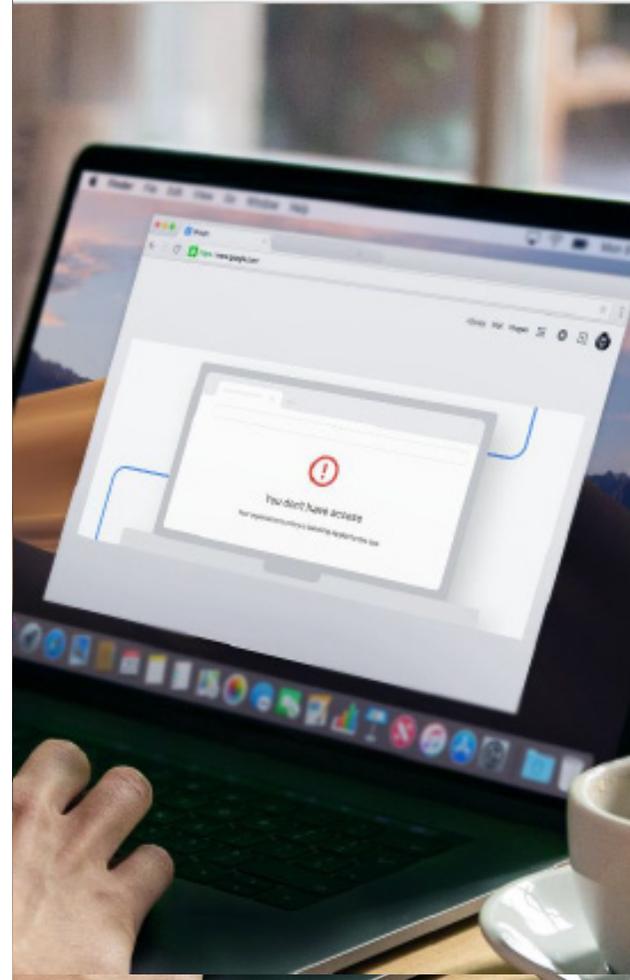


Mehr Browserschutz für Unternehmen – dank Google Chrome

Immer mehr Arbeiten werden im Web ausgeführt. Daher sollten Browser heutzutage sowohl die Produktivität fördern als auch wie eine zusätzliche Sicherheitsebene funktionieren. Dieser Wandel bedeutet, dass IT- und Sicherheitsteams gemeinsam dafür sorgen müssen, sowohl die Unternehmensdaten als auch die Nutzer zu schützen und gleichzeitig der Belegschaft ein nahtloses Arbeiten zu ermöglichen.

Der Browser stellt eine der wenigen Technologien dar, die Nutzer und Sicherheit eines Unternehmens gekonnt miteinander verbinden. Da Chrome bereits von Millionen geschäftlichen Nutzern verwendet wird, gibt es *keinen besseren Ort*, um den Browserschutz für Unternehmen zu optimieren.

Chrome bietet Unternehmen die Einstellungen und Sicherheitsmaßnahmen, mit denen Daten sicher geschützt werden. In Kombination mit [BeyondCorp Enterprise](#), der Zero-Trust-Sicherheitslösung von Google, können Unternehmen kontextsensitiven Zugriff erzwingen und für zusätzlichen Datenschutz auf verwalteten und nicht verwalteten Geräten sorgen. Außerdem stellen sie so ein einheitliches Sicherheitsniveau für hybride Belegschaften und Mitarbeiter im Homeoffice bereit. **Mit Chrome setzt Google höhere Standards bei der Browsersicherheit für Unternehmen.**



Die Cyberkriminalität ist seit 2020 um **600 %** gestiegen.¹

Der sichere Browser für moderne Mitarbeiter



Schutz vor Datenverlust

Ob Versehen oder Exfiltration – den Verlust sensibler Unternehmensdaten erkennen und verhindern sowie Datenschutzrichtlinien erzwingen



Den Zugriff auf SaaS-Apps absichern

Kontextsensitiven Zero-Trust-Zugriff auf SaaS-Anwendungen bereitstellen sowie unautorisierte Zugriffe und Verstöße reduzieren



Verwaltete und nicht verwaltete Geräte schützen

Dank Malware- und Phishing-Schutz eine zentrale Ebene der Sicherheitsverwaltung auf allen Geräten ermöglichen, einschließlich BYOD-Umgebungen – ganz ohne Agent



Remote-Mitarbeiter, hybride Beschäftigte und erweiterte Belegschaft besser schützen

Sicherer Zugriff auf Unternehmensressourcen und -informationen – auch für Nutzer außerhalb des Unternehmensnetzwerks und Teilzeitarbeiter

Datenschutz

Datenverlust und -exfiltration in Unternehmen verhindern

Mit der Unterstützung von BeyondCorp Enterprise lässt sich der Schutz vor Datenverlust direkt auf Browserebene einrichten – darunter Upload, Download, Drucken, Speichern, Kopieren und Einfügen von Inhalten.



Schutz vor Malware und Phishing

Nutzer während der Arbeit im Web vor Echtzeit-Bedrohungen schützen

Es stehen Richtlinien zur Verfügung, mit denen nicht vertrauenswürdige Dateien blockiert oder Nutzer davon abgehalten werden, unsichere URLs aufzurufen.



Sicherheitsberichte und Statistiken

Sicherheitspläne in Unternehmen effizienter machen und auf Informationen zu wichtigen Sicherheitsereignissen zugreifen – dank ausführlicher Browser-Statistiken

Für zusätzliche forensische Untersuchungen kann Chrome Informationen über die Wiederverwendung von Passwörtern, den Aufruf unsicherer Websites, die Übertragung von Malware, die Anmeldung sowie gehackte Passwörter an verschiedene Google-Lösungen und weitere integrierte Drittanbietertools senden.



Erweiterungen verwalten

Installation von Erweiterungen blockieren oder erzwingen und Endnutzern erlauben, bestimmte Erweiterungen anzufordern – für noch mehr Browsersicherheit

Erweiterungsanfragen lassen sich zentral verwalten und genehmigen. Mit den Richtlinien für Erweiterungen können Sie die Anfragen Ihrer Nutzer beschränken oder mehr Einblick in diesbezügliche Informationen gewinnen.



Risikomanagement von Geräten

Schnelle und automatische Updates für Zero-Day-Sicherheitslücken

Nach jeder automatischen Aktualisierung wird der Nutzer aufgefordert, Chrome neu zu starten, um das Update zu aktivieren. Schließlich hängt die Unternehmenssicherheit davon ab, dass alle Chrome-Browser immer über die neuesten Sicherheitspatches verfügen.



Adaptive Richtlinienverwaltung

Hunderte von Richtlinien zentral verwalten, um Nutzern ein sicheres und geschütztes Surfen im Web zu ermöglichen

Mit nur einem Browser sorgen Sie für den bestmöglichen Schutz von Nutzern mit hohem Risiko – ohne dabei die Produktivität der Nutzer mit niedrigem Risiko zu beeinträchtigen.



Wir von Roche haben uns für Google Chrome und BeyondCorp Enterprise Essentials entschieden, um die Browsersicherheit in unserem Unternehmen zu stärken. So verfügen wir über einen umfassenden Einblick und profitieren von Sicherheitsmaßnahmen, mit denen sich Nutzer und Unternehmensdaten gleichermaßen schützen lassen. Da die Sicherheitsfunktionen in den Browser integriert sind, profitieren wir auf all unseren verwalteten und nicht verwalteten Geräten davon. Sobald diese Lösung aktiviert wurde, konnten wir einen großflächigen Exfiltrationsangriff auf unsere Unternehmensdaten binnen weniger Stunden identifizieren und aufhalten. Die Möglichkeit, erweiterte Sicherheitsberichte zu Ereignissen wie dem Transfer von Inhalten direkt in Chrome zu erhalten, bietet einen enormen Vorteil: Wir können so sowohl ungewollte Datenübertragungen blockieren als auch verstehen, wie Daten bei Roche weitergegeben werden.“

Tim Ehrhart
Domain Head, Informationssicherheit



Weitere Informationen dazu, warum Millionen von Unternehmen Google Chrome als Browser nutzen, finden Sie unter <https://chromeenterprise.google/browser/security/>