DELL Technologies

Het bestrijden van moderne cyberdreigingen

met geïntegreerde eindpuntbeveiliging en beheerbaarheid

CROWDSTRIKE intel ABSOLUTE®

DELL Technologies

Beknopte samenvatting

Opkomende aanvalsvectoren creëren nieuwe risico's. Blijf moderne eindpuntdreigingen een stap voor met meerdere verdedigingslagen die samenwerken. Ontdek hoe hardwaretelemetrie kan worden geïntegreerd met software om de beveiliging en beheerbaarheid van alle apparaten te verbeteren. Verstoor aanvallen sneller, ondersteun zero trust-principes en innoveer veilig met eenvoudig te beheren apparaten en oplossingen.

Inhoudsopgave

Het bedreigingslandschap

Casestudy

In 2023 ontdekte Eclypsium een fout in de firmware van moederborden die door een Taiwanese fabrikant werden verkocht. Onderzoekers ontdekte dat de code, die simpelweg bedoeld was om de firmware up-to-date te houden, onveilig was geïmplementeerd waardoor het mechanisme mogelijk kon worden gekaapt en gebruikt om malware te installeren.

Enkele redenen waarom deze ontdekking bijzonder alarmerend was

- Klanten werden blootgesteld via een kwetsbaarheid in de firmware.
- De kwetsbaarheid bevond zich in een deel van het apparaat waar het traditioneel moeilijk was om bedreigingen te detecteren.
- Het kon worden gebruikt om een aanval op afstand uit te voeren die de referentiecontrole omzeilt.

Uit de krantenkoppen...

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS MORE SIGN IN SUBSCRIBE

Millions of PC Motherboards Were Sold With a Firmware Backdoor

Verborgen code in honderden modellen moederborden downloadt programma's onzichtbaar en onveilig – een functie die volgens onderzoekers wacht op misbruik.

Het bedreigingslandschap

Implicaties

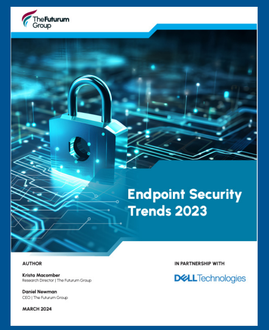
Dat is een belangrijke drijfveer die IT- en beveiligingsteams 's nachts wakker houdt:

Aanvallen op basis van een apparaat.

Deze geavanceerde, kwaadaardige aanvallen kunnen aanvallers in staat stellen geprivilegieerde toegang te krijgen. Bovendien kunnen veel van deze aanvallen op traditionele softwaregebaseerde beveiligingen, zoals antivirus, volledig onopgemerkt uitschakelen.

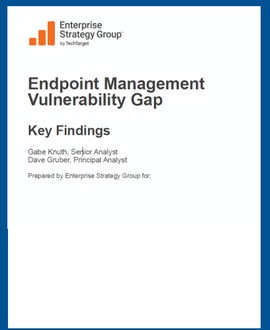
Volgens een recente wereldwijde enquête onder IT- en beveiligingsprofessionals[1] is een van de belangrijkste beoordelingscriteria als organisaties de aanschaf van nieuwe hardware:

Detectie van BIOS-firmwaregebeurtenissen automatiseren



69% van de organisaties meldde ten minste ÉÉN aanval op apparaatniveau in de afgelopen twaalf maanden. Dat is 1,5 keer meer dan uit onderzoek van 2020![2]

Configuraties met hoog risico



Meer dan 75% van de organisaties meldt dat ze ten minste één cyberaanval hebben meegemaakt die werd veroorzaakt door een onbekend, onbeheerd of slecht beheerd eindpuntapparaat.[3]

Uitdagingen

Wat maakt van een apparaat een gemakkelijk doelwit?

Zichtbaarheid

Deze aanvallen zijn moeilijk te zien en worden uitgevoerd op een deel van het apparaat dat traditioneel slecht zichtbaar is en observability mist.

Bruikbaarheid

Vaak hebben organisaties tientallen tools die in silo's werken, dus als een aanval wordt gedetecteerd, is een snelle respons en herstel een grote uitdaging en kost dit veel handmatig werk.

Oplossing

Zichtbaarheid

Bruikbaarheid

Als een van de grootste technologieleveranciers ter wereld is Dell veel bezig met beveiliging. Daarom zijn **onze zakelijke pc's zo ontworpen dat zichtbaarheid en bruikbaarheid vanaf het begin prioriteit krijgen**. Hiermee komt de macht in handen van IT- en beveiligingsactiviteiten.

Onze zakelijke pc's worden geleverd met **unieke geïntegreerde beveiligingsfuncties** zoals BIOS-verificatie[4] en Indicators of Attack[4] om bedreigingen te helpen detecteren voordat ze schade veroorzaken. We maken deze detecties zichtbaar met **alleen voor Dell beschikbare apparaattelemetrie**[4]. Wanneer een zakelijke Dell pc op Intel vPro® een potentiële bedreiging op apparaatniveau detecteert, kan het-deze informatie naar het besturingssysteem sturen voor sneller, effectiever onderzoek en respons

Leiders in de branche

Dell biedt de veiligste zakelijke pc's ter wereld[4]

Ontdek wat er nodig is om het vertrouwen in apparaten te behouden ondanks moderne bedreigingen.

Lees het onderzoek van Principled Technologies over apparaatbeveiliging →


Principled Technologies®

A Principled Technologies report: In-depth research. Real-world value.

A comparison of security features in Dell, HP, and Lenovo PC systems

Approach

Dell™ commissioned Principled Technologies to investigate 10 security features in the PC security and system management space:

- Support for monitoring solutions
- BIOS security and protection features
  - Platform integrity validation
  - Device integrity validation via off-site measurements
  - Component integrity validation for Intel® Management Engine (ME) via off-site measurements
  - BIOS image capture for analysis
  - Built-in hardware cache for monitoring BIOS changes with security information and event management (SIEM) integration
- Microsoft Intune management
  - BIOS setting management integrations for Intune
  - BIOS access management security enhancements for Intune
- Remote management
  - Intel vPro® remote management
  - PC management using cellular data

These features rely on manufacturer-enabled communication between the hardware and the operating system (OS). We reviewed publicly available marketing claims and feature documentation for three Windows original equipment manufacturers (OEMs): Dell, HP, and Lenovo®. Many of the Dell features relate to the Dell Trusted Device application.

In this report, we indicate that an OEM supports a given feature if its published materials mention that feature is present. We have done our best to determine which features each OEM supports, using a variety of search terms and brand-specific phrasing to locate features. Some of the features we mark as being absent might be present but not covered in the OEM marketing or documentation. It is also possible that, despite our best efforts, we missed or overlooked some features that the OEM marketing or documentation does address.

We completed no hands-on validation of any of the features we discuss below. Therefore, we cannot verify the functionality, scope, or reliability of these features. We do not cover system requirements or any licensing, services, or additional hardware or software that might be necessary to use the features.

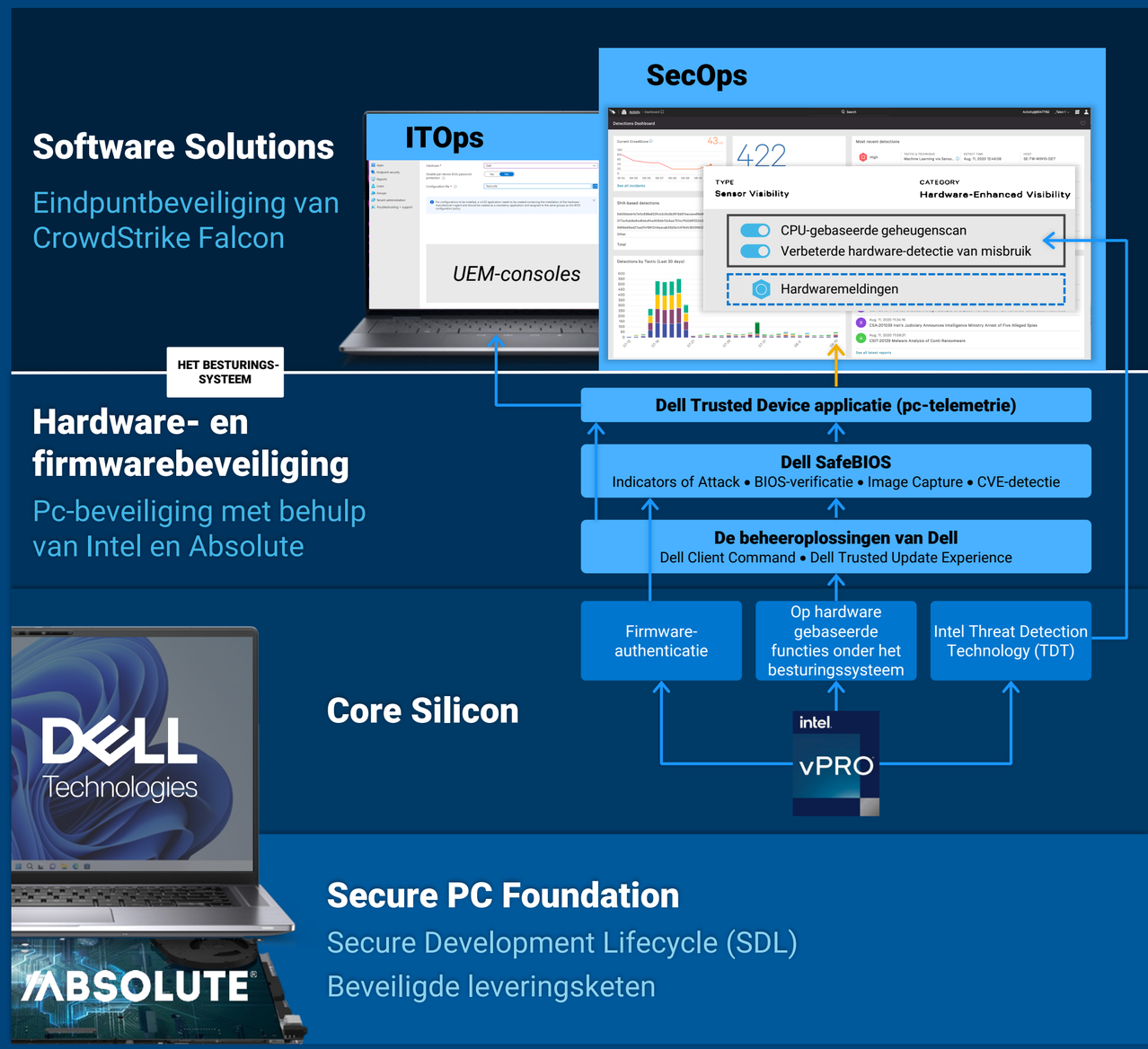
Oplossing

Bestrijd bedreigingen door samen te werken op het gebied van beveiliging en beheerbaarheid

Dell en ons verbonden ecosysteem voor partners werken eraan om zichtbaarheid en bruikbaarheid te bieden op de werkruimte. Waaronder:

- Beveiliging van de leveringsketen en geïntegreerd hardware- en firmwareverdediging van Dell
- Core Silicon en 'onder het besturingssysteem'-beveiliging van Intel
- Beheerbaarheid via Dell en Unified Endpoint Management consoles
- Geavanceerde bescherming tegen bedreigingen voor eindpunten, netwerken en de cloud van partners zoals CrowdStrike en Absolute

Het ecosysteem maakt gebruik van pc-telemetrie als connector en helpt de kloof tussen IT- en beveiligingsoplossingen te dichten waar bedreigingen doorheen kunnen glippen. Deze aanpak kan niet alleen helpen aanvallen te voorkomen, maar kan ze ook detecteren, erop reageren, ervan herstellen en ze herstellen.



Gebruiksscenario's en tegenmaatregelen

Om aan te tonen hoe geïntegreerde beveiliging en beheerbaarheid werken om de cybertolerantie te verbeteren, kijken we naar twee gebruiksscenario's, waaronder aanvalsscenario's en tegenmaatregelen.

Ten eerste een aanval op de BIOS-firmware. Hier bekijken we hoe de cyber kill chain[5] van een BIOS-downgrade-aanval kan verlopen.

BIOS-downgradeaanval

Eerste toegang: replicatie via verwisselbare media + phishing

Stap 1a

Kwaadwillende insider maakt misbruik van een bestaande BIOS-kwetsbaarheid om op afstand inloggegevens voor het besturingssysteem te stelen. Hackt apparaat en downgradet BIOS.

Stap 1b

Aanvaller initieert een spear-phishing-aanval en steelt een sessietoken wanneer een beheerder zich per ongeluk verifieert op een schadelijke site.

Stap 2

Toegang tot referenties

De aanvaller bereikt persistentie door extra beheerdersaccounts aan te maken en zich vervolgens door het netwerk te verplaatsen.

Stap 3

Laterale verplaatsing

De aanvaller brengt het netwerk in kaart en lokaliseert systeembeheerservers.

Stap 4

Exfiltratie

De aanvaller exfiltreert data via een webservice.

Gebruiksscenario's en tegenmaatregelen

BIOS-downgrade-tegenmaatregelen

Aanvallers dringen sneller dan ooit door in het netwerk. Volgens CrowdStrike's Global Threat Report is de gemiddelde eCrime-uitbraaktijd (de tijd die nodig is om in een systeem in te breken en lateraal te handelen) in 2023 zelfs gedaald van 84 minuten in 2022 tot 62 minuten. De snelst waargenomen uitbraaktijd was slechts 2 minuten en 7 seconden![6]

Hier leest u hoe Dell en onze partners Intel® en CrowdStrike helpen om een BIOS-downgradeaanval in de kill chain op te vangen en af te weren met door hardware ondersteunde beveiliging.

Voorkomen | **Detecteren en reageren** | **Terughalen en herstellen**

Beveiligde leveringsketen: strenge controles beschermen pc's vanaf het ontwerp en de ontwikkeling, tot inkoop en assemblage tot en met levering. Dell en Intel zetten zich voortdurend in om te zorgen dat producten zo worden ontwikkeld dat ze het risico op kwetsbaarheden en sabotage van producten gedurende de hele levenscyclus beperken.




Security	Integrity	Quality	Resilience
• Secure development lifecycle • Software partners securely onboarded • Information exchange with partners securely • Quality Process Audit • Separation of Duties • Least Privilege Access	• Supplier accountability • Supplier due diligence • Piece-Part Identification • SAFECode • US Exec Order 14028 SBOM -SPDX	• Counterfeit prevention & detection • Enhanced manufacturing security program • Enterprise code signing • Secured Component Verification • Freight Tracking	• Silicon Root of Trust • Platform Firmware Resiliency Guidelines • BIOS Protection Guidelines • Built-in Supplier Redundancy

Gebruiksscenario's en tegenmaatregelen

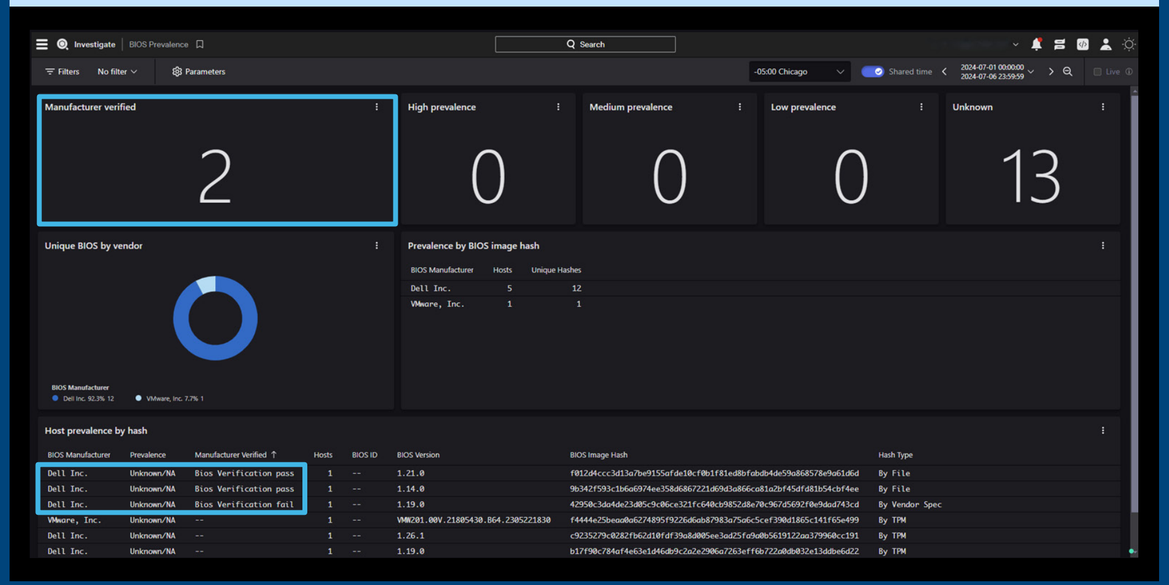
BIOS-downgrade-tegenmaatregelen

Aanvallers dringen sneller dan ooit door in het netwerk. Volgens CrowdStrike's Global Threat Report is de gemiddelde eCrime-uitbraaktijd (de tijd die nodig is om in een systeem in te breken en lateraal te handelen) in 2023 zelfs gedaald van 84 minuten in 2022 tot 62 minuten. De snelst waargenomen uitbraaktijd was slechts 2 minuten en 7 seconden![6]

Hier leest u hoe Dell en onze partners Intel® en CrowdStrike helpen om een BIOS-downgradeaanval in de kill chain op te vangen en af te weren met door hardware ondersteunde beveiliging.

Voorkomen | **Detecteren en reageren** | **Terughalen en herstellen**

Een BIOS-attestatie detecteren op het CrowdStrike Falcon platform: wanneer Dell apparaattelemetrie is ingeschakeld, kan een beheerder meldingen van ingebouwde beveiligingsfuncties bekijken, zoals BIOS-verificatie of op afstand in CrowdStrike Falcon, waardoor verdachte activiteiten sneller kunnen worden gedetecteerd voordat er blijvende schade optreedt.



Gebruiksscenario's en tegenmaatregelen

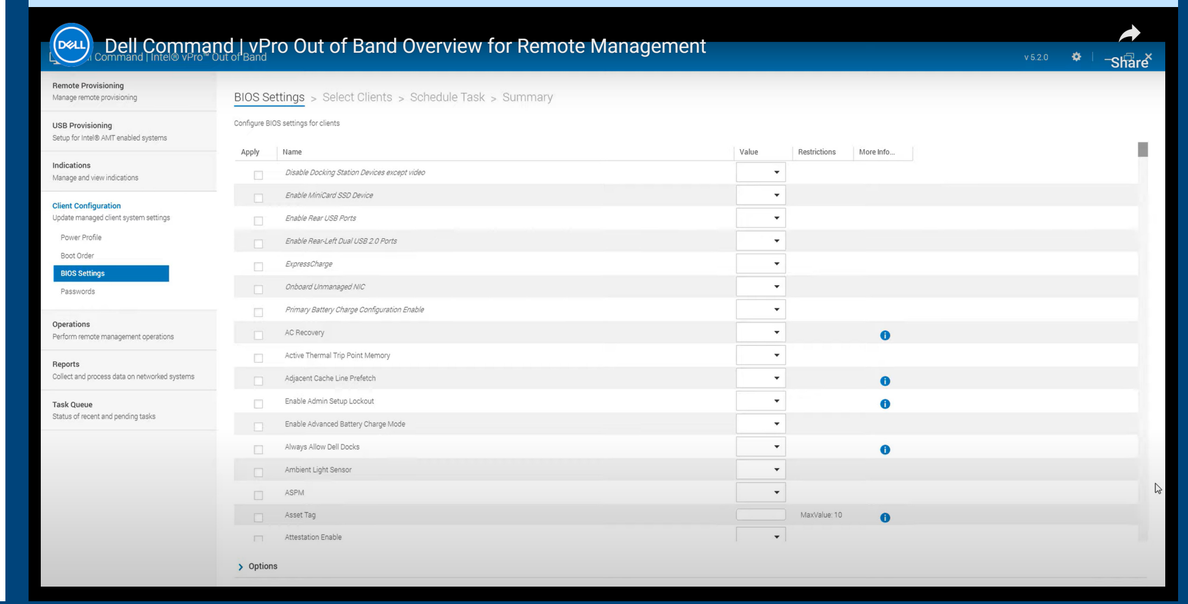
BIOS-downgrade-tegenmaatregelen

Aanvallers dringen sneller dan ooit door in het netwerk. Volgens CrowdStrike's Global Threat Report is de gemiddelde eCrime-uitbraaktijd (de tijd die nodig is om in een systeem in te breken en lateraal te handelen) in 2023 zelfs gedaald van 84 minuten in 2022 tot 62 minuten. De snelst waargenomen uitbraaktijd was slechts 2 minuten en 7 seconden![6]

Hier leest u hoe Dell en onze partners Intel® en CrowdStrike helpen om een BIOS-downgradeaanval in de kill chain op te vangen en af te weren met door hardware ondersteunde beveiliging.

Voorkomen | **Detecteren en reageren** | **Terughalen en herstellen**

BIOS-downgrade herstellen: help toekomstige bedreigingen voor out-of-band systemen te voorkomen. Dell Client Command Suite met Intel vPro maakt herstel op afstand mogelijk.



Gebruiksscenario's en tegenmaatregelen

In dit tweede gebruiksscenario is dit hoe de stap in de kill chain van een aanval op de software leveringsketen zou kunnen verlopen.

Aanval op de leveringsketen van software

Stap 1

Initiële toegang: aantasting van de leveringsketen

De aanvaller injecteert schadelijke code in een hulpprogramma (BIOS/firmware).

Stap 2

Persistentie

Klanten downloaden de schadelijke code wanneer ze hun apparaten updaten.

De aanvaller installeert malware.

Stap 3

Laterale verplaatsing

De aanvaller spooft een gebruiker die zojuist is aangevallen en stuurt een schadelijke link naar een andere gebruiker. Die gebruiker klikt op de link en de aanvaller steelt de inloggegevens.

Stap 4

Exfiltratie

Aanvaller exfiltreert data.

Gebruiksscenario's en tegenmaatregelen

De leveringsketen is een belangrijk doelwit geworden voor aanvallers. Hoewel deze aanvallen minder vaak voorkomen, kunnen de resultaten van een succesvolle aanval verwoestend zijn, omdat organisaties nog steeds leren hoe ze hun verdediging hiertegen kunnen versterken.

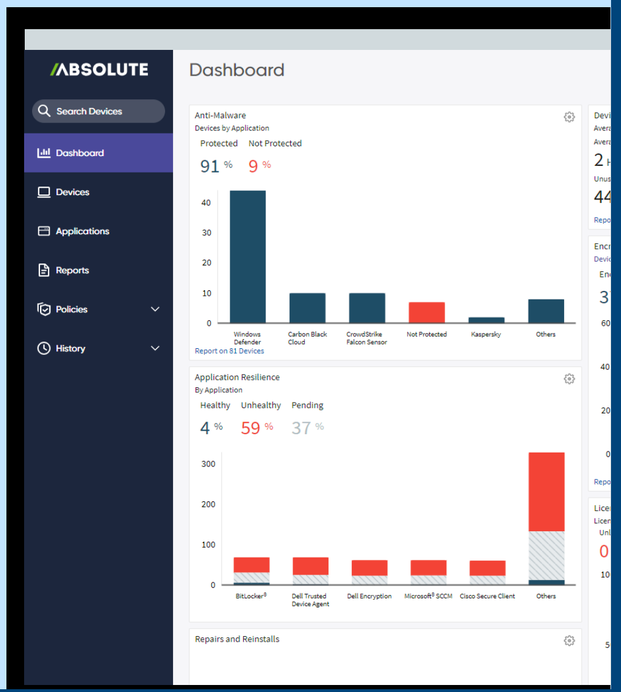
Een kernverantwoordelijkheid van alle technologieleveranciers is ervoor te zorgen dat wat ze verkopen niet onbedoeld een risico vormt voor gebruikers via van kwetsbaarheden.

Om aanvallen te voorkomen en tolerantie te bieden aan de beveiligingsstack, houden Dell en Intel® zich aan het strikte proces en de protocollen van onze Secure Development Cycle[7]. Extra zekerheid in de leveringsketen, zoals Dell Secured Component Verification[8], plus beveiliging op firmwareniveau van Absolute (rechts afgebeeld), geeft klanten vertrouwen gedurende de hele levensduur van de pc.

Voorkomen | **Detecteren en reageren** | **Terughalen en herstellen**

Zichtbaarheid van eindpunten vanuit de fabriek: bekijk alle apparaten in en buiten het netwerk met Absolute geïntegreerd in door Dell beheerde fabrieken. Met Absolute Custom Factory Install (CFI) wordt een stap in de implementatie verwijderd en worden apparaten beschermd die mogelijk naar magazijnen en meerdere locaties van eindgebruikers worden verzonden. Beperk risico's met een volledig overzicht van elk apparaat vanuit een cloudgebaseerd dashboard.

- Vind en onderhoud eenvoudig al uw IT-assets en applicaties
- Breng al uw apparaten in kaart
- Optimaliseer het gebruik van assets en monitor de beveiliging
- Support voor meerdere platforms (Windows, Mac en Chrome)
- Geïntegreerd in de BIOS van 27 toonaangevende pc-OEM's



Gebruiksscenario's en tegenmaatregelen

De leveringsketen is een belangrijk doelwit geworden voor aanvallers. Hoewel deze aanvallen minder vaak voorkomen, kunnen de resultaten van een succesvolle aanval verwoestend zijn, omdat organisaties nog steeds leren hoe ze hun verdediging hiertegen kunnen versterken.

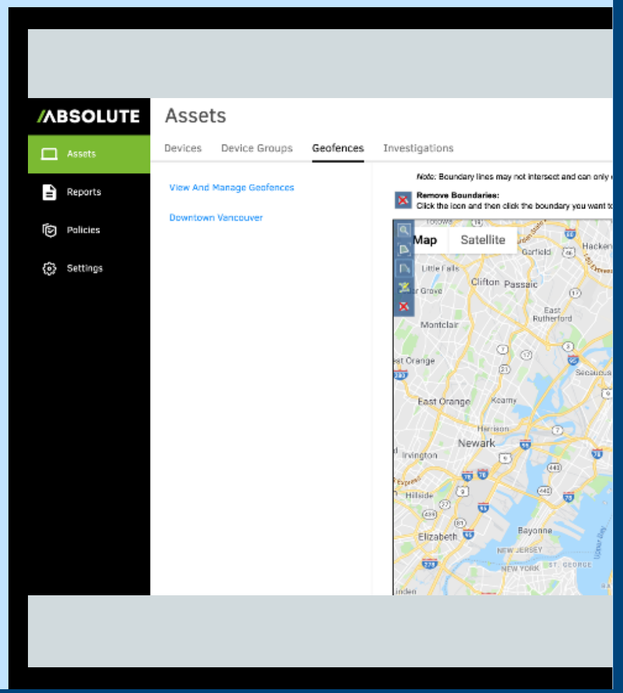
Een kernverantwoordelijkheid van alle technologieleveranciers is ervoor te zorgen dat wat ze verkopen niet onbedoeld een risico vormt voor gebruikers via van kwetsbaarheden.

Om aanvallen te voorkomen en tolerantie te bieden aan de beveiligingsstack, houden Dell en Intel® zich aan het strikte proces en de protocollen van onze Secure Development Cycle[7]. Extra zekerheid in de leveringsketen, zoals Dell Secured Component Verification[8], plus beveiliging op firmwareniveau van Absolute (rechts afgebeeld), geeft klanten vertrouwen gedurende de hele levensduur van de pc.

Voorkomen | **Detecteren en reageren** | **Terughalen en herstellen**

Eindpunten beheren: met Absolute kunt u detecteren wanneer eindpunten zijn aangetast (bijvoorbeeld als een kritieke app is beschadigd door malware of als een pc zoekraakt tijdens transport). Onderneem actie op afstand om bedreigingen onmiddellijk te herstellen door apparaten onbruikbaar te maken en/of de data die ze bevatten te verwijderen.

- Bescherm apparaten wanneer ze zich buiten het afgebakende terrein bevinden
- Bescherm en wis kritieke data eenvoudig op afstand
- Wis data aan het eind van de levenscyclus volgens nalevingscertificaten
- Vergrendel apparaten on-demand om kritieke assets te beschermen
- Bied firmwarebescherming op afstand



Gebruiksscenario's en tegenmaatregelen

De leveringsketen is een belangrijk doelwit geworden voor aanvallers. Hoewel deze aanvallen minder vaak voorkomen, kunnen de resultaten van een succesvolle aanval verwoestend zijn, omdat organisaties nog steeds leren hoe ze hun verdediging hiertegen kunnen versterken.

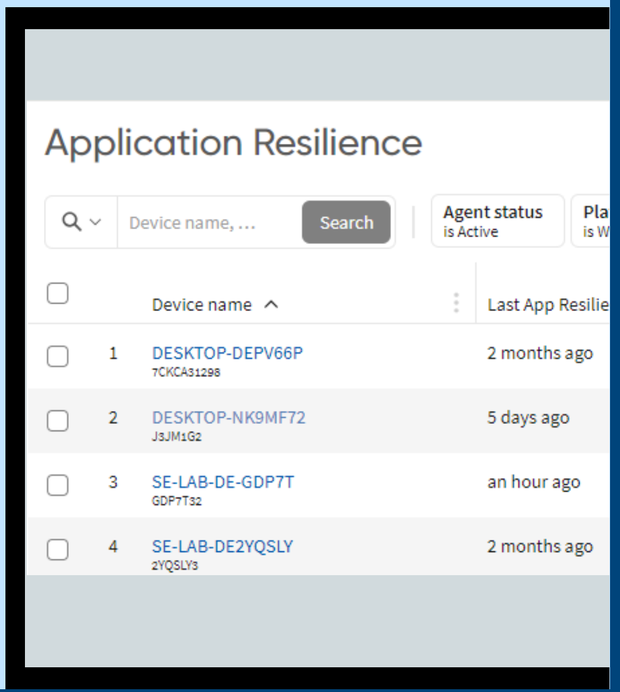
Een kernverantwoordelijkheid van alle technologieleveranciers is ervoor te zorgen dat wat ze verkopen niet onbedoeld een risico vormt voor gebruikers via van kwetsbaarheden.

Om aanvallen te voorkomen en tolerantie te bieden aan de beveiligingsstack, houden Dell en Intel® zich aan het strikte proces en de protocollen van onze Secure Development Cycle[7]. Extra zekerheid in de leveringsketen, zoals Dell Secured Component Verification[8], plus beveiliging op firmwareniveau van Absolute (rechts afgebeeld), geeft klanten vertrouwen gedurende de hele levensduur van de pc.

Voorkomen | **Detecteren en reageren** | **Terughalen en herstellen**

Zelfherstel: met Absolute Persistence geïntegreerd in de Dell BIOS-firmware, keert u terug naar de oorspronkelijke staat wanneer sabotage wordt gedetecteerd. Absolute kan elk gecompromitteerd eindpunt of ondersteunde applicatie in de Application Resilience-catalogus (80+ applicaties) zelf herstellen of aanhouden, inclusief een bibliotheek met andere tegenmaatregelen, zoals Dell Trusted Device-applicatie, Zscaler.

- Vind en verwijder met gemak gevoelige data op eindpunten
- Onderneem stappen voor herstel van apparaten met behulp van een bibliotheek met aangepaste scripts
- Monitor en voer zelfherstel uit van applicaties
- Grote en groeiende Application Resilience-catalogus met eindpuntcontroles van derden
- Zoek en vind zoekgeraakte of gestolen apparaten met Absolute Investigations Team



Belangrijke voordelen

Een groep apparaten is slechts zo veilig als de afzonderlijke pc's.

Om moderne bedreigingen het hoofd te bieden, moeten apparaten veilig zijn gebouwd en voorzien zijn van geïntegreerde beveiliging.

Aanvallen opvangen, afweren en ervan herstellen door eindpuntbeveiliging en beheerbaarheid samen te laten werken.

Beveiliging is een teamsport. Maak gebruik van zowel hardware als software voor de beste verdediging.

Meer informatie:

Neem contact met ons op: Global.Security.Sales@Dell.com.

Ga dan naar: Dell.com/Endpoint-Security

Volg ons: LinkedIn @DellTechnologies | X @DellTech

Zet de volgende stap

Beveiliging is een groot onderwerp voor organisaties groot en klein. **Schakel een ervaren beveiligings- en technologiepartner in om de beveiliging van eindpunten te moderniseren**.

Dell Trusted Workspace helpt om eindpunten te beveiligen voor een moderne IT-omgeving die klaar is voor Zero Trust. Verminder de aanvalsmogelijkheden met een uitgebreid portfolio hardware- en softwarebeschermingen, uitsluitend van Dell. Onze zeer gecoördineerde verdedigingsgebaseerde aanpak pakt bedreigingen aan door geïntegreerde bescherming te combineren met doorlopende waakzaamheid. Eindgebruikers blijven productief en IT kan vertrouwen op beveiligingsoplossingen die zijn gemaakt voor de moderne cloudgebaseerde wereld.

1. Bron: Enterprise Strategy Group, een afdeling van TechTarget, Custom Research Survey in opdracht van Dell Technologies, *Assessing Organizations' Security Journeys*, november 2023.
2. Bron: Futurum Group, Endpoint Security Trends, 2023.
3. Bron: Enterprise Strategy Group, een afdeling van TechTarget, onderzoeksrapport, *Managing the Endpoint Vulnerability Gap: The Convergence of IT and Security to Reduce Exposure*, mei 2023.
4. Gebaseerd op een interne analyse van Dell, oktober 2024. Van toepassing op pc's met Intel processors. Niet alle functies zijn beschikbaar voor alle pc's. Extra aankoop vereist voor sommige functies. Gevalideerd door Principled Technologies. A comparison of security features, april 2024.
5. Bron: What is the Cyber Kill Chain? Introductiegids - CrowdStrike.
6. Bron: CrowdStrike 2024 Global Threat Report.
7. Bron: Three Considerations for Establishing Device Trust | Dell USA.
8. Bron: How to Keep Device Trust Close to the Vest | Dell USA.