DELL Technologies

La seguridad de puntos finales es un elemento esencial para la adopción de la confianza cero

Tres recomendaciones para prepararse para la confianza cero

DELL Technologies

Resumen ejecutivo

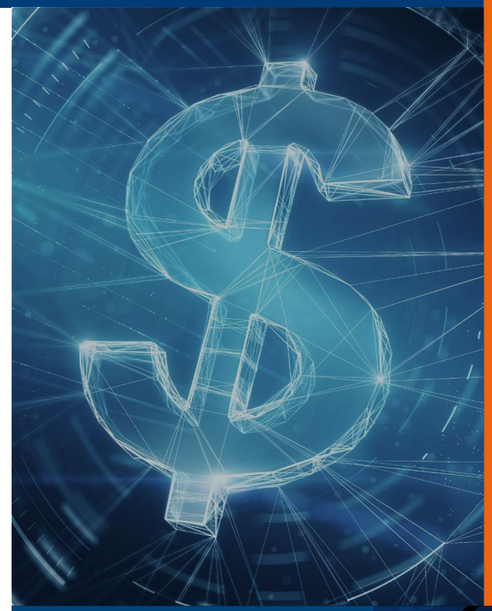
La adopción de la confianza cero es un recorrido a largo plazo. No es un producto ni una solución que implementan las organizaciones; es una infraestructura estratégica de gestión de la seguridad que se desarrolla gradualmente. Este eBook ofrece una guía práctica para los responsables de la toma de decisiones de TI que se enfrentan a una transformación basada en la confianza cero, y se centra sobre todo en el rol que desempeña la seguridad de puntos finales a la hora de crear unas bases modernas y realmente seguras para un mundo en el que prima el teletrabajo.

Tabla de contenidos

El panorama de ciberseguridad

En un mundo cada vez más basado en el trabajo híbrido, el teletrabajo y la cloud, cada vez son más las amenazas de seguridad.

La complejidad de la protección de los recursos de datos de una organización ha crecido exponencialmente en los últimos años. La cloud ha supuesto toda una revolución para la productividad de las empresas en un contexto en el que el trabajo híbrido y el teletrabajo no han parado de crecer. Pero todo tiene un precio. La transición de gestionar solo una infraestructura en las instalaciones a integrar soluciones en la cloud ha generado una superficie de ataque más amplia, y esto también multiplica las consecuencias. Por ejemplo, si un atacante consigue su objetivo, puede afectar no solo a un cliente, sino también a todos los clientes de ese servicio de cloud y a los clientes de esos clientes en toda la cadena de suministros. Los beneficios para estos atacantes, ya se trate de estados nación o de delincuentes comunes, pueden ser enormes, y esto significa que seguirán buscando nuevas vulnerabilidades para explotar.



Se espera que el coste de los daños de la ciberdelincuencia a nivel mundial ascienda a **10,5 billones de USD de aquí a 2025**[i]

En un estudio de Verizon de 2022, se confirmaron **5200** vulneraciones de datos, **hasta 1,3 veces más que el año anterior**[ii]

Implicaciones para un mundo basado en el teletrabajo

Las organizaciones deben encontrar la manera de estar preparadas frente a un panorama de amenazas en constante evolución.

¿Qué implica que el mundo laboral sea cada vez más remoto? Dos cosas:

Todas las organizaciones son vulnerables...

> "Si una entidad quiere entrar de verdad en su sistema, tiene muchas probabilidades de conseguirlo".
>
> — *Almirante Michael Rogers, exdirector de la Agencia de Seguridad Nacional y excomandante del Cibercomando de Estados Unidos*[iii]

... y el coste de no estar a la altura puede ser devastador.

> "El coste de las vulneraciones de datos, que alcanzó un importe sin precedentes, ascendió a un promedio de 4,88 millones de USD en 2024".[iv]

Cada vez son más los vectores de ataque, las superficies de ataque no paran de crecer, y no hay empresa que pueda estar completamente segura. Las organizaciones deben prepararse para el peor de los escenarios, y reforzar sus defensas frente a un ataque inevitable.

El **69 % de las organizaciones** ha sufrido algún tipo de ciberataque provocado por una mala gestión de los recursos expuestos a Internet.[v]

Las estrategias de seguridad deben evolucionar

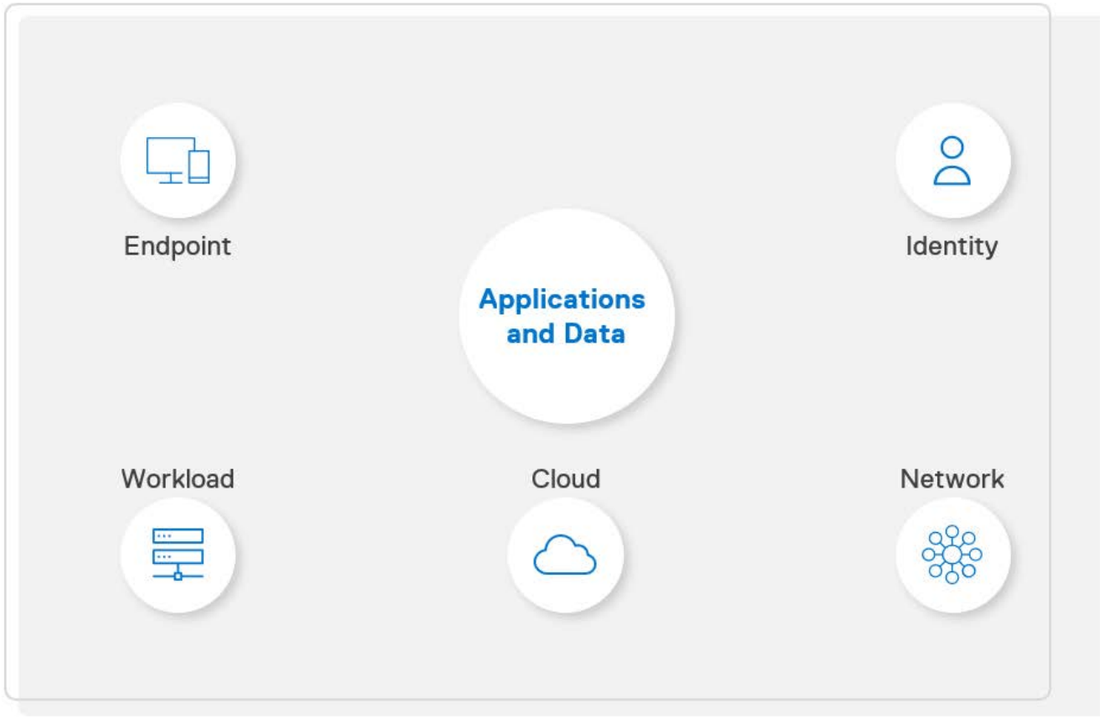
Debemos adoptar un entorno basado en la cloud. Aquí es donde entra en juego el enfoque de confianza cero.

Los modelos tradicionales de seguridad ya no funcionan. Estos son los motivos.

Para que las organizaciones tengan un buen estado de seguridad, deben abordar cinco puntos de control: puntos finales, cargas de trabajo, identidades, redes y cloud. El objetivo es proteger las aplicaciones y los datos.

Los enfoques tradicionales suelen estar divididos en silos, lo que hace que las organizaciones que los utilizan sean más susceptibles a ataques.

Siguiente...

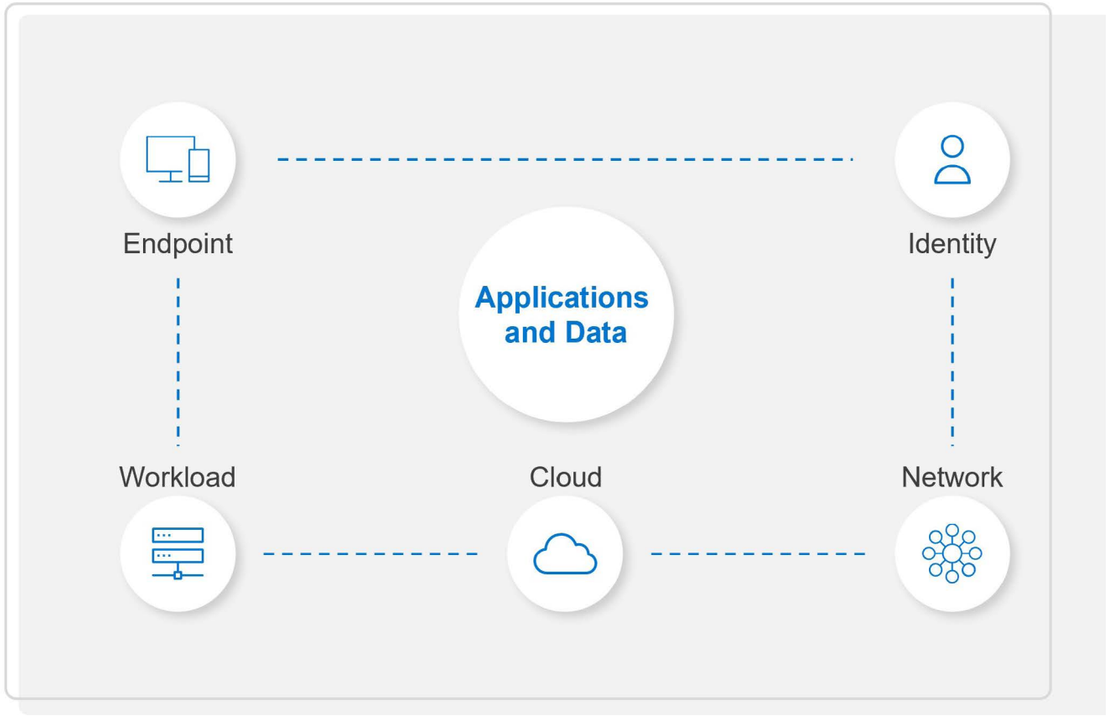


Las estrategias de seguridad deben evolucionar

Debemos adoptar un entorno basado en la cloud. Aquí es donde entra en juego el enfoque de confianza cero.

En los enfoques modernos, se ha aumentado el nivel de control y se ha mejorado la comunicación entre los puntos de control. No obstante, a medida que adoptamos un entorno cada vez más basado en el trabajo híbrido o el teletrabajo, resulta fundamental reforzar el perímetro.

Siguiente...

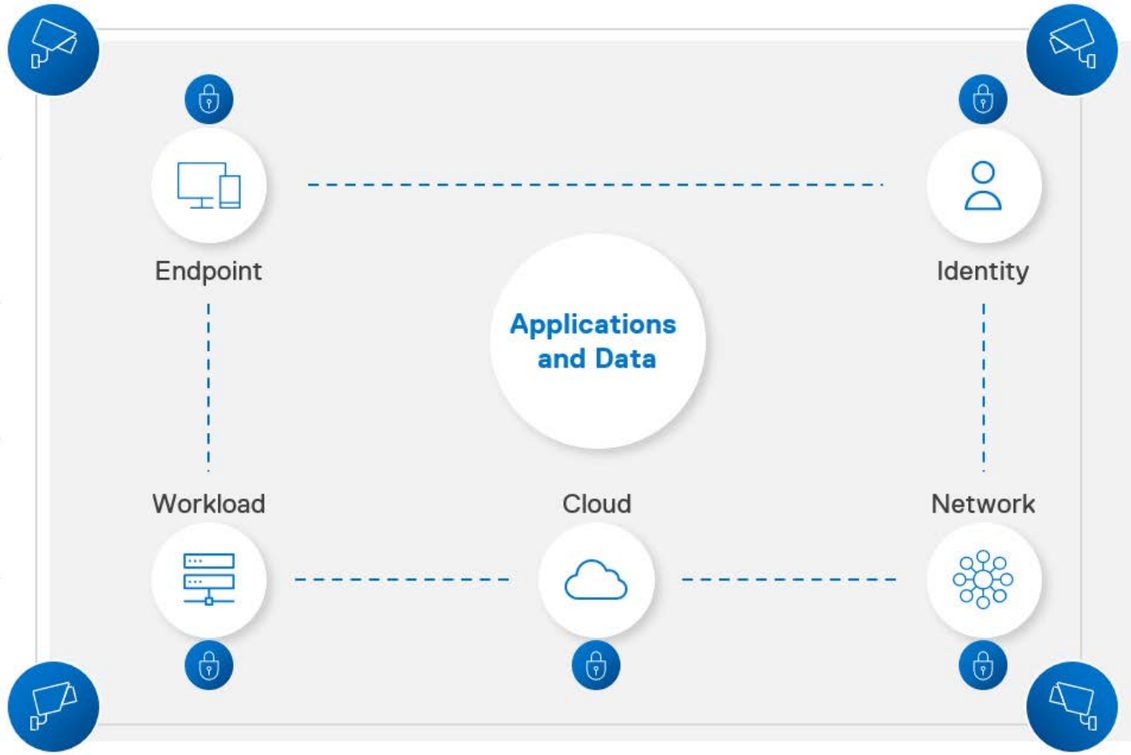


Las estrategias de seguridad deben evolucionar

Debemos adoptar un entorno basado en la cloud. Aquí es donde entra en juego el enfoque de confianza cero.

En la actualidad, los empleados trabajan desde cualquier lugar, como cafeterías, hoteles o su casa, y a menudo utilizan redes wifi poco seguras y tienen poca o ninguna conectividad con las oficinas y los centros de datos protegidos con firewalls. El esquema habitual suele ser una conexión directa entre sus dispositivos e internet, donde se conectan con servidores de archivos en la cloud y aplicaciones de software como servicio (SaaS) para trabajar con datos empresariales.

Con la creciente sofisticación de los ataques y la cantidad de vectores de ataque existentes, las estrategias tradicionales de seguridad basadas en un enfoque de confianza implícita ya no funcionan. Aquí es donde entra en juego el enfoque de confianza cero.



Fundamentos de la confianza cero

La confianza cero representa un nuevo concepto de la seguridad. Sustituye la confianza *implícita*, es decir, una vez que se han autenticado, los usuarios pueden moverse libremente por la red. La confianza cero cambia el paradigma para ofrecer a las organizaciones un control explícito del entorno de TI.

Ilustremos la confianza cero con un concepto con el que estamos muy familiarizados: la creación de protocolos de seguridad.

Imagínese que trabaja en una oficina corporativa. Cuando lo contrataron, recibió un distintivo y aprendió ciertos protocolos de seguridad. Todos los días va hasta su oficina. Hay cámaras en todos lados. Utiliza su distintivo en varios puntos de control. Cuando se sienta en el escritorio, desbloquea su equipo con una contraseña.

An employee arrives at their office building and gets their badge out to gain entry.

Siguiente...

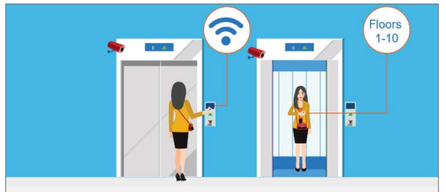
Fundamentos de la confianza cero

La confianza cero representa un nuevo concepto de la seguridad. Sustituye la confianza *implícita*, es decir, una vez que se han autenticado, los usuarios pueden moverse libremente por la red. La confianza cero cambia el paradigma para ofrecer a las organizaciones un control explícito del entorno de TI.

Ilustremos la confianza cero con un concepto con el que estamos muy familiarizados: la creación de protocolos de seguridad.

Imagínese que trabaja en una oficina corporativa. Cuando lo contrataron, recibió un distintivo y aprendió ciertos protocolos de seguridad. Todos los días va hasta su oficina. Hay cámaras en todos lados. Utiliza su distintivo en varios puntos de control. Cuando se sienta en el escritorio, desbloquea su equipo con una contraseña.

An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.

Siguiente...

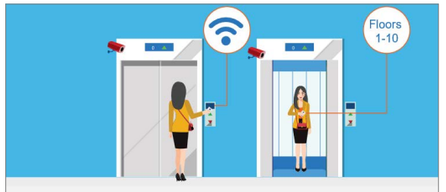
Fundamentos de la confianza cero

La confianza cero representa un nuevo concepto de la seguridad. Sustituye la confianza *implícita*, es decir, una vez que se han autenticado, los usuarios pueden moverse libremente por la red. La confianza cero cambia el paradigma para ofrecer a las organizaciones un control explícito del entorno de TI.

Ilustremos la confianza cero con un concepto con el que estamos muy familiarizados: la creación de protocolos de seguridad.

Imagínese que trabaja en una oficina corporativa. Cuando lo contrataron, recibió un distintivo y aprendió ciertos protocolos de seguridad. Todos los días va hasta su oficina. Hay cámaras en todos lados. Utiliza su distintivo en varios puntos de control. Cuando se sienta en el escritorio, desbloquea su equipo con una contraseña.

An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.

Siguiente...

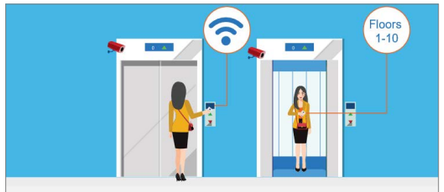
Fundamentos de la confianza cero

La confianza cero representa un nuevo concepto de la seguridad. Sustituye la confianza *implícita*, es decir, una vez que se han autenticado, los usuarios pueden moverse libremente por la red. La confianza cero cambia el paradigma para ofrecer a las organizaciones un control explícito del entorno de TI.

Ilustremos la confianza cero con un concepto con el que estamos muy familiarizados: la creación de protocolos de seguridad.

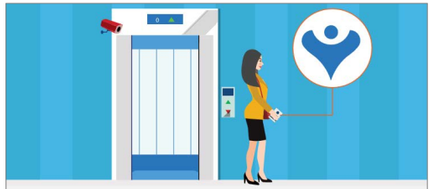
Imagínese que trabaja en una oficina corporativa. Cuando lo contrataron, recibió un distintivo y aprendió ciertos protocolos de seguridad. Todos los días va hasta su oficina. Hay cámaras en todos lados. Utiliza su distintivo en varios puntos de control. Cuando se sienta en el escritorio, desbloquea su equipo con una contraseña.

An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.

Siguiente...

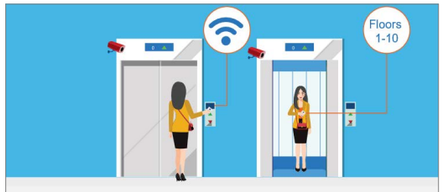
Fundamentos de la confianza cero

La confianza cero representa un nuevo concepto de la seguridad. Sustituye la confianza *implícita*, es decir, una vez que se han autenticado, los usuarios pueden moverse libremente por la red. La confianza cero cambia el paradigma para ofrecer a las organizaciones un control explícito del entorno de TI.

Ilustremos la confianza cero con un concepto con el que estamos muy familiarizados: la creación de protocolos de seguridad.

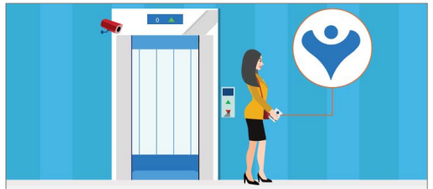
Imagínese que trabaja en una oficina corporativa. Cuando lo contrataron, recibió un distintivo y aprendió ciertos protocolos de seguridad. Todos los días va hasta su oficina. Hay cámaras en todos lados. Utiliza su distintivo en varios puntos de control. Cuando se sienta en el escritorio, desbloquea su equipo con una contraseña.

An employee arrives at their office building and gets their badge out to gain entry.

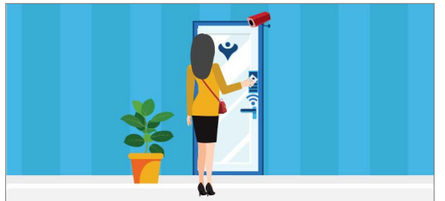


They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.



They swipe their ID card to gain entry to their suite.

Siguiente...

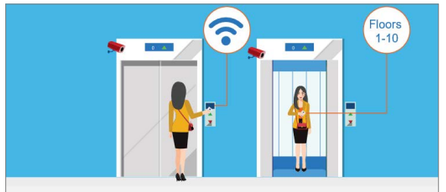
Fundamentos de la confianza cero

La confianza cero representa un nuevo concepto de la seguridad. Sustituye la confianza *implícita*, es decir, una vez que se han autenticado, los usuarios pueden moverse libremente por la red. La confianza cero cambia el paradigma para ofrecer a las organizaciones un control explícito del entorno de TI.

Ilustremos la confianza cero con un concepto con el que estamos muy familiarizados: la creación de protocolos de seguridad.

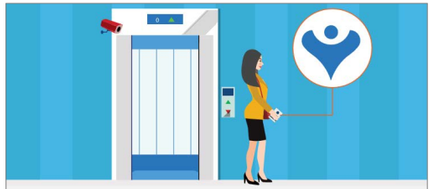
Imagínese que trabaja en una oficina corporativa. Cuando lo contrataron, recibió un distintivo y aprendió ciertos protocolos de seguridad. Todos los días va hasta su oficina. Hay cámaras en todos lados. Utiliza su distintivo en varios puntos de control. Cuando se sienta en el escritorio, desbloquea su equipo con una contraseña.

An employee arrives at their office building and gets their badge out to gain entry.

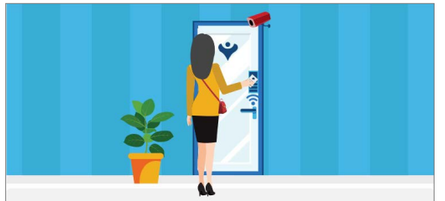


They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.



They swipe their ID card to gain entry to their suite.

The employee arrives at their desk and unlocks their computer using a password.

Siguiente...

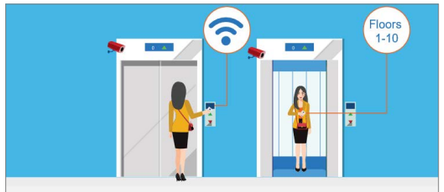
Fundamentos de la confianza cero

Así es como funciona la confianza cero.

El día que empezó a trabajar, su empleador lo identificó. Todos los accesos que ha solicitado desde entonces se han verificado para proteger los recursos de la organización (usuarios, datos, etc.). Para añadir una capa adicional de seguridad, los guardas de seguridad vigilan todos los movimientos dentro del edificio desde sus monitores. Se investiga cualquier comportamiento extraño, por ejemplo, intentar acceder a una estancia en la que no debería entrar.

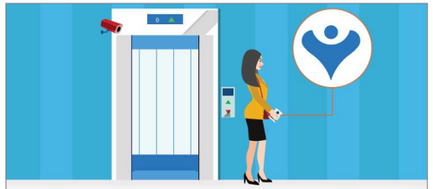
Hoy en día, es más frecuente que nunca encontrar usuarios, dispositivos, aplicaciones y datos fuera de las redes corporativas a las que pertenecen. Como consecuencia, la identidad de los usuarios se ha convertido en un punto ciego, y la exposición de la identidad es el elemento clave de la mayoría de vulneraciones. El curso de confianza cero lo soluciona.

An employee arrives at their office building and gets their badge out to gain entry.

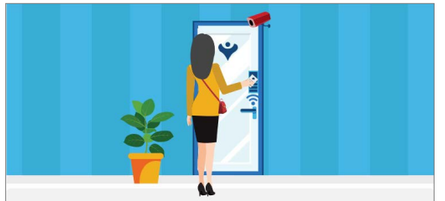


They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.



They swipe their ID card to gain entry to their suite.

The employee arrives at their desk and unlocks their computer using a password.

Activación de los principios de confianza cero

La seguridad de puntos finales es una parte fundamental de la transformación basada en la confianza cero.

Para activar una buena estrategia de confianza cero, debe proteger los puntos finales.

Según el marco MITRE ATT&CK®, en la actualidad, hay nueve "técnicas de acceso inicial" que utilizan los atacantes para obtener acceso a las redes (*consulte la ilustración*)[vi]. Los estudios han demostrado que, en nuestro mundo basado en la cloud, las defensas tradicionales no son capaces de proteger los puntos finales. Los atacantes solo necesitan un único punto de acceso. En el caso de los puntos finales, los atacantes pueden explotar docenas de vulnerabilidades en todo el ciclo de vida de un dispositivo.

A medida que crece la cantidad de dispositivos en una red, los puntos finales se convierten en un vector de ataque cada vez más amplio.

Las políticas de seguridad de un modelo de confianza cero definen lo "bueno conocido" con un nivel de detalle explícito; todo lo demás se bloquea. De esta manera, la gestión de amenazas se centra en detectar todo aquello que se desvíe de lo bueno conocido, marcar el comportamiento poco habitual y desencadenar la acción correspondiente para corregir cualquier posible amenaza.

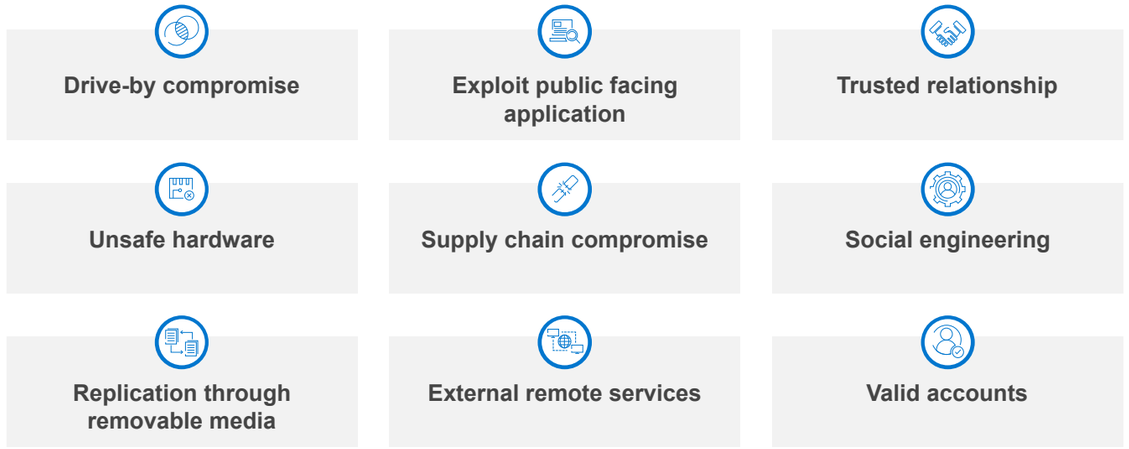


Ilustración 1/3

Activación de los principios de confianza cero

La seguridad de puntos finales es una parte fundamental de la transformación basada en la confianza cero.

Para activar una buena estrategia de confianza cero, debe proteger los puntos finales.

Según el marco MITRE ATT&CK®, en la actualidad, hay nueve "técnicas de acceso inicial" que utilizan los atacantes para obtener acceso a las redes (*consulte la ilustración*)[vi]. Los estudios han demostrado que, en nuestro mundo basado en la cloud, las defensas tradicionales no son capaces de proteger los puntos finales. Los atacantes solo necesitan un único punto de acceso. En el caso de los puntos finales, los atacantes pueden explotar docenas de vulnerabilidades en todo el ciclo de vida de un dispositivo.

A medida que crece la cantidad de dispositivos en una red, los puntos finales se convierten en un vector de ataque cada vez más amplio.

Las políticas de seguridad de un modelo de confianza cero definen lo "bueno conocido" con un nivel de detalle explícito; todo lo demás se bloquea. De esta manera, la gestión de amenazas se centra en detectar todo aquello que se desvíe de lo bueno conocido, marcar el comportamiento poco habitual y desencadenar la acción correspondiente para corregir cualquier posible amenaza.

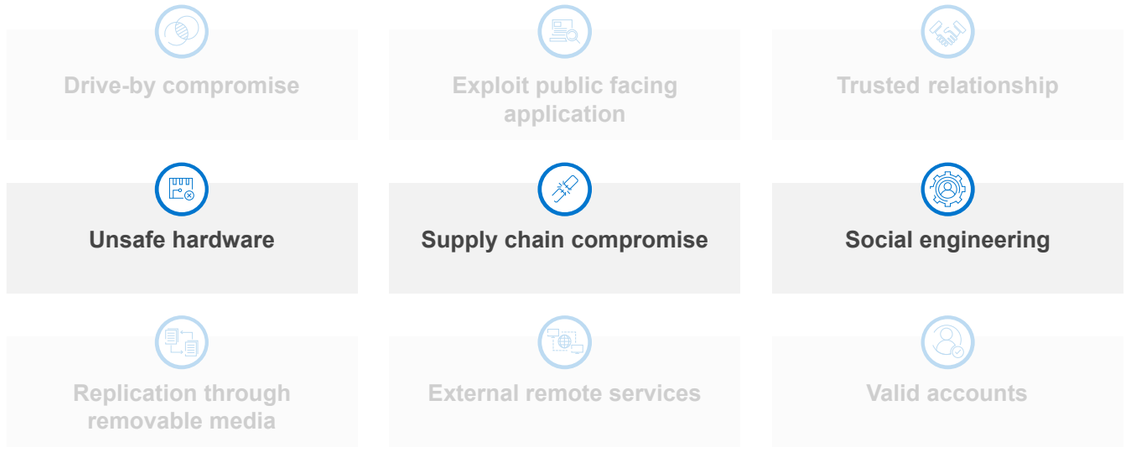


Ilustración 2/3

Activación de los principios de confianza cero

La seguridad de puntos finales es una parte fundamental de la transformación basada en la confianza cero.

Para activar una buena estrategia de confianza cero, debe proteger los puntos finales.

Según el marco MITRE ATT&CK®, en la actualidad, hay nueve "técnicas de acceso inicial" que utilizan los atacantes para obtener acceso a las redes (*consulte la ilustración*)[vi]. Los estudios han demostrado que, en nuestro mundo basado en la cloud, las defensas tradicionales no son capaces de proteger los puntos finales. Los atacantes solo necesitan un único punto de acceso. En el caso de los puntos finales, los atacantes pueden explotar docenas de vulnerabilidades en todo el ciclo de vida de un dispositivo.

A medida que crece la cantidad de dispositivos en una red, los puntos finales se convierten en un vector de ataque cada vez más amplio.

Las políticas de seguridad de un modelo de confianza cero definen lo "bueno conocido" con un nivel de detalle explícito; todo lo demás se bloquea. De esta manera, la gestión de amenazas se centra en detectar todo aquello que se desvíe de lo bueno conocido, marcar el comportamiento poco habitual y desencadenar la acción correspondiente para corregir cualquier posible amenaza.

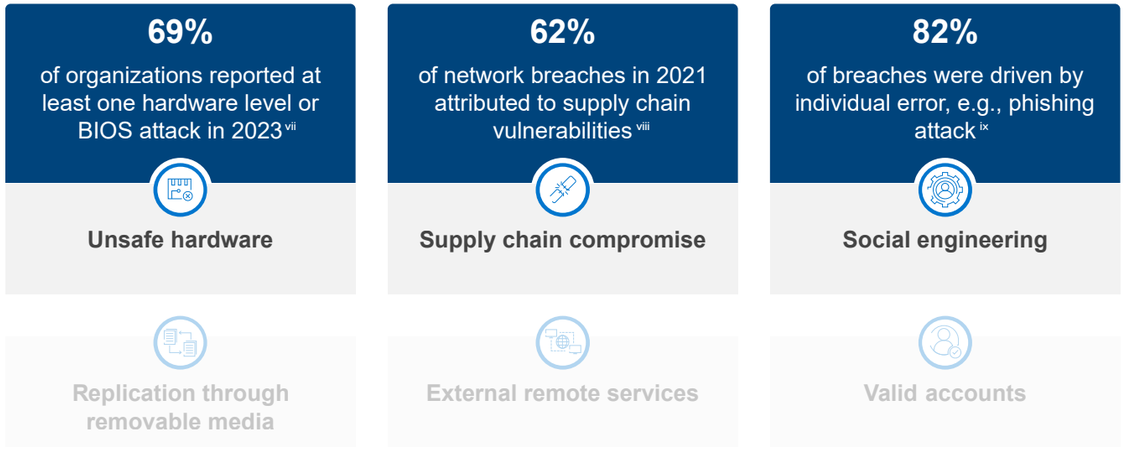


Ilustración 3/3

Tres recomendaciones para prepararse para la confianza cero

Prepare su organización para una correcta transformación basada en la confianza cero.

1

Establezca los controles y las políticas adecuados para respaldar las prioridades empresariales

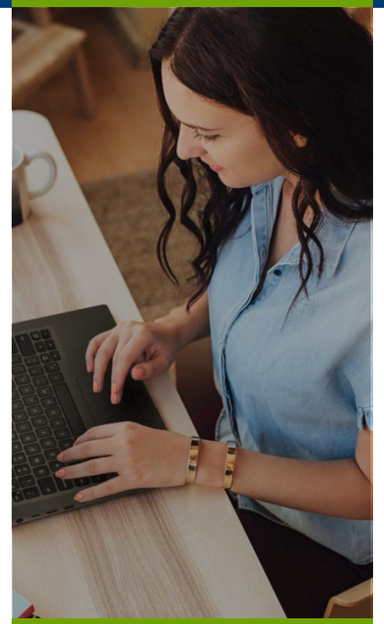
Los motores y la gestión de políticas son fundamentales para implementar un buen plan de confianza cero. Pero ninguna organización tiene un presupuesto ilimitado para la seguridad, así que el primer paso es determinar sus prioridades. ¿Cuáles son los recursos y la propiedad intelectual más importantes que trata de proteger? Valore esa superficie de ataque en comparación con el riesgo que puede permitirse su organización.

Luego, revise las políticas y los controles empleados. En la actualidad, los riesgos se generan en el mundo basado en la cloud en el que vivimos. ¿Tiene esto en cuenta su motor de políticas?

Si aplica políticas para controlar el acceso a sus recursos más valiosos, podrá ampliar después su alcance.

MÁS INFORMACIÓN

Para obtener más información, *vea este vídeo* donde ciberexpertos de Dell hablan sobre los riegos principales de seguridad a los que se enfrentan las organizaciones hoy en día.



Con más usuarios, aplicaciones, datos y dispositivos fuera de las redes corporativas que nunca, el **82 %** de los responsables de la toma de decisiones de seguridad de tecnología informática afirman que han tenido que reevaluar sus políticas de seguridad[x].

Tres recomendaciones para prepararse para la confianza cero

Prepare su organización para una correcta transformación basada en la confianza cero.

2 Empiece por proteger los dispositivos

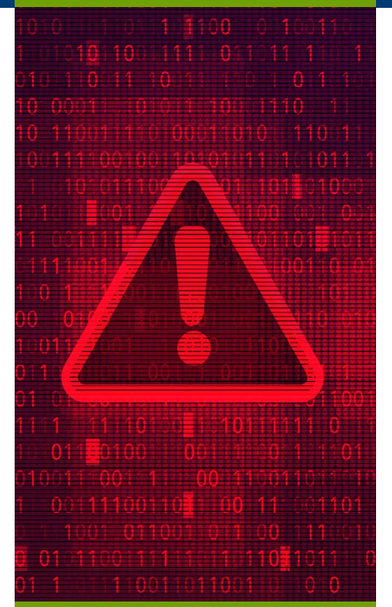
Desarrolle la planificación de confianza cero sobre unas bases sólidas. Refuerce sus defensas con dispositivos diseñados y desarrollados con la seguridad en mente. Esto incluye:

A. **Protecciones basadas en hardware y firmware** que garanticen la seguridad de la pila de puntos finales y faciliten la visibilidad (por ejemplo, se detecta que un BIOS ha quedado expuesto y se avisa al departamento de tecnología informática). Equipe su organización con tecnologías que verifiquen la identidad en cada nueva solicitud de acceso, con el menor impacto posible en la productividad del empleado.

B. **Protecciones de la cadena de suministros y controles de integridad** en cada paso del ciclo de vida de los PC. Como hemos visto en los últimos años, los ataques en la cadena de suministros pueden ser devastadores. Para implantar una buena arquitectura de confianza cero, la autenticación, la verificación y la supervisión deben comenzar en la cadena de suministro. Trabaje con proveedores que 1) empleen prácticas seguras y 2) le permitan validar la integridad de los dispositivos, desde el momento de la compra hasta la entrega, pasando por la fabricación.

MÁS INFORMACIÓN

Si necesita más información sobre procedimientos recomendados para la seguridad de los dispositivos, lea el documento técnico de Dell e Intel Achieving Pervasive Security Above and Below the OS.



En **2021**, una empresa de administración de tecnología informática distribuyó un ataque de ransomware al menos a **1500** clientes[xi].

Tres recomendaciones para prepararse para la confianza cero

Prepare su organización para una correcta transformación basada en la confianza cero.

3

Trate de conseguir una integración e interoperabilidad perfectas en todo su ecosistema

Para conseguir un buen estado de seguridad, en términos generales, es fundamental contar con tres elementos:

A. Integración de todas las defensas en el ecosistema de tecnología informática.

B. Visibilidad en tiempo real.

C. Capacidad para actuar siempre que sea necesario.

En nuestro mundo basado en la cloud, en el que la más mínima de las vulnerabilidades que no se detecte puede convertirse en una pesadilla, es importante que todos los sistemas reconozcan posibles amenazas *y* estén configurados para tomar las medidas necesarias.

¿Sus sistemas están integrados o funcionan en silos? ¿Su motor de políticas es capaz de desencadenar un flujo de trabajo específico cuando un administrador de tecnología informática recibe una alerta de que hay un BIOS dañado en la red? En un entorno integrado, las automatizaciones deberían poner en cuarentena cualquier BIOS que pueda estar en riesgo, limitar todos los accesos adicionales y ejecutar los parches necesarios, todo ello de forma inmediata.

¿Tiene visibilidad de todos sus puntos finales? Lo ideal es contar con un buen sistema de telemetría en todas las capas, desde la cadena de suministros (por ejemplo, muelles de carga) hasta el firmware (como alertas de alteraciones en el BIOS).

Pero la eficacia de ese sistema de telemetría dependerá de la calidad de sus integraciones. ¿Puede tomar medidas en función de sus datos? Es importante contar con los recursos adecuados, como empleados cualificados en ciberseguridad, para saber interpretar los datos y programar flujos de trabajo que aborden los problemas.

El 41 % de las organizaciones están implementando un enfoque de confianza cero[xii]

DELL Technologies

Nociones clave

El futuro de la seguridad es la confianza cero.

- Con el avance hacia el futuro del trabajo, se multiplicaron los vectores de ataque.
- Es inevitable que se produzcan vulneraciones. Lo importante es minimizar la superficie de ataque con defensas que nos preparen para el peor de los casos.
- La confianza cero representa un nuevo concepto de la seguridad que ofrece a las organizaciones control explícito sobre el entorno de TI.
- Las protecciones de puntos finales que activan principios de confianza cero son fundamentales para mantener unas bases modernas y seguras.
- Identifique los recursos más importantes para definir las prioridades al desarrollar su arquitectura de confianza cero.
- Adquiera dispositivos de proveedores que ofrezcan protecciones integradas e inviertan significativamente en controles para su cadena de suministros.
- Evalúe la seguridad y la interoperabilidad de la tecnología informática. Siga integrando flujos de trabajo que refuercen su estado de seguridad.

Un paso hacia delante

La seguridad es un tema abrumador para organizaciones de todos los tamaños. Colabore con un socio de tecnología y seguridad con experiencia que le ayude a simplificar su transformación basada en la confianza cero.

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.

Contacte con nosotros: global.security.sales@dell.com
Visítenos: Dell.com/Endpoint-Security
Síganos: LinkedIn @DellTechnologies | Twitter @DellTech

DELL Technologies

[i] Cybersecurity Almanac, 2.ª edición. Cybersecurity Ventures, 2022, https://cybersecurityventures.com/cybersecurity-almanac-2022/.

[ii] Ponemon Institute e IBM, Cost of a Data Breach Report, 2024, https://www.ibm.com/security/data-breach

[iii] American College of Cardiology, You Will Be Hacked. Plan Now: Cybersecurity in Health Care, 2021, https://www.acc.org/Latest-in-Cardiology/Articles/2021/11/01/01/42/Feature-You-Will-Be-Hacked-Plan-Now-Cybersecurity-in-Health-Care.

[iv] Ponemon Institute e IBM, Cost of a Data Breach Report, 2024, https://www.ibm.com/security/data-breach

[v] ESG Complete Survey Results, Security Hygiene and Posture Management, 2022, https://www.esg-global.com/research/esg-complete-survey-results-security-hygiene-and-posture-management.

[vi] MITRE ATT&CK, https://attack.mitre.org/tactics/TA0001/.

[vii] Futurum Group, Endpoint Security Trends, 2023. https://www.delltechnologies.com/asset/en-us/solutions/business-solutions/industry-market/futurum-group-endpoint-security-trends-research-report.pdf

[viii] Verizon Data Breach Investigations Report, 2022, https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/.

[ix] Verizon Data Breach Investigations Report, 2022, https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/.

[x] Absolute Endpoint Risk Report, 2021, https://www.absolute.com/go/reports/endpoint-risk-report/.

[xi] TechTarget, 2021, https://www.techtarget.com/searchsecurity/news/252503605/Kaseya-1500-organizations-affected-by-REvil-attacks.

[xii] Ponemon Institute e IBM, Cost of a Data Breach Report, 2022, https://www.ibm.com/security/data-breach.