De anatomie van een vertrouwd apparaat

Ontdek waarom Dell de veiligste zakelijke AI-pc's ter wereld heeft[1]

DREIGINGSLANDSCHAP EN UITDAGINGEN

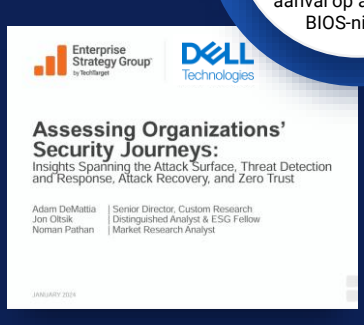
Opkomende aanvalsvectoren onder het besturingssysteem die nieuwe risico's creëren

Eindpuntapparaten zijn een belangrijke toegangspoort voor inbreuken. Naarmate hybride werk het aanvalsoppervlak uitbreidde, nam ook de bezorgdheid over beveiliging op apparaatniveau de afgelopen jaren toe. Aanvallers richtten zich steeds vaker op de leveringsketen, evenals op rootkits en andere kwetsbaarheden in de firmware die grotendeels niet kunnen worden gedetecteerd door alleen legacy EDR-software.

Apparaatgebaseerde bedreigingen zijn sinds 2020 met een factor 1,5 toegenomen.[2]

69%

van de organisaties meldt minstens ÉÉN aanval op apparaat-/BIOS-niveau[2]



Belangrijkste beoordelingscriteria bij de aanschaf van nieuwe pc's:

- Geautomatiseerde detectie van BIOS-gebeurtenissen[3]
- Aanpak van configuraties met een hoog risico[3]

Om moderne bedreigingen te bestrijden, moeten apparaten veilig zijn gebouwd en moeten ze geïntegreerde beveiliging hebben om aanvallen op te vangen en af te weren.

DE OPLOSSING

Voorkom, detecteer, reageer op en herstel van aanvallen op de basis met 's werelds veiligste zakelijke pc's[1]

Een groep apparaten is slechts zo veilig als de afzonderlijke pc's. Maar wat maakt een apparaat vertrouwd en veilig? Zichtbaarheid en bruikbaarheid. Toegang hebben tot meer data leidt tot weloverwogen besluitvorming, waardoor zelfs de meest stiekeme opkomende bedreigingen kunnen worden onderschept. Automatisering maakt snellere oplossing van potentiële problemen mogelijk.

De hardware- en firmwarebeveiliging van zakelijke pc's van Dell (op zowel Intel als AMD) zijn ontworpen om die zichtbaarheid en bruikbaarheid aan uw computerpark te bieden.

De anatomie van een Dell Trusted Device

Voordelen

- Wees veilig vanaf de eerste opstart met rigoureuze controles van de leveringsketen
- Behoud de integriteit van het BIOS met diepe zichtbaarheid op firmwareniveau
- Bescherm de identiteit van eindgebruikers tegen malware die inloggegevens probeert te stelen
- Verrijk data op besturingssysteemniveau met telemetrie 'onder het besturingssysteem' om detectie, respons en herstel te versnellen

Verbeter de beveiliging met pc-telemetrie

Verklein de kloof in IT-beveiliging en verbeter softwareoplossingen met inzichten onder het besturingssysteem. Alleen Dell integreert pc-telemetrie met toonaangevende softwareleveranciers om de beveiliging van de volledige computeromgeving te verbeteren.[1]
Meer informatie →

Behoud van BIOS-integriteit

Detecteer bedreigingen en bestrijd ze met de unieke BIOS-verificatie van Dell. Beoordeel een beschadigd BIOS, herstel het en krijg inzichten waarmee u de blootstelling aan toekomstige bedreigingen kunt verminderen met BIOS Image Capture.[1]
Meer informatie →

Ontdek tikkende tijdbommen

Indicators of Attack, een functie voor vroegtijdige waarschuwing die alleen door Dell wordt aangeboden, scant bedreigingen die op gedrag zijn gebaseerd voordat ze schade kunnen veroorzaken.[1]
Meer informatie →

Verifieer de firmware-integriteit

Exclusieve firmwareverificatie van Dell (hardwaregebaseerde beveiliging in Intel-processors) beschermt tegen ongeoorloofde toegang tot en manipulatie van firmware met hoge bevoegdheden. [1]

Spoor bekende kwetsbaarheden op

De unieke CVE-detectie (Common Vulnerabilities & Exposures) van Dell controleert op openbaar gemelde BIOS-beveiligingsfouten en raadt updates aan om risico's te beperken.[1]
Meer informatie →

Beveilig eindgebruikersreferenties

Controleer de toegang van gebruikers met het unieke SafeID van Dell, een speciale beveiligingschip die inloggegevens van gebruikers verborgen houdt voor malware.[1]
Meer informatie →

Wees veilig gedurende de hele levenscyclus van de pc

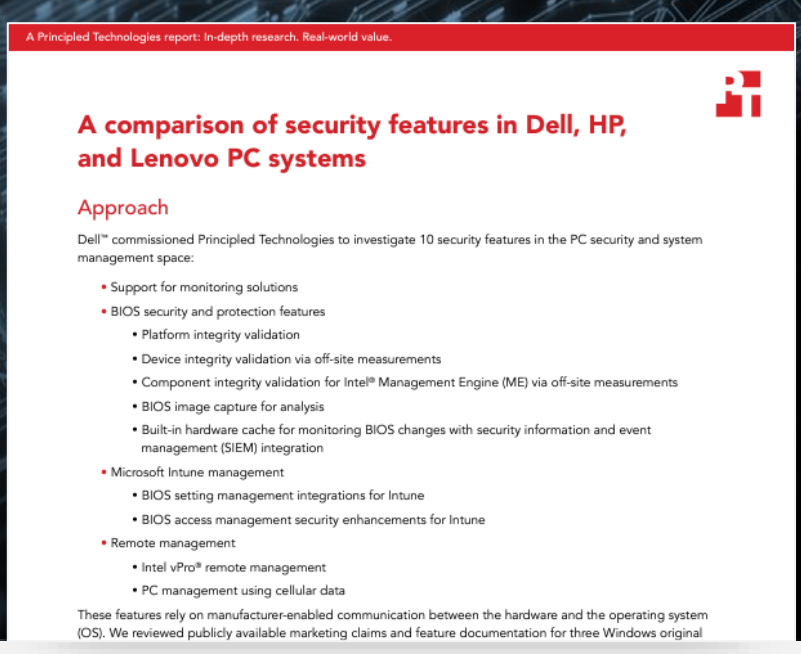
Strikte, geavanceerde controles van de leveringsketen en optionele add-ons, zoals de unieke Secured Component Verification van Dell, bieden zekerheid over de integriteit van de pc, bij levering en gedurende de gehele levensduur van de pc.[1]
Meer informatie →

LEIDERS IN DE BRANCHE

Geen enkele pc-fabrikant biedt de zichtbaarheid op BIOS-niveau die Dell biedt.[1]

Ontdek wat er nodig is om het vertrouwen in apparaten te behouden ondanks moderne bedreigingen.[4]

Meer informatie →



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

Ontdek Dell Trusted Devices

Laptops →

Desktops →

Workstations →

Werk overal veilig met Dell Trusted Workspace

Hardwarebeveiliging in ontwerp en geïntegreerd

Toegevoegde softwarebeveiliging

Ga naar:
dell.com/endpoint-security

Neem contact met ons op
global.security.sales@dell.com

Meer informatie
Blogs over eindpuntbeveiliging →

Deelnemen aan het gesprek
delltechnologies @delltech

Bronnen en disclaimers

[1]Gebaseerd op interne analyse van Dell, oktober 2024 (Intel) en maart 2025 (AMD). Van toepassing op pc's met Intel en AMD 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.

[2]Bron: Futurum Group, Endpoint Security Trends, 2023.

[3]Bron: Enterprise Strategy Group, een afdeling van TechTarget, Custom Research Survey in opdracht van Dell Technologies, *Assessing Organizations' Security Journeys*, november 2023.

[4]*Onderzoeksresultaten van Principled Technologies alleen beschikbaar voor apparaten met Intel.