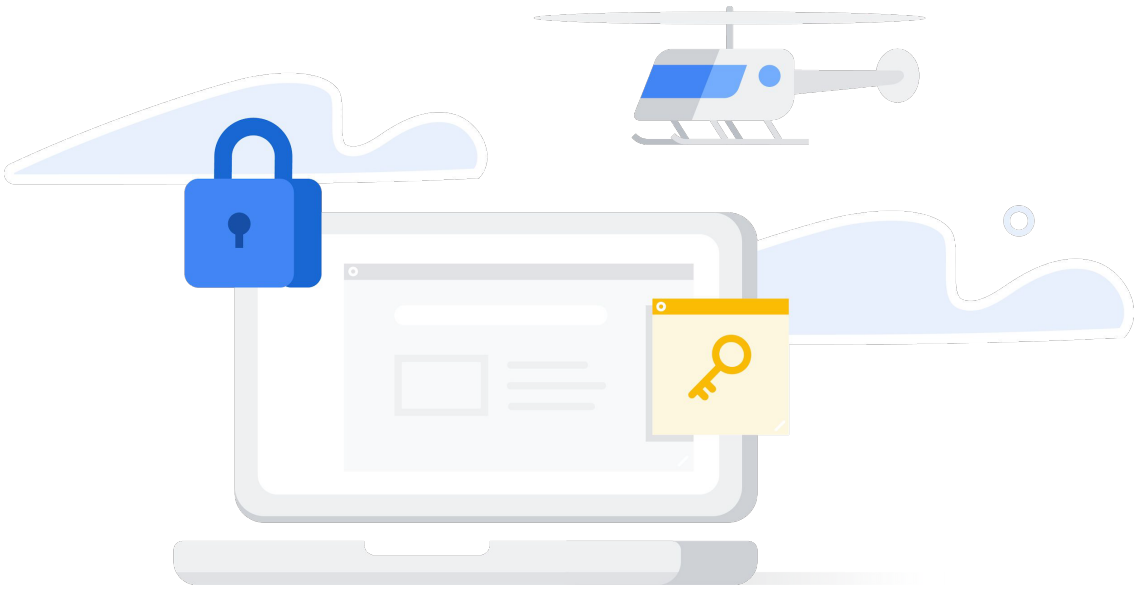
chrome enterprise

De browser is de nieuwe frontlinie voor eindpuntbeveiliging

Hoe de Chrome-browser een centrale rol kan spelen bij de beveiligingsstrategie van je bedrijf



Browsers als strategische beveiligingstool

Veel mensen onderschatten browsers. Ze denken dat je ze alleen maar kunt gebruiken om op internet te gaan. Maar browsers hebben zich inmiddels ontwikkeld tot geavanceerde platforms. Ze stellen scripts en code samen en voeren deze uit en zorgen dat gebruikers efficiënt kunnen zoeken en het web en apps kunnen gebruiken. Ze bieden rijke, meeslepende ervaringen waarin tekst, afbeeldingen, audio, video en virtual reality worden gecombineerd, en integreren naadloos meerdere apps en extensies.

Browsers bevatten al een heleboel functies om netwerk- en eindpuntbeveiliging te verbeteren. Ze bevinden zich zelfs in de unieke positie om te dienen als strategische laag in de beveiliging van bedrijven. In browsers komen het web, gebruikers en apps namelijk samen. Browsers zijn perfect om het volgende te doen:

In realtime communiceren met gebruikers en ze wegleiden van gevaarlijk gedrag.

Op gebruikers gericht beveiligingsbeleid afdwingen op eindpunten.

Makkelijk en consequent dezelfde opties voor eindpuntbeveiliging instellen voor verschillende apparaten en besturingssystemen.

In dit artikel leggen we uit hoe browsers dit doen aan de hand van voorbeelden met de Google Chrome-browser.

Gebruikers wegleiden van gevaarlijk gedrag

Bedrijven investeren miljarden euro's in krachtige beveiligingstools om malware en andere indicatoren van schadelijke activiteit te detecteren in hun systemen en netwerken. Helaas kunnen hackers die tools meestal omzeilen door de zwakste schakels van de bedrijfsbeveiliging uit te buiten: computer- en smartphone-gebruikers, zoals werknemers, contractanten, klanten en leveranciers.

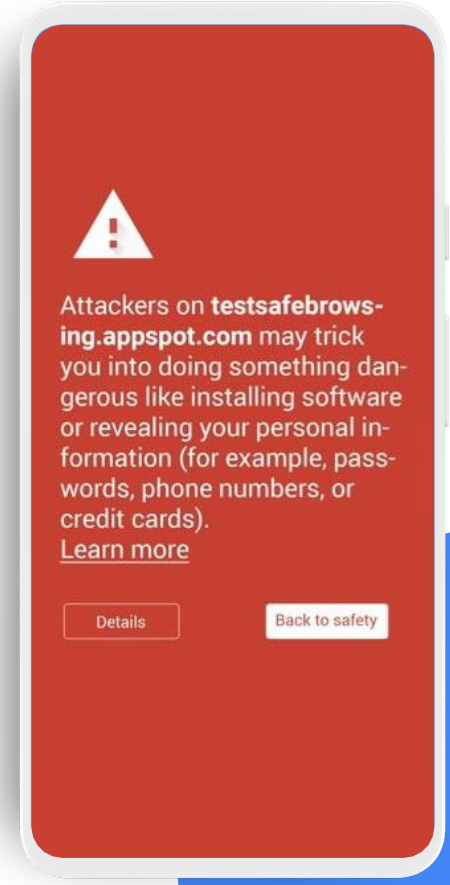
Tegenwoordig leiden aanvallen van phishing en social engineering gebruikers op slimme manieren naar websites die door de hackers worden beheerd. Daar downloaden ze schadelijke bestanden, voeren ze hun inloggegevens in op formulieren of maken ze zelfs geld over naar onbekende bankrekeningen. Zelfs de beste beveiligingsprogramma's kunnen deze schadelijke acties alleen maar verminderen, niet helemaal voorkomen.

Browsers kunnen voorkomen dat gebruikers fouten maken door ze weg te leiden van gevaarlijk gedrag. De Chrome-browser bevat enkele hele handige functies waarmee gebruikers een melding krijgen van mogelijke aanvallen van phishing en social engineering en zien wat ze kunnen doen.

Safe Browsing: Realtime bescherming tegen phishing en schadelijke software

Safe Browsing in Chrome zorgt dat gebruikers niet naar geïnfecteerde en schadelijke websites gaan.

De Safe Browsing-service van Google onderzoekt de content van miljarden webpagina's en houdt een lijst bij met onveilige websites. Dit zijn niet alleen sites die zijn gemaakt door hackers, maar ook legitieme websites die zijn gehackt. Google herkent deze sites doordat er malware op aanwezig is, doordat ze eerder zijn gebruikt in aanvallen van phishing en social engineering, of doordat ze links of code bevatten die gebruikers naar een aanvalssite sturen. Andere indicatoren zijn pogingen om de site te laten lijken op andere, vertrouwde entiteiten en websites, en tekst en formulieren waarin gebruikers wordt gevraagd hun wachtwoord in te voeren, een nummer voor technische support te bellen of software te downloaden. De Safe Browsing-service herkent momenteel meer dan 21.000 malware-aanvalssites en 1,8 miljoen phishingsites. De service stuurt elke dag meer dan 3 miljoen waarschuwingen naar gebruikers.



> Elke keer dat gebruikers naar een website proberen te gaan die op de Safe Browsing-lijst staat, zien ze een waarschuwing in de Chrome-browser waarin het risico wordt uitgelegd en een knop waarmee ze teruggaan naar een veilige pagina (zie figuur 1). In 2019 is deze waarschuwing meer dan een miljard keer getoond.

De Safe Browsing-service updatet de lijst elke 30 minuten met nieuw ontdekte malware- en phishingsites. Safe Browsing staat standaard aan. Als een beheerder of eindgebruiker de uitgebreide versie van Safe Browsing aanzet, inspecteert de Chrome-browser elke webpagina in realtime. Zo zijn gebruikers beschermd tegen hackers die elke paar minuten een nieuwe URL maken om beveiligingstools te omzeilen die conventionele URL-blokkeerlijsten gebruiken. IT-teams kunnen Safe Browsing centraal instellen voor hun organisatie via een beleidsregel.

Volgens analyses van Google zijn gebruikers die deze functie gebruiken 30-50% beter beschermd tegen phishing.

Safe Browsing beschermt gebruikers ook tegen schadelijke extensies en software. Als Chrome wordt opgestart of de Safe Browsing-lijst wordt geüpdatet, scant Chrome de extensies die zijn geïnstalleerd in de browser en worden deze vergeleken met schadelijke extensies op de Safe Browsing-lijst. Als de extensie op de lijst staat, zet Chrome de extensie uit. De gebruiker wordt geïnformeerd en ziet in sommige gevallen opties om de extensie te verwijderen of weer aan te zetten.

Als gebruikers een bestand downloaden, checkt de Chrome-browser ook of het bestandstype op een lijst met gevaarlijke bestandstypen staat, zoals uitvoerbare bestanden en documenttypen die vaak worden misbruikt. Als Chrome de veiligheid van het bestand niet kan bevestigen, worden de gegevens naar de servers van Google gestuurd om te bepalen of het bestand veilig is. Als Chrome een negatieve reactie van de servers krijgt, zien de gebruikers een waarschuwing.[1]

De uitgebreide versie van Safe Browsing biedt nog meer bescherming tegen schadelijke websites en downloads. Door in realtime gegevens te delen met Google Safe Browsing kan Chrome gebruikers proactief beschermen tegen gevaarlijke sites. Als gebruikers zijn ingelogd, krijgen ze in Chrome en andere Google-apps (zoals Gmail en Drive) uitgebreidere bescherming, doordat aanvallen die zich voordoen op het web en aanvallen tegen dat Google-account samen worden herkend. Met andere woorden: met de uitgebreide versie van Safe Browsing krijg je de intelligentie van de toonaangevende beveiligingstools van Google, rechtstreeks in de browser.

Safe Browsing beschermt mensen ook als ze verschillende taken uitvoeren via Google Zoeken, Gmail en Android-smartphones.

[1]Je vindt meer informatie over Google Safe Browsing in het Google Transparantierapport en het artikel over privacy in Chrome.

Geavanceerde wachtwoordbeveiliging

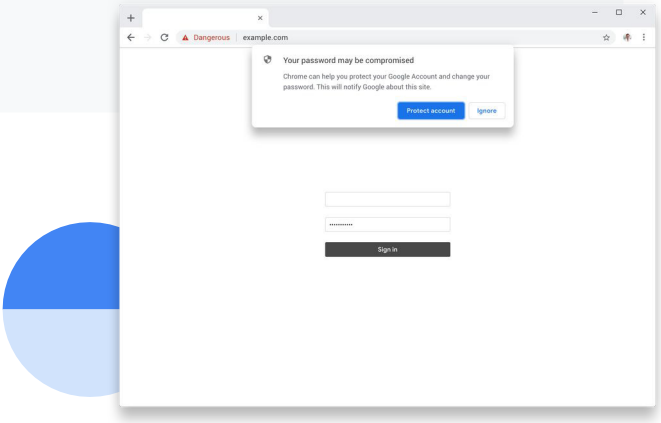
Met gebruikerswachtwoorden kunnen hackers toegang krijgen tot netwerken, apps en gegevens. Dit is een groot probleem, omdat veel mensen hetzelfde wachtwoord gebruiken voor meerdere accounts en dit niet wijzigen als het is gehackt. Een uitgebreide studie naar hergebruik van wachtwoorden toont aan dat 52% van de gebruikers hetzelfde wachtwoord gebruikt voor 2 of meer accounts of slechts kleine wijzigingen aanbrengt die kunnen worden voorspeld door trainingsgebaseerde algoritmen. Bovendien gebruikt 70% van de gebruikers uit het onderzoek nog steeds hetzelfde wachtwoord meer dan een jaar nadat het is blootgelegd bij een gegevenslek. 40% van de gebruikers gebruikt een gehackt wachtwoord zelfs 3 jaar later nog.[2]

> Chrome bevat verschillende functies om te zorgen dat gebruikers wachtwoorden niet kunnen hergebruiken en wachtwoorden die zijn blootgelegd bij een gegevenslek helemaal niet meer kunnen gebruiken.

Met **voorspellende bescherming tegen phishing** zien gebruikers een waarschuwing als ze een wachtwoord dat is opgeslagen in de Chrome Wachtwoordmanager invoeren op een mogelijke phishingsite. Zo krijgen hackers geen zakelijke inloggegevens in handen waarmee ze kunnen inbreken bij de organisatie (of die ze kunnen verkopen aan andere hackers).

Password Alert is een beleid voor de Chrome-browser dat organisaties kunnen gebruiken. Als beheerders deze functie aanzetten, detecteert de Chrome-browser het als gebruikers hun bedrijfswachtwoord hergebruiken op niet-goedgekeurde websites. De gebruikers krijgen een melding waarin staat dat ze een beleidsregel schenden en ze worden gevraagd hun wachtwoord te resetten (zie figuur 2).[3]

Eindgebruikers kunnen ook inzicht krijgen in de status van hun wachtwoord. Als gebruikers hun inloggegevens invoeren op een website, stuurt **Wachtwoordcheck** ze een waarschuwing als de gebruikersnaam en het wachtwoord zijn blootgelegd in een gegevenslek en worden ze gevraagd het wachtwoord te wijzigen in elk account waarin het wordt gebruikt. Gebruikers kunnen Wachtwoordcheck ook altijd uitvoeren om te checken of wachtwoorden openbaar zijn gemaakt tijdens een gegevenslek, zwak zijn of worden gebruikt in meerdere accounts (zie figuur 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] Bekijk meer informatie over Password Alert in Essentiële beheertools: zakelijke inloggegevens beschermen met Password Alert, en Veelgestelde vragen over phishing voorkomen met Password Alert.

Beleid afdwingen op alle eindpunten

Je stelt beveiligingsbeleid in om te voorkomen dat gebruikers gevaarlijke acties uitvoeren, zoals schadelijke websites bezoeken of schadelijke apps downloaden en installeren vanuit online stores. In beide gevallen kun je via de browser instellen dat dit beleid wordt afgedwongen op verschillende soorten eindpunten.

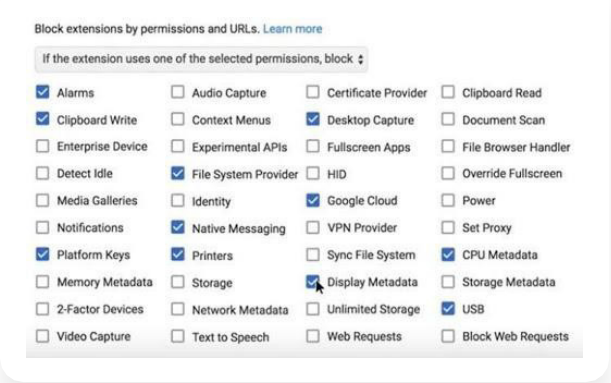
Browsergebruikers kunnen sommige beleidsregels zelf instellen, maar hier zie je voorbeelden van beleidsregels die je centraal kunt beheren met Cloudbeheer voor de Chrome-browser of via Groepsbeleid en die je kunt afdwingen op beheerde eindpunten met de Chrome-browser. Met Cloudbeheer voor de Chrome-browser kun je beleid afdwingen binnen en buiten je bedrijfsnetwerk. Dit is ideaal als mensen thuiswerken.

Toelatings- en blokkeerlijsten voor URL's

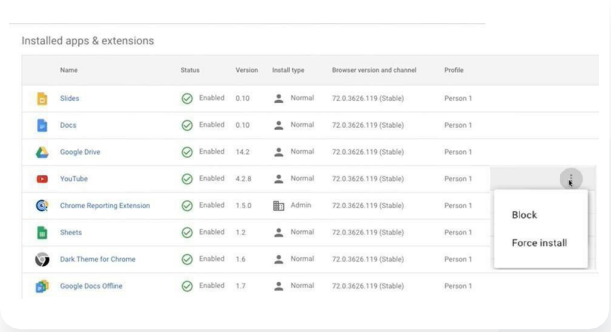
Beheerders kunnen blokkeerlijsten maken om te zorgen dat gebruikers niet naar gevaarlijke of ongepaste URL's gaan. Ze kunnen toelatingslijsten gebruiken om gebruikers te beperken tot bepaalde goedgekeurde URL's. Je kunt blokkeerlijsten en toelatingslijsten toepassen op alleen bepaalde leden van specifieke organisatie-eenheden of gebruikersgroepen.

Controle over apps en extensies

Het is belangrijk dat gebruikers apps en extensies kunnen downloaden. Ze voegen meer functies toe aan de browser, bieden app-functionaliteit en geven toegang tot gegevens, documenten en computingresources. Maar veel hackers proberen gebruikers te misleiden zodat ze schadelijke software downloaden en installeren die is vermomd als nuttige app.



Met Cloudbeheer voor de Chrome-browser kunnen beheerders blokkeerlijsten met bekende gevaarlijke apps en extensies maken en afdwingen. Ze kunnen ook instellen dat gebruikers alleen goedgekeurde apps en extensies kunnen downloaden, door een toelatingslijst te maken.



Bovendien kunnen beheerders alle apps en extensies blokkeren die om bepaalde rechten vragen, bijvoorbeeld toegang tot printers of USB-poorten, schrijftoegang tot het klembord, rechten om audio of video vast te leggen of om webverzoeken te doen (zie figuur 4). Deze rechten kunnen problemen opleveren als een extensie schadelijk is.

Daarnaast kunnen beheerders zien welke apps en extensies zijn geïnstalleerd op elk beheerd eindpunt. Ze kunnen specifieke apps en extensies blokkeren of de installatie ervan afdwingen op alle beheerde eindpunten in hun organisatie (zie figuur 5). Zo worden apps en extensies die niet nodig zijn voor het werk, of die verdacht zijn, geblokkeerd en bevatten alle systemen de software die nodig is voor beveiliging of uitvoering van het werk. Beheerders kunnen meer informatie over extensies exporteren via een API. Zo kunnen ze extensies nog uitgebreider analyseren of beveiligings- en nalevingsrapporten maken.

Het risico op aanvallen verkleinen

Beheerders kunnen het risico verkleinen dat schadelijke web-apps en extensies eindpuntresources misbruiken, bijvoorbeeld door de toegang tot microfoons, camera's en USB-apparaten te blokkeren of door in te stellen dat JavaScript niet kan worden uitgevoerd.

Verificatie in 2 stappen afdwingen

Met verificatie in 2 stappen blijven systemen en gegevens beschermd, zelfs als wachtwoorden zijn gelekt. Met de Chrome-browser kunnen beheerders het gebruik van verificatie in 2 stappen afdwingen met verschillende verificatiemethoden, zoals een code uit een sms invoeren, op een prompt op een smartphone tikken of een fysieke beveiligingssleutel insteken in een USB-poort op de laptop of het apparaat.

Verouderde browsers beheren

Sommige gebruikers moeten oude web-apps kunnen openen, die plug-ins en ActiveX-technologie gebruiken die niet wordt ondersteund door de huidige generatie browsers. Maar als je toestaat dat gebruikers onveilige verouderde browsers gebruiken die wel werken met die apps, loop je het risico dat eindpunten worden gehackt en gegevens worden gelekt. Ook kan dit problemen opleveren met prestaties en ondersteuning.

De functie Ondersteuning voor oudere browsers is geïntegreerd in Chrome om deze problemen zo klein mogelijk te maken en te zorgen dat gebruikers zo min mogelijk tijd doorbrengen in minder veilige browsers. Beheerders kunnen beleid instellen zodat gebruikers Chrome moeten gebruiken om up-to-date zakelijke web-apps en externe websites te openen, en de verouderde browser alleen gebruiken voor specifieke apps waarvoor dit vereist is. Gebruikers kunnen indien nodig naadloos schakelen tussen de 2 browsers.

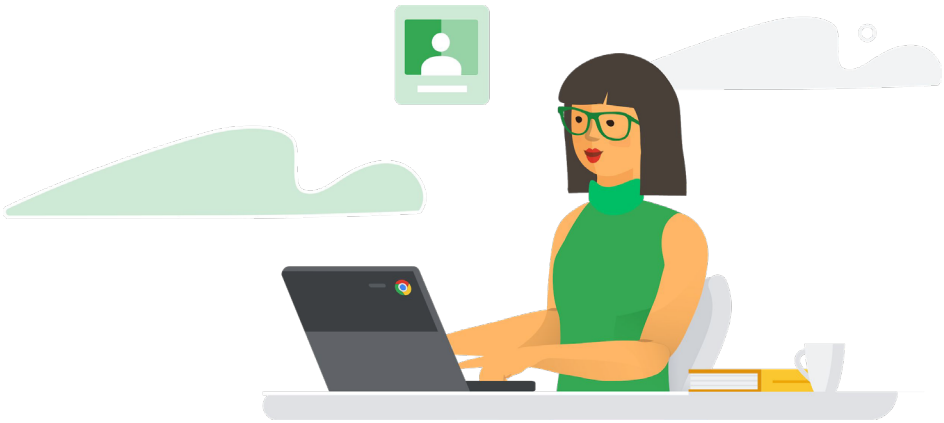
Zorgen voor privacy en vertrouwelijkheid

Tegenwoordig worden veel eindpunten gedeeld, bijvoorbeeld als uitleenapparaten en tijdelijke systemen voor gasten en contractanten, als openbare apparaten zoals kiosks, als tijdelijke werkstations voor mobiele werknemers en als parttime persoonlijke apparaten die worden uitgeleend aan vrienden en gezinsleden buiten het werk. In deze situaties is het erg belangrijk dat gebruikers die apparaten delen, elkaars activiteiten niet kunnen zien. In veel gevallen is het zelfs wenselijk dat die activiteiten worden gewist zodra gebruikers de sessie beëindigen.

> Op gedeelde systemen met de Chrome-browser kunnen beheerders de gastmodus en de kortstondige modus afdwingen. In beide modi kunnen gebruikers de Chrome-profielgegevens van andere gebruikers niet zien of aanpassen.

In de gastmodus beginnen gebruikers met een schone lei, zonder bookmarks of actieve apps en extensies. Aan het eind van de sessie wist de browser alle gegevens in de browsegeschiedenis, zoals bezochte URL's, paginatekst in het cachegeheugen, momentopnamen van bezochte pagina's, records van opgeslagen bestanden en IP-adressen van pagina's gelinkt op de bezochte websites.

In de kortstondige modus kunnen gebruikers Chrome-synchronisatie aanzetten om toegang te krijgen tot hun bookmarks (inclusief zakelijke bookmarks), de browsegeschiedenis, apps en extensies, intranetpagina's van het bedrijf en hun zakelijke webmail. Ook kunnen ze functies als cloudbeleid en wachtwoordopslag gebruiken. Maar aan het eind van de sessie worden alle records van browse-activiteit gewist, net als in de gastmodus.



Eindpuntbeveiliging beheren op alle apparaten en besturingssystemen

Eindpuntbeheer is een uitdaging voor IT-beheerders en beveiligingsorganisaties. Traditioneel stellen beheerders verschillende beleidsregels in en implementeren ze verschillende agents voor verschillende soorten eindpunten. Het is een hele klus om beveiligingstools voor eindpunten te updaten en te patchen, maar als je dit niet doet, zijn eindpunten kwetsbaar voor de nieuwste aanvallen.

Met een browser als Chrome daarentegen kunnen beheerders één reeks beleidsregels maken en die toepassen op alle eindpunten, zonder meerdere agents te hoeven implementeren, updaten of patchen. Dit heeft ook voordelen voor gebruikers, omdat ze op alle apparaten hetzelfde beleid volgen.

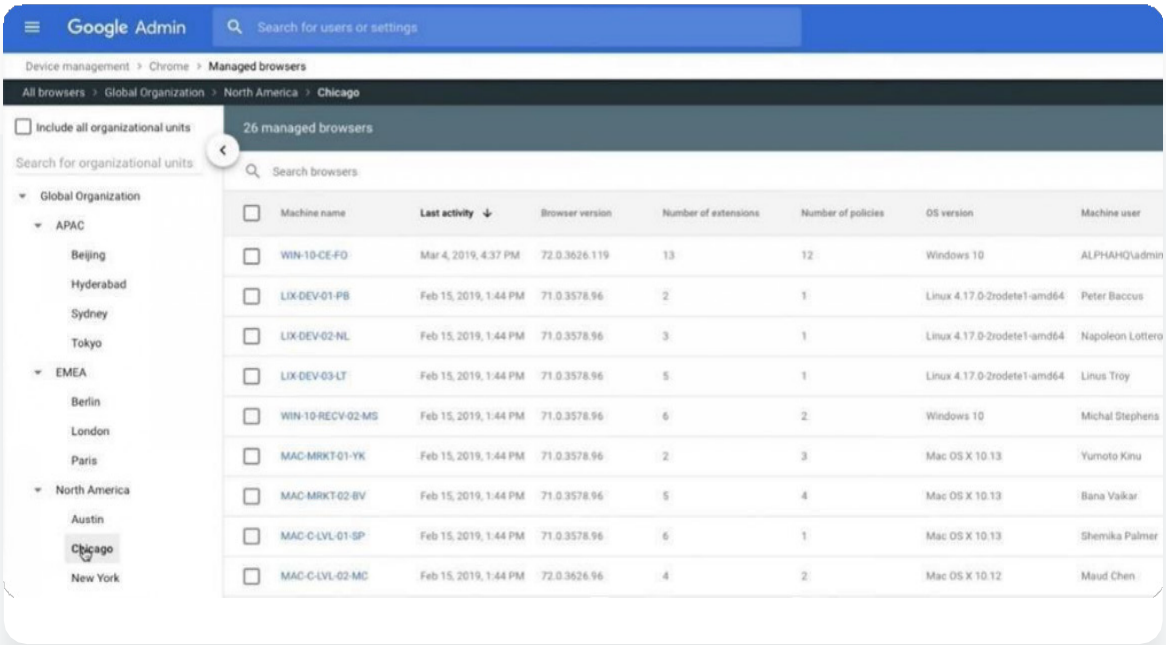
Eén tool voor alle desktopbesturingssystemen

Met Cloudbeheer voor de Chrome-browser kunnen beheerders beveiligingsbeleid instellen en beheren vanuit één console voor Chrome-browsers op eindpunten met de besturingssystemen van Windows, MacOS, Linux en Chrome.

> Beveiliging is belangrijk omdat ons werk zo gevoelig is. Met de Chrome-browser kunnen we de beveiliging beheren voor elk contactpunt, elke laptop en elke gebruiker in onze organisatie."
>
> **Chief Technology Officer,**
> **The Climate Corporation**

Zichtbaarheid

Met Cloudbeheer voor de Chrome-browser krijg je centraal inzicht in beheerde apparaten in je organisatie, zoals het besturingssysteem, de versie van de Chrome-browser, geïnstalleerde extensies en hoeveel beleidsregels er worden afgedwongen (zie figuur 6).



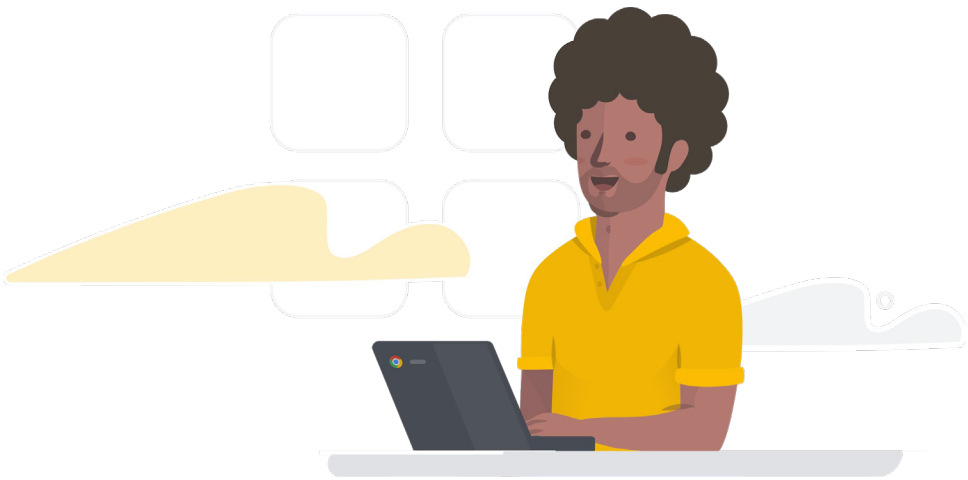
Makkelijk beheer

Met Cloudbeheer voor de Chrome-browser kunnen beheerders snel honderden beleidsregels maken en implementeren voor onder andere beveiliging, extensies, toegankelijkheid, content, weergaven, verificatie, ondersteuning voor oudere browsers, netwerkinstellingen, wachtwoordbeheer en rapporten.

Ze kunnen Chrome-browsers inschrijven via Windows Groepsbeleid of het Preference-bestand op de Mac. Ze kunnen ook een bestand rechtstreeks op het apparaat uitvoeren. Beleid kan worden toegepast gebaseerd op gebruikersrollen die zijn opgegeven in Active Directory. Browsers kunnen worden beheerd in groepen gebaseerd op onder andere locatie en apparaattype. Beheerders hoeven geen agents meer te implementeren op elk eindpunt. Geüpdatet beleid wordt automatisch naar de browser gepusht. Beheerders kunnen bepaalde taken voor browserbeheer delegeren aan IT-professionals op verschillende plekken in de organisatie.

Integratie met andere beveiligingstools

Cloudbeheer voor de Chrome-browser gebruikt je bestaande beveiligings- en beheeroplossingen. Het deelt informatie via API's met producten als VMware Workspace One, Intune en JAMF, en met SIEM's en andere beveiligingstools. Groepsbeleid-templates zijn beschikbaar voor organisaties die traditionele Windows-beheertools willen gebruiken.



Beveiliging inbouwen in de browser

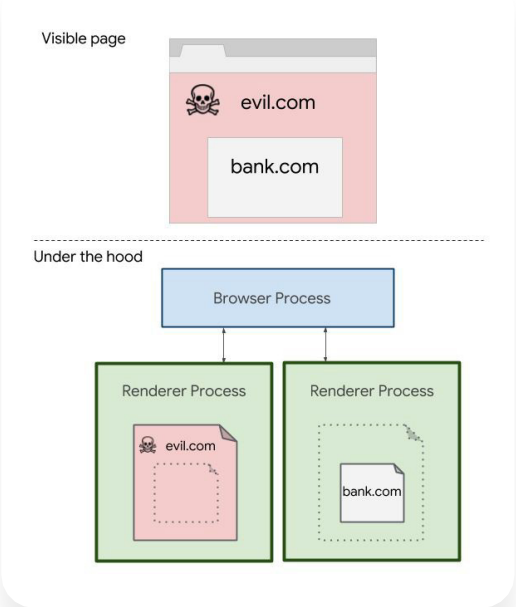
De browser moet natuurlijk zelf ook veilig zijn om te kunnen dienen als effectieve beveiligingstool.

Sandboxes en site-isolatie

De Chrome-browser gebruikt sandboxes In plaats van alle taken uit te voeren als één groot browserproces, splitst de Chrome-browser taken in meerdere aparte processen die geen toegang hebben tot elkaar en andere resources in het systeem. Elke app en extensie wordt ook uitgevoerd in een eigen proces.

Als een HTML-pagina bijvoorbeeld verschillende JavaScripts bevat, voert de browser de HTML-weergave uit in één proces en wordt elk JavaScript uitgevoerd in een eigen, apart proces. De Chrome-browser wijzigt de toegangstokens voor de processen, zodat schadelijke code geen andere processen kan openen of crashen, bestanden of registersleutels kan wijzigen, kan schrijven op het klembord, schermscraping of keylogging kan uitvoeren of andere gevaarlijke acties kan uitvoeren. Dit houdt veel hackers tegen die anders apps kunnen verstoren, hardnekkige malware kunnen installeren, toegang kunnen krijgen tot vertrouwelijke gegevens op de harde schijf of inloggegevens van gebruikers kunnen vastleggen.

De Chrome-browser gaat zelfs nog verder op Windows-, Mac-, Linux- en ChromeOS-systemen met de functie site-isolatie. Eén webpagina bevat mogelijk content van 2 of meer websites. Met site-isolatie wordt de content van elke site uitgevoerd in een eigen proces (zie figuur 7). Hiermee worden ook processen van iframes op meerdere sites in een ander proces uitgevoerd dan de bovenliggende iframes.



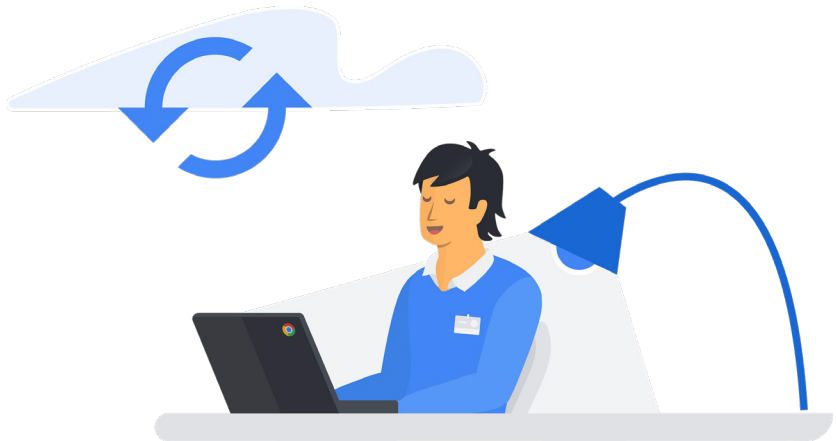
Site-isolatie vermindert zo het effect van arbitrary code execution-aanvallen en speculative execution side-channel-aanvallen, zoals Spectre en Meltdown. Als een aanvaller toch schadelijke code naar de browser stuurt via een gehackte website (zoals evil.com in figuur 7), kan die code geen informatie stelen van andere websites (zoals bank.com in figuur 7), omdat de code van die websites wordt uitgevoerd in een apart, beveiligd proces.

Regelmatig automatische updates

Het is belangrijk om browsers up-to-date te houden om je werknemers te beschermen.
Dit kan alleen als updates en patches zo snel en makkelijk mogelijk kunnen worden uitgerold.

Chrome is speciaal gemaakt om snel te updaten. Elke browser checkt regelmatig op beveiligingsupdates, die dan automatisch worden uitgevoerd, zonder dat gebruikers iets hoeven te doen. Google distribueert patches bovendien erg snel. Het bedrijf heeft de gemiddelde tijd van wanneer een beveiligingsbug is opgelost in een opensource-bibliotheek tot wanneer de fix is geïmplementeerd in het veld (het patchgat) verlaagd tot slechts 20 dagen. Dit is sneller dan andere veelgebruikte browsers.

> We vinden patching en het beheer van kwetsbaarheden heel belangrijk. Omdat de Chrome-browser automatisch wordt geüpdatet, hoeven we ons minder zorgen te maken over beveiliging."
>
> **Head of Security, Blend**



Conclusie

De browser staat aan de basis van zakelijke productiviteit. Werknemers vertrouwen elke dag, de hele dag op de browser. In browsers werken gebruikers slimmer en efficiënter, omdat ze op het web werken op verschillende apparaten en platforms.

Maar browsers zijn er niet alleen om mensen productiever te maken. IT-beveiligingsprofessionals moeten anders gaan denken over browsers, als belangrijke verdediging aan de frontlinie voor eindpunten. Op eindpunten zijn browsers de plek waar het web samenkomt met gebruikers en browsers. Ze bieden dus de mogelijkheid om gebruikersgedrag in realtime te controleren en te sturen en om belangrijk beveiligingsbeleid af te dwingen.

De Chrome-browser kan dienstdoen als strategische laag in de beveiligingsstrategie van bedrijven. Met functies als Safe Browsing en Password Alert worden gebruikers gewaarschuwd voor dreigingen op het web en schendingen van beveiligingsbeleid. Zo worden ze in een veiligere richting gestuurd. Beheerders kunnen beleid instellen en afdwingen op eindpunten met onder andere blokkeer- en toelatingslijsten voor URL's, apps en extensies, op rechten gebaseerd blokkeren van apps en extensies, apps en extensies blokkeren en afgedwongen installeren, het gebruik van verificatie in 2 stappen afdwingen en het gecontroleerd gebruik van verouderde browsers toestaan. Met de Chrome-browser en Cloudbeheer voor de Chrome-browser kunnen beheerders makkelijk gegevens verzamelen over apparaten en gebruikersactiviteit en kunnen ze beleid consequent afdwingen op meerdere apparaten en besturingssystemen.

> Als je IT-beveiligingsprofessional bent, moet je anders gaan denken over browsers, als belangrijke verdediging aan de frontlinie voor eindpunten. Begin door te bekijken hoe de Chrome-browser je bedrijf veiliger kan maken terwijl jij productiever en effectiever werkt.