chrome enterprise

Beveilig je bedrijf in een cloudgebaseerde wereld

Organisaties investeren flink in hun beveiliging met producten die claimen hackers en spionage tegen te houden en zwakke plekken aan te pakken. Maar ondanks alle moeite neemt het aantal beveiligingsincidenten toe.

De beveiligingsmarkt groeit in 2019 naar verwachting **met 8,7% tot $ 124 miljard.**[1]

Het aantal grote, gerichte cyberaanvallen in de VS **groeit echter met meer dan 27%** per jaar.[2]

Hoewel het aantal aanvallen toeneemt en ze steeds verfijnder worden, zijn het typen dreigingen die we al kennen: voornamelijk malware, ransomware en phishing. De traditionele aanpak van beveiliging is duidelijk niet meer afdoende. Het wordt tijd om naar een nieuwe oplossing te kijken voor een bestaand probleem.

Kies voor een unieke aanpak van eindpuntbeveiliging met Chrome Enterprise

Apparaatbeveiliging met meerdere lagen

Elke laag van een Chromebook werkt samen met de andere om je unieke beveiligingsvoordelen te bieden.

- Versleutel gebruikersgegevens
- Voorkom dat er wordt geknoeid met het OS
- Minder gegevens op apparaten
- Regelmatige patches en updates
- Voorkom achteloosheid van gebruikers

Geïsoleerde en beheerde apps

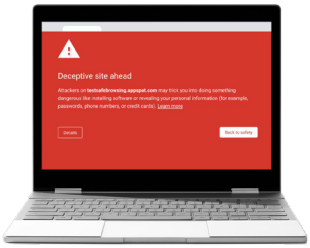
Zorg dat gebruikers geen schadelijke apps kunnen gebruiken.

- Beperk het bereik van aanvallen met sandboxing
- Dwing toegangsbeleid af
- Beveilig meerdere ecosystemen, waaronder de Chrome Web Store, Google Play, het web en native Linux-apps

[1] Ponemon en Accenture, 2017; [2] Gartner, 2018

chrome enterprise

Bescherm je bedrijf tegen bekende dreigingen met Chrome Enterprise en de kracht van Google Cloud



Phishing

Met Google Safe Browsing krijgen gebruikers een waarschuwing te zien voordat ze naar schadelijke sites gaan.

Met **beveiligingssleutels en verificatie in twee stappen** kun je voorkomen dat hackers gestolen wachtwoorden kunnen gebruiken.

Als de aanval toch slaagt: met het Password Alert-beleid moeten gebruikers hun wachtwoord wijzigen als ze dit hebben gebruikt op een niet-geautoriseerde site.

Ransomware

De beperkte hoeveelheid gegevens op het apparaat zorgt dat er minder gegevens kunnen worden gegijzeld.

Het **alleen-lezen OS** voorkomt dat exe-bestanden lokaal kunnen worden uitgevoerd.

Als de aanval toch slaagt: Verified boot controleert bij het opstarten of er is gerommeld met het systeem.

Schadelijke apps

Een zwarte lijst voor specifieke rechten bepaalt tot welke apps mensen toegang hebben.

Managed Google Play biedt mogelijkheden voor groeps- en beleidsbeheer per app.

Als de aanval toch slaagt: sandboxing beperkt het aanvaloppervlak.

Waarom Chromebooks geen virusscanner nodig hebben

Alleen lezen: geïnstalleerde apps en extensies kunnen het OS niet aanpassen.

Met sandboxing worden aanvallen beperkt.

Met **Verified Boot** wordt voorkomen dat een apparaat waarmee is geknoeid, kan opstarten.

Controleproces vereist voor alle extensies en apps.

Waarom Chromebook-updates zo effectief zijn

Geen onderbrekingen: updates worden op de achtergrond uitgevoerd terwijl gebruikers werken.

Doordat er **twee versies van het OS** op een apparaat staan, kan de ene versie worden gebruikt terwijl de andere wordt geüpdatet.

Updates worden uitgevoerd als het apparaat opnieuw wordt opgestart en duren slechts enkele seconden.

Meer informatie over Chrome Enterprise-beveiliging:
cloud.google.com/chrome-enterprise/security