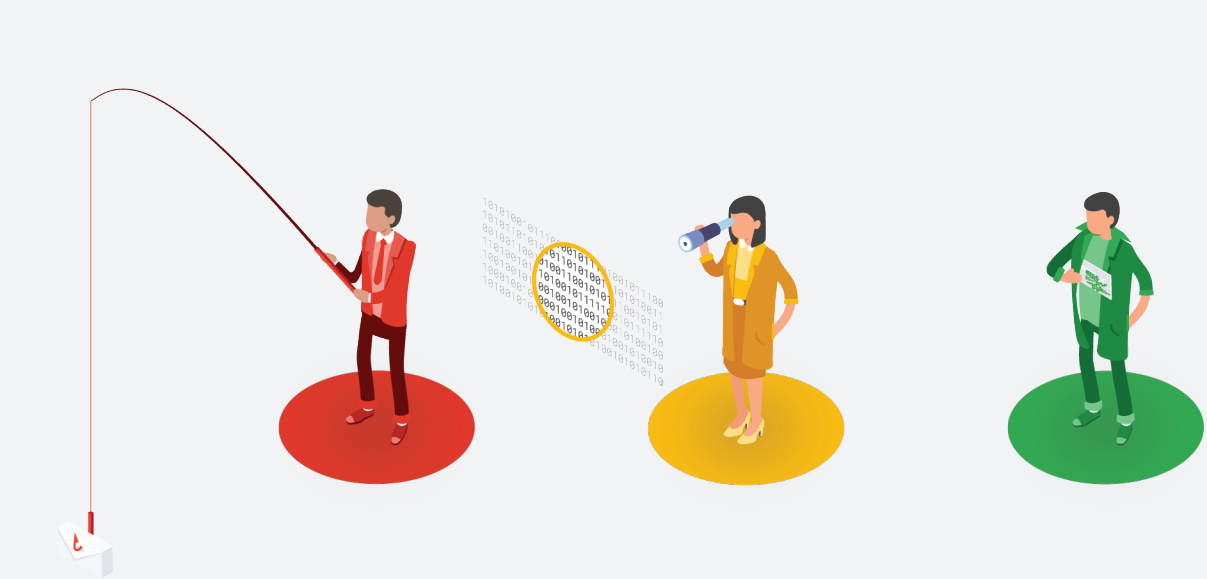
Cloud-native beveiliging voor eindpunten

De innovatieve manier waarop Chrome Enterprise gegevens beschermt en IT-beheer vereenvoudigt



chrome enterprise

chrome enterprise

Inhoudsopgave

Er moet een betere manier zijn

De beveiliging van eindpunten is een rommeltje

De beveiliging van eindpunten is een van de grootste uitdagingen voor experts op het gebied van cybersecurity en IT-werkzaamheden. Ze krijgen te maken met lastige problemen en continu veranderende aanvallen.

Traditionele eindpunten zijn ingewikkeld. Deze eindpunten hebben vaak de volgende kenmerken:

1. Ze bevatten honderden softwarefragmenten die een doelwit voor kwaadwillenden vormen, zoals oude en niet-gepatchte versies en niet-goedgekeurde softwarepakketten.
2. Ze zijn kwetsbaar als gebruikers schadelijke websites bezoeken, onbekende apps downloaden of voorkomen dat noodzakelijke software-updates worden toegepast.
3. Ze bevatten gigabytes aan intellectueel eigendom, persoonlijk identificeerbare informatie (PII) en gebruikersgegevens.
4. Ze beschikken over slecht afgedwongen grenzen tussen processen, waardoor één gehackte softwaremodule hackers toegang kan geven tot het volledige systeem en bedrijfsnetwerk.

In deze situatie steken cybersecurity-teams vaak enorm veel tijd en moeite in pogingen om eindpunten te controleren, kwetsbaarheden te identificeren en aanvallen te detecteren. De operations-teams zijn doorlopend bezig om consequente images te maken en firmware, besturingssystemen, programma's, drivers, browsers en apps op honderden verspreide apparaten te patchen en updaten. En om alles nog wat complexer te maken: steeds meer gebruikers werken vanuit huis of onderweg, waardoor tools en processen die zijn ontworpen voor bedrijfsnetwerken steeds minder effectief zijn.

Tijd om het model in een nieuw kader te zetten

Je hebt nu de kans om aan deze chaos te ontsnappen en baanbrekende verbeteringen door te voeren in de beveiliging en het beheer van eindpunten.

Zo kunnen IT-organisaties de vruchten plukken van de ingebouwde voordelen van cloudgebaseerde architecturen voor beveiliging en operations. Informatiemiddelen kunnen makkelijker worden gecontroleerd als ze zijn opgeslagen en gedeeld in de cloud, in plaats van op kwetsbare eindpunten. Het is veel eenvoudiger om software op een centraal cloudplatform bij te houden en te updaten dan op honderden externe apparaten.

Daarnaast ontwikkelen technologieleveranciers cloud-native beveiliging en introduceren ze opmerkelijke nieuwe mogelijkheden om de beveiliging van eindpunten te versterken en het beheer van eindpunten te vereenvoudigen.

In deze whitepaper kijken we hoe Google de beveiliging van eindpunten opnieuw heeft ontworpen door gebruik te maken van de ingebouwde voordelen van cloudcomputing en door innovatieve beveiliging in meerdere lagen te ontwikkelen op vijf niveaus: apparaat, firmware, besturingssysteem, browser en app.

We bespreken ook voorbeelden van het volgende:

1. Hoe de innovatieve beveiligingsfuncties van Google bescherming bieden tegen specifieke dreigingen, zoals malware, phishing, drive-by-downloads en APT's
2. Hoe Chrome Enterprise operationele taken aanzienlijk vereenvoudigt, zoals het updaten van software, de verwerking van kwijtgeraakte en gestolen apparaten, en het beheer van beveiligingsbeleid voor verspreide apparaten
3. Hoe je Microsoft Active Directory en toonaangevende tools van derden voor zakelijk mobiliteitsbeheer kunt inzetten om het beheer van eindpunten te automatiseren

Gebruikmaken van de ingebouwde voordelen van cloudcomputing

Minder middelen op eindpunten

Een van de ingebouwde voordelen van cloudgebaseerde architecturen is dat de meeste informatiemiddelen zijn opgeslagen in de cloud en niet op eindpunten. Je hoeft je geen zorgen te maken dat klantenlijsten, bedrijfsplannen, inkomstenrapporten, HR-gegevens en softwareprogramma's risico lopen als een laptop zoek is of is gestolen. Als een apparaat is gehackt, is het veel onwaarschijnlijker dat de hacker creditcardgegevens van klanten, medische informatie van medewerkers of wachtwoorden voor toegang tot de financiële systemen van het bedrijf kan vinden.

Een kleiner bereik voor aanvallen

Met een cloudgebaseerde architectuur worden er veel minder softwarefragmenten op eindpunten geïnstalleerd. Verspreide apparaten hebben nog steeds firmware en een besturingssysteem nodig, maar geen tientallen programma's, drivers, browser, bedrijfsapps en persoonlijke apps die zich opstapelen op traditionele eindpunten. In vergelijking met traditionele eindpunten zijn er niet zo veel kwetsbaarheden aanwezig die hackers kunnen targeten en hoeft slechts een fractie van de software-onderdelen te worden geïnstalleerd, beheerd en beschermd.

Snelle, frequente updates

In het geval van traditionele eindpunten moet je doorlopend software patchen en updaten op apparaten die door het hele land of zelfs over de hele wereld zijn verspreid. Daarnaast moeten cybersecurity- en operations-teams zich continu haasten om een patch te implementeren of instellingen toe te voegen aan honderden eindpunten als er een kwetsbaarheid of nieuwe aanvalstechniek is ontdekt. Hoe langer de deur op een kiertje blijft staan, hoe groter de kans dat agressieve hackers gebruikmaken van deze mogelijkheid.

Met cloudarchitecturen kun je software en instellingen centraal updaten, implementeren en beheren vanaf één centrale plek, zodat je het vereiste werk om eindpunten up-to-date te houden aanzienlijk kunt inperken.

Het apparaat: ingebouwde beveiliging en consistentie

Een cloudarchitectuur biedt een aanzienlijk aantal mogelijkheden voor innovatieve functies op het gebied van beveiliging en beheer. Deze beginnen bij Chrome-apparaten zoals laptops en tablets met Chrome OS en de Chrome-browser van Google. Er zijn Chromebooks verkrijgbaar van verschillende toonaangevende technologiebedrijven, zoals Acer, ASUS, Dell, Google, HP, Lenovo en Samsung.

De hardwarebeveiligingsmodule

Alle recente Chromebooks bevatten een hardwarebeveiligingsmodule die speciaal is ontworpen aan de hand van Google-specificaties. De module omvat flashgeheugen, ROM, RAM en detectiefuncties voor manipulatie op een speciale chip, waardoor het extreem moeilijk wordt om de in de module opgeslagen informatie te manipuleren. In de hardwarebeveiligingsmodule worden essentiële informatie en cryptografische sleutels opgeslagen, zodat deze niet toegankelijk zijn voor het besturingssysteem. Daarnaast biedt deze module bescherming tegen bepaalde typen side-channel gegevenslekaanvallen en technieken voor fysieke foutinjectie.

Versleuteling en scheiding van gebruikersgegevens

Gebruikersgegevens en -instellingen worden standaard op alle Chromebooks versleuteld. Deze versleuteling kan niet worden uitgeschakeld door gebruikers (of anderen).

Daarnaast worden alle gegevens en instellingen van elke gebruiker versleuteld met een unieke sleutel. Een hacker moet vrijwel altijd over zowel het gebruikerswachtwoord als toegang tot de beveiligingsmodule beschikken om deze sleutel te kunnen gebruiken. Het is dus heel lastig voor kwaadwillenden om gebruikersgegevens te lezen en zelfs als kwaadwillenden in het bezit zijn van een Chromebook en de bijbehorende toegangscode, kunnen ze de gegevens van andere gebruikers niet ontsleutelen en lezen.

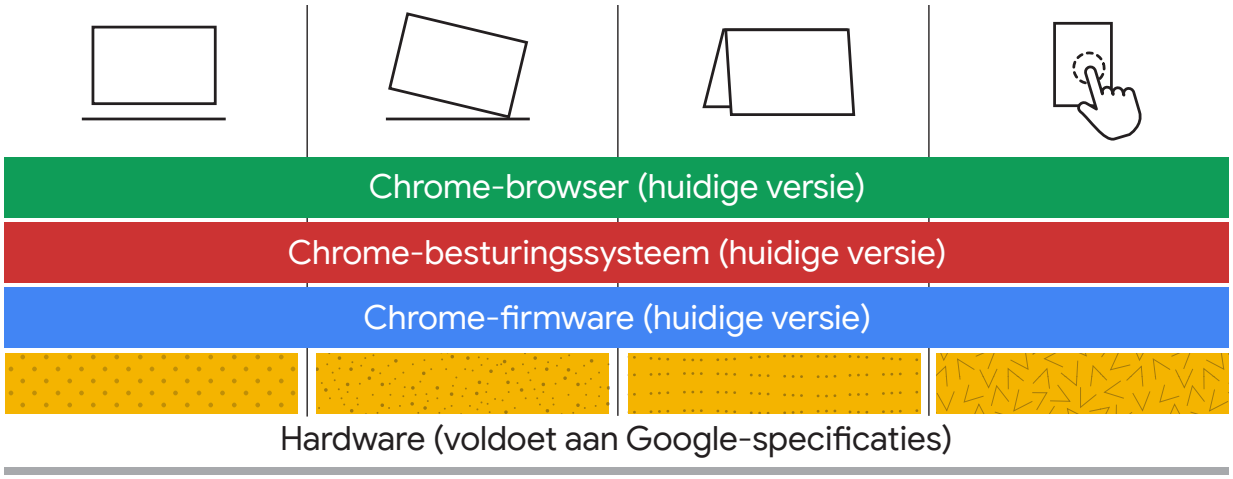
De scheiding van gebruikersgegevens heeft nog een voordeel: het maakt het makkelijker om apparaten te delen met collega's en familieleden, en om toonaangevende benaderingen zoals Grab and Go te implementeren voor leenapparaten en tijdelijke medewerkers.

Scenario: Inbreuk door een insider voorkomen

Xavier, Yao en Zainab, drie aannemers die op verschillende dagen werken, delen een Chromebook. Helaas is Xavier een amateurhacker die toegang wil tot een server die door Zainab wordt gebruikt. Hij weet dat daarop waardevolle algoritmen en eigen software zijn opgeslagen. Xavier logt in op de Chromebook en gebruikt deze voor zijn eigen werk, maar hij heeft geen toegang tot de inloggegevens, netwerkverbindingen en andere gegevens of instellingen van Zainab. De gegevens op die specifieke server zijn veilig.

Consistentie op alle eindpunten

Chromebook-fabrikanten zijn ermee akkoord gegaan te voldoen aan Google-specificaties voor kwaliteit, prestaties en beveiliging, of deze specificaties te overtreffen. Google controleert de hardware-ontwerpen en moet deze goedkeuren voordat de apparaten op de markt kunnen worden gebracht met het Chrome-merk. De fabrikanten gaan er ook mee akkoord consistente firmware en dezelfde Chrome OS en Chrome-browser te gebruiken voor elke Chromebook. (Afbeelding 1)



Afbeelding 1: Voor een naadloze gebruikerservaring en vereenvoudigd beheer beschikken alle Chromebooks over consistente versies van de firmware, het Chrome-besturingssysteem en de Chrome-browser.

Deze gemeenschappelijke kenmerken vormen een belangrijk voordeel voor zowel gebruikers als beheerders. Gebruikers beschikken over consistente functionaliteit en meer gebruiksgemak op alle Chromebooks. Beveiligings- en operations-teams kunnen een standaard werkomgeving bieden. Er hoeven geen meerdere versies van firmware, besturingssystemen, systeemprogramma's en browsers te worden beheerd. Daarnaast hoeven ze zich geen zorgen te maken dat ongeschikte softwarereleases kwetsbaarheden veroorzaken. Als er zich problemen voordoen, kunnen deze veel makkelijker en sneller worden verholpen.

Goede beslissingen op het gebied van beveiliging

Google werkt samen met de ecosysteempartners om functies en standaardinstellingen te identificeren die voor een betere beveiliging zorgen voor gebruikers die weinig tot geen kennis van cybersecurity (of zelfs computers) hebben. We hebben hierboven aangegeven dat alle gebruikersgegevens standaard worden versleuteld. Later in dit document kom je meer voorbeelden hiervan tegen.

Firmware: een verificatieketen

‘Persistentie’ is een belangrijk element binnen de meest geavanceerde getargete aanvallen. Geavanceerde aanvallen zijn meestal afhankelijk van het achterlaten van code of scripts op eindpunten waarmee de hackers toegang blijven houden tot het eindpunt als dit opnieuw is opgestart of als er zich een systeemfout heeft voorgedaan.

Cloudarchitecturen zorgen ervoor dat veel technieken die hackers gebruiken op traditionele eindpunten niet meer werken. Als er bijvoorbeeld geen door de gebruiker te installeren drivers zijn of scripts kunnen worden opgeslagen op de eindpunten, kunnen deze niet worden gebruikt om schadelijke code te behouden na het opnieuw opstarten van het apparaat.

Kwaadwillenden kunnen echter nog wel proberen code te injecteren in de schrijfbare firmware, besturingssystemen en browsers die zijn opgeslagen op de apparaten.

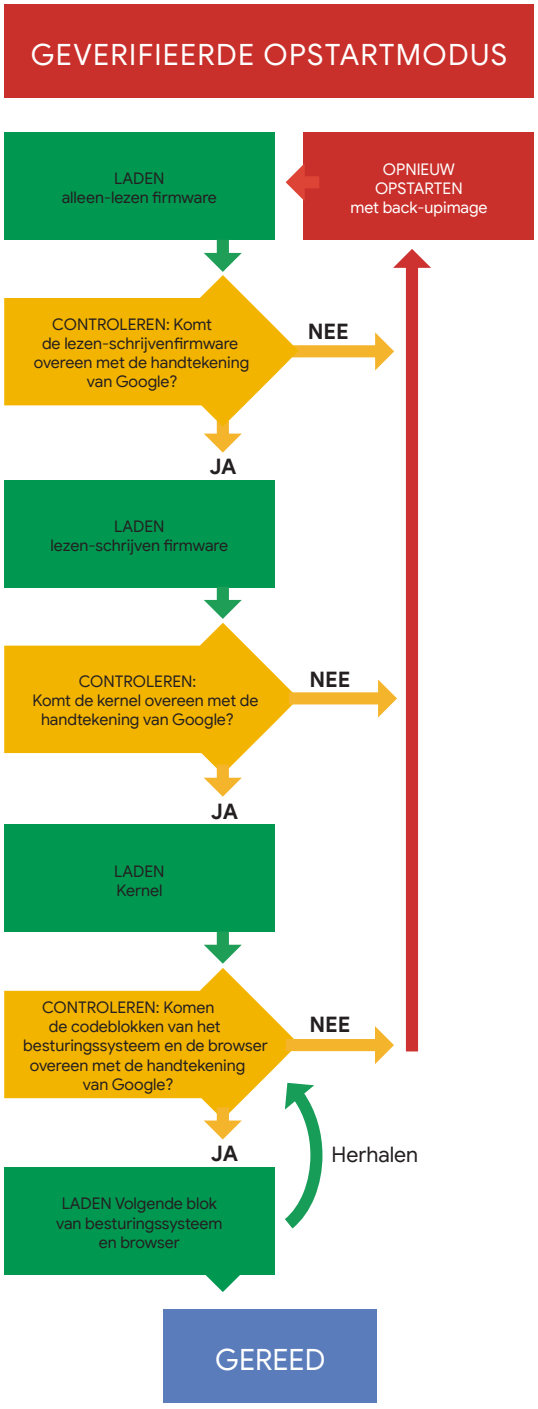
Google gebruikt om dit te voorkomen een techniek met de naam ‘Geverifieerde opstartmodus’ (Verified boot) om ervoor te zorgen dat de code van de firmware, het besturingssysteem en de browser na het opstarten ongewijzigde software van Google is.

Scenario: Blokkeer die rootkit!

Cybercrimineel Bela krijgt toegang tot een Chromebook en verkrijgt supergebruikerprivileges. Ze mount de rootpartitie rechtstreeks opnieuw als lezen-schrijven, en voegt vervolgens een rootkit toe in de vorm van een kernel-module. Als het apparaat echter weer opnieuw wordt opgestart, komt de handtekening van dat deel van de rootpartitie niet meer overeen met de verwachte handtekening. Het opstartproces wordt gestopt en het apparaat start opnieuw op met de back-upimage van de firmware en het besturingssysteem. Na het opnieuw opstarten kan Bela de rootkit niet meer gebruiken om controle te krijgen over het apparaat.

Als een Chromebook wordt opgestart, gebruikt de alleen-lezen firmware een handtekening en ondertekende hash om te verifiëren dat de schrijfbare firmware exact overeenkomt met de door Google goedgekeurde image (er wordt een hash berekend voor de firmwarecode en er wordt gecontroleerd of deze overeenkomt met de ondertekende hash). De nu geverifieerde schrijfbare firmware gebruikt vervolgens hetzelfde proces om de kernel te verifiëren, waarna alle codefragmenten in het besturingssysteem en de Chrome-browser worden geverifieerd. Als er bewijzen worden gevonden voor malware of andere afwijkingen, wordt het opstartproces gestopt en start het apparaat opnieuw op met een back-upversie van de schrijfbare firmware en het besturingssysteem. (Afbeelding 2)

Het geverifieerde opstartproces biedt niet alleen bescherming tegen gevaarlijke aanvallen, maar zorgt er ook voor dat IT-teams geen tijd meer hoeven te verspillen aan het herstellen van gehackte firmware en bestanden.



Afbeelding 2: De geverifieerde opstartmodus zorgt ervoor dat de firmware, het besturingssysteem en de browser niet zijn gemanipuleerd.

Besturingssysteem: sandboxing van processen en naadloze updates

Het Chrome-besturingssysteem omvat verschillende beveiligingsfuncties die apps beschermen en de obstakels wegnemen die vaak komen kijken bij het updaten en patchen van besturingssystemen.

Scheiding van privileges en sandboxing van processen

Verschillende klassen cyberaanvallen gebruiken gehackte websites of cloudgebaseerde apps om controle te krijgen over softwarecomponenten op een eindpunt.

In een cloud-native omgeving zijn er veel minder besturingssysteemcomponenten, programma's, drivers en andere softwarefragmenten die kunnen worden gehackt. Maar de architectuur van Chrome OS doet nog meer om te voorkomen dat gehackte apps andere software beïnvloeden.

Zo maakt Chrome OS gebruik van sandboxing van processen. Hiermee worden strenge grenzen tussen processen getrokken op het moment dat ze worden uitgevoerd. Op deze manier kunnen apps niet met elkaar communiceren, behalve onder strikte voorwaarden. Elk uitgevoerd proces kan uitsluitend de daadwerkelijk benodigde privileges gebruiken. Net zoals beveiligingsgerichte organisaties de toegang tot vertrouwelijke gegevens beperken tot mensen die deze informatie absoluut moeten weten, beperkt Chrome OS de interactie tussen processen tot de processen die hier daadwerkelijk gebruik van moeten maken.

Scenario: Ransomware de deur wijzen

Arjan heeft even een paar minuten pauze en gaat op zoek naar een nieuwe digitale achtergrond voor zijn Chromebook-scherm. Helaas is de Fortnite-fansite waarop hij belandt een nepwebsite die door cybercriminelen wordt beheerd. Als hij op een link klikt om een bestand te downloaden, wordt er via schadelijke code geprobeerd alle gegevens en bestanden op de Chromebook te versleutelen. Gelukkig worden de acties van de code allemaal uitgevoerd in de sandbox van één proces. Arjan krijgt de melding 'Je kunt dit bestand niet uitvoeren' en de ransomware-aanval wordt stopgezet voordat de gebruikersgegevens kunnen worden buitgemaakt.

Naadloze updates van het besturingssysteem

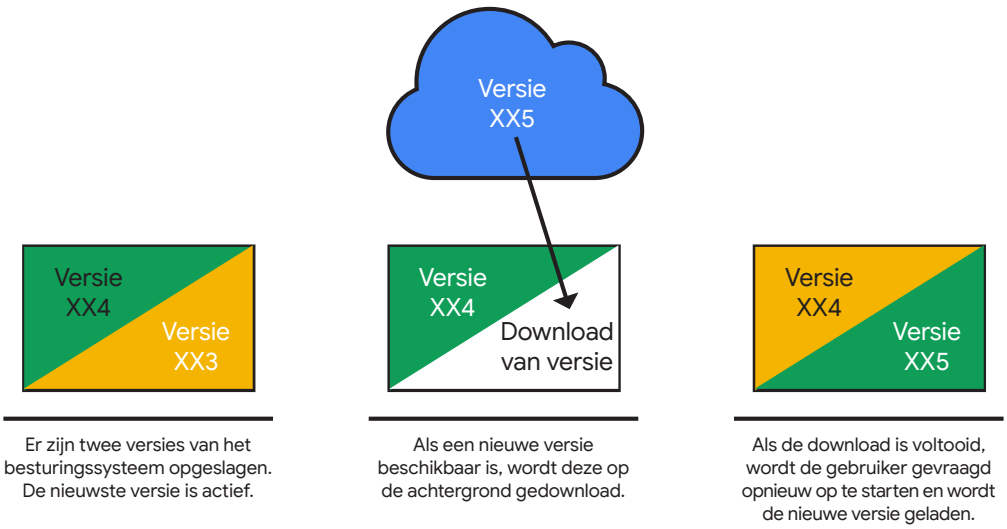
Besturingssystemen actueel houden is een enorm zorgpunt voor de meeste beveiligings- en operations-teams. Updates van besturingssystemen op traditionele eindpunten zorgen voor onderbrekingen voor eindgebruikers. Ze kunnen eindpunten enkele minuten onbruikbaar maken, met soms pieken van meer dan een uur. Dit draagt grote kosten met zich mee als je kijkt naar verloren productiviteit. Daarnaast kan dit leiden tot frustratie onder gebruikers en negatieve gedachten over de IT-organisatie.

Erger nog: vaak weigeren gebruikers de updates, waardoor ze hun apparaten kwetsbaar maken voor aanvallen.

Google biedt een innovatieve oplossing voor dit probleem. Op elk apparaat worden twee versies van het besturingssysteem opgeslagen: de huidige versie en een eerdere versie. Terwijl het systeem wordt gebruikt met het huidige besturingssysteem, kan een geüpdatete versie op de achtergrond worden gedownload en opgeslagen, zonder onderbrekingen voor de gebruiker. Als het systeem opnieuw wordt opgestart door de gebruiker, wordt het geüpdatete besturingssysteem in enkele seconden geladen. (Afbeelding 3)

Dit zorgt ook voor een vereenvoudiging van het geverifieerde opstartproces, dat we eerder hebben besproken. Als het systeem tijdens het opstarten ontdekt dat iemand de code van de actieve versie van het besturingssysteem heeft gemanipuleerd, staat de eerdere, schone versie al klaar op het apparaat en kan deze meteen worden gebruikt.

Chromebooks nemen de zorgen van routine-updates voor onderdelen van het besturingssysteem weg. Het is zelfs zo dat Google Chrome OS ongeveer om de zes weken kan updaten, wat veel frequenter is dan andere grote besturingssystemen. Daarnaast worden beveiligingspatches voor net ontdekte kwetsbaarheden in het besturingssysteem razendsnel geïmplementeerd om zo de blootstellingsperiode zo kort mogelijk te houden.



Afbeelding 3: Nieuwe versies van het besturingssysteem worden op de achtergrond gedownload, zonder het werk van de gebruiker te onderbreken.

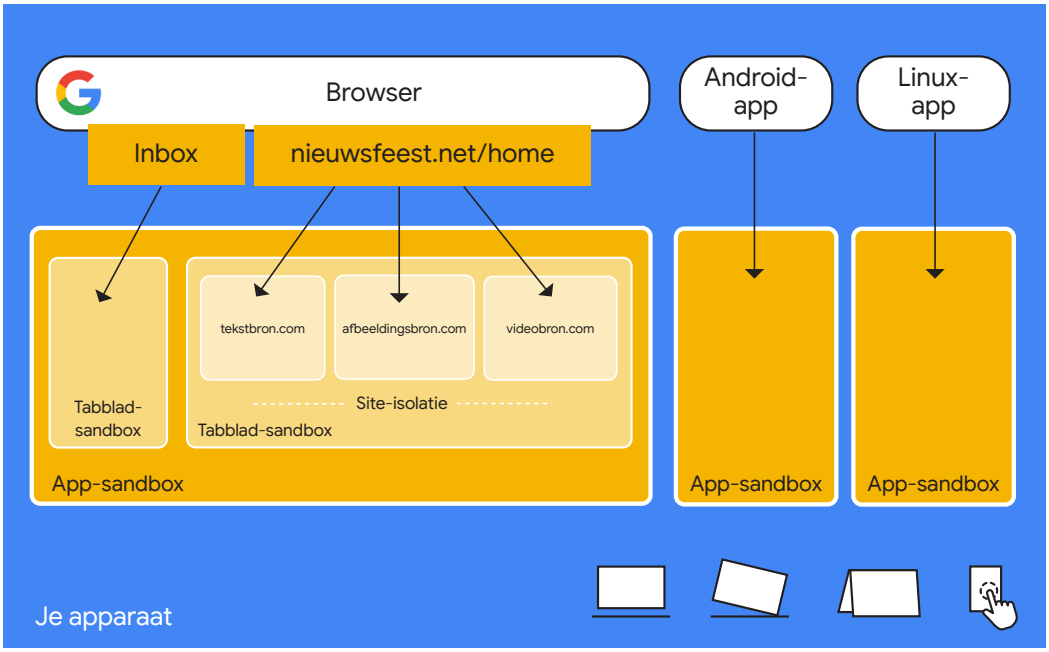
Browser: site-isolatie, Safe Browsing en verificatie in twee stappen

Op Chromebooks vindt alle interactie op internet plaats in de Chrome-browser. Gebruikers plukken de vruchten van de innovatieve beveiligingsfuncties die zijn ingebouwd in de toonaangevende browser van Google.

Sandboxing van tabbladen en site-isolatie

Het concept van sandboxing dat we eerder in verband met Chrome OS hebben bespreken, is ook toegepast in de Chrome-browser. Elk open tabblad in de browser heeft een eigen sandbox. Hiermee wordt de kans dat een aanval in het ene tabblad kan worden voortgezet in andere tabbladen aanzienlijk beperkt.

Op dit principe kan nog verder worden voortgebouwd met site-isolatie. Het komt vaak voor dat verschillende websites worden geopend op één tabblad. Zo kan het bijvoorbeeld voorkomen dat als je een html-webpagina op de ene site leest, de afbeeldingen op die pagina via een tweede site worden gedownload, de video's van een derde site en een script van een vierde site. Met site-isolatie worden de processen van elk van die sites gescheiden. (Afbeelding 4) Met de Chrome-browser kunnen beheerders ervoor kiezen alle of geselecteerde sites te isoleren.



Afbeelding 4: Chrome OS en de Chrome-browser bieden meerdere isolatieniveaus: site, tabblad en app.

Deze mogelijkheden bieden bescherming tegen dreigingen zoals universal cross-site scripting (UXSS) en speculatieve side-channel aanvallen (zoals Spectre en Meltdown) waarbij een schadelijke website toegang probeert te krijgen tot processen of gegevens in het geheugen dat eigendom is van een andere website.

Safe Browsing

Tegenwoordig draaien veel van de grootste gevaren voor ondernemingen rond malware en phishing-aanvallen die vanaf gehackte websites worden geactiveerd.

De Google-functie Safe Browsing laat gebruikers waarschuwingen zien als ze naar websites proberen te gaan die malware of phishing-content bevatten of als ze op het punt staan verdachte bestanden te downloaden. Deze functie is gebaseerd op een Google-service die elke dag duizenden onveilige websites ontdekt en drie miljard apparaten beschermd.

De Safe Browsing-meldingen worden niet alleen in Chrome-browserschermen weergegeven, maar ook in Google-zoekopdrachten en Android-apps om mensen te waarschuwen voor gevaarlijke sites, en in Gmail-berichten om mensen te waarschuwen voor links naar schadelijke sites.

Scenario: Een phishing-aanval vermijden

Emily is de Chief Financial Officer bij een klein productiebedrijf. Ze ontvangt een e-mail van de CEO waarin ze wordt gevraagd meteen $ 20.000 over te maken naar een nieuwe leverancier in China om een voorraad te kopen van een bepaald onderdeel dat moeilijk verkrijgbaar is. Emily weet dat de CEO in China is om leveranciers te bezoeken, dus de e-mail lijkt betrouwbaar. Maar als ze op een link in de e-mail klikt om naar de website van de nieuwe leverancier te gaan, ontvangt ze een melding dat de site misleidend is. Ze wordt op het waarschuwingsscherm gevraagd om op de link 'Terug naar de veiligheid' te klikken. Dankzij Safe Browsing heeft Emily een phishing-aanval via een zakelijke gehackte e-mail (BEC, Business Email Compromise) voorkomen.

Beveiligingssleutels en verificatie in twee stappen

Verificatie in twee stappen (ook wel tweestapsverificatie genoemd) kan systemen en gegevens beschermen, ook als de inloggegevens van een gebruiker zijn gehackt. Gebruikers worden gevraagd iets op te geven wat ze weten, meestal een wachtwoord, met iets wat ze hebben, vaak een verificatiesleutel of code die naar hun smartphone wordt gestuurd.

Google biedt een van 's werelds snelste en makkelijkste manieren om effectieve verificatie in twee stappen te implementeren. Gebruikers hoeven alleen maar naar hun Google-account te gaan, 'Authenticatie in twee stappen' te selecteren en een optie te kiezen voor hun tweede verificatiemethode. Onder de opties vallen het versturen van een code per sms, het tikken op een melding op de telefoon of het gebruiken van een Titan-beveiligingssleutel die via een USB-poort wordt aangesloten op een Chromebook. Gebruikers kunnen ook apparaten markeren als vertrouwde apparaten en op die apparaten inloggen zonder de tweede verificatiemethode.

Apps: malwaredetectie, witte lijsten en zwarte lijsten

Op Chromebooks kunnen verschillende apps worden uitgevoerd, waaronder Android-apps, apps voor kantoorproductiviteit zoals Gmail, Google Documenten, Google Spreadsheets, Google Presentaties en Google Tekeningen, Chrome-extensies, Linux-apps, en PWA's (progressive web-apps: apps die snel laden en functionaliteit en responsiviteit bieden vergelijkbaar met lokaal geïnstalleerde apps).

Als ondernemingen gebruikers toegang geven tot door Google aangeleverde apps via de Chrome Web Store en tot Android-apps via de Google Play Store, hebben ze verschillende mogelijkheden om de beveiliging te versterken en het beheer te vereenvoudigen.

Malwaredetectie aan de serverzijde en externe verwijdering

Google Play Protect is de meest gebruikte mobiele beveiligingsservice ter wereld, die dagelijks twee miljard gebruikers beschermt tegen verschillende dreigingen. Experts in het beveiligingsteam voor Android voeren zeer strenge beveiligingstests uit voor alle Android-apps voordat deze mogen worden aangeboden in de Google Play Store. Apps en ontwikkelaars die in strijd zijn met het Google-beleid, worden niet geaccepteerd voor de Store.

Daarnaast worden apps in de Google Play Store doorlopend gescand en geverifieerd door Google Play Protect. Als er malware wordt gevonden in een app, wordt die app niet alleen onmiddellijk verwijderd uit de Google Play Store, maar wordt deze ook verwijderd van alle systemen waarop de app is gedownload.

App-beheer en -whitelisting via de Google Play Store

Gebruikers zorgen te vaak dat er kans is op gegevenslekken door apps te downloaden die kwetsbaarheden bevatten of zijn ontwikkeld door kwaadwillenden.

IT-beheerders hebben decennia lang geprobeerd de wildgroei aan downloads de kop in te drukken door gebruikers uitsluitend toe te staan goedgekeurde apps te downloaden of door eindpunten te vergrendelen zodat hierop alleen goedgekeurde apps kunnen

Scenario: Schaduw-IT een halt toeroepen

Carlos beheert een internationaal marketingteam op vier continenten. Hij wil een samenwerkingsprogramma implementeren om de communicatie en planning te verbeteren. Als hij online een artikel met een top 20 van online samenwerkingsprogramma's tegenkomt, houdt hij er geen rekening mee dat veel van deze apps niet beschikken over beveiligings- en beheerfuncties op ondernemingsniveau. Gelukkig controleert hij eerst de Managed Google Play Store van zijn bedrijf voordat hij te veel tijd verspilt aan het onderzoeken van deze twintig apps. Hij ontdekt dat de lijst twee goedgekeurde apps voor teamsamenwerking bevat, namelijk Slack en Google Hangouts. Beide bieden uitstekende functies en beveiliging. Ze worden ook nog eens ondersteund door de IT-afdeling van het bedrijf en via deze apps kan zijn team samenwerken met alle andere groepen die dezelfde apps gebruiken.

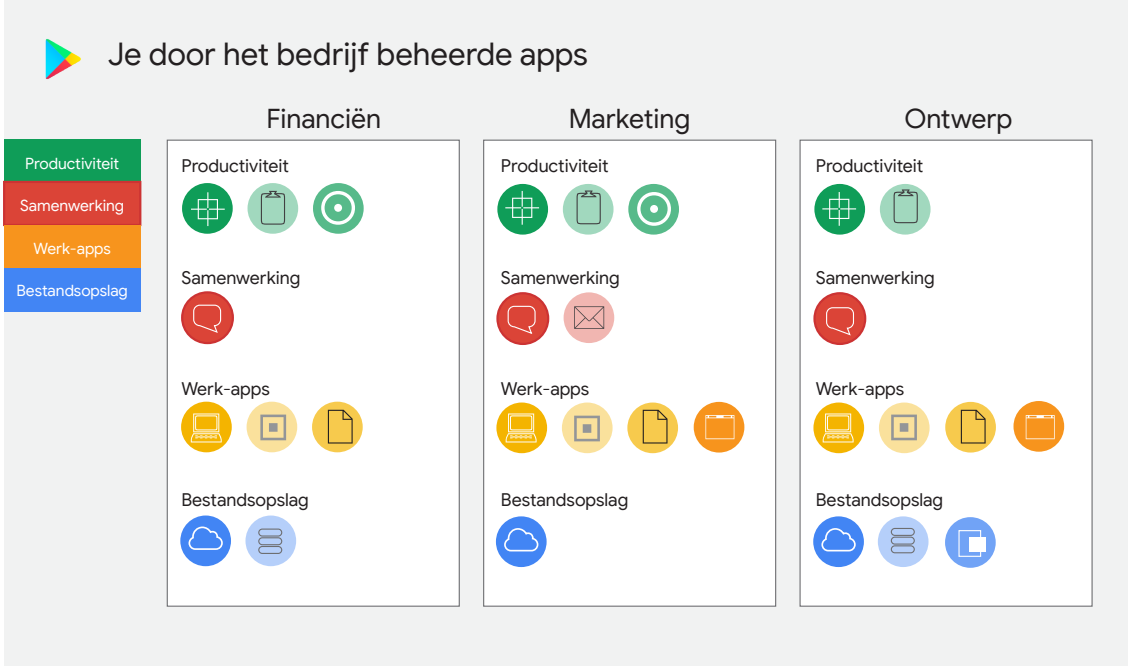
worden uitgevoerd. De eerste methode is niet effectief gebleken omdat de lijst met goedgekeurde apps vaak te klein is om aan iedereens behoeften op het gebied van zakelijke apps en persoonlijke apps en entertainment te voldoen. De tweede methode is ook niet geslaagd, omdat de technologie om traditionele eindpunten te vergrendelen moeilijk is te implementeren en meestal gepaard gaat met protest van gebruikers.

Webgebaseerde technologieën bieden beveiligings- en operations-teams nieuwe mogelijkheden om de stroom van niet-goedgekeurde apps in te perken zonder gebruikers teleur te stellen of te irriteren.

In de Google Play Store vind je duizenden apps voor zakelijke productiviteit, communicatie en samenwerking, het beheer van zakelijke processen, nieuws, entertainment en games. Deze apps zijn allemaal getest door het Android-beveiligingsteam om er zeker van te zijn dat deze geen kwetsbaarheden of ernstige beveiligingsrisico's bevatten.

Beheerders kunnen een Managed Google Play Store voor hun organisatie opzetten en een groot aantal apps beheren. Zo kunnen ze medewerkers van hun bedrijf een grote selectie productiviteits- en samenwerkingsapps aanbieden, maar de beschikbaarheid van game- en social media-apps beperken. (Afbeelding 5)

Als dit bij je bedrijf past, kun je met een Managed Google Play Store eenvoudig een witte lijst implementeren, zodat iedereen in de organisatie verplicht is dezelfde productiviteits- en samenwerkingsprogramma's te gebruiken en kan kiezen uit een redelijk aantal andere apps.



Afbeelding 5: Met een Managed Google Play Store heeft elke groep in de onderneming toegang tot een beheerde lijst met goedgekeurde apps.

Gecentraliseerd beheer met Chrome Enterprise

Met Chrome Enterprise kunnen beveiligings- en operations-teams hun beleid op Chromebooks en andere eindpunten met Chrome OS centraal beheren, net als beleidsregels voor Chrome-browsers op Windows-, Mac- en Linux-systemen. Chrome Enterprise Upgrade combineert mogelijkheden voor apparaatbeheer met 24/7 support van Google, en helpt ondernemingen op te schalen naar omgevingen met tienduizenden gebruikers en apparaten.

Overzicht van geselecteerde Chrome Enterprise-beleidsregels

Beheerders kunnen met Chrome Enterprise meer dan driehonderd beleidsregels voor beveiliging en configuratie instellen en afdwingen op eindpunten. Beheerde Chrome-apparaten bieden onder andere de volgende belangrijke beveiligingsgerelateerde mogelijkheden:

Registratie en uitschrijving van apparaten. Beheerders kunnen apparaten registeren of gebruikers toestaan om dit te doen, zodat deze apparaten kunnen worden beheerd en beschermd door de Chrome Enterprise-beleidsregels die door de organisatie van de gebruiker zijn opgesteld. Beheerders kunnen apparaten uitschrijven om de beleidsregels uit te schakelen en te voorkomen dat de apparaten toegang krijgen tot bedrijfsbronnen.

Apparaten op afstand uitschakelen. Als apparaten kwijtraken of worden gestolen, kunnen ze op afstand worden uitgeschakeld.

Inloggen beperken. Beheerders kunnen mensen toestaan anoniem in te loggen op een apparaat (gebruiken als gast) of een Google- of G Suite-account vereisen, of de toegang beperken tot één of enkele individuele gebruikers.

Kortstondige modus instellen (gebruikersgegevens wissen nadat iemand uitlogt). Beheerders kunnen apparaten instellen op de kortstondige modus, zodat gegevens en instellingen (inclusief browsergeschiedenis, extensies en bijbehorende gegevens, en webgegevens zoals cookies) worden gewist als een gebruiker uitlogt. Dankzij de kortstondige modus kunnen apparaten veiliger worden gedeeld voor kiosks en tijdelijke gebruikers.

Web-apps en browserextensies beperken of vereisen. Beheerders kunnen voorkomen dat gebruikers Chrome-web-apps en -browserextensies (kleine softwareprogramma's die de browserfunctionaliteit aanpassen) installeren, of voorkomen dat ze specifieke apps en extensies installeren. Ook kunnen ze gebruikers toestaan apps en extensies van uitsluitend bepaalde URL's te installeren. Ze kunnen ook de installatie van bepaalde apps en extensies afdwingen.

Apps blokkeren op basis van rechten. Veel Chrome-apps en -browserextensies vragen om toestemming voor het gebruik van bronnen op het apparaat waarop ze worden geïnstalleerd. Beheerders kunnen de installatie van apps en extensies die specifieke rechten gebruiken blokkeren. Zo kunnen ze voorkomen dat apps en extensies worden geïnstalleerd die toestemming willen om content op het scherm, in het venster of op het tabblad vast te leggen, de inhoud van het klembord te lezen, audio of video via de microfoon of camera van het apparaat vast te leggen, de geolocatie van de gebruiker te verkrijgen, metadata over het apparaatnetwerk op te vragen, of de energiebeheerfuncties van het apparaat te overschrijven. Via deze optie kan de IT-afdeling de risico's beperken, terwijl gebruikers de vrijheid krijgen om 'onschuldige' apps te installeren die geen bedreiging vormen voor de veiligheid.

Bluetooth en geolocatie uitschakelen. Bluetooth en locatietracking kunnen worden uitgeschakeld op apparaten.

Het gebruik van externe opslagapparaten beperken. Het gebruik van externe opslagapparaten, zoals USB-sticks, externe harde schijven en optische opslagapparaten, en geheugenkaarten, kan volledig worden geblokkeerd of worden toegestaan in de modus 'Alleen lezen'.

Toegang op afstand en single sign-on beheren. Beheerders kunnen parameters instellen voor toegang op afstand en SAML-gebaseerde single sign-on (SSO), zodat gebruikers met de juiste balans tussen beveiliging en gemak toegang krijgen tot het netwerk en web-apps.

Apparaten en gebruikers volgen. Er zijn voor elk apparaat rapporten beschikbaar met gegevens zoals het besturingssysteem en firmwareniveaus, statistieken over CPU- en RAM-gebruik, verbonden opslagapparaten, gebruiksstatistieken, diagnostische gegevens, op welke apparaten gebruikers onlangs hebben ingelogd, en wanneer die gebruikers actief waren.

Gedelegeerd en flexibel beheer

Beheertaken kunnen met Chrome Enterprise worden gedelegeerd om zo het werk te verdelen en de juiste mensen de verantwoordelijkheid voor het beheer van groepen en afdelingen te geven. Er kunnen rollen worden gemaakt om beheerders verschillende toestemmingen te geven om instellingen voor beheerde apparaten, gebruikers en apps te lezen of schrijven.

Chrome Enterprise biedt flexibiliteit in de manier waarop beleidsregels worden gemaakt en toegepast. Beheerders kunnen beleidsregels maken voor gebruikers en gebruikersgroepen, waarbij voor elke gebruiker dezelfde beleidsregels worden toegepast op alle apparaten. Daarnaast kunnen beheerders beleidsregels maken voor apparaten en die beleidsregels afdwingen op elk apparaat, ongeacht wie dit gebruikt.

Scenario: Nee, je mag niet meeluisteren tijdens deze meeting

Je CEO en CFO gaan naar het buitenland om te onderhandelen over een belangrijke deal. Het kan je bedrijf veel geld kosten als de strategiesessies worden afgeluisterd door de andere partij of de informatiedienst van het gastland. Gelukkig kun je tijdelijk bluetooth uitschakelen en de Chrome-web-apps en -browserextensies blokkeren die toegang kunnen krijgen tot de microfoon en camera op de Chromebooks van je CEO en CFO (je moet ze wellicht vragen de apparaten opnieuw op te starten om de wijzigingen te activeren).

Je beheerinfrastructuur gebruiken

Chrome Enterprise biedt een eigen console voor beheerders, maar is ook ontworpen voor aansluiting op je bestaande beheerinfrastructuur.

Integratie met Active Directory en Google Cloud Identity

De Chrome Enterprise-beheerdersconsole is geïntegreerd met Microsoft Active Directory en Google Cloud Identity. Zo kun je Chrome-apparaten registreren in Active Directory. Je kunt ook Chrome-beleidsregels implementeren voor gebruikers en apparaten op basis van gebruikersgroepen die in Active Directory zijn gedefinieerd.

Werken met toonaangevende EMM-oplossingen

Producten voor zakelijk mobiliteitsbeheer (EMM) ondersteunen ondernemingen bij de registratie, het beheer en de support van laptops, tablets, smartphones en andere mobiele apparaten. Als je onderneming in EMM-oplossingen zoals Cisco Meraki, Citrix XenMobile, IBM MaaS360, ManageEngine Mobile Device Manager Plus en VMWare Airwatch heeft geïnvesteerd, kun je deze producten blijven gebruiken om Chromebooks en andere eindpunten te beheren.

Samenvatting: baanbrekende beveiliging en operationele beheermogelijkheden

Cloudcomputing biedt ondernemingen de mogelijkheid om het model met traditionele eindpunten opnieuw te bekijken. Met een cloud-native insteek kan de beveiliging van eindpunten enorm worden verbeterd en het beheer van eindpunten aanzienlijk worden vereenvoudigd.

Chrome-apparaten gebruiken de ingebouwde voordelen van cloudcomputing, zoals minder middelen op eindpunten, een kleiner aanvalsbereik en eenvoudige, snelle updates. Bovendien maakt een cloud-native aanpak de weg vrij voor innovatieve mogelijkheden op het gebied van beveiliging en beheer. Denk hierbij aan beveiligingsfuncties die zijn ingebouwd in de hardware en firmware, effectief gebruik van sandboxing en versleuteling op gebruikersniveau, snelle en naadloze updates van besturingssystemen, Safe Browsing, eenvoudige verificatie in twee stappen, whitelistings van apps, en eenvoudig beheer van beveiligings- en operationele beleidsregels voor tienduizenden gebruikers en apparaten.

Het resultaat is een computingomgeving met de volgende kenmerken:

1. Ontworpen om veilig te zijn
2. Veel eenvoudiger te beheren dan traditionele eindpunten
3. Voorbereid op integratie in je bestaande infrastructuur

Lees meer informatie over Chrome Enterprise-beveiliging

(op https://cloud.google.com/chrome-enterprise/security/)