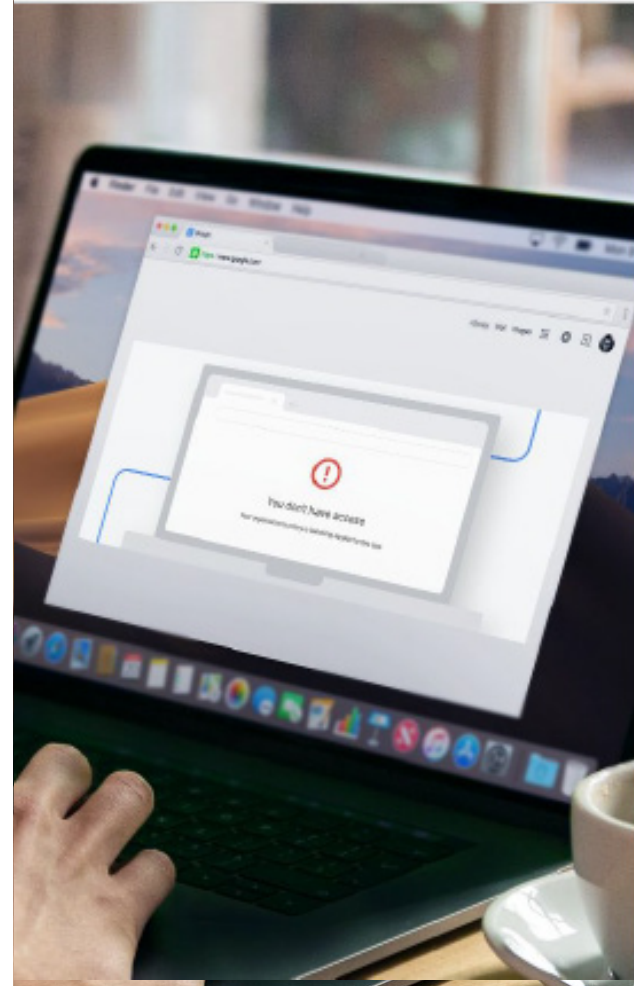


Beveiligd zakelijk browsen begint met Chrome

Mensen werken steeds meer op het web en in de cloud. De browser is dus zowel een manier om productief te zijn als een beveiligingslaag. IT- en beveiligingsteams moeten daarom samenwerken om te zorgen dat bedrijfsgegevens en gebruikers veilig blijven, terwijl werknemers zo efficiënt mogelijk kunnen werken.

Er zijn niet veel technologieën die het gat tussen zakelijke gebruikers en beveiliging zo goed overbruggen als de browser. Aangezien miljoenen gebruikers de Chrome-browser al met veel plezier gebruiken, is er geen betere plek om je zakelijke browserbeveiliging te vergroten dan *binnen* Chrome.

Met Chrome krijgen bedrijven de functies en mogelijkheden om hun gegevens te beveiligen. Als bedrijven Chrome samen gebruiken met [BeyondCorp Enterprise](#), de Zero Trust-toegangsooplossing van Google, kunnen ze functies voor contextbewuste toegang en extra gegevensbescherming afdwingen op beheerde en onbeheerde apparaten. Zo zorgen ze voor een constante beveiligingslaag voor hybride medewerkers en medewerkers op afstand. **Google legt de lat nog hoger voor zakelijke browserbeveiliging.**



Cybercriminaliteit is met **600%** gestegen sinds 2020.¹

De beveiligde browser voor het moderne bedrijf



'Gegevensverlies voorkomen' implementeren

Detecteer en voorkom verlies van gevoelige gegevens, voorkom dat gegevens per ongeluk of expres worden gelekt en dwing beleid voor gegevensbescherming af.



De toegang tot SaaS-apps bewaken

Bied contextbewuste Zero Trust-toegang tot SaaS-apps en voorkom ongeautoriseerde toegang en inbreuk op gegevens.



Beheerde en onbeheerde apparaten beveiligen

Voeg een uniforme beveiligingslaag toe aan alle apparaten, inclusief in BYOD-omgevingen (Bring Your Own Device), met bescherming tegen malware en phishing, zonder agents.



Hybride en externe medewerkers en thuiswerkers beschermen

Bied beveiligde toegang tot bedrijfsbronnen en -gegevens, zelfs als gebruikers niet het bedrijfsnetwerk gebruiken of niet fulltime medewerker zijn.

Gegevensbeveiliging

Voorkom verlies en onderschepping van bedrijfsgegevens.

Voeg DLP (Data Loss Prevention) toe aan de browser, inclusief voor het uploaden, downloaden, afdrukken, opslaan, kopiëren en plakken van content, mogelijk gemaakt door BeyondCorp Enterprise.

Bescherming tegen malware en phishing

Bescherm gebruikers tegen realtime bedreigingen terwijl ze werken op het web.

Stel beleid in om te voorkomen dat gebruikers niet-vertrouwde bestanden downloaden of naar onveilige URL's gaan.

Beveiligingsrapporten en -inzichten

Krijg inzichten in de browser om betere beveiligingsplannen voor het bedrijf te maken en belangrijke informatie over beveiligingsgebeurtenissen te bekijken.

Stuur gebeurtenissen over hergebruik van wachtwoorden, bezoeken aan onveilige sites, malwareoverdracht en inbreuk op wachtwoorden vanuit Chrome naar verschillende Google-oplossingen en integraties met derden voor meer analyse.

Extensies beheren

Blokkeer extensies, stel in dat extensies afgedwongen worden geïnstalleerd of sta gebruikers toe extensies aan te vragen voor meer browserbeveiliging.

Je kunt extensieverzoeken op één plek goedkeuren en beheren. Gebruik beleid voor extensies om extensies te beperken en/of zichtbaarheid te krijgen in de extensies die je gebruikers aanvragen.

Risicobeheer voor apparaten

Stuur snel en automatisch updates voor nieuwe zero-day-kwetsbaarheden.

Met automatische updates zien gebruikers een prompt om Chrome opnieuw op te starten, zodat de browser wordt geüpdatet naar de nieuwste versie. Het is een zakelijke best practice om de Chrome-browsers in je inventaris up-to-date te houden met de nieuwste beveiligingspatches.

Adaptief beleidsbeheer

Beheer honderden beleidsregels op één centrale plek om je gebruikers beveiligd te laten browsen op het web.

Gebruik één browser waarin je beveiliging op het hoogste niveau kunt instellen voor gebruikers die veel risico lopen, zonder dat de productiviteit van gebruikers met een laag risico achteruit gaat.



We hebben Chrome en BeyondCorp Enterprise Essentials gekozen als beveiligde zakelijke browseoplossing, omdat we hiermee uitgebreide zichtbaarheid en bescherming krijgen om onze gebruikers en bedrijfsgegevens veilig te houden. Omdat beveiligingsfuncties onderdeel zijn van de browser, kunnen we deze makkelijk en consequent schalen op alle beheerde en onbeheerde apparaten. Nadat we de oplossing hadden geactiveerd, waren we in staat om binnen enkele uren een poging te verijdelen om een grote hoeveelheid bedrijfsgegevens te onderscheppen. Het is een enorm voordeel om rechtstreeks vanuit Chrome geavanceerde beveiligingsrapporten te kunnen bekijken over gebeurtenissen als contentoverdracht, zowel om ongewenste gegevensoverdracht te blokkeren en om inzicht te krijgen in hoe gegevens worden gedeeld bij Roche."

Tim Ehrhart
Domain Head, Information Security



Bekijk waarom miljoenen bedrijven Chrome gebruiken als beveiligde zakelijke browser op

<https://chromeenterprise.google/browser/security/>