DELL Technologies

Så här bekämpar du moderna cyberhot

med integrerad slutpunktssäkerhet och hanterbarhet

CROWDSTRIKE intel ABSOLUTE®

DELL Technologies

Sammanfattning

Nya attackvektorer skapar nya risker. Ligg steget före moderna slutpunktshot med flera försvarslager som arbetar tillsammans. Läs om hur hårdvarutelemetri kan integreras med mjukvara för att förbättra säkerhet och hanterbarhet i hela datorflottan. Stoppa attacker snabbare, stöd nollförtroendeprinciper och förnya på ett säkert sätt med lätthanterliga enheter och lösningar.

Innehållsförteckning

Hotbilden

Fallstudie

År 2023 upptäckte Eclypsium ett fel i den fasta mjukvaran för moderkort som säljs av en taiwanesisk tillverkare. Koden var helt enkelt avsedd att hålla den fasta mjukvaran uppdaterad men forskare upptäckte att koden implementerades på ett osäkert sätt. Det innebar att mekanismen potentiellt kunde kapas och användas för att installera skadliga program.

Det finns flera skäl till att denna upptäckt är så oroväckande

- Kunder exponerades via en sårbarhet i den fasta mjukvaran.
- Sårbarheten fanns i ett område på enheten där det traditionellt har varit svårt att upptäcka hot.
- Den här sårbarheten kan användas för att starta en fjärrattack som kringgår kontroller av autentiseringsuppgifter.

Hämtat från rubrikerna …

Hotbilden

Implikationer

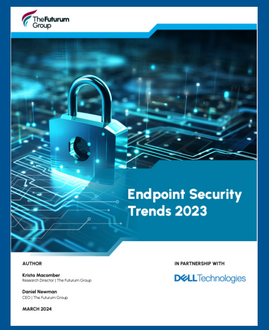
Det är en viktig drivkraft som håller IT- och säkerhetsteamen vakna om natten:

Enhetsbaserade attacker.

Dessa sofistikerade och skadliga attacker kan göra det möjligt för angripare att få privilegierad åtkomst. Dessutom kan många av dessa stänga av traditionella skydd som endast gäller mjukvara, exempelvis antivirus, helt utan att upptäckas.

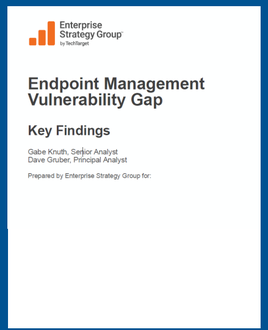
De främsta utvärderingskriterierna enligt en nyligen genomförd global undersökning bland IT- och säkerhetsproffs[1] när företag köper in ny hårdvara är följande

Automatisera identifiering av händelser i den fasta mjukvaran för BIOS



69 procent av organisationerna rapporterade minst EN attack på enhetsnivå under de senaste tolv månaderna. Det är en ökning med 1,5 gånger fler än i 2020 års studie![2]

Högriskkonfigurationer



Mer än 75 % av organisationerna rapporterar att de har upplevt minst en cyberattack orsakad av en okänd, ohanterad eller dåligt hanterad slutpunktsenhet.[3]

Utmaningar

Hur blir en enhet ett enkelt mål?

Synlighet

Dessa attacker är svåra att upptäcka – de utförs på en del av enheten som traditionellt saknar insyn och observerbarhet.

Handlingskraft

Företag har oftast mängder av verktyg på plats som arbetar i silor – så om en attack upptäcks blir snabb respons och hjälpande åtgärder en stor utmaning och innebär mycket manuellt arbete.

Lösning

Synlighet | **Handlingskraft**

Dell är en av världens största teknikleverantörer och vi fokuserar mycket på säkerhet. Det är därför **vi bygger våra kommersiella datorer så att de prioriterar synlighet och handlingskraft redan från början**. Detta gör att makten ligger i händerna på IT- och säkerhetsåtgärder.

Våra kommersiella datorer levereras med **unika inbyggda säkerhetsfunktioner** som BIOS Verification[4] och Indicators of Attack[4] för att upptäcka hot innan de hinner göra skada. Vi gör dessa identifieringar synliga med **enhetstelemetri som endast finns från Dell**[4]. När en kommersiell Dell-dator på Intel vPro® upptäcker ett potentiellt hot på enhetsnivå kan den skicka det till operativsystemet för snabbare och effektivare undersökning och respons.

Ledande i branschen

Dell erbjuder världens säkraste kommersiella datorer[4]

Läs om vad som krävs för att upprätthålla enhetsförtroendet mot moderna hot.

Läs Principled Technologies-studien om enhetssäkerhet →


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.

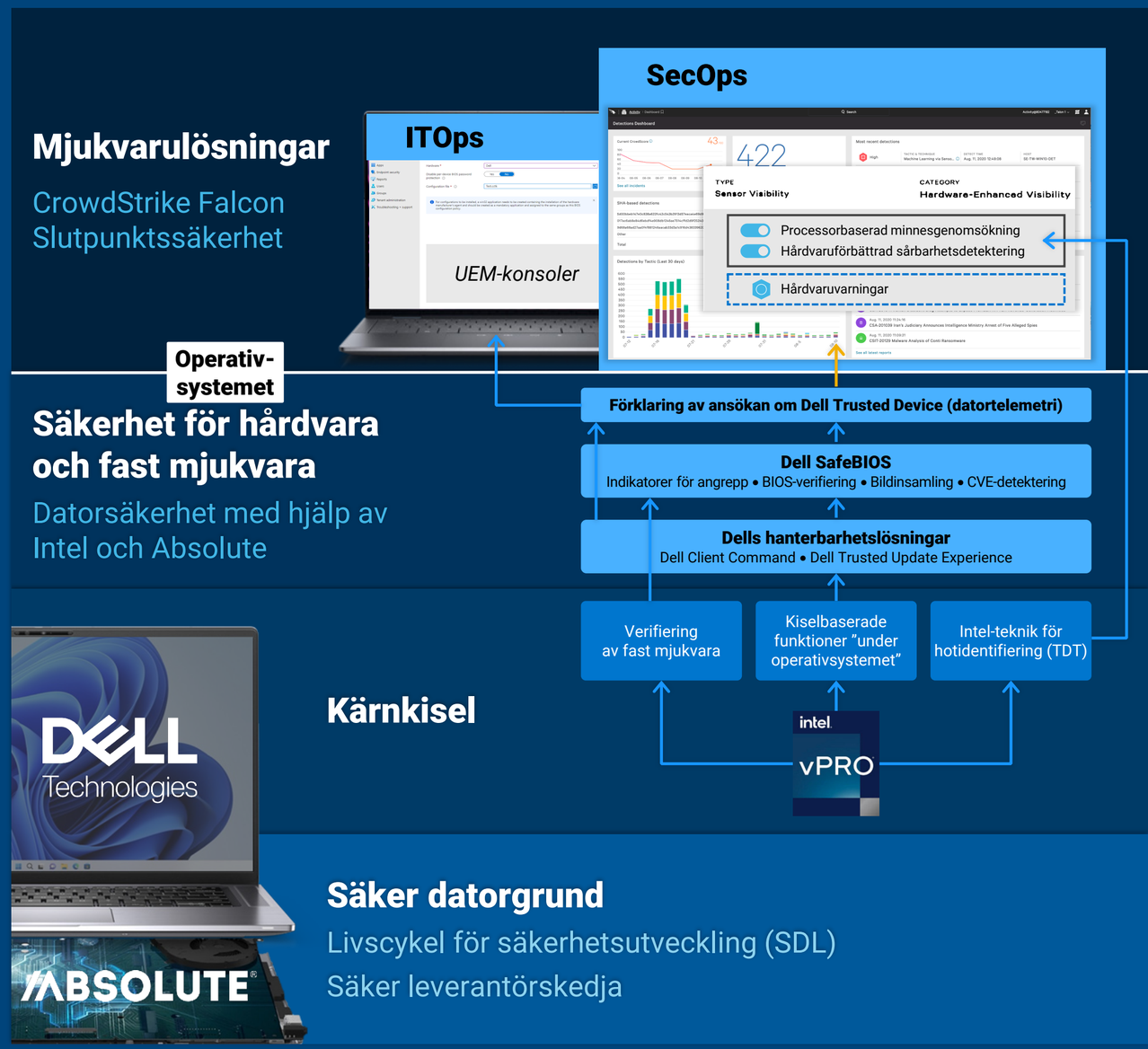
Lösning

Bekämpa hot genom att låta säkerhet och hanterbarhet samarbeta

Dell och vårt ekosystem med anslutna partner arbetar tillsammans för att skapa synlighet och handlingskraft på arbetsplatsen. Detta omfattar följande:

- Säkerhet i leverantörskedjan och inbyggt försvar för hårdvara och fast mjukvara från Dell
- Kärnkisel och ”under operativsystemet”-skydd från Intel
- Hanterbarhet via Dell och enhetliga hanteringskonsoler för slutpunkter
- Avancerat hotskydd som täcker slutpunkter, nätverk och molnet från partner, inklusive CrowdStrike och Absolute

Ekosystemet använder datortelemetri som kontakt. Det hjälper till att fylla igen luckan mellan IT- och säkerhetslösningar där hot kan slinka igenom. Den här metoden kan inte bara hjälpa till att förhindra attacker, utan den kan också identifiera, svara på, återställa och åtgärda dem.



Användningsfall och motåtgärder

Vi tittar nu närmare på två användningsfall för att demonstrera hur integrerad säkerhet och hanterbarhet fungerar för att förbättra cyberelasticiteten, inklusive attackscenarier och motåtgärder.

Först en attack på den fasta BIOS-mjukvaran. Här ser vi hur de olika cyberattacksfaserna[5] i en BIOS-nedgraderingsattack kan utspela sig.

BIOS-nedgraderingsattack

Inledande åtkomst: replikering genom löstagbara medier + nätfiske

Steg 1a

Ett insiderhot utnyttjar en befintlig BIOS-sårbarhet för att stjäla OS-inloggningsuppgifter på distans.

Hackar enheten och nedgraderar BIOS.

Steg 1b

Angriparen påbörjar en spear phishing-attack och stjäler en sessionstoken när en administratör av misstag autentiserar sig på en skadlig webbplats.

Steg 2

Åtkomst till inloggningsuppgifter

Angriparen uppnår beständighet genom att skapa ytterligare administratörskonton och fortsätter att röra sig runt i nätverket.

Steg 3

Lateral förflyttning

Angriparen mappar nätverket och lokaliserar systemhanteringsservrar.

Steg 4

Exfiltrering

Angriparen exfiltrerar data via en webbtjänst.

Användningsfall och motåtgärder

BIOS-nedgraderingsåtgärder

Angripare bryter sig in i nätverket snabbare än någonsin tidigare. Faktum är att den genomsnittliga eCrime-utbrottstiden (den tid det tar att bryta sig in i ett system och röra sig i sidled) minskade från 84 minuter år 2022 till 62 minuter under 2023 enligt CrowdStrike Global Threat Report. Den snabbaste observerade utbrottstiden var bara 2 minuter och 7 sekunder![6]

Så här hjälper Dell och våra partners Intel® och CrowdStike till att fånga upp och avvärja en BIOS-nedgraderingsattack längs alla attackfaser med hårdvarubaserad säkerhet.

Förebygga | **Upptäcka och svara** | **Återställa och åtgärda**

Säker leverantörskedja: rigorösa kontroller skyddar datorer från design och utveckling, genom inköp och montering, vidare till leverans. Dell och Intel arbetar oavbrutet för att säkerställa att produkterna utvecklas för att minska risken för produktsårbarheter och manipulering under hela livscykeln.




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

Användningsfall och motåtgärder

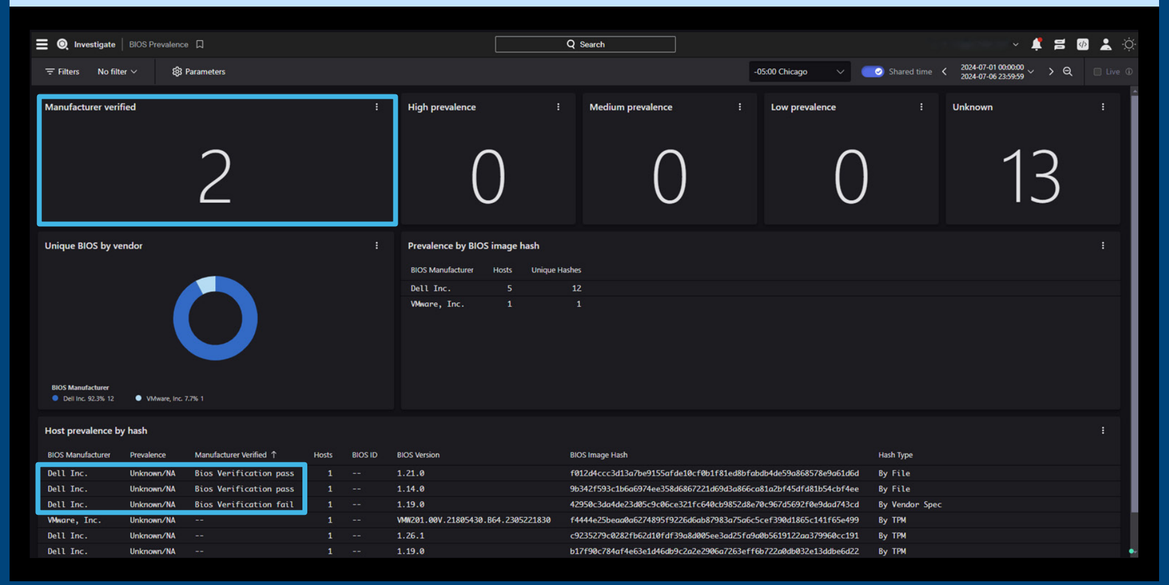
BIOS-nedgraderingsåtgärder

Angripare bryter sig in i nätverket snabbare än någonsin tidigare. Faktum är att den genomsnittliga eCrime-utbrottstiden (den tid det tar att bryta sig in i ett system och röra sig i sidled) minskade från 84 minuter år 2022 till 62 minuter under 2023 enligt CrowdStrike Global Threat Report. Den snabbaste observerade utbrottstiden var bara 2 minuter och 7 sekunder![6]

Så här hjälper Dell och våra partners Intel® och CrowdStike till att fånga upp och avvärja en BIOS-nedgraderingsattack längs alla attackfaser med hårdvarubaserad säkerhet.

Förebygga | **Upptäcka och svara** | **Återställa och åtgärda**

Upptäck BIOS-attestering i CrowdStrike Falcon-plattformen: Med Dells enhetstelemetri är aktiverad kan en administratör visa meddelanden från inbyggda säkerhetsfunktioner som BIOS-verifiering på distans i CrowdStrike Falcon. Det gör det lättare att upptäcka misstänkt aktivitet innan någon bestående skada uppstår.



Användningsfall och motåtgärder

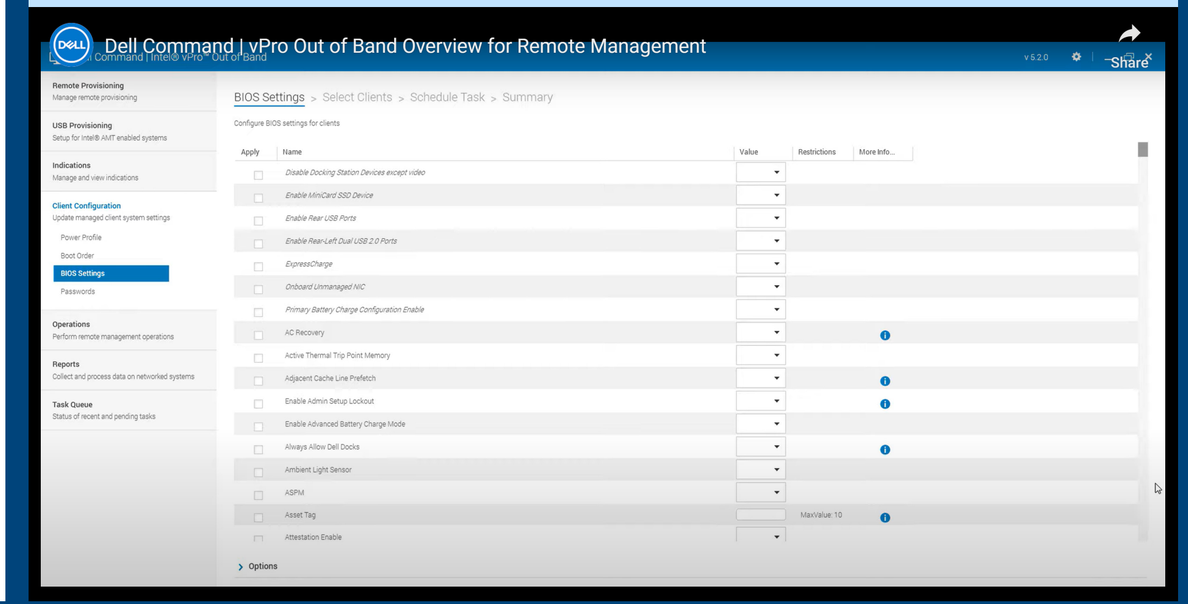
BIOS-nedgraderingsåtgärder

Angripare bryter sig in i nätverket snabbare än någonsin tidigare. Faktum är att den genomsnittliga eCrime-utbrottstiden (den tid det tar att bryta sig in i ett system och röra sig i sidled) minskade från 84 minuter år 2022 till 62 minuter under 2023 enligt CrowdStrike Global Threat Report. Den snabbaste observerade utbrottstiden var bara 2 minuter och 7 sekunder![6]

Så här hjälper Dell och våra partners Intel® och CrowdStike till att fånga upp och avvärja en BIOS-nedgraderingsattack längs alla attackfaser med hårdvarubaserad säkerhet.

Förebygga | **Upptäcka och svara** | **Återställa och åtgärda**

Åtgärda BIOS-nedgradering: förhindra framtida hot för out-of-band-system. Dell Client Command Suite med Intel vPro möjliggör fjärråtgärder.



Användningsfall och motåtgärder

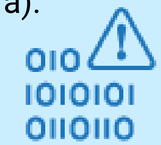
I det här andra användningsfallet visar vi hur de olika stegen eller attackfaserna i en attack mot mjukvaruförsörjningskedjan kan se ut.

Attack mot leverantörskedjan för mjukvara

Steg 1

Initial åtkomst: leverantörskedjan utsätts för intrång

Angriparen matar in skadlig kod i ett mjukvaruverktyg (BIOS/fast mjukvara).



Steg 2

Beständighet

Kunderna laddar ned den skadliga koden när de ska uppdatera sina enheter.

Angriparen installerar skadlig kod.

Steg 3

Lateral förflyttning

Angriparen fejkar en användare som de just attackerade och skickar en skadlig länk till en annan användare. Användaren klickar på länken och angriparen stjäl deras autentiseringsuppgifter.

Steg 4

Exfiltrering

Angriparen exfiltrerar data.

Användningsfall och motåtgärder

Leverantörskedjan har blivit ett viktigt mål för angripare. Även om dessa attacker är mindre vanliga kan resultatet av en lyckad attack vara förödande eftersom företag fortfarande lär sig hur de ska stärka sitt försvar mot dem.

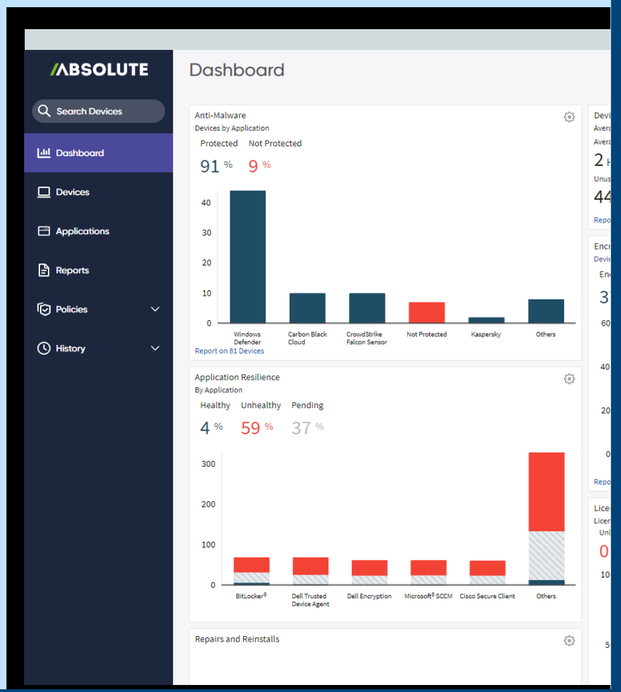
Ett grundläggande ansvar för alla teknikleverantörer är att se till att det de säljer inte oavsiktligt utgör en risk för användarna genom sårbarheter.

För att hjälpa till att förhindra attacker och ge motståndskraft till säkerhetsstacken följer Dell och Intel® de strikta processerna och protokollen i vår Secure Development Cycle[7]. Ytterligare kontroller av leverantörskedjan, exempelvis Dell Secured Component Verification[8] och säkerhet på fast mjukvarunivå från Absolute (visas till höger), ger kunderna förtroende under hela datorns livslängd.

Förebygga | Upptäcka och svara | Återställa och åtgärda

Slutpunktssynlighet från fabriken: se alla enheter i och utanför nätverket med Absolute inbäddat i Dell-hanterade fabriker. CFI (Absolute Custom Factory Installation) tar bort ett steg i driftsättningen och skyddar enheter som kan levereras till lager och flera slutanvändarplatser. Minska riskerna med en fullständig översikt över produkterna från en molnbaserad instrumentpanel.

- Hitta och bibehåll enkelt ett komplett inventarium av era IT-tillgångar och program
- Hitta och kartlägg alla era enheter
- Optimera tillgångsanvändning och övervaka säkerhetsställningen
- Stöd för flera plattformar (Windows, Mac och Chrome)
- Inbyggt i BIOS för 27 ledande dator-OEM:er



Användningsfall och motåtgärder

Leverantörskedjan har blivit ett viktigt mål för angripare. Även om dessa attacker är mindre vanliga kan resultatet av en lyckad attack vara förödande eftersom företag fortfarande lär sig hur de ska stärka sitt försvar mot dem.

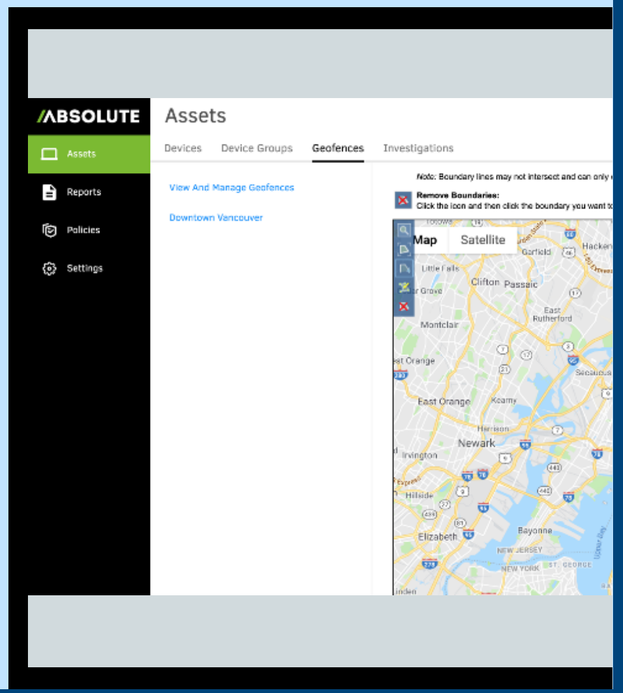
Ett grundläggande ansvar för alla teknikleverantörer är att se till att det de säljer inte oavsiktligt utgör en risk för användarna genom sårbarheter.

För att hjälpa till att förhindra attacker och ge motståndskraft till säkerhetsstacken följer Dell och Intel® de strikta processerna och protokollen i vår Secure Development Cycle[7]. Ytterligare kontroller av leverantörskedjan, exempelvis Dell Secured Component Verification[8] och säkerhet på fast mjukvarunivå från Absolute (visas till höger), ger kunderna förtroende under hela datorns livslängd.

Förebygga | **Upptäcka och svara** | **Återställa och åtgärda**

Kontrollera slutpunkter: med Absolute kan du upptäcka när slutpunkter komprometteras (exempelvis om en kritisk app skadas av skadliga program eller om en dator försvinner under transporten). Vidta åtgärder på distans för att omedelbart åtgärda hot genom att göra enheterna oanvändbara eller ta bort data de innehåller.

- Skydda enheter när de går bortom definierade gränser
- Skydda och sanera kritiska data på distans
- Rensa data vid slutet på livslängden med överensstämmelsecertifikat
- Lås enheter för att skydda viktiga tillgångar vid begäran
- Möjliggör fjärrskydd av fast programvara



Användningsfall och motåtgärder

Leverantörskedjan har blivit ett viktigt mål för angripare. Även om dessa attacker är mindre vanliga kan resultatet av en lyckad attack vara förödande eftersom företag fortfarande lär sig hur de ska stärka sitt försvar mot dem.

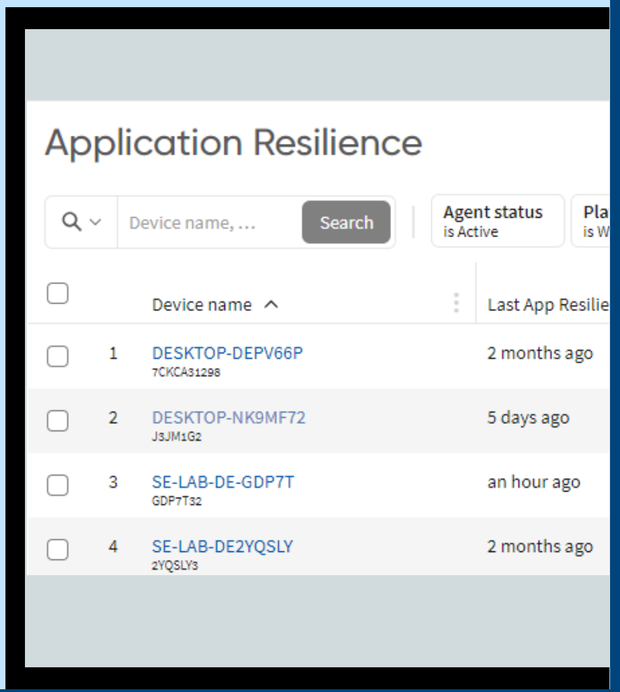
Ett grundläggande ansvar för alla teknikleverantörer är att se till att det de säljer inte oavsiktligt utgör en risk för användarna genom sårbarheter.

För att hjälpa till att förhindra attacker och ge motståndskraft till säkerhetsstacken följer Dell och Intel® de strikta processerna och protokollen i vår Secure Development Cycle[7]. Ytterligare kontroller av leverantörskedjan, exempelvis Dell Secured Component Verification[8] och säkerhet på fast mjukvarunivå från Absolute (visas till höger), ger kunderna förtroende under hela datorns livslängd.

Förebygga | **Upptäcka och svara** | **Återställa och åtgärda**

Självkorrigering: med Absolute Persistence inbäddat i den fasta Dell BIOS-mjukvaran återgår du till ursprungsläget när manipulering upptäcks. Absolute kan självkorrigera eller bevara alla komprometterade slutpunkter eller program som stöds i Application Resilience-katalogen (mer än 80 program), inklusive ett bibliotek med andra motåtgärder som Dell Trusted Device och Zscaler.

- Hitta och ta enkelt bort känsliga data på slutpunkter
- Utför sanering på enheter via ett bibliotek med anpassade skript
- Övervaka program och låt dem fixa sig själva
- Stor och växande Application Resilience-katalog med slutpunktskontroller från tredje part
- Utred och hitta förlorade eller stulna enheter med Absolutes undersökningsteam



Nyckelpunkter

En datorflotta är bara så säker som dess enskilda datorer.

Enheter måste byggas på ett säkert sätt och ha inbyggd säkerhet för att kunna hantera moderna hot.

Fånga upp, stöta bort och återställa sig från attacker genom att se till att slutpunktssäkerhet och hanterbarhet arbetar tillsammans.

Säkerhet är ett lagarbete. Använd både hårdvara och mjukvara för bästa möjliga försvar.

För mer information:

Kontakta oss: Global.Security.Sales@Dell.com

Besök oss: Dell.com/Endpoint-Security

Följ oss: LinkedIn @DellTechnologies | X @DellTech

Ta nästa steg

Säkerhet är ett överväldigande ämne för organisationer av alla storlekar. **Samarbeta med en erfaren säkerhets- och teknikpartner för att modernisera slutpunktssäkerheten**.

Dell Trusted Workspace hjälper till med att säkra slutpunkter för en modern, nollförtroende-redo IT-miljö. Minska attackytan med en heltäckande portfölj av hård- och mjukvaruskydd – bara hos Dell. Vår mycket koordinerade och försvarsbaserade strategi avvärjer hot genom att kombinera inbyggda skydd med kontinuerlig vaksamhet. Slutanvändare håller produktiviteten uppe och IT-avdelningen känner sig trygg med säkerhetslösningar som är byggda för dagens molnbaserade värld.

1. Källa: Enterprise Strategy Group, en avdelning inom TechTarget, anpassad forskningsundersökning på uppdrag av Dell Technologies, *Assessing Organizations' Security Journeys*, november 2023.
2. Källa: Trender inom slutpunktssäkerhet i Futurum Group 2023.
3. Källa: Enterprise Strategy Group, en avdelning inom TechTarget, forskningsrapport, *Hantera sårbara slutpunkter: konvergensen mellan IT och säkerhet för att minska exponering*, maj 2023.
4. Baserat på Dells interna analys i oktober 2024. Gäller datorer med Intel-processorer. Alla funktioner är inte tillgängliga för alla datorer. För vissa funktioner krävs ytterligare köp. Validerad av Principled Technologies. En jämförelse av säkerhetsfunktioner, april 2024.
5. Källa: Vad är cyberattacksfaser? Introduktionsmanual – CrowdStrike.
6. Källa: CrowdStrike 2024 rapport om globala hot.
7. Källa: Tre saker att tänka på när du skapar enhetsförtroende | Dell USA.
8. Källa: Så här behåller du enhetsförtroendet hemligt | Dell USA.