozesse beeinflussen noch Dateien und Registrierungsschlüssel ändern, Dateien in die Zwischenablage kopieren oder Screen Scraping, Keylogging und sonstige gefährliche Aktionen durchführen kann. Dies hält viele Angreifer davon ab, in Anwendungen einzudringen, persistente Malware zu installieren, auf vertrauliche Daten auf der Festplatte zuzugreifen oder Anmeldedaten der Nutzer abzufangen.

Auf Systemen wie Windows, Mac, Linux und ChromeOS geht Chrome sogar noch einen Schritt weiter – mit einer Funktion namens „Website-Isolierung“. Eine einzelne Webseite enthält möglicherweise Inhalte von zwei oder mehr Websites. Mit der Website-Isolierung laufen die Inhalte dieser Seiten in jeweils eigenen Prozessen (Abbildung 7). Auch Prozesse von websiteübergreifenden iFrames werden in separate Prozesse aufgeteilt.



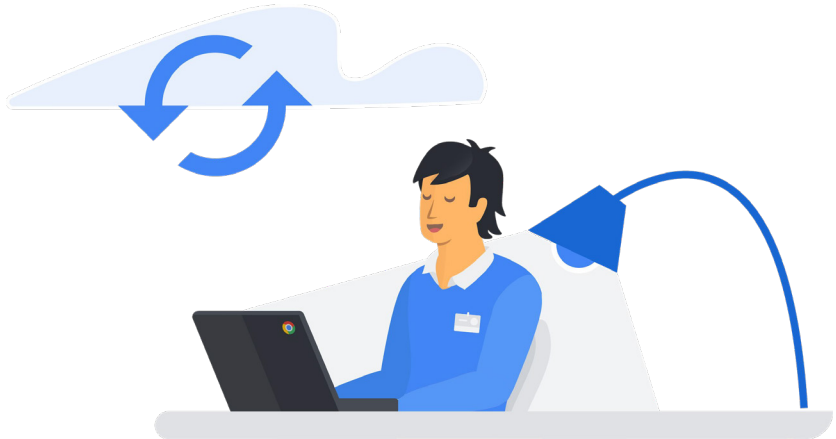
Die Website-Isolierung beschränkt die Auswirkungen von schädlichem Code und Seitenkanalangriffen mit spekulativer Ausführung, wie bei Spectre und Meltdown. Wenn ein Angreifer schädlichen Code von einer gehackten Website (wie evil.com in Abbildung 7) an den Browser sendet, kann dieser Code keine Informationen von anderen Websites (wie bank.com in Abbildung 7) stehlen, da der Code dieser Websites in separaten, geschützten Prozessen läuft.

Regelmäßige, automatische Updates

Zum Schutz Ihrer Belegschaft ist es äußerst wichtig, dass Browser auf dem neuesten Stand gehalten werden. Dies erreicht man ausschließlich dadurch, dass Updates und Patches schnell bereitgestellt werden können – ohne viel Aufwand und Mühe.

Chrome ist genau dafür optimiert. Jeder Browser führt in regelmäßigen Abständen eine Prüfung auf Sicherheitsupdates durch, die anschließend automatisch installiert werden und keine Handlung vonseiten des Nutzers erfordern. Außerdem sorgt Google dafür, dass die Patches schnell verteilt werden. Wir haben die üblicherweise benötigte Dauer zwischen dem Zeitpunkt, an dem ein Sicherheitsproblem in einer Open-Source-Bibliothek als behoben gilt, bis zu dem Zeitpunkt, an dem die entsprechende Fehlerkorrektur bereitgestellt wird („Patch Gap“), auf nur 20 Tage reduziert – schneller als bei anderen gängigen Browsern.

> “Patches und der Umgang mit Sicherheitslücken sind für uns ein großes Thema. Seit Chrome sich automatisch aktualisiert, können wir in puncto Sicherheit aufatmen.“
>
> **Head of Security, Blend**



Fazit

Der Browser ist das Herzstück der Unternehmensproduktivität und wird Tag für Tag für die unterschiedlichsten Aufgaben genutzt. Er ermöglicht es Nutzern, intelligenter und effizienter im Web zu arbeiten – unabhängig von Gerät und Plattform.

Browser steigern aber nicht nur die Produktivität. IT-Sicherheitsexperten sollten Browser aus einem neuen Blickwinkel betrachten – nämlich als Software, die in puncto Endpunktsicherheit die erste Abwehrlinie bildet. Da Browser sich genau dort befinden, wo Internet, Nutzer und Anwendungen aufeinandertreffen, eignen sie sich hervorragend dazu, Nutzer in Echtzeit zu schützen und wichtige Sicherheitsrichtlinien zu erzwingen.

So kann Chrome im Rahmen der umfassenden Sicherheitsstrategien von Unternehmen als taktische Schutzmaßnahme zum Einsatz kommen. Dank Funktionen wie Safe Browsing und Passwort-Warnung sind Nutzer besser vor Gefahren im Web und Verstößen gegen Sicherheitsrichtlinien geschützt. Außerdem werden sie vor unsicheren Aktionen gewarnt. Administratoren können Richtlinien auf Endpunkten mithilfe von Zulassungs- und Sperrlisten (auch für URLs) festlegen und erzwingen. Anwendungen und Erweiterungen können (auch nach Berechtigung) blockiert oder erzwungen installiert werden. Darüber hinaus lässt sich die Bestätigung in zwei Schritten erzwingen und die Nutzung älterer Browser in einem geregelten Rahmen genehmigen. Der Chrome-Browser und die Chrome-Verwaltung über die Cloud machen es einfach, Daten zu Geräten und Nutzeraktivitäten zu erfassen und Richtlinien einheitlich auf allen Geräten und Betriebssystemen zu verwalten und zu erzwingen.

> Als IT-Sicherheitsexperte sollten Sie in Browsern die erste Abwehrlinie in puncto Endpunktsicherheit sehen. Chrome kann die Sicherheit Ihres Unternehmens stärken und dazu beitragen, dass Sie produktiver und effektiver arbeiten.