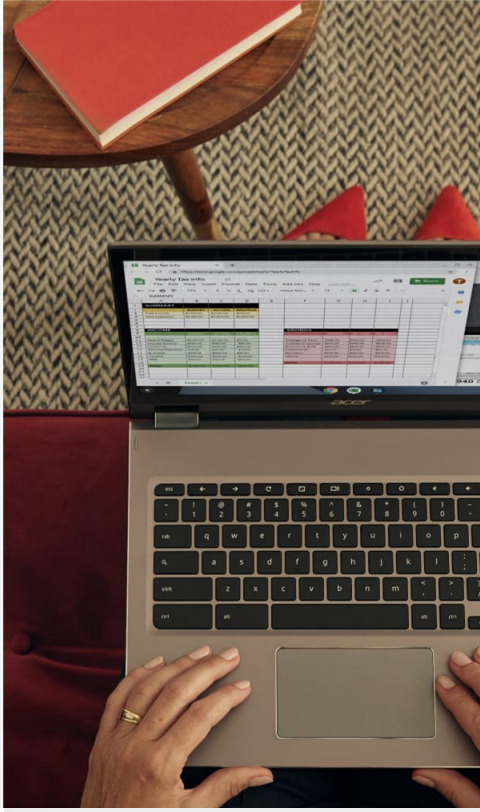
chrome

Configuratiehandleiding voor bedrijfsbeveiliging in de Chrome-browser

Gebaseerd op Chrome 90

chrome

Configuratiehandleiding voor bedrijfsbeveiliging in de Chrome-browser



Gebaseerd op Chrome 90
Laatst geüpdatet: 20 mei 2021

Doel van deze handleiding

Dit document richt zich op de Chrome-browser in het Windows-besturingssysteem, maar de meeste adviezen gelden voor alle desktopplatforms. Beheerders moeten bepaalde compromissen sluiten tussen de beveiliging van hun organisatie en de technologie en functies waartoe gebruikers toegang willen hebben.

In dit document wordt uitgebreid behandeld welk beveiligingsbeleid Chrome biedt en welke overwegingen beheerders moeten nemen voordat ze deze beleidsregels aan- of uitzetten.

De behandelde onderwerpen

Aanbevelingen en belangrijke overwegingen voor organisaties met grote beveiligingsbehoeften voordat ze beleidsregels voor beveiliging in Chrome aan- of uitzetten.

Primaire doelgroep

Beheerders van Microsoft® Windows® en de Chrome-browser

IT-omgeving

Microsoft Windows 7 en hoger

Conclusies

Overwegingen voor zakelijke beveiliging en de gevolgen voor gebruikers bij het instellen van beveiligingsbeleid voor de Chrome-browser.

Inleiding

Chrome is gemaakt als beveiligde browser. Team Chrome neemt beveiliging heel serieus. We zijn trots op onze reputatie dat we de browserbranche vooruithelpen op meerdere gebieden, zoals sandboxing, TLS-standaarden en bruikbare beveiliging.

Chrome streeft ernaar de balans te vinden tussen beveiliging en gebruiksgemak, zodat alle gebruikers de beste prestaties krijgen. Bedrijven hebben mogelijk andere doelen voor het gebruik van een beveiligde browser in hun organisatie. In dit document zie je hoe je Chrome kunt instellen om die doelen te behalen.

Standaard levert Chrome zowel gebruiksgemak als beveiliging. Maar soms is er een conflict tussen gebruiksgemak en beveiliging. Chrome geeft je dan de mogelijkheid te kiezen door je een beleidsoptie te tonen. Jij, de IT-beheerder, bepaalt wat het beste beleid is om in te stellen in die specifieke gevallen.

In dit document worden enkele gevallen beschreven waarin je kunt kiezen tussen gebruiksgemak en beveiliging en wat de voor- en nadelen zijn in elk geval. In elk geval moet je de problemen op het gebied van beveiliging en gebruiksgemak overwegen en bepalen wat de juiste beleidsinstelling is voor jouw bedrijf.

In dit document behandelen we 3 verschillende beveiligingsbehoeften van bedrijven:

- Bedreigingspreventie
- Privacy
- Beheer en prestaties

In veel van de aanbevelingen in dit document verwijzen we naar bepaalde beleidsinstellingen. Je vindt de volledige documentatie daarvan op https://chromeenterprise.google/policies.

Bedreigingspreventie

Chrome bevat al bepaalde instellingen om bedreigingen van schadelijke websites in de kiem te smoren, zoals:

- Site-isolatie. Hiermee wordt elke website geïsoleerd in een eigen geheugenruimte (proces in het besturingssysteem). Ga voor meer informatie naar dit Helpcentrum-artikel.
- Sandboxes worden toegepast op deze processen om te voorkomen dat de rest van de computer het slachtoffer wordt van een kwetsbaarheid.
- Safe Browsing vindt schadelijke en misleidende content/software door continu het web te scannen en het gevaarniveau te classificeren. Gebruikers zien een waarschuwing voordat ze een site openen die is gemarkeerd als mogelijk schadelijk.

Chrome is gemaakt om veilig te zijn. De standaardinstellingen zorgen dus voor gebruikersveiligheid bij het browsen. Je kunt in de browser nog meer opties instellen om bedreigingen te voorkomen. Dit kan op 2 manieren:

- Standaard Chrome-gedrag afdwingen, zodat gebruikers het niet kunnen overschrijven.
- Nog meer beveiliging toevoegen, waardoor het gebruiksgemak minder prioriteit krijgt dan beveiliging.

In de volgende 2 subgedeelten krijg je informatie over mogelijke configuraties op deze gebieden.

chrome

Laatst geüpdatet: 20 mei 2021

Instellingen waarmee bestaand standaardgedrag in Chrome wordt afgedwongen

Chrome is standaard een veilig product. In de standaardinstellingen krijgt beveiliging prioriteit, zodat gebruikers zo veilig mogelijk kunnen browsen. Gebruikers kunnen sommige instellingen wijzigen, maar dit kan ertoe leiden dat Chrome minder veilig wordt. Beheerders kunnen sommige instellingen afdwingen via beleidsregels.

Behoefte van het bedrijf	Gevolgen voor gebruikers	Mogelijke negatieve gevolgen voor de beveiliging	Opties en opmerkingen

Ik wil checken of vorige beheerders geen onveilig beleid hebben ingesteld voor onze organisatie.	● Geen	● Geen	Check of de volgende beleidsregels niet al zijn ingesteld, zodat je de veiligste configuratie hebt:
			
			`EnableDeprecatedWebPlatformFeatures`
			`RunAllFlashInAllowMode`
			`SuppressUnsupportedOSWarning`
			`EnableOnlineRevocationChecks`
			`OverrideSecurityRestrictionsOnInsecureOrigin`
			`CertificateTransparencyEnforcementDisabledForCas`
			`CertificateTransparencyEnforcementDisabledForLegacyCas`
			`LegacySameSiteCookieBehaviorEnabled`
			`LegacySameSiteCookieBehaviorEnabledForDomainList`
			`ChromeVariations`
			`DnsOverHttpsMode`
			`LookalikeWarningAllowlistDomains`
			`SafeBrowsingAllowlistDomains`
			`RemoteAccessHostAllowRemoteAccessConnections`
			
			Dit is geen volledige lijst met beveiligingsbeleid, maar deze beleidsregels worden gebruikt door veel bedrijven. Bekijk de lijst met Chrome Enterprise-beleid voor meer beleidsopties.

Ik wil zorgen dat gebruikers belangrijke beveiligingsfuncties niet kunnen uitzetten.	● Geen	● Geen	Stel de beleidsregels `AllowOutdatedPlugins`, `SafeBrowsingProtectionLevel` en `ThirdPartyBlockingEnabled` expliciet zelf in. Er verandert dan niets aan de gebruikerservaring, maar gebruikers kunnen deze instellingen dan zelf niet meer wijzigen.

Instellingen waarmee bestaand standaardgedrag in Chrome wordt afgedwongen (vervolg)

Behoefte van het bedrijf	Gevolgen voor gebruikers	Mogelijke negatieve gevolgen voor de beveiliging	Opties en opmerkingen
Ik wil instellen dat gebruikers geen malware kunnen downloaden of kunnen reageren op phishingpogingen, en zorgen dat ze deze beveiligingsmaatregelen niet kunnen overschrijven.	● **Laag**	● **Geen**	Safe Browsing is de Chrome-functie die zorgt voor beveiliging tegen malware en phishing. Lees meer over Safe Browsing in Chrome. Sommige bedrijven zetten Safe Browsing uit, omdat ze vinden dat hun bestaande beveiligingsproducten (antivirusprogramma's, firewall) voor genoeg bescherming zorgen. Maar Safe Browsing werkt samen met deze oplossingen. Antivirusproducten richten zich bijvoorbeeld vooral op de inhoud van downloads, terwijl Safe Browsing zich richt op de context: de serie navigaties waardoor de gebruiker bij de link terecht is gekomen. Als je Safe Browsing uitzet, gebeurt dit niet meer. Het Chrome-beveiligingsteam raadt je aan Safe Browsing aan te laten staan. Je kunt instellen dat gebruikers Safe Browsing niet kunnen uitzetten door het beleid `SafeBrowsingProtectionLevel in te stellen op 1`. Safe Browsing is dan actief in de standaardmodus. Gebruikers merken hier niets van, alleen kunnen ze Safe Browsing niet meer uitzetten. In M79 introduceerden we de uitgebreide versie van Safe Browsing in Chrome, een nieuwe optie voor gebruikers die een grotere beveiligingsbehoefte hebben tijdens browsen op het web. 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. Je zet de uitgebreide versie van Safe Browsing aan door `SafeBrowsingProtectionLevel in te stellen op 2.`

Instellingen waarmee bestaand standaardgedrag in Chrome wordt afgedwongen (vervolg)

Behoefte van het bedrijf	Gevolgen voor gebruikers	Mogelijke negatieve gevolgen voor de beveiliging	Opties en opmerkingen
Ik wil instellen dat gebruikers geen malware kunnen downloaden of kunnen reageren op phishingpogingen, en zorgen dat ze deze beveiligingsmaatregelen niet kunnen overschrijven.	Laag	Geen	Je kunt Safe Browsing nog sterker afdwingen door deze optie in te stellen: `DisableSafeBrowsingProceedAnyway` Dit kan negatieve gevolgen hebben voor gebruikers, omdat ze niet verder kunnen navigeren als Safe Browsing een fout heeft gemaakt en een website verkeerd heeft geclassificeerd als phishing. Je kunt ook `DownloadRestrictions` instellen op 2 om Safe Browsing strenger af te dwingen. Zie Voorkomen dat gebruikers schadelijke bestanden downloaden voor meer informatie. Sommige bedrijven blokkeren afdrukken, omdat ze denken dat opgeslagen pdf's een andere manier zijn waarop malware kan worden opgeslagen op een schijf. Het Chrome-beveiligingsteam vindt dit geen handige oplossing. In vrijwel alle gevallen wordt bij de conversie van een webpagina naar een pdf eventuele schadelijke content verwijderd. We raden je wel aan een beveiligde pdf-viewer (zoals Chrome zelf) te gebruiken om dit soort bestanden te openen.
Ik wil software van derden gebruiken die code wil injecteren in Chrome.	Hoog	Hoog	Chrome staat niet toe dat software van derden op een pc eigen code injecteert in Chrome. Dit is namelijk een grote oorzaak van crashes en bugs die (theoretisch) kunnen worden uitgebuit door schadelijke websites. We raden je aan de standaardinstelling te behouden (`ThirdPartyBlockingEnabled` waar). Andere beveiligingsproducten raden je misschien aan hun code te deblokkeren, zodat ze Chrome kunnen instrumenteren of op een andere manier kunnen beïnvloeden. Als je dit doet, kun je de functies van dat product gebruiken, maar loop je meer risico's op crashes en kwetsbaarheden. Als je een beveiligingsproduct gebruikt dat uitvoerbare code wil injecteren in Chrome, raden we je aan de leverancier te vragen of deze de functie ook kan aanbieden via een Chrome-extensie.

Instellingen waarmee gebruikersfunctionaliteit wordt verminderd, maar er minder risico is op aanvallen

Je kunt Chrome aanpassen om minder kwetsbare functies te gebruiken die kunnen worden uitgebuit door schadelijke websites. Voor elk item dat je blokkeert, kunnen gebruikers merken dat ze minder functies tot hun beschikking hebben.

Bij veel van deze wijzigingen zet je Chrome-functies uit. We willen benadrukken dat al deze functies zijn gemaakt om veilig te zijn. Het zou dus niet nodig moeten zijn om Chrome-functies uit te zetten. Maar we weten dat veel bedrijven dit toch willen of moeten doen. Hieronder zie je enkele overwegingen die je kunnen helpen de juiste beslissing te nemen.

Behoefte van het bedrijf	Gevolgen voor gebruikers	Mogelijke negatieve gevolgen voor de beveiliging	Opties en opmerkingen
Mijn organisatie heeft eigen vertrouwde rootcertificaten op de eindpunten waarmee zakelijke servers worden vertrouwd. Als aanvallers de privésleutel van die vertrouwde roots in handen krijgen, wil ik de certificaten kunnen intrekken.	Laag	Geen	Je kunt controles voor intrekken aanzetten voor deze certificaten met: `RequireOnlineRevocationChecksForLocalAnchors` We garanderen niet dat Chrome het verschil kan zien tussen certificaten gebaseerd op lokale ankers. Dit wordt namelijk bepaald door instellingen in het besturingssysteem die verschillen per platform en versie van het besturingssysteem. Als het intrekken niet toegankelijk is, kunnen deze certificaten niet worden gebruikt (hard-fail), waardoor websites mogelijk niet meer toegankelijk zijn.
Oudere versies van Chrome die worden uitgevoerd in mijn omgeving kunnen worden uitgebuit door schadelijke websites.	Laag	Geen	Je kunt afdwingen dat gebruikers Chrome herstarten en updates sneller worden toegepast met de beleidsregels `RelaunchNotification` en `RelaunchNotificationPeriod`. We raden dit sterk aan in zakelijke omgevingen, omdat gebruikers zo de nieuwste versie van Chrome met de bijbehorende beveiligingsfixes gebruiken.
Ik wil geen enkel risico lopen dat de wachtwoorden van gebruikers worden onderschept als deze met oudere verificatieprotocollen (digest, basic auth) over het internet worden gestuurd.	Laag	Geen	Je kunt deze oudere schema's uitzetten met `AuthSchemes`. Er zijn tegenwoordig weinig legitieme websites die deze schema's nog gebruiken, dus we raden je aan het gebruik van deze schema's uit te zetten voor je bedrijf. Vanaf Chrome 75 raden we NTLM en Negotiate aan. Zorg dat je zakelijke services ook moderne verificatiemechanismen gebruiken.

Instellingen waarmee gebruikersfunctionaliteit wordt verminderd, maar er minder risico is op aanvallen (vervolg)

Behoefte van het bedrijf	Gevolgen voor gebruikers	Mogelijke negatieve gevolgen voor de beveiliging	Opties en opmerkingen
Ik wil niet dat documenten uit de cloud schade kunnen toebrengen aan kwetsbare printers.	Laag	Geen	Je kunt voorkomen dat de printers in je bedrijf documenten krijgen via Google Cloudprinter door de optie `CloudPrintProxyEnabled in te stellen.`
Ik maak me zorgen dat hackers die zich al in het netwerk bevinden, WPAD kunnen hacken om zich lateraal te verplaatsen.	Laag	Geen	Je kunt `ProxyMode` gebruiken om in te stellen dat proxy's niet automatisch kunnen worden gevonden.
Ik maak me zorgen dat als bestanden automatisch worden gedownload, hackers onvoorziene DDL-plantingaanvallen kunnen uitvoeren of wachtwoordhashes kunnen doorsturen naar schadelijke SMB-servers. Ik wil automatisch downloaden uitzetten.	Gemiddeld	Geen	Als je wilt dat gebruikers een prompt zien voor elke download, pas je `PromptForDownloadLocation` aan.
Ik wil 3D-graphics uitzetten, omdat ik denk dat we hierdoor meer risico lopen op aanvallen en onze gebruikers weinig websites bezoeken waarop 3D-graphics worden gebruikt.	Gemiddeld	Geen	Je kunt dit uitzetten met `Disable3DAPIs.` Chrome biedt al veel bescherming tegen aanvallen via 3D-graphics, zoals de laag ANGLE die 3D-invoeren opschoont en isolatie van alle GPU-gerelateerde code in een sandboxproces. Als je WebGL uitzet, werken virtuele wereldbol- en kaartproducten niet meer.
Ik wil minder risico lopen dat side-channelaanvallen worden gebruikt door een website om gegevens op te halen van een andere website.	Gemiddeld	Geen	Je kunt site-isolatie verfijnen met `IsolateOrigins`. Bekijk meer informatie op Je gegevens beveiligen met site-isolatie. Opmerking: Dit gebruikt meer geheugen.

Instellingen waarmee gebruikersfunctionaliteit wordt verminderd, maar er minder risico is op aanvallen (vervolg)

Behoefte van het bedrijf	Gevolgen voor gebruikers	Mogelijke negatieve gevolgen voor de beveiliging	Opties en opmerkingen
Ik wil geen risico lopen dat externe gebruikers via Chrome Remote Desktop toegang krijgen tot computers in ons netwerk.	Gemiddeld	Geen	Je kunt de Chrome Remote Desktop-app op dezelfde manier blokkeren als andere apps en extensies. Bekijk meer informatie op Het gebruik van Chrome Remote Desktop beheren.
Ik wil extensies en apps uitzetten, omdat ik denk dat ze het risico op aanvallen vergroten. Ik vind het niet erg dat dit gevolgen heeft voor de workflow van gebruikers.	Hoog	Laag	Als je alle extensies blokkeert, kan dit grote gevolgen hebben voor de productiviteit van gebruikers. Bovendien bieden sommige extensies zelfs meer beveiliging voor gebruikers, bijvoorbeeld als ze een wachtwoordmanager van derden gebruiken voor hun persoonlijke wachtwoorden. We raden je aan extensies te beheren per recht: 1. Blokkeer extensies die om rechten vragen die je riskant vindt en sta andere extensies toe. 2. Blokkeer voor de overige extensies de toegang tot gevoelige hosts. Voorbeeld: Sta alle extensies toe, behalve extensies die de webcam willen gebruiken of schermafbeeldingen willen kunnen maken. Daarnaast stel je in dat andere extensies geen toegang hebben tot je gevoeligste bedrijfssites. Zie Rechten voor Chrome-apps en -extensies en de handleiding Extensies beheren in je bedrijf voor meer informatie. Je kunt ook je Chrome Enterprise-specialist om meer materiaal vragen waarin staat uitgelegd waarom bedrijven deze aanpak gebruiken. Als je niet goed weet welke rechten risicovol zijn, kun je bepaalde extensies blokkeren door `ExtensionInstallBlacklist in te stellen.` De waarde * op de blokkeringslijst betekent dat alle extensies worden geblokkeerd, tenzij ze expliciet op de toelatingslijst staan. We raden je aan een goedkeuringsproces te ontwikkelen voor toegevoegde extensies. We raden je af specifieke extensies te blokkeren/goed te keuren, omdat dit proces niet handig is op grote schaal. Alle Chrome-extensies moeten worden gedistribueerd via de Chrome Web Store of de mechanismen die hieronder beschreven staan. Lees meer over externe extensies. Met het beleid `BlockExternalExtensions` kun je voorkomen dat externe extensies worden geïnstalleerd.

Instellingen waarmee gebruikersfunctionaliteit wordt verminderd, maar er minder risico is op aanvallen (vervolg)

Behoefte van het bedrijf	Gevolgen voor gebruikers	Mogelijke negatieve gevolgen voor de beveiliging	Opties en opmerkingen
Ik wil niet dat gebruikers uitzonderingen kunnen toevoegen om gemengde content voor specifieke sites toe te staan.	Hoog	Laag	Met DefaultInsecureContentSetting kun je instellen of gebruikers uitzonderingen voor onveilige content kunnen toevoegen. Als je dit beleid niet instelt, kunnen gebruikers uitzonderingen toevoegen om blokkeerbare gemengde content toe te staan en automatische upgrades voor optioneel blokkeerbare gemengde content uitzetten.
Ik wil op afstand problemen kunnen oplossen die te maken hebben met cookies of het cachegeheugen op gebruikersapparaten.	Hoog	Geen	Je kunt vanuit de Beheerdersconsole opdrachten op afstand sturen om cookies en het cachegeheugen te wissen.

Privacy

Chrome streeft ernaar de privacy van gebruikers te beschermen. Veel bedrijven willen dat er zo min mogelijk persoonlijk identificeerbare informatie of persoonsgegevens (samen PII genoemd) op pc's staat. Maar veel bedrijven weten niet hoe goed Chrome deze gegevens beschermt.

Voor enkele van de sterkste beveiligingsfuncties van Chrome (zoals Safe Browsing en wachtwoordmanagers) moet informatie worden uitgewisseld met Google-services. Het Chrome-beveiligingsteam raadt je sterk aan deze functies aan te zetten. Als je je zorgen maakt over hoe deze verstuurde gegevens worden gebruikt, bespreek je dit met je Chrome Enterprise-specialist.

Deze behoeften worden onderverdeeld in 3 categorieën:

- PII die wordt opgeslagen op bedrijfsapparaten
- Gegevens die naar het internet worden gestuurd
- Gegevens die naar Google worden gestuurd

Instellingen voor als PII wordt opgeslagen op bedrijfsapparaten

Behoefte van het bedrijf	Gevolgen voor gebruikers	Mogelijke negatieve gevolgen voor de beveiliging	Opties en opmerkingen
Ik maak me zorgen dat andere gebruikers (**die geen beheerder zijn**) die zijn ingelogd op hetzelfde apparaat (later of tegelijkertijd via VDI) toegang hebben tot gevoelige gegevens, zoals wachtwoorden van gebruikers die op de schijf van het apparaat staan. Ik maak me zorgen dat apparaten worden gestolen en dat de dieven de wachtwoorden kunnen lezen vanaf de schijf.	**N.v.t.**	**N.v.t.**	Alle persoonlijke gegevens van de gebruiker (browsegeschiedenis, cachegeheugen, wachtwoorden, gegevens voor automatisch invullen) worden in een informatiepakket opgeslagen dat het 'profiel' van de gebruiker wordt genoemd. Deze profielen worden beschermd door standaard rechtenmodellen van het besturingssysteem en zijn dus niet toegankelijk voor andere gebruikersaccounts op het apparaat. Als andere gebruikers of dieven onbeperkte toegang hebben tot het apparaat, kunnen ze die bestanden uiteraard wel lezen. Maar de gevoeligste delen van het Chrome-profiel (zoals wachtwoorden en creditcardgegevens) worden versleuteld met de Data Protection API (DPAPI) van Microsoft. Deze API is gemaakt om te voorkomen dat gegevens toegankelijk zijn voor beheerders of anderen met volledige schijftoegang. De gegevens worden versleuteld met het inlogwachtwoord van de gebruiker. (Bekijk de DPAPI-documentatie van Microsoft voor meer informatie. Beheerders kunnen deze gegevens mogelijk ontsleutelen als ze toegang hebben tot privésleutels op een domeincontroller.) Dit zijn de enige soorten gebruikers waarvoor je mogelijk speciale stappen moet uitvoeren: • Beheerders of andere gebruikers die fysieke toegang hebben tot de schijf. • Gebruikers die toegang hebben tot het cachegeheugen van de browser of andere delen van het Chrome-profiel die niet versleuteld zijn. Bekijk de volgende rij voor meer informatie hierover.

Instellingen voor als PII wordt opgeslagen op bedrijfsapparaten (vervolg)

Behoefte van het bedrijf	Gevolgen voor gebruikers	Mogelijke negatieve gevolgen voor de beveiliging	Opties en opmerkingen
Ik maak me zorgen dat **beheerders** die zijn ingelogd op hetzelfde apparaat (later of tegelijkertijd via VDI) toegang hebben tot gevoelige gegevens, zoals het cachegeheugen van de browser van andere gebruikers op de schijf van het apparaat.	Hoog	Geen	Dit is een erg specifiek geval en de meeste bedrijven voeren geen extra acties uit om hiertegen te beschermen. Deze gebruikers hebben geen toegang tot de gevoeligste gegevens, zoals wachtwoorden en creditcardnummers. Zie de vorige rij voor meer informatie. Als je toch niet wilt dat beheerders toegang hebben tot minder gevoelige delen van het profiel, zoals het cachegeheugen van de browser, gebruik je het beleid `ForceEphemeralProfiles` en dwing je af dat gebruikers moeten inloggen bij Chrome (`ForceBrowserSignin`) zodat hun belangrijke bookmarks en andere voorkeuren elke keer worden gedownload. Je kunt ook de instelling `BackgroundModeEnabled` uitzetten, zodat sessies een bepaalde maximale duur hebben. De gevolgen voor gebruikers zijn groot, omdat ze moeten inloggen elke keer dat ze Chrome gebruiken. De prestaties zullen ook verminderen, omdat elke keer de profielgegevens worden gedownload en het cachegeheugen wordt gemaakt. Bekijk meer informatie over de kortstondige modus. Neem contact op met je Chrome Enterprise-specialist voor meer informatie. Sommige bedrijven stellen in plaats hiervan in dat cookies niet worden bewaard, met de instelling `DefaultCookiesSetting`. We raden dit af, omdat dit normaal gebruik van het internet sterk verstoort. Het kan ook grote gevolgen hebben voor de beveiliging, omdat gebruikers vaker hun wachtwoord moeten invoeren, waardoor het risico op phishing groter wordt. Een kwaadwillende beheerder of andere persoon met fysieke toegang tot de computer kan keyloggers of andere spyware installeren, of zelfs een schadelijk nep-binair bestand voor Chrome. Dit antwoord heeft specifiek te maken met gebruikerstoegang tot de profielgegevens op de schijf. Het is geen allesomvattende oplossing voor problemen met een kwaadwillende beheerder. Een bredere oplossing dan alleen Chrome-instellingen is versleutelde homedirectory's voor gebruikers.

Instellingen voor als PII wordt opgeslagen op bedrijfsapparaten (vervolg)

Behoefte van het bedrijf	Gevolgen voor gebruikers	Mogelijke negatieve gevolgen voor de beveiliging	Opties en opmerkingen
Ik maak me zorgen dat mensen die fysieke toegang hebben tot een ontgrendeld apparaat de wachtwoorden van andere gebruikers kunnen bekijken.	Hoog	Hoog	Sommige bedrijven zetten de wachtwoordmanager van Chrome uit door het beleid `PasswordManagerEnabled` uit te zetten. We raden je aan de wachtwoordmanager aan te laten staan. Zo zorg je dat gebruikers makkelijker sterke wachtwoorden gebruiken op meerdere websites, een van de belangrijkste dingen die je kunt doen op het gebied van gebruikersbeveiliging. Zie Instellingen voor als gegevens naar Google worden gestuurd voor meer informatie over opties voor wachtwoordbeheer. We raden je aan in plaats hiervan in het besturingssysteem de beleidsregels voor de schermvergrendeling in te stellen en te zorgen dat je sterke wachtwoorden gebruikt voor het besturingssysteem.

Instellingen voor als gegevens naar het internet worden gestuurd (gegevensverlies)

Behoefte van het bedrijf	Gevolgen voor gebruikers	Mogelijke negatieve gevolgen voor de beveiliging	Opties en opmerkingen
Ik wil niet dat gebruikers items uploaden.	N.v.t.	N.v.t.	Op dit moment bevat Chrome geen beleidsregels waarmee je kunt voorkomen dat gebruikers bestanden uploaden. Dit kan ook niet met het beleid `AllowFileSelectionDialogs`, omdat gebruikers dan nog steeds bestanden kunnen uploaden via bijvoorbeeld slepen en neerzetten.

Instellingen voor als gegevens naar het internet worden gestuurd (gegevensverlies) (vervolg)

Behoefte van het bedrijf	Gevolgen voor gebruikers	Mogelijke negatieve gevolgen voor de beveiliging	Opties en opmerkingen
Ik wil kunnen zien wat gebruikers doen om verdacht gedrag te kunnen herkennen.	Geen	Geen	Je kunt het resourcegebruik van de Chrome-browser, inlogstatus, verbinding, gebruikspatronen en browsegedrag volgen. Zie Chrome-browsergebruik in Windows controleren.
Ik wil zorgen dat gebruikers vertrouwelijke gegevens alleen kunnen bekijken op het hoofdscherm van de computer, dus ik wil Chromecast uitzetten.	Gemiddeld	Geen	Pas het beleid `EnableMediaRouter` aan.
Ik wil niet dat websites video of audio kunnen vastleggen (bijvoorbeeld via WebRTC).	Gemiddeld	Geen	`Met VideoCaptureAllowed` en `AudioCaptureAllowed` kun je de mogelijkheid uitzetten om video en audio vast te leggen. Je kunt daarnaast een toelatingslijst maken met een overeenkomend AllowedUrls-beleid. Bedrijven krijgen soms het advies om WebRTC uit te zetten. Je kunt de WebRTC-stack niet helemaal uitzetten. Het is beter de specifieke sensoren uit te zetten die risicovol kunnen zijn voor je bedrijf. We verwachten dat steeds meer tools voor videovergaderingen en telefonie naar het web worden verplaatst. Dit zal dus steeds grotere gevolgen hebben voor je gebruikers. We raden je aan over een jaar nog eens te kijken of je dit echt wilt.
Ik wil niet dat websites schermafbeeldingen kunnen maken.	Gemiddeld	Geen	In de huidige versies van Chrome kunnen API's het scherm niet delen zonder een extensie te gebruiken. We verwachten dat deze API's in de toekomst beschikbaar worden voor websites. Ze vallen dan onder het beleid `VideoCaptureAllowed` dat we hebben genoemd in de vorige aanbeveling. Neem contact op met je Chrome Enterprise-specialist voor up-to-date informatie.

Instellingen voor als gegevens naar het internet worden gestuurd (gegevensverlies) (vervolg)

Behoefte van het bedrijf	Gevolgen voor gebruikers	Mogelijke negatieve gevolgen voor de beveiliging	Opties en opmerkingen
Ik wil niet dat schadelijke websites om leestoegang kunnen vragen tot seriële poorten, zelfs als legitieme websites hierdoor ook geen toegang hebben.	Gemiddeld	Geen	`Met DefaultSerialGuardSetting` kun je het gebruik van de File System API voor lezen bepalen. Als je het beleid instelt op 3, kunnen websites leestoegang vragen tot bestanden en directory's in het bestandssysteem van het besturingssysteem van de host via de File System API. Als je het beleid instelt op 2, wordt de toegang geblokkeerd. Als je dit beleid niet instelt, vragen websites om toegang maar kunnen gebruikers deze instelling wijzigen.
Ik wil niet dat schadelijke websites om leestoegang kunnen vragen tot bestanden en directory's in het bestandssysteem van het hostbesturingssysteem via de File System API, zelfs als legitieme websites hierdoor ook geen toegang hebben.	Gemiddeld	Geen	`Met DefaultFileSystemReadGuardSetting` kun je het gebruik van de File System API voor lezen bepalen. Als je het beleid instelt op 3, kunnen websites leestoegang vragen tot bestanden en directory's in het bestandssysteem van het besturingssysteem van de host via de File System API. Als je het beleid instelt op 2, wordt de toegang geblokkeerd. Als je het beleid niet instelt, vragen websites om toegang maar kunnen gebruikers deze instelling wijzigen.
Ik wil niet dat schadelijke websites om toegang kunnen vragen en sensoren kunnen gebruiken zoals voor beweging en licht, zelfs als legitieme websites hierdoor ook geen toegang hebben.	Gemiddeld	Geen	`Met DefaultSensorsSetting` kun je het gebruik van de standaardinstelling voor sensoren bepalen. Als je het beleid instelt op 1, hebben websites toegang tot sensoren, zoals voor beweging en licht. Als je het beleid instelt op 2, wordt de toegang tot sensoren geblokkeerd. Als je het beleid niet instelt, wordt AllowSensors toegepast, maar kunnen gebruikers deze instelling wijzigen.

Ik wil niet dat schadelijke websites toegang hebben tot USB- of bluetooth-apparaten, zelfs als legitieme websites hierdoor ook geen toegang hebben.	Gemiddeld	Gemiddeld	`DefaultWebUsbGuardSetting`
			`DefaultWebBluetoothGuardSetting`
			
			Sommige websites vragen mogelijk legitiem USB- of bluetooth-toegang tot hardwaretokens voor verificatie in meerdere stappen. Als je USB of bluetooth uitzet, kan dit negatieve gevolgen hebben voor de beveiliging van die websites.

Instellingen voor als gegevens naar het internet worden gestuurd (gegevensverlies) (vervolg)

Behoefte van het bedrijf	Gevolgen voor gebruikers	Mogelijke negatieve gevolgen voor de beveiliging	Opties en opmerkingen
Ik wil niet dat schadelijke websites toegang hebben tot locatiegegevens, zelfs als legitieme websites hierdoor ook geen toegang hebben tot de locatie.	Hoog	Laag	Zet de locatietoegang uit met het beleid `DefaultGeolocationSetting` Dit is erg verstorend voor gebruikers. Het is aannemelijk dat bepaalde websites locatiegegevens gebruiken om de beveiliging te verbeteren, dus dit kan negatieve gevolgen hebben voor de beveiliging.
Ik wil niet dat sites van derden onze gebruikers volgen op het web.	Hoog	Laag	Sommige bedrijven zetten cookies van derden uit met het beleid `BlockThirdPartyCookies`. Dit kan ertoe leiden dat sommige websites niet meer werken, inclusief bepaalde webservices voor verificatie. Dit kan dus negatieve gevolgen hebben voor de beveiliging.

Instellingen voor als gegevens naar Google worden gestuurd

Behoefte van het bedrijf	Gevolgen voor gebruikers	Mogelijke negatieve gevolgen voor de beveiliging	Opties en opmerkingen
Ik wil niet dat Chrome informatie lekt naar de DNS-servers van Google.	N.v.t.	N.v.t.	Mensen denken vaak ten onrechte dat je het beleid `BuiltInDnsClientEnabled` moet uitzetten om te voorkomen dat Chrome de DNS-servers van Google gebruikt. Dit klopt niet. Deze optie heeft alleen te maken met de DNS-softwarestack aan de clientzijde op het eindpunt en bepaalt niet welke servers er worden gebruikt. De DNS-stack van Google communiceert alleen met de Google-servers als het eindpunt op die manier is ingesteld. Bedrijven hoeven deze optie niet aan te passen voor beveiligingsdoeleinden.
Ik wil niet dat vertrouwelijke informatie over crashes en gebruik naar Google wordt gestuurd.	Laag	Geen	Je kunt anonieme crashrapporten uitzetten met het beleid `MetricsReportingEnabled`. Deze statistieken zijn anoniem. Als je toestaat dat statistieken worden gemeld, heeft je bedrijf hier ook voordeel van. Google begrijpt dan beter je behoeften en achterhaalt eventuele problemen.
Ik wil niet dat Google malware op de pc's van mijn organisatie vindt.	Laag	Laag	Met het beleid `ChromeCleanupReportingEnabled` bepaal je of informatie naar Google wordt gestuurd. Er is nog een ander beleid, `ChromeCleanupEnabled`, waarmee je bepaalt of Chrome scant op malware en gebruikers vraagt die te verwijderen als deze wordt gevonden. Met deze 2 beleidsregels kun je apart instellen of de ingebouwde verwijderservice voor malware van Chrome wordt gebruikt en of detectiegegevens worden gedeeld met Google.
Ik wil niet dat vertrouwelijke documenten van Google naar cloudprinters worden gestuurd.	Gemiddeld	Geen	Pas het beleid `CloudPrintSubmitEnabled` aan. Bekijk voor meer informatie Wie kan zien wat ik afdruk?
Ik wil niet dat de tekst van meldingen via Google wordt gestuurd.	Gemiddeld	Geen	Sommige bedrijven zetten meldingen uit via het beleid `DefaultNotificationsSetting`, omdat de meldingstekst dan niet via de backendservices van Google wordt gestuurd. Zie Push messaging (Pushberichten) voor meer informatie.

Instellingen voor als gegevens naar Google worden gestuurd (vervolg)

Behoefte van het bedrijf	Gevolgen voor gebruikers	Mogelijke negatieve gevolgen voor de beveiliging	Opties en opmerkingen
Ik wil niet dat Google onze wachtwoorden te zien krijgt.	● Gemiddeld	● Gemiddeld	Google raadt je sterk aan functies voor wachtwoordbeheer aan te laten staan voor je gebruikers. Zo kunnen gebruikers sterke wachtwoorden gebruiken, wat een groot beveiligingsvoordeel oplevert. Lees bijvoorbeeld de post van NCSC over wachtwoordmanagers. Als Chrome-browsersynchronisatie uitstaat, worden die wachtwoorden niet geüpload naar Google. Ze worden alleen opgeslagen op het eindpunt en worden versleuteld met het inlogwachtwoord van de gebruiker. Zo kunnen zelfs mensen met fysieke toegang tot de schijf ze niet lezen. (Bekijk de eerdere antwoorden over PII op het eindpunt.) Als Chrome-browsersynchronisatie aanstaat, worden deze wachtwoorden standaard opgeslagen in de infrastructuur van Google. Google neemt de beveiliging van deze gegevens erg serieus, maar moet deze gegevens mogelijk delen, bijvoorbeeld om juridische redenen. In het volgende item vind je meer informatie over hoe je kunt zorgen dat Google helemaal geen toegang heeft tot deze gegevens. Google wil dat zakelijke gebruikers zo goed mogelijk beveiligd zijn door een wachtwoordmanager te gebruiken. Als er andere functies of opties zijn waardoor je genoeg vertrouwen krijgt om de wachtwoordmanager aan te zetten, kun je deze bespreken met je Google Chrome Enterprise-specialist. Sommige bedrijven zetten de mogelijkheid uit om wachtwoorden te importeren uit andere browsers (`ImportSavedPasswords`). Net als met wachtwoordmanagers in het algemeen, vinden we het belangrijk dat gebruikers zo makkelijk mogelijk sterke wachtwoorden kunnen gebruiken, dus we raden je aan deze importmogelijkheid aan te laten staan.

Instellingen voor als gegevens naar Google worden gestuurd (vervolg)

Behoefte van het bedrijf	Gevolgen voor gebruikers	Mogelijke negatieve gevolgen voor de beveiliging	Opties en opmerkingen
Ik wil niet dat Google de profielgegevens van gebruikers kan zien, inclusief wachtwoordzinnen en bookmarks.	Gemiddeld	Gemiddeld	Je gebruikers kunnen een synchronisatiewachtwoordzin instellen waarmee hun profiel (wachtwoorden, bookmarks etc.) zo wordt versleuteld dat deze gegevens nooit in niet-versleutelde tekst worden geüpload. Meer informatie Met een wachtwoordzin kunnen gebruikers de Google-cloud gebruiken om hun Chrome-gegevens op te slaan en te synchroniseren zonder dat Google deze kan lezen. Met deze instelling moeten gebruikers de wachtwoordzin invoeren op nieuwe apparaten en wordt niet alle geschiedenis gesynchroniseerd, dus deze is wel verstorend voor hun workflow. Op dit moment bevat Chrome geen beleidsregels waarmee je zo'n wachtwoordzin kunt afdwingen. Als je meer vragen hebt, stel die dan aan je Chrome Enterprise-specialist.
Ik wil helemaal geen gegevens naar Google sturen vanwege nalevingsdoeleinden.	Hoog	Hoog	We raden je sterk aan Safe Browsing aan te laten staan om gebruikers te beschermen tegen malware en phishing. Safe Browsing in Chrome heeft toegang tot de context waarmee gebruikers op een pagina terechtkomen en kan daarom soms beter beoordelen of een pagina veilig is dan andere zakelijke beveiligingsproducten. Bekijk meer informatie over het Beveiligings- en privacybeleid van Chrome. Je kunt daarnaast instellen dat bookmarks/de geschiedenis/wachtwoorden niet worden gesynchroniseerd met Google via het beleid `SyncDisabled`. We raden je sterk aan de wachtwoordmanager wel aan te laten staan. Bekijk de vorige 2 rijen in deze tabel voor de mogelijke opties. Verschillende bedrijven maken hierin verschillende keuzes. De meeste bedrijven laten bijvoorbeeld functies aanstaan die worden getriggerd door expliciete gebruikersacties (zoals Google Translate) en functies die duidelijke beveiligingsvoordelen bieden. Neem contact op met je Chrome Enterprise-specialist om uitgebreider te bespreken welke gegevens worden uitgewisseld voor elke service en wat de juiste beleidsopties zijn in jouw geval.

Beheer en prestaties

In dit gedeelte bespreken we behoeften van bedrijven voor Chrome-beheer en -prestaties. Een deel hiervan is ook van toepassing op beveiliging/privacy en andere gebieden.

Behoefte van het bedrijf	Gevolgen voor gebruikers	Mogelijke negatieve gevolgen voor de beveiliging	Opties en opmerkingen
Ik maak me zorgen dat de Chrome-wachtwoordmanager kan leiden tot meer vragen aan de supportafdeling omdat deze niet is gesynchroniseerd met de echte wachtwoorden van gebruikers.	N.v.t.	N.v.t.	Het Chrome-beveiligingsteam raadt je sterk aan een wachtwoordmanager te gebruiken, zodat gebruikers makkelijker sterke wachtwoorden kunnen maken. We proberen de wachtwoordmanager zo naadloos en makkelijk mogelijk te maken. Als je vragen hebt, neem je contact op met je Chrome Enterprise-specialist.
Ik wil zorgen dat het Google Workspace-wachtwoord van gebruikers niet kan worden achterhaald via een phishing-aanval.	● Geen	● Geen	Zet Password Alert aan. Bekijk de instructies op Hergebruik van wachtwoorden voorkomen.
Vanwege de testbehoeften van mijn organisatie kunnen we niet altijd meteen de laatste versie van Chrome uitrollen.	● Geen	● Geen	Chrome heeft meerdere releasekanalen waarmee je bedrijf vroege toegang krijgt tot nieuwe functies, bugfixes en beveiligingsverbeteringen. We raden je aan een deel van je team het Bèta- of Dev-kanaal te laten gebruiken om nieuwe functies te testen en je de tijd te geven om je bedrijfsapparaten te updaten. Je hebt dan ook de kans om eventuele zorgen te bespreken met je Chrome Enterprise-specialist voordat een schadelijke wijziging op het Stabiele kanaal terechtkomt. We raden deze aanpak sterk aan. We raden je af updates uit te stellen, omdat je organisatie hierdoor gevoeliger wordt voor bekende kwetsbaarheden. Chrome wordt grotendeels openbaar ontwikkeld. Zodra een beveiligingsfix is vrijgegeven voor het Stabiele kanaal, is de informatie over die bug openbaar zichtbaar. Het is dus erg belangrijk dat je gebruikers de nieuwste versie van Chrome gebruiken.

Beheer en prestaties (vervolg)

Behoefte van het bedrijf	Gevolgen voor gebruikers	Mogelijke negatieve gevolgen voor de beveiliging	Opties en opmerkingen
Ik maak me zorgen dat Chrome Cleanup gevolgen heeft voor de prestaties en niet nodig is, vanwege onze bestaande antivirussoftware. Mijn organisatie wil in plaats van Chrome antivirussoftware van het bedrijf gebruiken om problemen te herkennen en aan ons te melden.	Geen	Gemiddeld	Sommige bedrijven willen Chrome Cleanup uitzetten vanwege zorgen over de prestaties (vooral in VDI-omgevingen) of omdat ze willen dat malware wordt gedetecteerd door zakelijke antivirussoftware, zodat de meldingen via hun Security Information and Event Management-tools (SIEM) en andere processen worden gestuurd. Dit heeft wel gevolgen voor de beveiliging. De Chrome Cleanup-tool richt zich op ongewenste software in plaats van virussen, dus het kan andere software detecteren en verwijderen dan je bedrijfssysteem. Als je Chrome Cleanup toch wilt uitzetten, pas je het beleid `ChromeCleanupEnabled` aan. Opmerking: Als je alleen maar niet wilt dat Chrome Cleanup bevindingen naar Google stuurt, zijn er betere manieren om dit te doen. Bekijk het eerdere antwoord bij Ik wil niet dat Google malware op de pc's van mijn organisatie vindt.
Het intranet van mijn organisatie staat nog niet in HTTPS en mijn gebruikers zien steeds beveiligingswaarschuwingen.	Geen	Gemiddeld	Je kunt instellen dat deze waarschuwingen niet worden getoond met het beleid `OverrideSecurityRestrictionsOnInsecureOrigin`. Dit beleid wordt waarschijnlijk op den duur beëindigd, dus we raden je aan zo snel mogelijk over te stappen naar HTTPS.
Ik wil zorgen dat er een volledig controlepad is voor als ik een compromis met terugwerkende kracht moet onderzoeken.	Laag	Geen	Gebruikers kunnen normaal gesproken instellen dat de browsegeschiedenis niet wordt opgeslagen. Je kunt dit voorkomen door het beleid `SavingBrowserHistoryDisabled` aan te passen. Je kunt ook de incognitomodus uitzetten met het beleid `IncognitoModeAvailability`.
Ik wil dat gebruikers onze door het bedrijf goedgekeurde wachtwoordmanager gebruiken in plaats van de ingebouwde wachtwoordmanager van Chrome.	Laag	Laag	Het is een goede beslissing om gebruikers toegang te geven tot een wachtwoordmanager. Zet de ingebouwde wachtwoordmanager uit met het beleid `PasswordManagerEnabled`. We raden je aan dit beleid alleen toe te passen op bedrijfsprofielen, zodat gebruikers de Chrome-wachtwoordmanager kunnen blijven gebruiken als ze inloggen op hun persoonlijke Chrome-profiel.

Beheer en prestaties (vervolg)

Behoefte van het bedrijf	Gevolgen voor gebruikers	Mogelijke negatieve gevolgen voor de beveiliging	Opties en opmerkingen
Ik wil niet dat gebruikers bepaalde sites bezoeken vanwege het beleid van ons bedrijf.	Gemiddeld	Geen	Je kunt dit instellen met toelatings- en blokkeringslijsten. Zie Toegang tot bepaalde websites toestaan of blokkeren.
Ik wil dat het Chrome-gedrag voorspelbaar is, zodat het alleen verandert als de versie wordt geüpgraded.	Gemiddeld	Geen	Met varianten kun je aanpassingen aanbieden in Google Chrome zonder te upgraden naar een nieuwe versie van de browser, door bestaande functies selectief aan- of uit te zetten. Door `ChromeVariations` in te stellen op `VariationsEnabled (waarde 0)` of het beleid niet ingesteld te laten, kunnen alle varianten worden toegepast op de browser. We raden je af het framework voor Chrome-varianten uit te zetten. Als je dit wel doet, kan Google mogelijk niet snel belangrijke beveiligingsfixes leveren en loopt je organisatie meer risico op beveiligings- en compatibiliteitsproblemen.
Ik wil dat de browser elke keer dat deze wordt geopend naar een centrale inlogpagina of andere bedrijfspagina gaat, zodat gebruikers akkoord gaan met beleid of belangrijke informatie van de organisatie te zien krijgen.	Gemiddeld	Geen	Gebruik `RestoreOnStartupURLs`, `HomepageIsNewTabPage`, `NewTabPageLocation`, `HomepageLocation`.
Ik wil niet dat gebruikers de incognitomodus gebruiken, omdat ze dan misschien naar websites gaan die niet geschikt zijn in een werkomgeving.	Gemiddeld	Geen	Pas het beleid `IncognitoModeAvailability` aan.

Beheer en prestaties (vervolg)

Behoefte van het bedrijf	Gevolgen voor gebruikers	Mogelijke negatieve gevolgen voor de beveiliging	Opties en opmerkingen
Ik gebruik eindpuntsoftware die niet werkt met de DNS-stack van Chrome.	Gemiddeld	Gemiddeld	Chrome heeft een ingebouwde DNS-stack die je kunt uitzetten met het beleid `BuiltInDnsClientEnabled`. (Dit heeft alleen gevolgen voor de DNS-softwarestack die wordt gebruikt, niet voor welke DNS-servers er worden gebruikt.) Als je software gebruikt op je eindpunt die het normale gedrag van DNS-API's aanpast, raden we je aan in te stellen dat Chrome de DNS-stack van het systeem gebruikt. Dit kan gevolgen hebben voor de snelheid en responsiviteit van websites. Het kan ook gevolgen hebben voor de beveiliging, omdat Chrome de verbinding in de toekomst niet kan upgraden naar DNS-over-TLS of een ander beveiligingsprotocol.
Ik wil internetverkeer inspecteren met middleboxes.	Gemiddeld	Gemiddeld	Je moet dan een rootcertificaat installeren op elk eindpunt. Google neemt extreme maatregelen om de veiligheid van certificaten op het internet in het algemeen te controleren (zoals Certificaattransparantie), maar we kunnen natuurlijk niet controleren of je bedrijfscertificaten juist worden gebruikt. Bekijk om gedeeltelijk minder risico te lopen het eerdere antwoord onder Mijn organisatie heeft eigen vertrouwde rootcertificaten op de eindpunten waarmee zakelijke servers worden vertrouwd. Als aanvallers de privésleutel van die vertrouwde roots in handen krijgen, wil ik de certificaten kunnen intrekken om deze risico's gedeeltelijk te beperken. Google raadt je af de TLS-versie te downgraden zodat deze werkt met oudere middleboxes. Oudere TLS-versies dan versie 1.2 bevatten bekende kwetsbaarheden en TLS 1.3 is gemaakt om te beschermen tegen een grote hoeveelheid onbekende kwetsbaarheden.

Beheer en prestaties (vervolg)

Behoefte van het bedrijf	Gevolgen voor gebruikers	Mogelijke negatieve gevolgen voor de beveiliging	Opties en opmerkingen
Ik wil Chrome-gebruikersgedrag inspecteren met een product van derden.	Gemiddeld	Geen	Je kunt afdwingen dat beveiligingsextensies van derden worden geïnstalleerd met het beleid `ExtensionInstallForcelist`. Hiermee krijgen die extensies wel toegang tot de browsegeschiedenis, gebruikersgegevens en geladen pagina's. Dit is echter beter dan code van derden toestemming geven om code te injecteren in de browserprocessen door het beleid `ThirdPartyBlockingEnabled` aan te passen. Team Chrome heeft gemerkt dat injectie van code van derden ertoe kan leiden dat bedrijven meer risico lopen, omdat een deel van de ingebouwde oplossingen in Chrome hierdoor niet meer werkt.
Mijn organisatie past beleid toe met Google Cloud-configuratie, per gebruiker. Ik wil dat deze instellingen altijd worden toegepast voor gebruikers, dus ik wil dat gebruikers in Chrome altijd zijn ingelogd op ons bedrijfsprofiel.	Hoog	Geen	Dwing af dat gebruikers inloggen bij de Chrome-browser met een werkprofiel. Meer informatie Gebruikers kunnen dan niet inloggen op hun eigen Chrome-profiel en dus geen eigen bookmarks en wachtwoorden synchroniseren. Je kunt instellingen apparaatbreed toepassen met Cloudbeheer voor de Chrome-browser of Windows Groepsbeleid.

Chrome beheren

Als IT-beheerder kun je Chrome implementeren voor gebruikers op verschillende platforms. Je kunt dan honderden beleidsregels beheren voor het gebruik van Chrome.

Chrome nu beheren

BeyondCorp Enterprise

BeyondCorp is een Zero Trust-beveiligingsframework gevormd door Google waarmee toegangsbeheer wordt verplaatst van de buitengrens van het bedrijf naar individuele apparaten en gebruikers. Zo kunnen werknemers overal beveiligd werken, zonder dat ze een traditioneel VPN hoeven te gebruiken. Met BeyondCorp Enterprise kunnen gebruikers een Zero Trust-aanpak instellen volgens de principes die we gebruiken bij Google, en de toegang beheren tot hun SaaS-apps die worden gehost op Google Cloud, in andere clouds of op locatie. BeyondCorp Enterprise bevat nieuwe services voor bescherming tegen bedreigingen en gegevensbescherming, waardoor gebruikers een extra beveiligingslaag krijgen, rechtstreeks geïntegreerd in de Chrome-browser, zonder dat er een agent nodig is.

In de nieuwe whitepaper Secure access to SaaS applications with BeyondCorp Enterprise (Beveiligde toegang tot SaaS-apps met BeyondCorp Enterprise) lezen IT-leiders veelvoorkomende scenario's om over na te denken en hoe ze deze situaties kunnen aanpakken. Net als met andere nieuwe implementaties zijn er beveiligingsfactoren waarover organisaties moeten nadenken, zoals:

- Zero Trust-toegang beheren tot goedgekeurde SaaS-apps
- Voorkomen dat gevoelige gegevens worden gelekt vanuit SaaS-apps
- Malwareoverdracht en laterale bewegingen via goedgekeurde apps voorkomen
- Voorkomen dat gebruikers phishing-URL's bezoeken die zijn ingesloten in app-content

We behandelen deze en andere scenario's uitgebreid in de whitepaper. Lees de whitepaper hier en krijg meer informatie over BeyondCorp Enterprise in de on demand overzichtswebinar of op de productpagina.

Meer bronnen

Hier zie je meer hulpbronnen om je te helpen Chrome te beheren in je organisatie:

Implementatiehandleiding voor de Chrome-browser (Windows)
Lijst met Chrome Enterprise-beleid
Release-opmerkingen voor Chrome Enterprise
Helpcentrum van Chrome Enterprise
Extensies beheren in je bedrijf