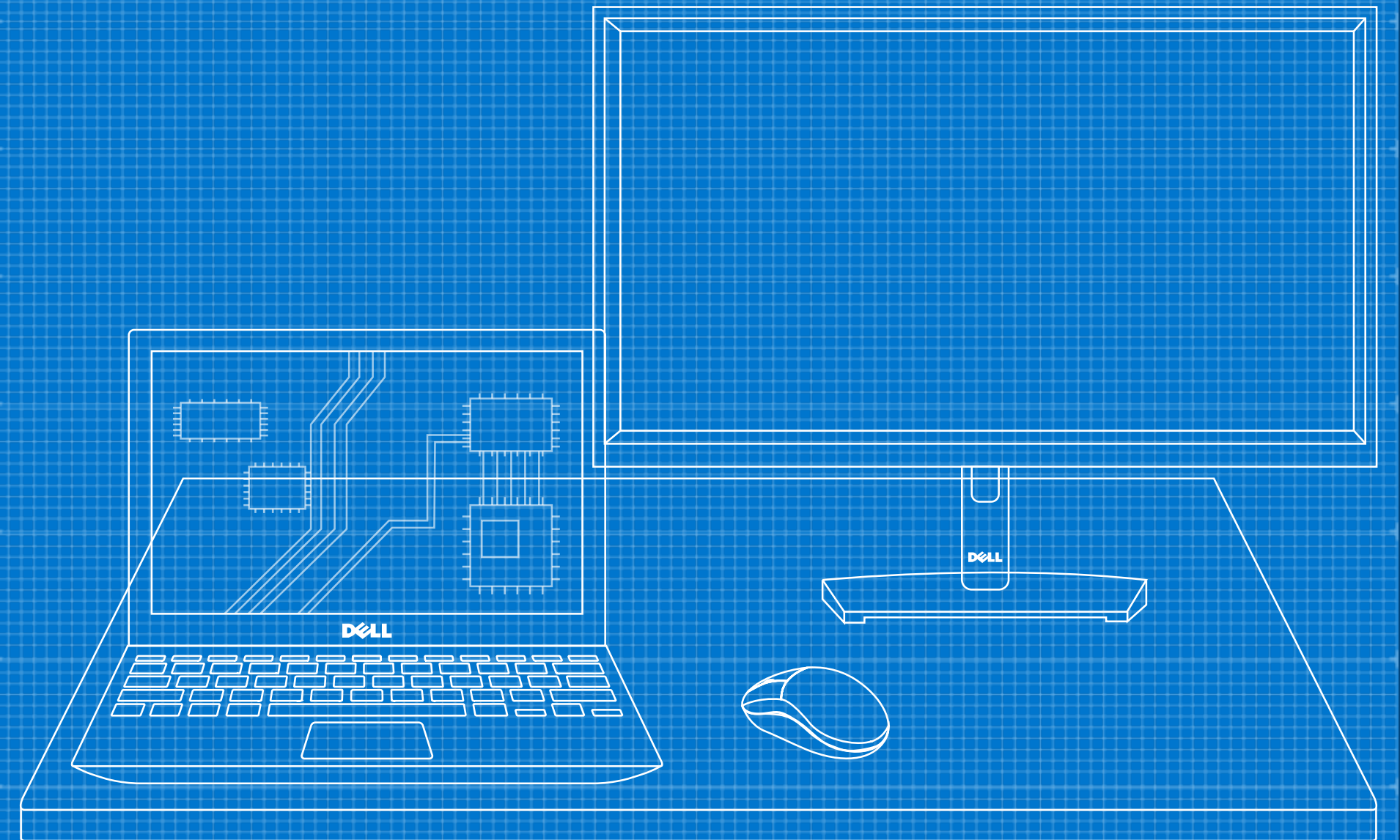


La anatomía de un espacio de trabajo de confianza

Mejore la seguridad de su flota con múltiples capas de defensa



Resumen ejecutivo

Los ciberataques son inevitables y su volumen y sofisticación son cada vez mayores. Los dispositivos de punto final, las redes y los entornos de cloud se han convertido en objetivos clave.

En este eBook, se ofrece a los responsables de toma de decisiones de seguridad y TI una guía para saber cuáles son los elementos necesarios para lograr una defensa más eficaz de los puntos finales en medio de este panorama de amenazas en aumento.



Índice

- 1 [El panorama de amenazas](#)
- 2 [Desafíos](#)
- 3 [Protección del espacio de trabajo moderno](#)
- 4 [La anatomía de un espacio de trabajo de confianza](#)
- 5 [Enfoque de Dell](#)
- 6 [Combínelo todo con Dell](#)
- 7 [Conclusiones y llamada a la acción](#)



El panorama de amenazas

El paso al trabajo híbrido ha introducido un nuevo nivel de complejidad y nuevos vectores de ataque, y **los puntos finales, las redes y las clouds se han convertido en superficies de ataque en expansión.**

Además, ahora los atacantes emplean técnicas sofisticadas que se dirigen a diferentes capas de la pila informática y se mezclan con los procesos válidos del sistema. Algunos métodos permiten incluso a los atacantes obtener un acceso privilegiado y desactivar las protecciones de software *sin ser detectados en ningún momento.*

Muchas organizaciones han iniciado un proceso de transformación hacia un modelo de confianza cero con el fin de combatir estas amenazas. Pero para activar los principios de la confianza cero, es necesario poder mantener la confianza en los dispositivos.

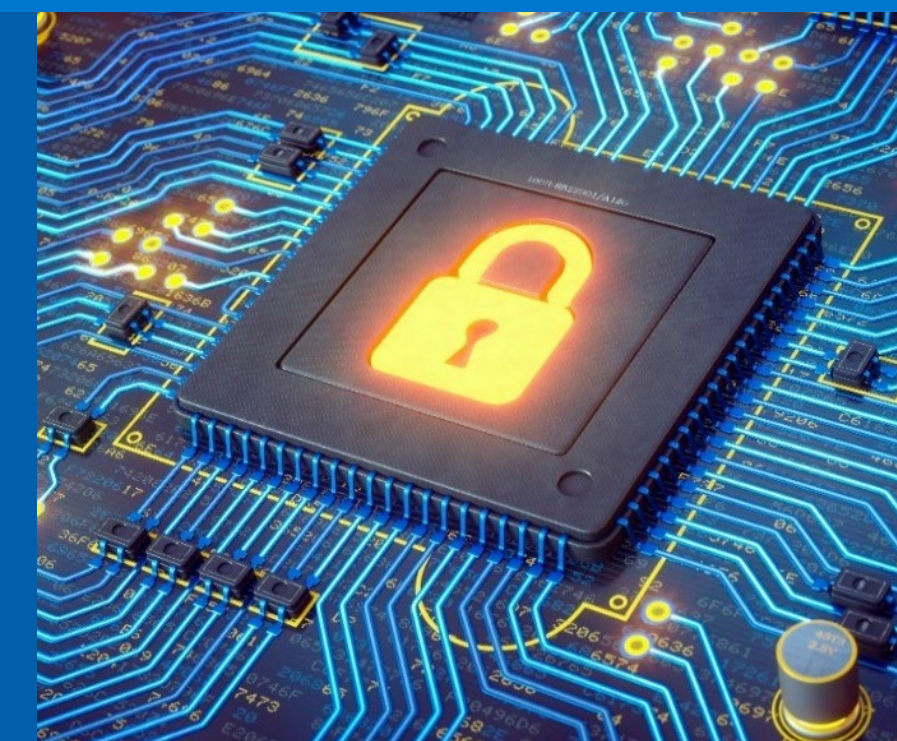
¿Cómo se mantiene la confianza en los dispositivos cuando los ataques son cada vez más frecuentes y la tecnología avanzada crea nuevos vectores de ataque?

¹CrowdStrike Global Threat Report, 2023.

²Dell Innovation Index, 2023.

Sabía que...

El 71 % de los ataques en 2022 no eran ataques basados en malware, lo que supone un aumento interanual del 9 %¹



Solo el 41 % de las organizaciones encuestadas pueden afirmar, con toda confianza, que su tecnología y sus aplicaciones llevan seguridad integrada²

¿Desea explorar la confianza cero para avanzar hacia una madurez en cuanto a ciberseguridad? Consulte nuestro eBook *"La seguridad de punto final es un elemento esencial de su trayecto de confianza cero"* (en inglés).

Desafíos

Para lograr una seguridad de puntos finales eficaz, es importante comprender al adversario y saber cómo trabaja.

Dada la rentabilidad que se puede obtener de una única vulneración, **los atacantes suelen hacer varios intentos para penetrar en la misma organización, aprovechando distintos métodos y puntos de entrada con el fin de incrementar sus posibilidades de éxito.** Por ejemplo, durante todo el ciclo de vida de un único dispositivo, los atacantes pueden tratar de aprovechar sus vulnerabilidades a través de decenas de vectores.

Las defensas antiguas ya no son suficientes para mantener la seguridad de los puntos finales. Cuando las organizaciones refuerzan una superficie de ataque, los autores de las amenazas simplemente se desplazan a otros objetivos menos seguros. Cuando el mundo se volvió híbrido, los autores de amenazas identificaron nuevos vectores de ataque a puntos finales que han tenido unas consecuencias devastadoras.

Vea ejemplos de ataque a la derecha

Ataque a la cadena de suministros: se dirige a los proveedores para acceder a sus sistemas, datos y/o redes y, por extensión, a los de sus clientes. **EJEMPLO:** Un ataque a la cadena de suministros de hardware iniciado por una manipulación de componentes:

Los atacantes interceptan un envío de PC y cambian las unidades de disco duro.



El equipo de TI implementa los dispositivos comprometidos en la empresa.



El atacante instala el malware para extraer las credenciales cuando los usuarios inicien sesión.



Ataque de ingeniería social: engaña a los usuarios finales para que proporcionen información confidencial que luego se puede utilizar para acceder a redes y dispositivos. **EJEMPLO:** Un ataque de spoofing iniciado mediante un correo electrónico de phishing:

El usuario final cae en la trampa de un correo electrónico de phishing e introduce sus credenciales en una página web falsificada.



El atacante utiliza esas credenciales válidas para acceder a la red de forma remota.



El atacante extrae datos a través de un servicio web, cifra los datos robados y los retiene para pedir un rescate.



Protección del espacio de trabajo moderno

Cuando se trata de protección de puntos finales, se necesita prevención, detección y respuesta, así como recuperación y corrección en varios estados a lo largo de todo el ciclo de vida de un dispositivo: desde el aprovisionamiento y la fabricación de los PC hasta el envío y la implementación, durante su tiempo de uso y hasta el momento de su retirada. Imagine el tamaño de esa superficie de ataque combinada.

La estrategia de ciberseguridad más eficaz se prepara para el peor escenario. Da por hecho que se puede producir una vulneración e incorpora múltiples capas de protección para bloquear el ataque lo más rápido posible y con la mayor frecuencia que se pueda. También incluye capacidades de corrección para minimizar el riesgo de que se repita el ataque.

³[Dell Innovation Index, 2023.](#)

PREVENCIÓN

Reduzca sus opciones de convertirse en objetivo fácil con unas defensas diseñadas para bloquear ataques.

DETECCIÓN Y RESPUESTA

Asuma siempre que se puede producir una vulneración y manténgase alerta.

RECUPERACIÓN Y CORRECCIÓN

Mitigue el impacto de un ataque y vuelva a su actividad habitual.

¿Sabía que...?

Solo el 33 %

de las organizaciones emplean una estrategia de seguridad integral con protecciones basadas tanto en hardware como en software.³



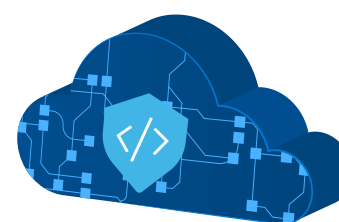
La anatomía de un espacio de trabajo de confianza

La seguridad de puntos finales moderna necesita tres elementos:

- 1 Seguridad de software:** actualmente hay más usuarios, dispositivos y datos que nunca fuera de las redes corporativas. La seguridad de software no solo protege los dispositivos, sino que extiende la protección a los entornos de red y de cloud, que es donde se suele originar la actividad maliciosa.
- 2 Seguridad de hardware:** los dispositivos deben contar con funciones de seguridad integradas. Esto se refiere a la seguridad de hardware y firmware que protege el dispositivo en uso. Para proteger el espacio de trabajo, debe tener funcionalidades integradas que le permitan ver y controlar el dispositivo.
- 3 Seguridad de la cadena de suministros:** los dispositivos deben estar fabricados de forma segura. Esto supone trabajar con proveedores que a) conozcan el panorama de las amenazas y b) puedan hacer uso de ese conocimiento cuando el panorama evolucione. La seguridad a la hora de diseñar, probar y desarrollar los PC ayuda a reducir el riesgo de vulnerabilidades en los productos, al mismo tiempo que los controles en la cadena de suministros mitigan el riesgo de manipulación del producto.

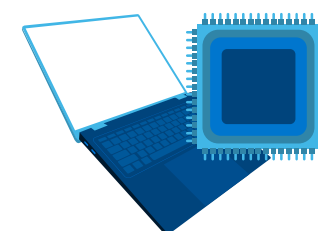
Análisis de las múltiples capas de seguridad

(con ejemplos representativos de medidas de seguridad)



Seguridad de software

- Antivirus de última generación (NGAV)
- Detección y respuesta en puntos finales (EDR)
- Detección y respuesta ampliadas (XDR).
- Protección de datos en la cloud
- Protección de la red
- Autorreparación automática



Seguridad de hardware y firmware

- Verificación del tiempo de arranque
- Verificación del tiempo de ejecución
- Autenticación de usuarios
- Alertas/telemetría y notificaciones de seguridad



Seguridad de la cadena de suministros

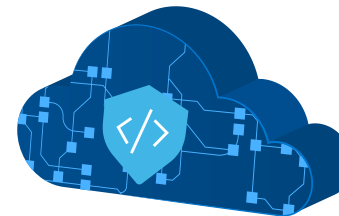
- Procedimientos de desarrollo seguros
- Procedimientos de la cadena de suministros seguros
- Verificación de los componentes
- Precintos visibles a prueba de manipulación del embalaje

Nuestro enfoque: Dell Trusted Workspace

Dell es un socio de seguridad y TI para organizaciones de todo el mundo. A diferencia de las soluciones puntuales, Dell se centra en los resultados generales de seguridad, creando un conjunto de soluciones que bloquea las cadenas de ciberataque y aumenta su resiliencia a los ciberataques. **Dell Trusted Workspace incluye:**

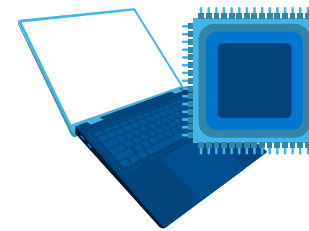
- Unas **protecciones de hardware y firmware** únicas que convierten los PC de Dell en los PC comerciales más seguros del sector.⁴ (*Seguridad complementaria e integrada*)
- Un ecosistema de socios de **software líder en el sector** que ofrece una protección contra amenazas avanzada tanto para el dispositivo como para la red y la cloud. (*Seguridad complementaria*)

⁴Según análisis internos de Dell, septiembre de 2023. Aplicable a PC con procesadores Intel. No todas las funciones están disponibles en todos los PC. Para algunas funciones, se requiere una compra adicional.



Complementaria: seguridad de software del ecosistema de socios

- **Dell SafeGuard and Response:** CrowdStrike, VMware Carbon Black y Secureworks ofrecen capacidades de detección de amenazas, respuesta y corrección.
- **Dell SafeData:** Netskope proporciona visibilidad, supervisión y prevención de la pérdida de datos para aplicaciones de cloud. **Absolute** permite la autorreparación automática para aplicaciones y redes.



Integrada: seguridad de hardware y firmware mediante los PC comerciales más seguros del sector⁴

Ejemplos de funciones que protegen el dispositivo en uso:

- **Dell SafeBIOS:** la verificación del BIOS* fuera del host y los indicadores de ataque* ayudan a detectar actividad maliciosa antes de que comprometa al PC.
- **Dell SafeID:** protege las credenciales del usuario final en un chip de seguridad dedicado.*
- **Verificación del firmware fuera del host:** protege la integridad del firmware altamente privilegiado.*
- **Dell Trusted Device software:** con este software, Dell integra la telemetría del dispositivo con software líder en el sector para mejorar la seguridad de todo el parque informático.*



Conjunta: seguridad de la cadena de suministros que ayuda a garantizar que los PC sean seguros desde el primer arranque

- **Dell SafeSupply Chain:** complementos como la verificación de componentes seguros de Dell ofrecen una garantía adicional de la integridad del producto.

** Exclusivo de Dell*

Combínelo todo con Dell

Al tener implementadas contramedidas de hardware y software, se reduce la superficie de ataque con defensas que ayudan a evitar ataques comunes.

Las capacidades de detección y respuesta hacen frente a ataques sigilosos que puedan pasar desapercibidos.

En el caso del ataque a la cadena de suministros presentado en la página 4, si trabaja con Dell, se tomarán medidas preventivas como los **procedimientos de la cadena de suministros seguros**, que permiten bloquear un ataque en las primeras etapas de la cadena de ataque. Si finalmente se produce el ataque, se implementarán también contramedidas adicionales, como **SCV**.

En el caso del ataque de ingeniería social, aunque el atacante consiga engañar al usuario para que le proporcione las credenciales válidas, un sistema de **verificación de usuario basada en hardware como SafeID** permitirá detener al atacante y denegarle cualquier otro acceso. El software de seguridad como, por ejemplo, una **puerta de enlace web segura de última generación**, ofrece otra capa de protección y supervisión.

Contrarrestar un ataque a la cadena de suministros de hardware iniciado por una manipulación de componentes:

Los atacantes interceptan un envío de PC y cambian las unidades de disco duro.



- **Procedimientos de la cadena de suministros seguros**
- Precintos visibles a prueba de manipulación del embalaje
- Candados en las puertas

El equipo de TI implementa los dispositivos comprometidos en la empresa.



- Verificación de componentes seguros (SCV)
- Verificación del tiempo de ejecución

El atacante instala el malware para extraer las credenciales cuando los usuarios inicien sesión.



- Agente de seguridad de acceso a la cloud
- Puerta de enlace web segura de última generación

Contrarrestar un ataque de ingeniería social iniciado por un correo electrónico de phishing:

El usuario final cae en la trampa de un correo electrónico de phishing e introduce sus credenciales en una página web falsificada.



- NGAV
- EDR
- XDR

El atacante utiliza esas credenciales válidas para acceder a la red de forma remota.



- **Autenticación de varios factores con SafeID**
- Acceso a la red de confianza cero

El atacante extrae datos a través de un servicio web, cifra los datos robados y los retiene para pedir un rescate.



- Puerta de enlace web segura de última generación y análisis del comportamiento de las entidades de usuario

Nociones clave

Las vulneraciones son inevitables.

Una seguridad de puntos finales eficaz asume siempre el peor escenario y se centra en bloquear las cadenas de ataque independientemente de dónde se produzcan, desde el dispositivo a la red y a la cloud.

Ninguna solución bloquea el 100 % de los ataques. Combine contramedidas de hardware y software para optimizar su defensa.

Estará tan protegido como lo estén sus proveedores. Anime a sus proveedores a que perfilen sus medidas de seguridad.



Más información:

Contáctenos: Global.Security.Sales@Dell.com

Visítenos: Dell.com/Endpoint-Security

Síguenos: LinkedIn [@DellTechnologies](https://www.linkedin.com/company/delltechnologies) | X [@DellTech](https://twitter.com/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 tecnología informática 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.

