chrome enterprise

Zero Trust-beveiliging implementeren met Chrome Enterprise en BeyondCorp Enterprise

Inleiding

Netwerkfirewalls bieden organisaties al tientallen jaren bescherming tegen aanvallen van buiten het bedrijfsnetwerk. Maar zoals nieuwsberichten over gegevenslekken aantonen, kunnen hackers zelfs de krachtigste firewalls omzeilen en zo de bedrijfsvoering en reputatie van organisaties in gevaar brengen.

Tegenwoordig is het nog moeilijker om firewalls veilig te houden, omdat steeds meer organisaties en werknemers mobiele apparaten en technologie in de cloud gebruiken.

Met BeyondCorp Enterprise, de Zero Trust-oplossing van Google, verplaats je toegangsbeheer van het netwerk naar individuele gebruikers. Zo wordt de toegang tot zakelijke bronnen beveiligd gebaseerd op contextuele inloggegevens van apparaten en gebruikers. Het maakt niet uit of gebruikers fysiek aanwezig zijn op kantoor of thuiswerken. Als hun apparaat en inloggegevens niet kunnen worden geverifieerd, hebben ze geen toegang tot bronnen in het bedrijfsnetwerk.

Met BeyondCorp Enterprise kunnen IT-professionals gedetailleerde toegang tot zakelijke apps en bronnen afdwingen en kunnen gebruikers werken vanuit elk netwerk zonder verbinding te hoeven maken met het bedrijfsnetwerk via een traditioneel VPN.

De Chrome-browser is de primaire en meest beveiligde plek waar gebruikers toegang hebben tot gevoelige bedrijfsbronnen. Enkele functies voor gegevensbescherming en beveiliging tegen dreigingen van de Chrome-browser in BeyondCorp Enterprise zijn gegevensverlies voorkomen in realtime, malwarescans en URL-controles. Je kunt dit allemaal in de gaten houden via de Google Beheerdersconsole.

chrome enterprise

Toepassingen

Chrome Enterprise en BeyondCorp Enterprise bieden Zero Trust-bescherming door de beste beveiligingstechnologieën van Google te combineren, zoals contextbewuste Zero Trust-toegang, gegevensbescherming en beveiliging tegen malware, phishing en ransomware.

Met de Zero Trust-functies van BeyondCorp Enterprises krijg je zakelijke bescherming in veel verschillende situaties, zoals:

- Nieuwe werknemers of leveranciers toevoegen en beveiligde toegang geven tot bedrijfsapps zonder dat ze een VPN of lokale agent hoeven te gebruiken.
- Zorgen dat een spreadsheet met gevoelige gegevens alleen wordt gedeeld als aan bepaalde beleidsregels (die jij instelt) wordt voldaan, zoals via een werkmailadres en vanaf een apparaat met zakelijke bescherming tegen phishing of ransomware.
- Checken welke werknemers hun bedrijfswachtwoord gebruiken op websites die niet van het bedrijf zijn en ze automatisch vragen hun wachtwoord te resetten.
- Bedrijfsbronnen beschermen tegen aanvallen met verificatie in 2 stappen.
- Een partner toegang geven tot bronnen in het bedrijfsnetwerk gebaseerd op verificatie en contextuele informatie over de partner en diens apparaten.
- Voorkomen dat gevoelige gegevens, zoals beveiligde medische gegevens (Protected Health Information, PHI), worden gelekt met functies om gegevenslekken te voorkomen in ChromeOS en de Chrome-browser.
- Malwareoverdracht en laterale bewegingen via goedgekeurde apps verbieden.
- Instellen dat gebruikers geen phishing-URL's kunnen bezoeken die zijn ingesloten in e-mails of app-content.

Zo krijgen geverifieerde gebruikers in een omgeving die end-to-end is beveiligd toegang tot bedrijfsbronnen, zonder dat dit ten koste gaat van hun productiviteit.

De rol van de Chrome-browser in BeyondCorp Enterprise

De Chrome-browser breidt Zero Trust-beveiliging uit naar het web. Met technologieën als Safe Browsing, site-isolatie en sandboxing is Chrome een beveiligde browser voor alle bedrijven. Doordat Chrome snel en automatisch wordt geüpdatet, hebben je gebruikers altijd de veiligste versie. BeyondCorp Enterprise biedt extra zakelijke verdedigingsfuncties toe aan Chrome om je bedrijf te beschermen tegen externe dreigingen van hackers, fouten van onvoorzichtige gebruikers, en interne dreigingen rond gevoelige gegevens en gegevensonderschepping.

Gebruikers besteden veel tijd op het werk in de webbrowser. Daarom moet je Chrome zien als integraal onderdeel van het Zero Trust-beveiligingsbeleid van je organisatie (zie figuur 1).

Als je de browsergebaseerde functies voor dreigingsdetectie en gegevensbescherming van Chrome inzet als onderdeel van je Zero Trust-beleid, kun je het volgende doen:

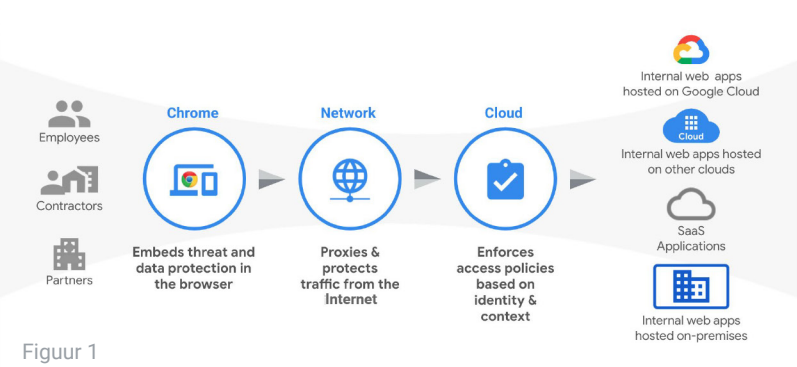
Een inventaris maken met apparaten waarop de Chrome-browser en ChromeOS worden uitgevoerd en die toegang hebben tot de gegevens van je organisatie. Met eindpuntverificatie voor je apparaatinventaris krijg je waardevolle informatie waarmee je apparaten zo goed mogelijk kunt beveiligen. Als je eindpuntverificatie combineert met contextbewuste toegang heb je nog gedetailleerder toegangsbeheer.

Bedrijfsgegevens in realtime beschermen door te voorkomen dat gebruikers het slachtoffer worden van phishing. Safe Browsing combineert de nieuwste informatie van Google over schadelijke sites met URL-scanning in realtime. Zo zorg je dat gebruikers geen bekende schadelijke sites bezoeken (zie figuur 2).

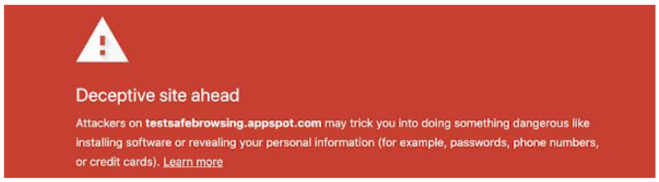
Verdachte bestanden in realtime tegenhouden voordat ze in je netwerk terechtkomen. Chrome scant en analyseert bestanden in realtime, rechtstreeks in Google Cloud (zie figuur 3).

Je kunt instellen of gebruikers het bestand alvast kunnen openen voordat de analyse is afgerond of moeten wachten totdat het bestand is goedgekeurd. Chrome ondersteunt ook malwaredetectie in 3 fasen, via reputatiegebaseerde detectie, statische analyse en geavanceerde sandboxing in de cloud.

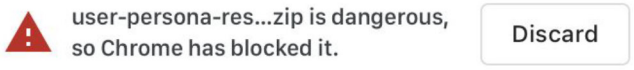
Voorkomen dat bedrijfsgegevens per ongeluk of expres worden gelekt. Bescherming tegen gegevenslekken gebruikt vooraf ingestelde en aangepaste regels om bepaalde acties te blokkeren of gebruikers een melding te laten zien als uploads op verschillende websites het bedrijfsbeleid schenden. Dit is met name handig voor organisaties die klantinformatie verwerken die is beschermd volgens wettelijke nalevingsvereisten (zie figuur 4).



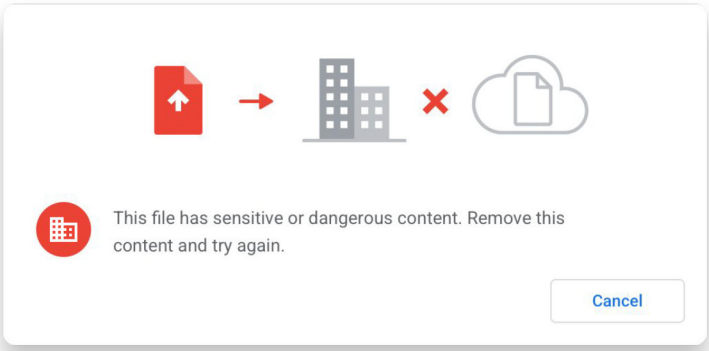
Figuur 1



Figuur 3



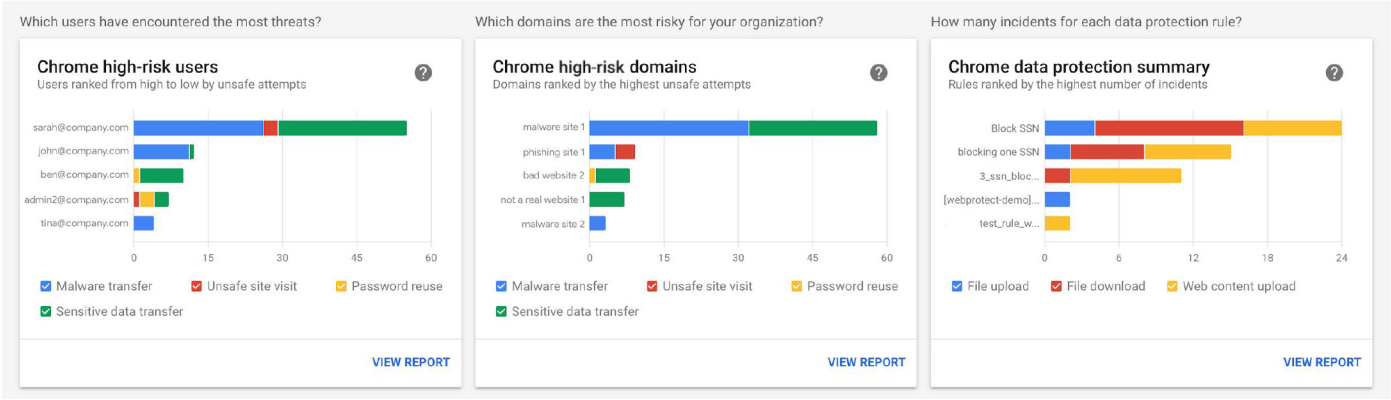
Figuur 3



Figuur 4

chrome enterprise

Meldingen, logboeken en rapporten van onveilige activiteit maken. IT-teams kunnen zorgen voor nog betere beveiliging en compliance door inzicht te krijgen in beveiligingsgebeurtenissen rond verdachte downloads, URL's, hergebruik van wachtwoorden en mogelijke gegevenslekken. Aan de hand van deze informatie kunnen ze ook risicovol gedrag en risicovolle gebruikers in kaart brengen.



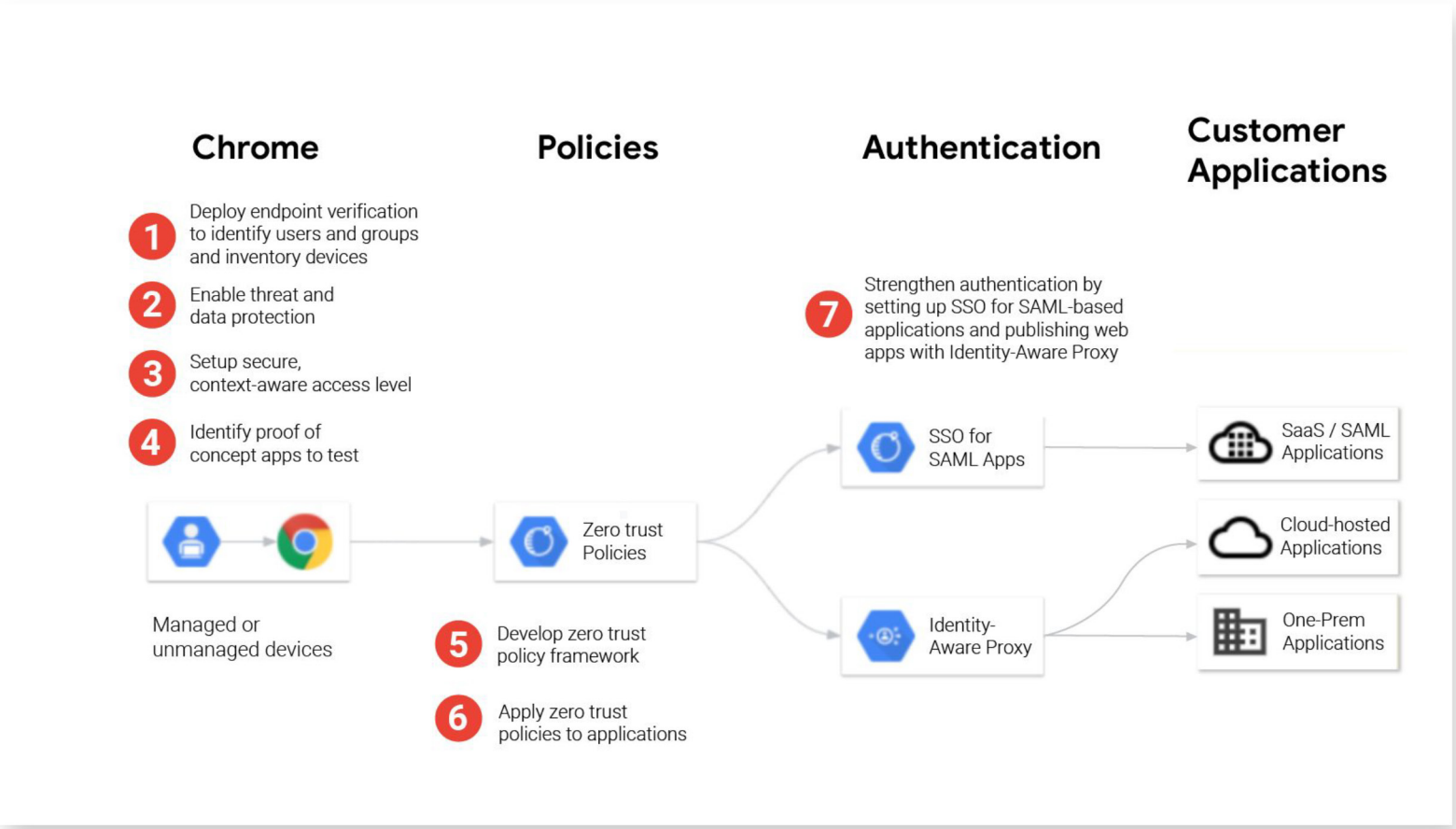
Zero Trust-beveiliging uitbreiden met ChromeOS

Naast de geavanceerde functies voor bescherming tegen dreigingen en gegevensbescherming van de Chrome-browser kun je je beveiligingsmaatregelen nog verder uitbreiden met ChromeOS. ChromeOS is een beveiligd ontworpen besturingssysteem en voegt een belangrijke extra laag toe aan Zero Trust-beveiligingsmodellen.

Als organisaties ChromeOS combineren met de Chrome-browser en BeyondCorp Enterprise kunnen ze risico's voorkomen op hardwareniveau, in interne en externe apps en zelfs op het openbare web.

Migreren naar BeyondCorp Enterprise

Het kost even tijd om elke netwerkgebruiker en app te migreren naar het Zero Trust-framework van BeyondCorp Enterprise. Door de migratie in fasen uit te voeren, kan de bedrijfsvoering gewoon doorgaan en kun je grotere groepen netwerkgebruikers migreren naar BeyondCorp Enterprise zonder dat dit gevolgen heeft voor hun productiviteit.



Conclusie

Chrome Enterprise en BeyondCorp Enterprise ondersteunen organisaties die een Zero Trust-beveiligingsframework willen instellen. Traditionele beveiligingsmodellen die alleen dreigingen van buiten het bedrijfsnetwerk tegenhouden zijn niet meer effectief, vooral nu steeds meer mensen thuiswerken. Organisaties met hybride werknemers moeten gebruikers toegang kunnen geven tot belangrijke apps en services voor het bedrijf, maar vinden het vaak lastig om dit makkelijk en veilig te doen.

Met BeyondCorp Enterprise krijgen gebruikers extra services voor bescherming tegen dreigingen en gegevensbescherming in Chrome. Zo kunnen organisaties een extra beveiligingslaag toevoegen door bescherming te bieden tegen phishing, malware en gegevensverlies, en tegelijk zichtbaarheid te krijgen in onveilige activiteiten.

Zie q.co/cloud/bce voor meer informatie over BeyondCorp Enterprise.

chrome enterprise

Bronnen

Bekijk deze bronnen voor meer informatie over de Chrome-browser, ChromeOS, Chrome Enterprise en BeyondCorp Enterprise:

Chrome-browser

- Download de Chrome-browser voor je bedrijf
- Bekijk meer informatie over Enterprise Support voor de Chrome-browser
- Lees de nieuwste release-opmerkingen voor de zakelijke Chrome-browser
- Blijf op de hoogte van de nieuwste release-updates van de Chrome-browser via de Chrome Releases-blog
- Bekijk de officiële Safety & Security-blog van Google
- Ga naar het Helpcentrum voor de zakelijke Chrome-browser en het Helpforum voor de Chrome-browser
- Bekijk de opties voor Cloudbeheer voor de Chrome-browser
- Lees de Privacyverklaring van Google Chrome
- Lees de whitepaper over privacy in Google Chrome

ChromeOS

- Bekijk meer informatie over het besturingssysteem in de cloud van Google
- Ga naar de Chromium-blog

Chrome Enterprise

- Bekijk hoe Google Chrome Enterprise je meer zakelijke mogelijkheden geeft in ChromeOS, in de Chrome-browser en op Chrome-apparaten
- Ga naar de Chrome Enterprise-blog

BeyondCorp Enterprise

- Lees meer over BeyondCorp Enterprise
- Ga naar de BeyondCorp Enterprise-blog

BeyondCorp Enterprise