DELL Technologies

Cómo combatir las ciberamenazas

con seguridad y capacidad de gestión de puntos finales integradas

CROWDSTRIKE intel ABSOLUTE®

Resumen ejecutivo

Los vectores de ataque emergentes están generando nuevos riesgos. Anticípese a las amenazas modernas en los puntos finales con varias capas de defensa que funcionan conjuntamente. Descubra cómo la telemetría de hardware puede integrarse con el software para mejorar la seguridad y la capacidad de gestión en toda la flota. Elimine los ataques más rápido, respalde los principios de confianza cero e innove de forma segura con dispositivos y soluciones fáciles de gestionar.

Índice

El panorama de amenazas

Retos

Solución

Casos de uso y medidas correctivas

Conclusiones y llamada a la acción

El panorama de amenazas

Caso práctico

En 2023, Eclypsium descubrió un defecto en el firmware de las placas base que un fabricante taiwanés vendía. Simplemente al intentar mantener el firmware actualizado, los investigadores descubrieron que el código se implementó de forma no segura, lo que podría permitir que el mecanismo se secuestrara y utilizara para instalar malware.

A continuación se muestran algunos motivos por los que este descubrimiento fue particularmente preocupante

- Los clientes quedaron expuestos a través de una vulnerabilidad del firmware.
- La vulnerabilidad existía en un área del dispositivo donde, tradicionalmente, ha sido difícil detectar amenazas.
- Podría usarse para lanzar un ataque remoto que eluda las comprobaciones de credenciales.

Visto en los titulares...

El panorama de amenazas

Implicaciones

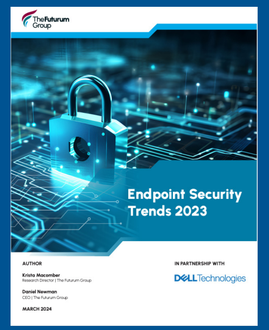
Se trata de un factor clave que le quita el sueño a los equipos de TI y seguridad:

Ataques basados en dispositivos.

Estos ataques sofisticados y maliciosos pueden permitir a los adversarios obtener acceso con privilegios. Es más, muchos de ellos pueden desactivar las protecciones tradicionales solo de software, como el antivirus, sin ser detectados.

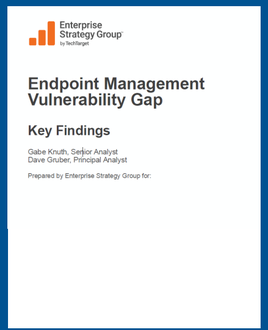
Según una encuesta global reciente llevada a cabo entre profesionales de TI y seguridad[1], cuando las organizaciones suministran hardware nuevo, algunos de sus principales criterios de evaluación son los siguientes:

Detección automatizada de eventos en el firmware del BIOS



El 69 % de las organizaciones afirman haber experimentado al menos UN ataque en el nivel de dispositivo en los últimos doce meses. Eso significa un aumento de 1,5 veces desde el estudio de 2020.[2]

Configuraciones de alto riesgo



Más del 75 % de las organizaciones afirman haber experimentado al menos un ciberataque a causa de un dispositivo de punto final desconocido, sin gestionar o gestionado de forma incorrecta.[3]

Retos

Entonces, ¿qué hace que un dispositivo sea un blanco fácil?

Visibilidad

Estos ataques son difíciles de detectar; se ejecutan en una parte del dispositivo que tradicionalmente ha carecido de visibilidad y capacidad de observación.

Capacidad de respuesta

A menudo, las organizaciones tienen implementadas decenas de herramientas que funcionan en silos, por lo que, si se detecta un ataque, la respuesta y la corrección rápidas son un gran desafío y requieren mucho trabajo manual.

Solución

Visibilidad

Capacidad de respuesta

Como uno de los proveedores de tecnología más importantes del mundo, Dell reflexiona mucho sobre la seguridad. Por eso **creamos PC comerciales para priorizar la visibilidad y la capacidad de respuesta desde el principio**. De esta forma, todo el poder está en manos de las operaciones de TI y seguridad.

Nuestros PC comerciales incluyen **características de seguridad integradas únicas**, como la verificación del BIOS[4] y los indicadores de ataque[4], para ayudar a detectar las amenazas antes de que causen daños. Hacemos que estas detecciones sean visibles con **la telemetría de dispositivos exclusiva de Dell**.[4] Cuando un PC comercial Dell con Intel vPro® detecta una amenaza potencial en el nivel de dispositivo, puede -enviar la información al sistema operativo para conseguir una investigación y una respuesta más rápidas y efectivas.

Liderazgo del sector

Dell ofrece los PC comerciales más seguros del mundo[4]

Descubra lo que se necesita para mantener la confianza de dispositivos contra las amenazas modernas.

Lea el estudio de Principled Technologies sobre la seguridad de los dispositivos →


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.

Solución

Combata las amenazas con una seguridad y una capacidad de gestión que funcionan de forma conjunta

Dell y nuestro ecosistema de socios conectados trabajan para aportar visibilidad y capacidad de respuesta al espacio de trabajo. Esto incluye:

- Seguridad de la cadena de suministro y defensas integradas de hardware y firmware de Dell
- Núcleo de chips y protecciones "por debajo del SO" de Intel
- Capacidad de gestión a través de Dell y consolas de gestión unificada de puntos finales
- Protección avanzada contra amenazas de socios como CrowdStrike y Absolute que cubre puntos finales, redes y la cloud

El ecosistema utiliza la telemetría para PC como el conector, lo que ayuda a cerrar la brecha entre las soluciones de TI y de seguridad, y por donde pueden colarse las amenazas. Este enfoque no solo puede ayudar a prevenir los ataques, sino que también puede detectarlos, responder a ellos, recuperarse y corregirlos.

Casos de uso y medidas correctivas

Para demostrar cómo funcionan la seguridad y la capacidad de gestión integradas para mejorar la ciberresiliencia, analizaremos dos casos de uso, incluidos los escenarios de ataque y las medidas correctivas.

En primer lugar, un ataque al firmware del BIOS. Aquí vemos cómo se puede desarrollar la cadena de ciberataque[5] de retroceso a una versión anterior del BIOS.

Ataque de retroceso a una versión anterior del BIOS

Acceso inicial: replicación con soportes extraíbles + phishing

Paso 1a

Un atacante malicioso aprovecha una vulnerabilidad existente del BIOS para robar las credenciales del SO de forma remota. Hackea el dispositivo y hace que el BIOS retroceda a una versión anterior.

Paso 1b

El atacante inicia un ataque de suplantación de identidad dirigido (spear-phishing) y roba un token de sesión cuando un administrador se autentica por error en un sitio malicioso.

Paso 2

Acceso a las credenciales

El atacante logra la persistencia mediante la creación de cuentas de administrador adicionales y procede a desplazarse por la red.

Paso 3

Desplazamiento lateral

El atacante correlaciona la red y localiza los servidores de gestión de sistemas.

Paso 4

Filtración

El atacante filtra los datos a través de un servicio web.

Casos de uso y medidas correctivas

Medidas correctivas contra el retroceso a una versión anterior del BIOS

Los adversarios están penetrando en la red más rápido que nunca. De hecho, de acuerdo con el informe CrowdStrike Global Threat Report, el tiempo medio de penetración de los ciberdelitos (el tiempo que se tarda en entrar en un sistema y desplazarse lateralmente) disminuyó de 84 minutos en 2022 a 62 minutos en 2023. El tiempo de penetración más rápido observado fue de tan solo 2 minutos y 7 segundos.[6]

Descubra cómo Dell y nuestros socios Intel® y CrowdStrike ayudan a detectar y repeler un ataque de retroceso a una versión anterior del BIOS a lo largo de la cadena de ataque con seguridad asistida por hardware.

Prevenir | **Detectar y responder** | **Recuperar y corregir**

Proteger la cadena de suministro: los rigurosos controles protegen los PC desde el diseño y el desarrollo, pasando por el suministro y el montaje, hasta la entrega. Dell e Intel trabajan incansablemente para garantizar que los productos se desarrollen de forma que mitiguen el riesgo de posibles vulnerabilidades y manipulaciones de los productos a lo largo de todo su ciclo de vida.




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

Casos de uso y medidas correctivas

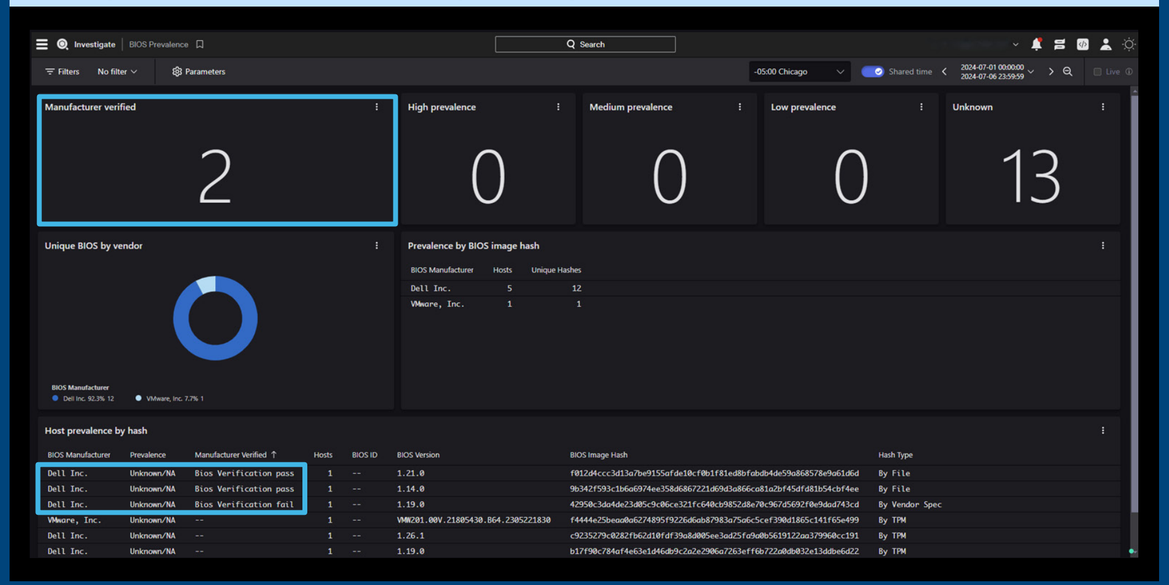
Medidas correctivas contra el retroceso a una versión anterior del BIOS

Los adversarios están penetrando en la red más rápido que nunca. De hecho, de acuerdo con el informe CrowdStrike Global Threat Report, el tiempo medio de penetración de los ciberdelitos (el tiempo que se tarda en entrar en un sistema y desplazarse lateralmente) disminuyó de 84 minutos en 2022 a 62 minutos en 2023. El tiempo de penetración más rápido observado fue de tan solo 2 minutos y 7 segundos.[6]

Descubra cómo Dell y nuestros socios Intel® y CrowdStrike ayudan a detectar y repeler un ataque de retroceso a una versión anterior del BIOS a lo largo de la cadena de ataque con seguridad asistida por hardware.

Prevenir | **Detectar y responder** | **Recuperar y corregir**

Detectar certificaciones del BIOS en la plataforma CrowdStrike Falcon: con la telemetría de dispositivos de Dell habilitada, un administrador puede ver las notificaciones de las características de seguridad integradas, como la verificación del BIOS, de forma remota en CrowdStrike Falcon, lo que ayuda a acelerar la detección de actividades sospechosas antes de que se produzcan daños duraderos.



Casos de uso y medidas correctivas

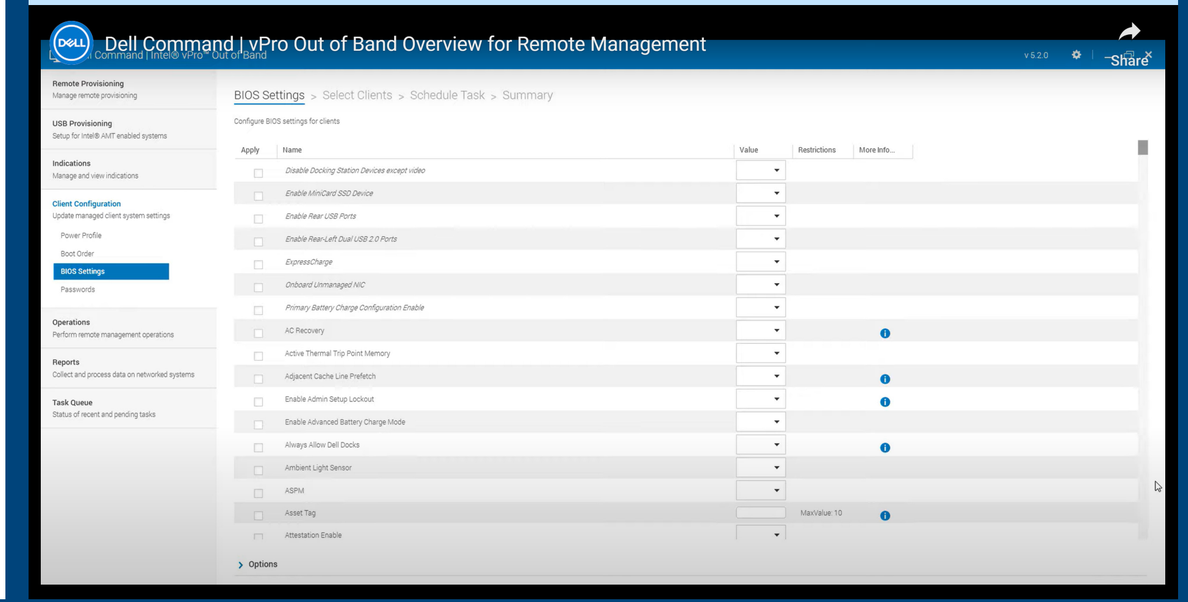
Medidas correctivas contra el retroceso a una versión anterior del BIOS

Los adversarios están penetrando en la red más rápido que nunca. De hecho, de acuerdo con el informe CrowdStrike Global Threat Report, el tiempo medio de penetración de los ciberdelitos (el tiempo que se tarda en entrar en un sistema y desplazarse lateralmente) disminuyó de 84 minutos en 2022 a 62 minutos en 2023. El tiempo de penetración más rápido observado fue de tan solo 2 minutos y 7 segundos.[6]

Descubra cómo Dell y nuestros socios Intel® y CrowdStrike ayudan a detectar y repeler un ataque de retroceso a una versión anterior del BIOS a lo largo de la cadena de ataque con seguridad asistida por hardware.

Prevenir | Detectar y responder | **Recuperar y corregir**

Corregir el retroceso a una versión anterior del BIOS: ayude a evitar futuras amenazas para los sistemas fuera de banda. Dell Client Command Suite con Intel vPro permite la corrección remota.



Casos de uso y medidas correctivas

En este segundo caso de uso, así es como podría desarrollarse el paso en la cadena de ataque de un ataque a la cadena de suministro de software.

Ataques a la cadena de suministros de software

Paso 1

Acceso inicial: riesgos para la cadena de suministro

El atacante inyecta código malicioso en una utilidad de software (BIOS/firmware).

Paso 2

Persistencia

Los clientes descargan el código malicioso cuando actualizan sus dispositivos.

El atacante instala el malware.

Paso 3

Desplazamiento lateral

El atacante burla al usuario que acaba de ser atacado y envía un enlace malicioso a otro usuario. Ese usuario hace clic en el vínculo y el atacante le roba las credenciales.

Paso 4

Filtración

El atacante filtra los datos.

Casos de uso y medidas correctivas

La cadena de suministro se ha convertido en un objetivo clave para los atacantes. Aunque estos ataques son menos habituales, los resultados de un ataque que se lleve a cabo con éxito pueden ser devastadores, ya que las organizaciones aún están aprendiendo a reforzar sus defensas frente a ellos.

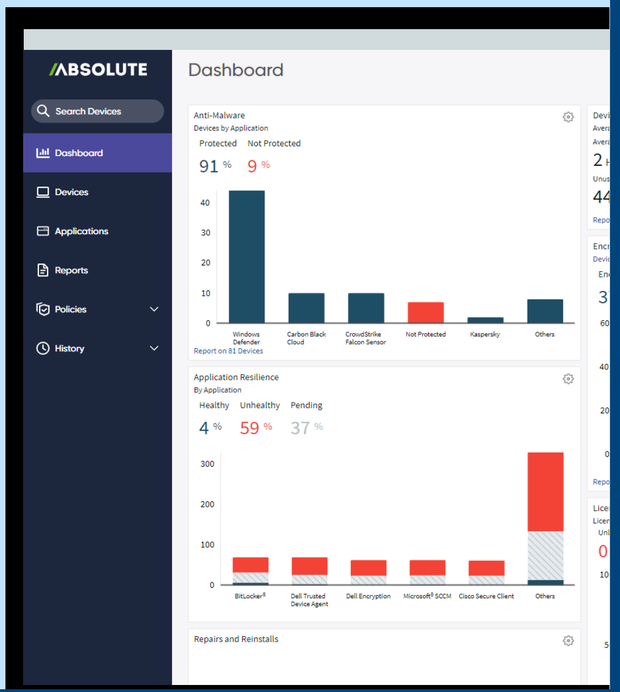
Una de las principales responsabilidades de todos los proveedores de tecnología es garantizar que lo que venden no suponga un riesgo involuntario para los usuarios a causa de vulnerabilidades.

Para ayudar a prevenir ataques y dotar de resiliencia a la pila de seguridad, Dell e Intel® siguen los estrictos procesos y protocolos de nuestro Ciclo de vida de desarrollo seguro[7]. La garantía adicional de la cadena de suministro, por ejemplo, Verificación de componentes seguros de Dell[8], además de la seguridad en el nivel de firmware de Absolute (consulte la imagen situada a la derecha), proporciona a los clientes confianza durante toda la vida útil del PC.

Prevenir | **Detectar y responder** | **Recuperar y corregir**

Visibilidad de los puntos finales desde la fábrica: vea todos los dispositivos existentes dentro y fuera de la red con Absolute integrado en las fábricas gestionadas por Dell. Absolute Custom Factory Install (CFI) elimina un paso en la implementación y protege los dispositivos que puedan enviarse a almacenes y a varias ubicaciones de usuarios finales. Mitigue los riesgos con una vista completa de la flota desde un panel basado en la cloud.

- Encuentre y mantenga fácilmente un inventario completo de sus aplicaciones y activos informáticos
- Localice e identifique todo su equipamiento
- Optimice el uso de los activos y supervise el estado de seguridad
- Compatibilidad en múltiples plataformas (Windows, Mac y Chrome)
- Incorporación en el BIOS de 27 OEM de PC líderes



Casos de uso y medidas correctivas

La cadena de suministro se ha convertido en un objetivo clave para los atacantes. Aunque estos ataques son menos habituales, los resultados de un ataque que se lleve a cabo con éxito pueden ser devastadores, ya que las organizaciones aún están aprendiendo a reforzar sus defensas frente a ellos.

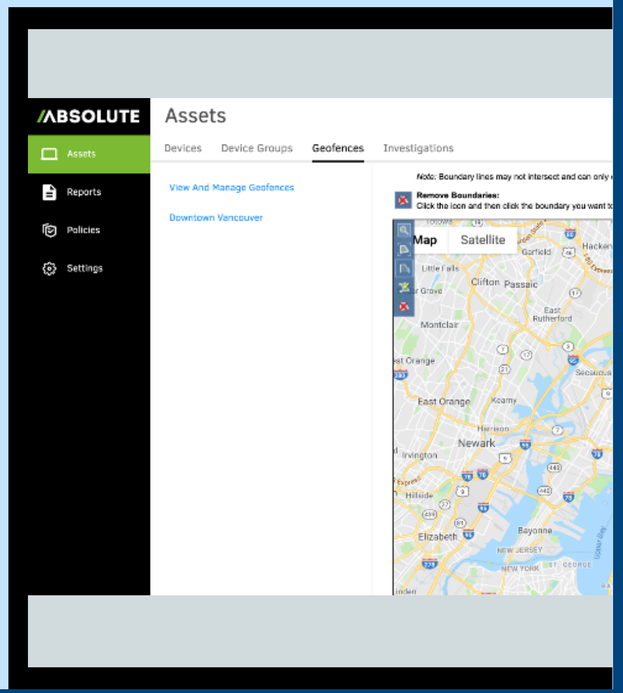
Una de las principales responsabilidades de todos los proveedores de tecnología es garantizar que lo que venden no suponga un riesgo involuntario para los usuarios a causa de vulnerabilidades.

Para ayudar a prevenir ataques y dotar de resiliencia a la pila de seguridad, Dell e Intel® siguen los estrictos procesos y protocolos de nuestro Ciclo de vida de desarrollo seguro[7]. La garantía adicional de la cadena de suministro, por ejemplo, Verificación de componentes seguros de Dell[8], además de la seguridad en el nivel de firmware de Absolute (consulte la imagen situada a la derecha), proporciona a los clientes confianza durante toda la vida útil del PC.

Prevenir | **Detectar y responder** | **Recuperar y corregir**

Controlar los puntos finales: con Absolute, puede detectar cuándo los puntos finales están en peligro (por ejemplo, si una aplicación crítica está dañada por malware o si un PC desaparece durante el tránsito). Tome medidas remotas para corregir las amenazas de inmediato: inutilice los dispositivos o elimine los datos que contienen.

- Proteja los dispositivos cuando salgan de las fronteras definidas
- Proteja y borre de manera remota los datos críticos
- Borre los datos que alcanzan el fin de la vida con certificados de cumplimiento normativo
- Bloquee los dispositivos para proteger los activos esenciales a petición
- Active la protección remota del firmware



Casos de uso y medidas correctivas

La cadena de suministro se ha convertido en un objetivo clave para los atacantes. Aunque estos ataques son menos habituales, los resultados de un ataque que se lleve a cabo con éxito pueden ser devastadores, ya que las organizaciones aún están aprendiendo a reforzar sus defensas frente a ellos.

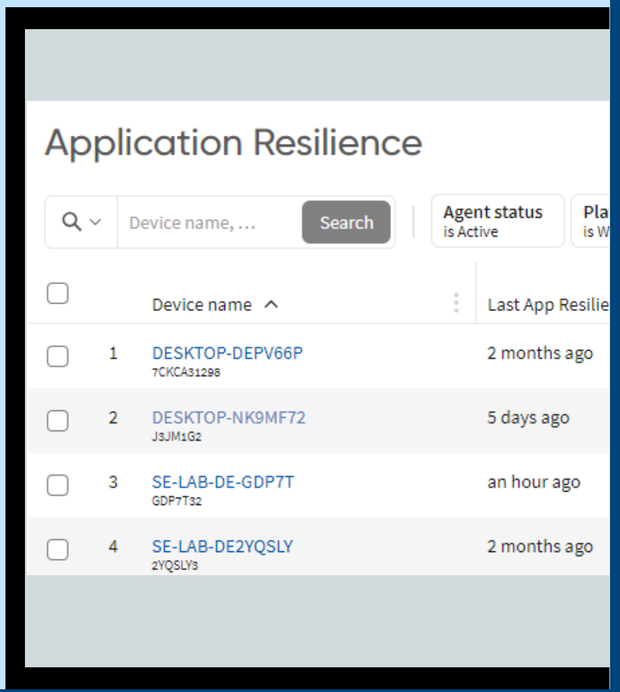
Una de las principales responsabilidades de todos los proveedores de tecnología es garantizar que lo que venden no suponga un riesgo involuntario para los usuarios a causa de vulnerabilidades.

Para ayudar a prevenir ataques y dotar de resiliencia a la pila de seguridad, Dell e Intel® siguen los estrictos procesos y protocolos de nuestro Ciclo de vida de desarrollo seguro[7]. La garantía adicional de la cadena de suministro, por ejemplo, Verificación de componentes seguros de Dell[8], además de la seguridad en el nivel de firmware de Absolute (consulte la imagen situada a la derecha), proporciona a los clientes confianza durante toda la vida útil del PC.

Prevenir | **Detectar y responder** | **Recuperar y corregir**

Autorreparación: con la tecnología Absolute Persistence integrada en el firmware del BIOS de Dell, el dispositivo puede volver a su estado original cuando se detecte una manipulación. Absolute puede autorreparar, o persistir, cualquier punto final vulnerado o aplicación compatible en el catálogo de Application Resilience (más de 80 aplicaciones), incluida una biblioteca de otras medidas correctivas implementadas, por ejemplo, la aplicación Dell Trusted Device, Zscaler, etc.

- Encuentre y elimine fácilmente datos confidenciales en los puntos finales
- Tome medidas correctivas en todos los dispositivos a través de una biblioteca de scripts personalizados
- Supervise aplicaciones y permita su autorreparación
- Catálogo de Application Resilience amplio y en crecimiento que ofrece controles de puntos finales de terceros
- Investigue y localice la pérdida o el robo de dispositivos con el equipo de investigaciones de Absolute



Nociones clave

El nivel de seguridad de una flota se define por el nivel de seguridad individual de cada PC.

Para combatir las amenazas modernas, los dispositivos deben estar diseñados de forma segura y con seguridad integrada.

Detenga y repela los ataques, y recupérese de ellos al garantizar que la seguridad y la capacidad de gestión de los puntos finales funcionan conjuntamente.

La seguridad es un deporte de equipo. Aproveche tanto el hardware como el software para la mejor defensa.

Más información:

Contáctenos: Global.Security.Sales@Dell.com

Visítenos: Dell.com/Endpoint-Security

Síganos: LinkedIn @DellTechnologies | X @DellTech

Un paso hacia delante

La seguridad es un tema abrumador para organizaciones de todos los tamaños. **Contrate a un socio de tecnología y seguridad experimentado para modernizar la seguridad de puntos finales**.

Dell Trusted Workspace ayuda a proteger los puntos finales para conseguir un entorno de TI moderno y preparado para la confianza cero. Reduzca la superficie de ataque con una cartera completa de protecciones de hardware y software exclusivas de Dell. Nuestro enfoque, ampliamente coordinado y basado en la defensa, desvía las amenazas mediante la combinación de protecciones integradas y una vigilancia constante. Los usuarios finales se mantienen productivos y el equipo de tecnología informática trabaja con confianza gracias a soluciones de seguridad creadas para el mundo basado en la cloud de hoy en día.

1. Fuente: Enterprise Strategy Group, una división de TechTarget, encuesta de investigación personalizada por encargo de Dell Technologies, *Assessing Organizations' Security Journeys*, noviembre de 2023.
2. Fuente: Futurum Group, Endpoint Security Trends, 2023.
3. Fuente: Enterprise Strategy Group, una división de TechTarget, informe de investigación, *Managing the Endpoint Vulnerability Gap: The Convergence of IT and Security to Reduce Exposure*, mayo de 2023.
4. Según análisis internos de Dell, octubre de 2024. Aplicable a PC con procesadores Intel. 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.
5. Fuente: What is the Cyber Kill Chain? Introduction Guide – CrowdStrike.
6. Fuente: CrowdStrike 2024 Global Threat Report.
7. Fuente: Three Considerations for Establishing Device Trust | Dell USA.
8. Fuente: How to Keep Device Trust Close to the Vest | Dell USA.