Anatomía de un dispositivo de confianza

Descubra lo que convierte a los PC con IA comerciales de Dell en los más seguros del mundo[1]

RETOS Y PANORAMA DE AMENAZAS

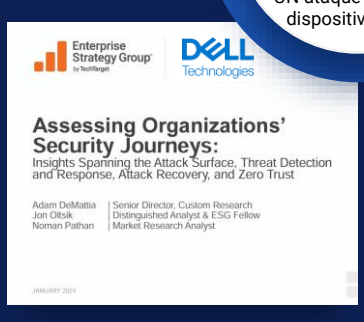
Vectores de ataque emergentes por debajo del SO que generan nuevos riesgos

Los dispositivos de punto final son una puerta de enlace importante para las vulneraciones. Dado que el modelo de trabajo híbrido ha ampliado la superficie de ataque, la preocupación por la seguridad en los dispositivos se ha disparado en los últimos años. Los atacantes recurrieron cada vez más a la cadena de suministro, así como a los rootkits y otras vulnerabilidades de firmware que, en gran medida, no los puede detectar ningún software EDR obsoleto por sí mismo.

Las amenazas basadas en dispositivos se han multiplicado por 1,5 desde 2020.[2]

69%

de las organizaciones informan al menos de UN ataque a nivel de dispositivo/BIOS[2]



Principales criterios de evaluación al adquirir nuevos PC:

- Detección automatizada de eventos del BIOS[3]
- Cómo se abordan configuraciones de alto riesgo[3]

Para combatir las amenazas modernas, los dispositivos deben estar construidos de forma segura e incluir seguridad para ayudar a detectar y repeler los ataques.

LA SOLUCIÓN

Evite, detecte, responda y recupérese de los ataques fundacionales con los PC comerciales más seguros del mundo[1]

El nivel de seguridad de una flota se define por el nivel de seguridad individual de cada PC. ¿Pero qué hace que un dispositivo sea seguro y de confianza? Su visibilidad y su capacidad de acción. Tener acceso a más datos permite tomar decisiones más fundamentadas, lo que ayuda a atrapar incluso las amenazas emergentes más furtivas. La automatización permite una resolución más rápida de los posibles problemas.

Las defensas de hardware y firmware de los PC comerciales Dell (tanto con Intel como con AMD) están diseñadas para aportar esa visibilidad y capacidad de acción a su flota.

Anatomía de un Dell Trusted Device

Beneficios

Garantice su seguridad desde el primer arranque con rigurosos controles de la cadena de suministro

Mantenga la integridad del BIOS con una visibilidad exhaustiva a nivel de firmware

Proteja la identidad de los usuarios finales frente al malware que pretende robar credenciales

Enriquezca los datos en el nivel del sistema operativo con telemetría "por debajo del SO" para acelerar la detección, la respuesta y la corrección

Mejore la seguridad con la telemetría del PC

Reduzca la brecha de seguridad de TI y potencie las soluciones de software con información por debajo del sistema operativo. Solo Dell integra la telemetría del PC con software líder en el sector para mejorar la seguridad de todo el parque informático.[1]
Más información →

Mantener la integridad del BIOS

Detecte y repela amenazas con la verificación del BIOS exclusiva de Dell. Evalúe un BIOS dañado, repárelo y obtenga información que reduzca la exposición a amenazas futuras con la captura de imágenes del BIOS.[1]
Más información →

Detecte bombas de relojería

Los indicadores de ataque, una característica de alerta temprana que solo Dell ofrece, analizan las amenazas basadas en el comportamiento antes de que puedan causar daños.[1]
Más información →

Verifique la integridad del firmware

La verificación del firmware exclusiva de Dell (seguridad basada en hardware de los procesadores Intel) protege frente al acceso no autorizado y la manipulación de firmware altamente privilegiado. [1]

Detecte vulnerabilidades conocidas

La detección de vulnerabilidades y exposiciones comunes (CVE) exclusiva de Dell supervisa los fallos de seguridad del BIOS que se hayan notificado públicamente y recomienda actualizaciones para mitigar el riesgo.[1]
Más información →

Proteger las credenciales del usuario final

Verifique el acceso de los usuarios con SafeID, un chip de seguridad específico y exclusivo de Dell que mantiene las credenciales de usuario ocultas frente al malware.[1]
Más información →

Garantice la seguridad en todo el ciclo de vida del PC

Los rigurosos y vanguardistas controles de la cadena de suministro y complementos opcionales, como la verificación de componentes seguros exclusiva de Dell, son garantía de la integridad del PC en el momento de la entrega y en toda su vida útil.[1]
Más información →

Liderazgo en el sector

Ningún fabricante de PC ofrece la visibilidad del BIOS que Dell proporciona.[1]

Descubra lo que se necesita para mantener la confianza en los dispositivos contra las amenazas modernas.[4]

Más información →


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

Explorar Dell Trusted Devices

Portátiles →

Equipos de sobremesa →

Estaciones de trabajo →

Protección del trabajo en cualquier lugar con Dell Trusted Workspace

Seguridad de hardware integrada y conjunta

Seguridad de software complementaria

Visítenos
dell.com/endpoint-security

Contacto
global.security.sales@dell.com

Más información
Blogs sobre seguridad de puntos finales →

Participe en la conversación
delltechnologies @delltech

Fuentes y renuncias:

[1] Según análisis internos de Dell en octubre de 2024 (Intel) y marzo de 2025 (AMD). Aplicable a PC con procesadores Intel y AMD. No todas las funciones están disponibles en todos los equipos. Algunas funciones requieren compras adicionales. Validado por Principled Technologies. A comparison of security features, abril de 2024.

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

[3] Fuente: Enterprise Strategy Group, una división de TechTarget, encuesta de investigación personalizada por encargo de Dell Technologies, *Assessing Organizations' Security Journeys*, noviembre de 2023.

[4] Los resultados del estudio de Principled Technology solo están disponibles para dispositivos con tecnología Intel.