DELL Technologies

Anatomin för en betrodd enhet

Läs mer om vad som gör Dell till världens säkraste kommersiella AI-datorer[1]

HOTBILD OCH UTMANINGAR

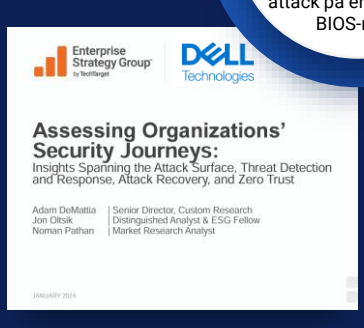
Nya attackvektorer under operativsystemnivå skapar nya risker

Slutpunktsenheter är en vanlig port för intrång. I takt med att hybridarbetandet har medfört större attackytor har oron för säkerhet på enskild enhetsnivå stigit kraftigt de senaste åren. Angripare har i allt högre grad riktat in sig på leverantörskedjan, samt spökprogram och andra sårbarheter i fast programvara som i stort sett inte kan upptäckas med enbart äldre EDR-programvara.

De enhetsbaserade hoten har ökat med 1,5 gånger sedan 2020.[2]

69%

av alla organisationer rapporterar minst EN attack på enhets- eller BIOS-nivå[2]



Viktigaste utvärderingskriterierna vid inköp av nya datorer:

- Automatisk identifiering av BIOS-händelser[3]
- Hantering av högriskkonfigurationer[3]

För att kunna hantera nutida hot måste enheter byggas med robust säkerhet, och de måste ha inbyggda säkerhetsfunktioner som fångar upp och avvärjer attacker.

LÖSNINGEN

Förhindra, identifiera, agera på och återställ efter fundamentala attacker med världens säkraste kommersiella datorer[1]

En datorflotta är bara så säker som dess enskilda datorer. Men vad gör en enhet betrodd och säker? Översikt och åtgärdsmöjligheter. Att ha tillgång till mer data leder till mer välgrundade beslut, vilket underlättar för att kunna upptäcka även de mest lömska nya hoten. Med automatisering går det snabbare att åtgärda potentiella problem.

Säkerhetsfunktionerna i hårdvaran och den fasta mjukvaran i Dells kommersiella datorer (på både Intel och AMD) är utformade för att ge din organisation den översikten och de åtgärdsmöjligheterna.

Anatomin för en Dell Trusted Device

Fördelar

- Var skyddad från första gången enheten startas tack vare rigorösa kontroller av leverantörskedjan
- Bibehåll BIOS-integriteten med djupgående översikt på nivån för den fast programvaran
- Skydda slutanvändarnas identiteter från skadliga program som försöker stjäla inloggningsuppgifter
- Förbättra data på operativsystemnivå med telemetri på ”under operativsystemnivå” för snabbare identifiering, åtgärd och korrigeringar

Förbättra säkerheten med datortelemetri

Minska IT-säkerhetsbrister och berika mjukvarulösningar med insikter” under operativsystemet”. Endast Dell integrerar datortelemetri med branschledande mjukvaruleverantörer för att förbättra säkerheten för hela datorflottor.[1]
Läs mer →

Upprätthåll BIOS-integritet

Identifiera och avvärj hot med Dells unika BIOS-verifiering. Utvärdera ett skadat BIOS, reparera det och få insikter som minskar exponeringen för framtida hot med BIOS Image Capture.[1]
Läs mer →

Upptäck tidsinställda bomber

Indicators of Attack är en funktion för tidig varning som bara erbjuds av Dell och som söker efter beteendebaserade hot innan de hinner orsaka skada.[1]
Läs mer →

Kontrollera integriteten för fast programvara

Den Dell-exklusiva verifieringen av fast mjukvara (hårdvarubaserad säkerhet som finns i Intels processorer) skyddar mot obehörig åtkomst till och manipulering av fast mjukvara med omfattande privilegier. [1]

Fånga in kända sårbarheter

Dells unika CVE-detektering (Common Vulnerabilities and Exposures, vanliga säkerhetsproblem och exponeringar) övervakar offentligt rapporterade BIOS-säkerhetsbrister och rekommenderar uppdateringar för att minska riskerna.[1]
Läs mer →

Skydda slutanvändaruppgifter

Verifiera användaråtkomst med hjälp av Dells unika SafeID, ett dedikerat säkerhetschip som döljer användaruppgifter från skadliga program.[1]
Läs mer →

Skydd under hela datorns livscykel

Rigorösa, toppmoderna kontroller av leverantörskedjan och valfria tillägg som Dells unika Secured Component Verification garanterar datorns integritet vid leverans och under hela dess livslängd.[1]
Läs mer →

LEDANDE I BRANSCHEN

Ingen annan datortillverkare erbjuder översikt på BIOS-nivå som Dell gör.[1]

Läs om vad som krävs för att upprätthålla enhetsförtroendet mot moderna hot.[4]

Läs mer →

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

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

Approach

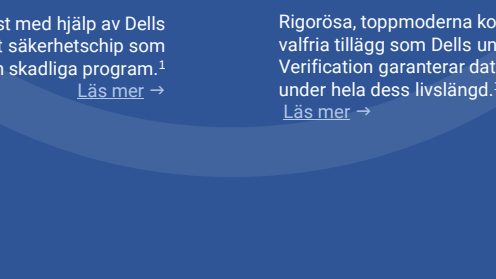
Dell™ commissioned Principled Technologies to investigate 10 security features in the PC security and system management space:

- 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

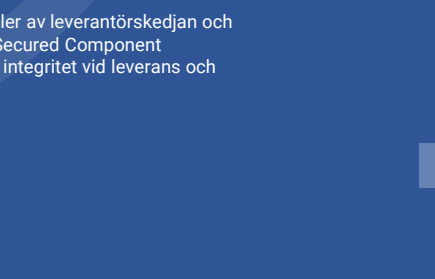
These features rely on manufacturer-enabled communication between the hardware and the operating system (OS). We reviewed publicly available marketing claims and feature documentation for three Windows original

Utforska Dell Trusted Devices

Bärbara datorer →



Stationära datorer →



Workstation-datorer →

Tryggt och säkert arbete var som helst tack vare Dell Trusted Workspace

Medbyggd och inbyggd hårdvarusäkerhet

Påbyggd mjukvarusäkerhet

Besök oss
dell.com/endpoint-security

Kontakta oss
global.security.sales@dell.com

Läs mer
Bloggar om slutpunktssäkerhet →

Delta i konversationen
delltechnologies @delltech

Källor och ansvarsfriskrivningar

[1] Enligt Dells interna analys, oktober 2024 (Intel) och mars 2025 (AMD). Gäller datorer med Intel och AMD 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.

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

[3] Källa: Enterprise Strategy Group, en avdelning inom TechTarget, anpassad studie på uppdrag av Dell Technologies, *Assessing Organizations' Security Journeys*, november 2023.

[4] Principled Technologys studieresultat är endast tillgängliga för Intel baserade enheter.