ABSOLUTE®

2023 ÍNDICE DE RESILIENCIA

Una Falsa Sensación de Seguridad Pone en Peligro a las Empresas Digitales

Resumen Ejecutivo

En el cuarto año de nuestra investigación recurrente sobre las tendencias de resiliencia de los endpoints, analizamos datos anónimos de 14 millones de dispositivos habilitados por Absolute, activos en organizaciones de clientes en América del Norte, Europa y APAC, así como datos e información de fuentes terceras confiables.

Este reporte examina el estado de la resiliencia en el nuevo modelo de trabajo “desde cualquier lugar", evaluando su complejidad, continuidad y postura de cumplimiento. Los hallazgos confirman que, a pesar de la creencia de larga data de que el despliegue de más soluciones de seguridad resultará en una mayor protección contra amenazas, la verdad del asunto es muy diferente.

Como resultado, las organizaciones están buscando formas de conectar de manera segura a sus empleados con las redes y recursos corporativos. Esto está impulsando una nueva tendencia de *cumplir para conectar* que equilibra la seguridad y la ciberresiliencia para asegurar que sus empleados puedan trabajar con confianza y seguir trabajando, sin importar dónde encuentren el riesgo.

Lea el Índice de Resiliencia 2023 para aprender cómo:

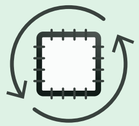
1. Evaluar la complejidad en su entorno y evaluar su postura de ciberresiliencia.
2. Obtener una comprensión de las prácticas de conectividad y cumplimiento necesarias hoy en día.
3. Aprender cómo Absolute hace que su seguridad existente funcione.

Asegurando la Fuerza Laboral Remota e Híbrida

A medida que las empresas y los empleados se ajustan a las normas post-pandémicas, un punto se vuelve claro: el trabajo híbrido ha llegado para quedarse y ya no es solo un beneficio para el empleado, sino una expectativa. Según Gartner1 para finales de 2023, el 48% de los trabajadores estarán trabajando de manera híbrida y completamente remota (en comparación con el 27% en 2019), con el 39% de esos empleados trabajando de manera híbrida, lo que representa un aumento del 12% en 2020.

1 *Gartner; Análisis de Pronóstico: Empleados del Conocimiento, Estilos de Trabajo Híbridos, Totalmente Remotos y en el Lugar de Trabajo, a Nivel Mundial, Enero de 2023*

WINDOWS 10
EN LA MAYORÍA DE LOS DISPOSITIVOS EMPRESARIALES



VERSIONES DE S.O. Y PARCHES

800+
COMPILACIONES/ PARCHES

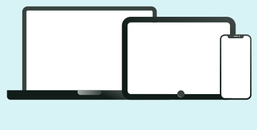
14
VERSIONES

Fuente: Datos de Telemetría de Dispositivos Absolute

El Panorama es Desordenado

El nuevo modelo de trabajo desde cualquier lugar está poniendo una tensión en los equipos de TI y de seguridad, generando una complejidad sin precedentes. Los empleados que cambian entre redes corporativas y fuera de la corporación están creando desafíos de visibilidad y control, lo cual está afectando la habilidad de estos equipos para diagnosticar y remediar problemas del usuario final y minimizar los riesgos de ciberseguridad. Además, tienen que lidiar con una amplia mezcla de redes, hardware, versiones del sistema operativo (SO) y parches.

Por ejemplo, más del 80% de los dispositivos utilizan el sistema operativo Microsoft® Windows®, con la gran mayoría en Windows 10. A primera vista, esto podría parecer homogéneo y fácil de manejar; sin embargo, la realidad es que los profesionales de TI están luchando para mantener los endpoints de sus empleados actualizados con 14 versiones diferentes y más de 800 compilaciones y parches presentes.



DISPOSITIVOS

> 80% **DISPOSITIVOS WINDOWS** EN ORGANIZACIONES MUY GRANDES

< 20% **CHROMEBOOKS** EN ORGANIZACIONES MUY GRANDES

LA MAYOR MOVILIDAD DE DISPOSITIVOS ABRE NUEVAS VULNERABILIDADES

4
UBICACIONES
DE DISPOSITIVOS EMPRESARIALES

Las múltiples ubicaciones de los empleados remotos añaden aún más a este ya significativo nivel de complejidad. Ahora están realizando trabajos importantes en redes que sus organizaciones no poseen ni controlan, lo cual incrementa dramáticamente la exposición al riesgo de una organización. E incluso dentro de las ubicaciones, los usuarios pueden cambiar con frecuencia entre dispositivos y redes, desde un portátil en el Wi-Fi de su cafetería favorita hasta un dispositivo móvil en la red celular de un operador, todo mientras intentan llevar a cabo una productiva reunión en línea en el camino de regreso a casa, por ejemplo. Por lo tanto, no es sorprendente que el número promedio de ubicaciones de dispositivos empresariales de los clientes de Absolute haya crecido un 15% año tras año, con un promedio de cuatro ubicaciones por dispositivo en febrero de 2023.

15%
CRECIMIENTO DE UBICACIONES DE DISPOSITIVOS EMPRESARIALES AÑO TRAS AÑO

Fuente: Datos de Telemetría de Dispositivos Absolute

EN LOS DISPOSITIVOS EMPRESARIALES HAY

67 APLICACIONES

DE TODO TIPO (PRODUCTIVIDAD, SEGURIDAD, APLICACIONES NO LABORALES, ETC.) EN PROMEDIO

10%

DE LOS DISPOSITIVOS EMPRESARIALES TIENEN

100 APLICACIONES

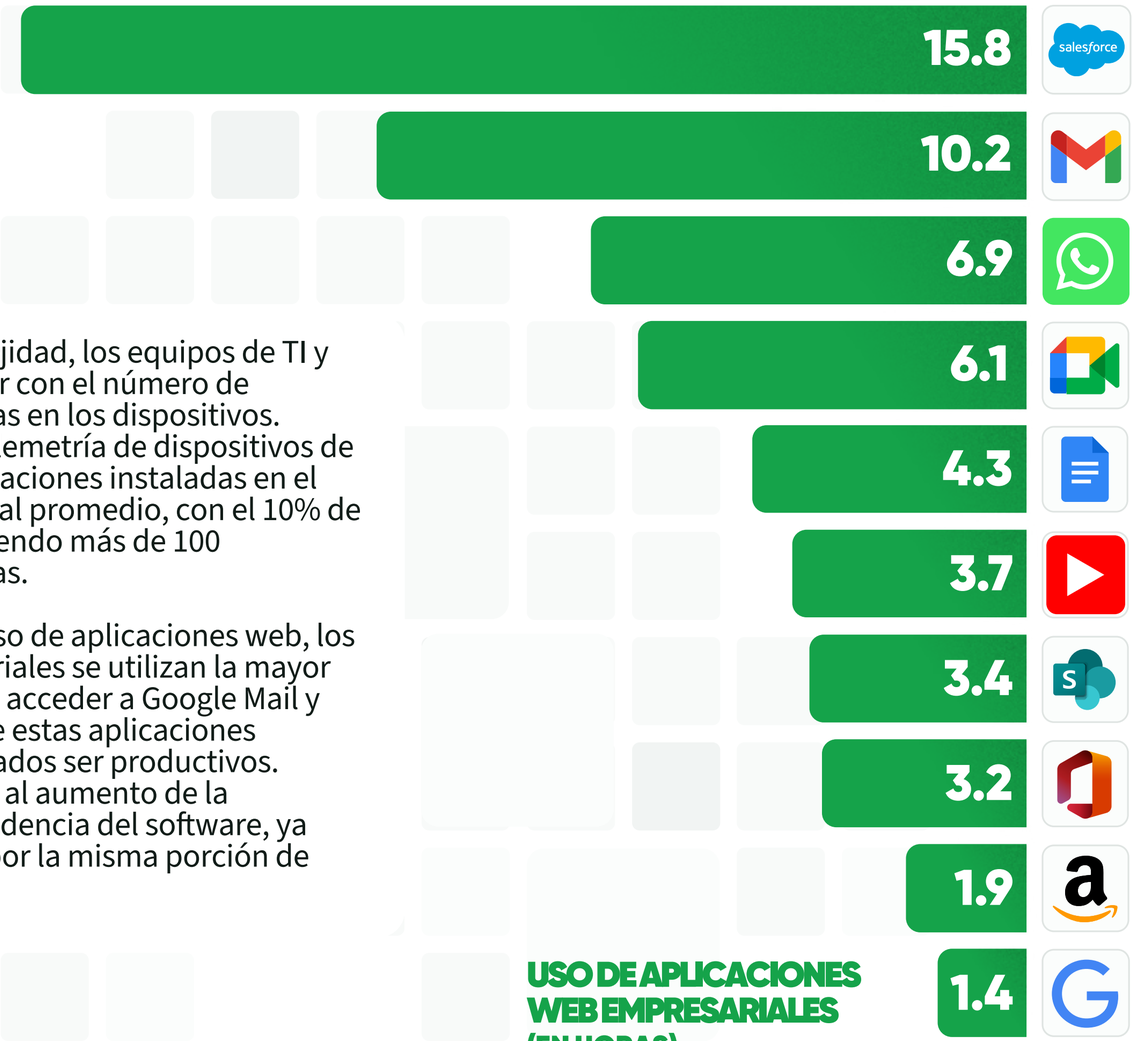
O MÁS

FUENTE:
Datos de Telemetría de Dispositivos Absolute

Sumando a la complejidad, los equipos de TI y seguridad deben lidiar con el número de aplicaciones instaladas en los dispositivos. Según los datos de telemetría de dispositivos de Absolute, hay 67 aplicaciones instaladas en el dispositivo empresarial promedio, con el 10% de esos dispositivos teniendo más de 100 aplicaciones instaladas.

Cuando se trata del uso de aplicaciones web, los dispositivos empresariales se utilizan la mayor parte del tiempo para acceder a Google Mail y Salesforce. Muchas de estas aplicaciones permiten a los empleados ser productivos. También contribuyen al aumento de la complejidad y la decadencia del software, ya que todas compiten por la misma porción de memoria.

USO DE APLICACIONES WEB EMPRESARIALES (EN HORAS)



TODO ESTO SUBRAYA EL PAISAJE DE **COMPLEJIDAD**

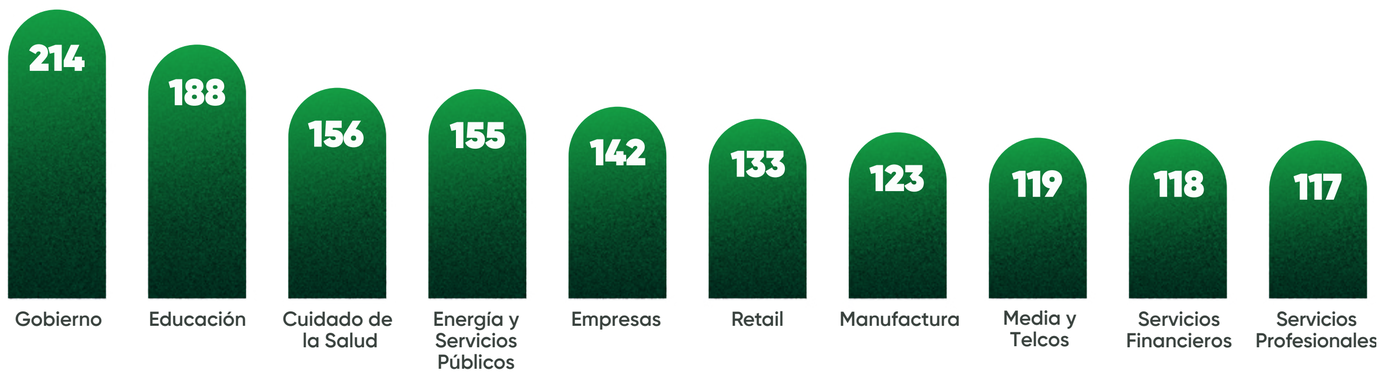
Además, el gran número de aplicaciones instaladas en los dispositivos empresariales, así como la variedad de versiones y compilaciones del sistema operativo, dificultan que los equipos de TI y seguridad mantengan esas aplicaciones o las parcheen. Esta situación impacta negativamente en su capacidad para minimizar la exposición a vulnerabilidades conocidas.

Esto supone que TI está intentando gestionar proactivamente hasta 50 o 100 aplicaciones. Más probablemente, están gestionando un subconjunto mucho menor y el resto son "aplicaciones en sombra" que en realidad no están siendo gestionadas o parcheadas pero que pueden seguir funcionando en segundo plano. Esto expone a las organizaciones a mayores riesgos y consume incluso más recursos del sistema.

EDAD DE LOS PARCHES DE WINDOWS 10

DÍAS POR VERTICAL

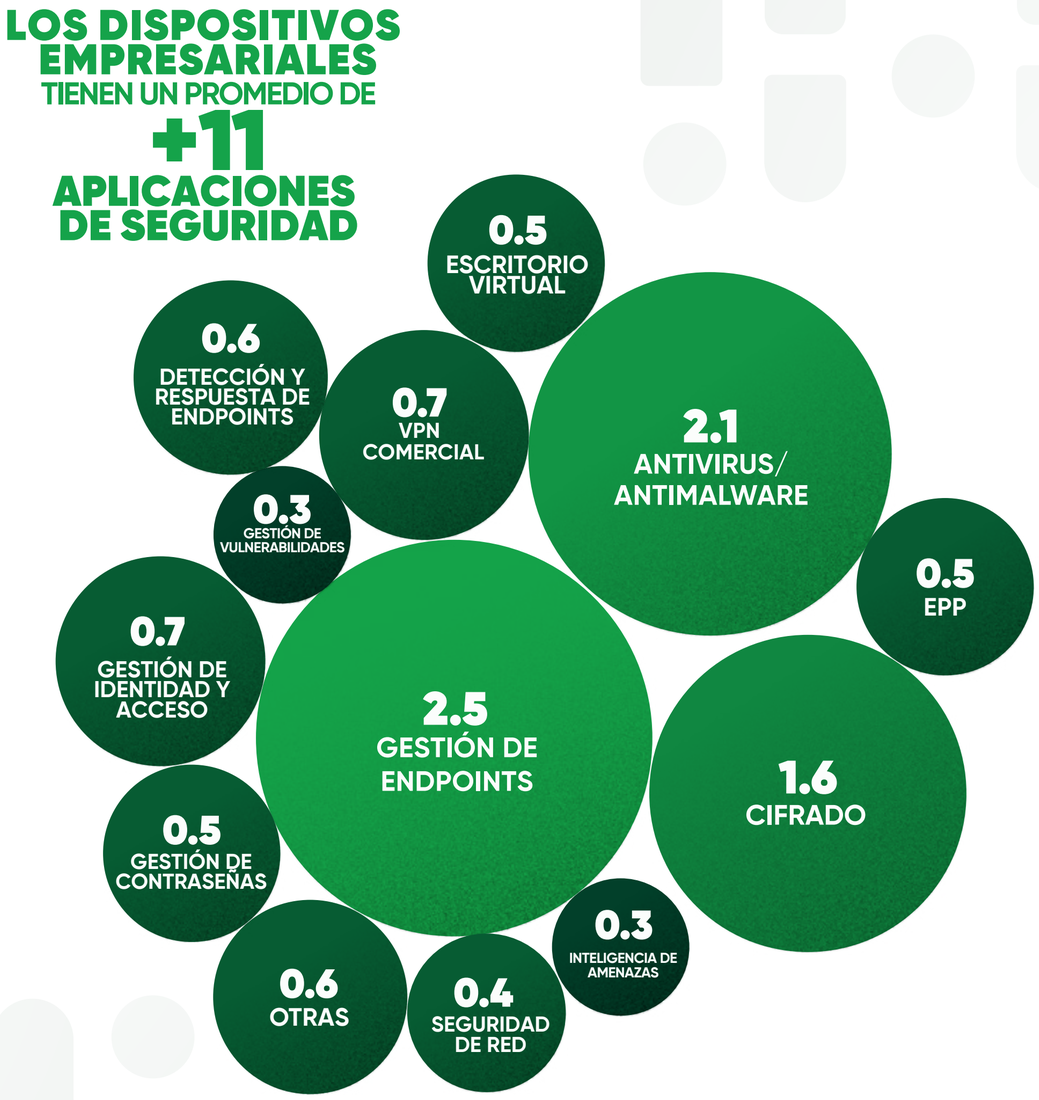
LOS PEORES INFRACTORES SON LA EDUCACIÓN Y EL GOBIERNO



DÍAS POR TAMAÑO

LAS CUENTAS MUY GRANDES SON LAS PEORES INFRACTORES

Fuente: Datos de Telemetría de Dispositivos Absolute



Una Falsa Sensación de Seguridad

Una creencia largamente sostenida entre las organizaciones empresariales es que cuanto más gastas en tecnología de TI y seguridad, más fuerte será tu postura de seguridad. Así que, para enfrentar un nuevo desafío o amenaza, compramos más soluciones. Estamos gastando decenas de miles de millones de dólares anualmente solo en seguridad de endpoints. A su vez, no es sorprendente que haya más de 11 aplicaciones de seguridad instaladas en el portátil promedio proporcionado por el trabajo.

Notablemente, los dispositivos empresariales tienen en promedio más de una aplicación de seguridad instalada para lidiar con la gestión de endpoints, antivirus, anti-malware y cifrado, que son considerados controles de seguridad esenciales por muchos estándares de la industria (por ejemplo, ISO/IEC 27001, NIST CSF, PCI DSS, GDPR) y regulaciones gubernamentales (por ejemplo, HIPAA, HITECH, FISMA). Esto indica que muchas organizaciones carecen de información sobre el inventario de software en toda su flota de dispositivos, están ejecutando más software del necesario, o simplemente creen que cuantas más herramientas desplieguen, más seguros estarán.

Fuente: Datos de Telemetría de Dispositivos Absolute

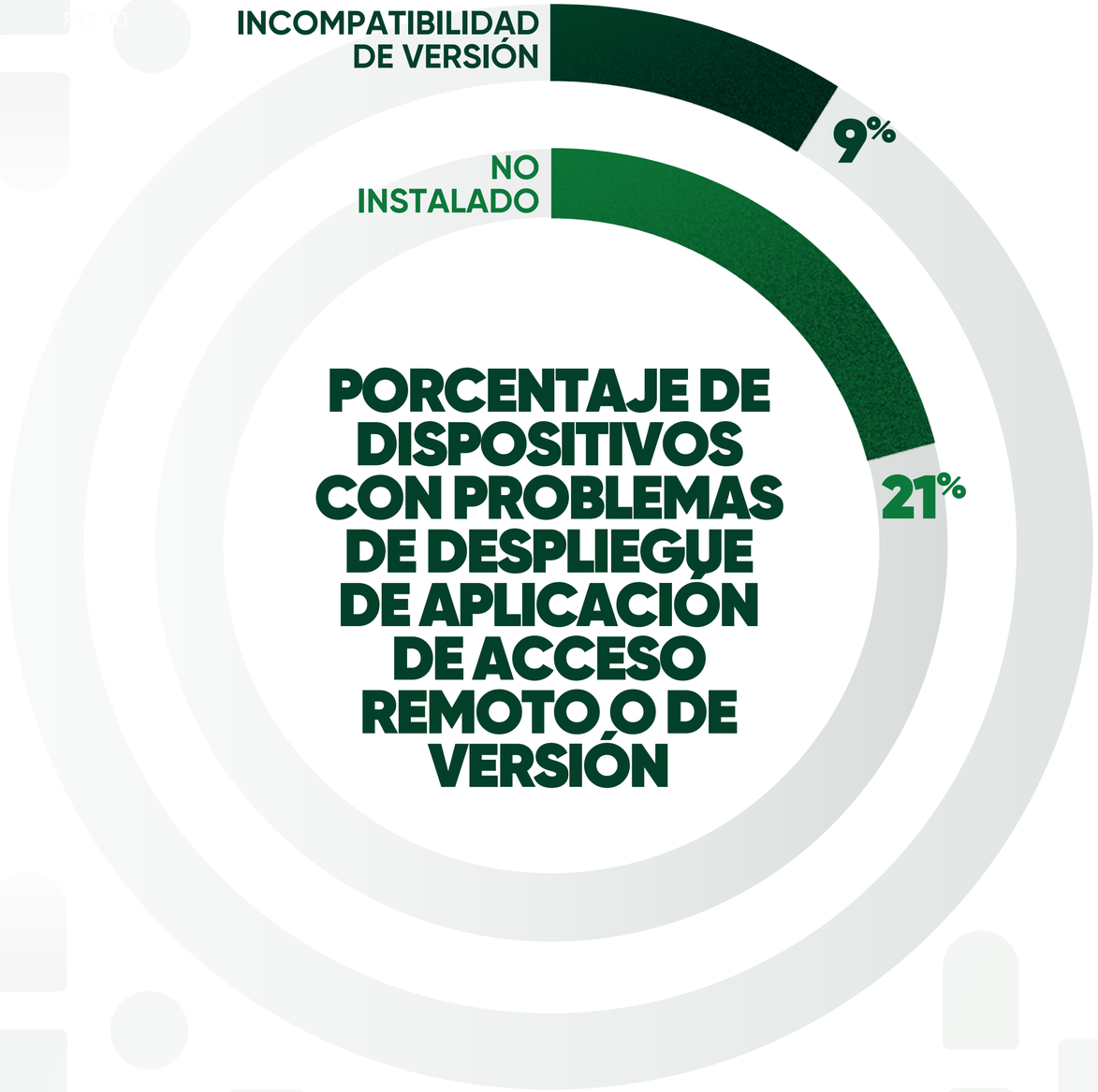
La Eficacia de las Aplicaciones de Seguridad Varía Ampliamente

Desafortunadamente, no puedes asegurar y garantizar la eficacia de lo que no puedes ver. La postura de seguridad de una empresa es tan fuerte como los controles de seguridad que la respaldan. Si se deja sin control, cada control de seguridad desplegado en el endpoint representa una vulnerabilidad potencial si no está funcionando y capaz de realizar su trabajo. La decadencia común, la eliminación no intencional o las acciones maliciosas afectan la integridad y la eficacia de las aplicaciones de seguridad y las herramientas de gestión de endpoints.

Algunos podrían sugerir que garantizar la coexistencia pacífica debería recaer en los propios proveedores de soluciones. Pero cuando se considera el número de permutaciones basadas en el número de herramientas, el número de versiones y compilaciones para cada una de ellas, y el número de versiones y compilaciones del sistema operativo, es imposible que cualquier proveedor de soluciones lo haga. Y esto sin mencionar el constante flujo de amenazas por parte de actores maliciosos a las que también deben mantenerse al tanto para proteger a sus clientes finales.

Los profesionales de TI y seguridad están de acuerdo en que herramientas de seguridad como la Plataforma de Protección de Endpoints (EPP), Detección y Respuesta de Endpoints (EDR), antivirus, etc., son esenciales para defenderse contra los ataques, y por lo tanto, siempre deben estar en funcionamiento y actualizadas. Los datos de Absolute muestran que del 25 al 30% de los dispositivos tenían controles de seguridad en mal estado.

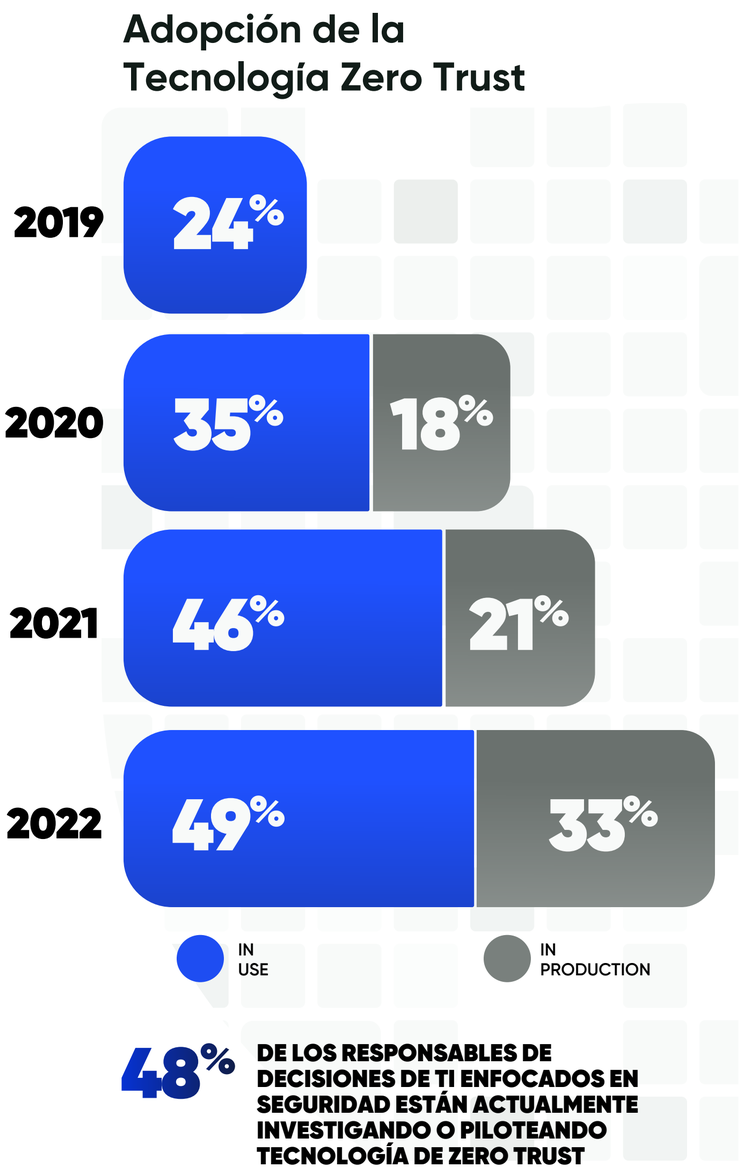
Fuente: Datos de Telemetría de Dispositivos Absolute



No podemos olvidarnos de las aplicaciones de acceso remoto y de Zero Trust Network Access (ZTNA, por sus siglas en inglés), ya que se han convertido en el sustento de las empresas.
Los trabajadores móviles requieren un acceso seguro, pero sin fricciones, a los recursos corporativos que hoy en día pueden residir en cualquier lugar. Es por eso que estas tecnologías se han convertido en la intersección entre los endpoints y las redes corporativas, ya que estamos viendo una fuerte adopción dentro de la empresa. A su vez, es esencial que la integridad de estas herramientas no sea manipulada.

Sin embargo, nuestros datos muestran que estas herramientas críticas no están instaladas o no se encuentran en el nivel de versión requerido en más del 30% de los dispositivos, exponiendo a las organizaciones a riesgos innecesarios.

Fuente: Datos de Telemetría de Dispositivos Absolute



Resiliencia Cibernética: la Nueva Estrategia para Enfrentar Amenazas Aumentadas

Considerando las implicancias de los hallazgos anteriores, es evidente que ya no es una cuestión de 'si' sino de 'cuándo' una organización sufrirá una brecha. Esto significa que en lugar de centrar los esfuerzos exclusivamente en prevenir un ataque, es importante desarrollar un plan para reducir el impacto cuando un ataque exitoso ocurre. Por eso, muchas organizaciones de pensamiento avanzado están adoptando una nueva estrategia para hacer frente a las crecientes amenazas cibernéticas de hoy en día, llamada resiliencia cibernética.

Primer Paso: Zero Trust

La aceleración de la adopción de la nube y el cambio hacia el trabajo desde cualquier lugar han disminuido la defensa perimetral común, dejando a las organizaciones más vulnerables que nunca. Un primer paso en esta nueva era es aplicar los principios de Zero Trust, que va de la mano con la resiliencia cibernética.
Forrester define a Zero Trust como un modelo de seguridad de la información que niega por defecto el acceso a aplicaciones y datos. La prevención de amenazas se logra concediendo acceso a redes y cargas de trabajo utilizando políticas informadas por la verificación continua, contextual y basada en el riesgo de los usuarios y sus dispositivos. El Zero Trust aboga por tres principios básicos: todas las entidades son desconfiadas por defecto, se aplica el acceso de mínimo privilegio y se implementa una vigilancia de seguridad integral.

Las arquitecturas y tecnologías de Zero Trust se están incorporando de manera constante a la seguridad corporativa, y este finalmente está reemplazando el antiguo enfoque centrado en el perímetro. En un estudio de Prioridades de Seguridad 2022 por Foundry (anteriormente IDG Communications), el 32% de los encuestados dijo que están investigando tecnologías de Zero Trust y el 16% mencionó que están "piloteándolas"[2].

[2]Fuente: Foundry (anteriormente IDG Communications), Estudio de Prioridades de Seguridad, 2020 - 2022

EN EL PAISAJE DE AMENAZAS ACTUAL, DEBES ASUMIR QUE LOS ATACANTES YA ESTÁN EN TU RED...

ZTNA, el punto de partida lógico para Zero Trust

Decidir dónde comenzar el viaje hacia Zero Trust puede ser desafiante. Un factor guía debería ser entender a tu adversario cibernético y evaluar sus tácticas, técnicas y procedimientos de explotación (TTPs). En este contexto, es importante entender que la definición moderna de los pilares de Zero Trust se extiende más allá de la red y abarca la superficie de ataque que se expande constantemente hoy en día.

La forma más fácil para que los atacantes obtengan acceso a datos sensibles es comprometiendo la identidad de un usuario. De hecho, un estudio de la Identity Defined Security Alliance (IDSA) revela que las violaciones de datos basadas en credenciales son tanto ubicuas (el 94% de los encuestados experimentó un ataque relacionado con la identidad) como altamente prevenibles (99%)[3]. En este contexto, ZTNA te ayuda a alejarte de la dependencia del nombre de usuario/contraseña y en cambio confiar en factores contextuales, como la hora del día, la geolocalización y la postura de seguridad del dispositivo, antes de otorgar acceso a los recursos empresariales.

Sin embargo, el error humano, las acciones maliciosas y el software inseguro a menudo dificultan la eficacia de la tecnología Zero Trust. Por lo tanto, el Instituto Nacional de Estándares y Tecnología (NIST) ha estado propagando el uso de sistemas de ciberseguridad auto-reparables o resilientes.

Lo que finalmente diferencia a los sistemas de ciberseguridad auto-reparables es su nivel relativo de habilidad para prevenir los mismos factores contra los que están construidos para proteger: error humano, decadencia, colisión de software y actividades maliciosas. Al final, son solo otra aplicación de software. Por lo tanto, es importante seleccionar soluciones que puedan perseverar frente a factores externos hostiles. Para alcanzar este estado de fortalecimiento , las capacidades de auto-reparación deberían estar incorporadas en el firmware del endpoint , protegiéndolo de cualquier manipulación intencional o no intencional.

[3] *Identity Defined Security Alliance (IDSA), Identity Security: A Work In Progress (Seguridad de Identidad: Un Trabajo en Progreso)*

Cómo volverse ciberresiliente para asegurar una fuerza laboral híbrida

Incluso una vez que se establecen los principios de Zero Trust, las organizaciones necesitan estar preparadas para el peor escenario y, por lo tanto, equilibrar las medidas defensivas con la ciberresiliencia. Esto se refleja en muchas recomendaciones de MITRE[4], NIST, la firma analista global Gartner e incluso la Casa Blanca de los Estados Unidos, que pide ciberresiliencia en su ambiciosa Estrategia Nacional de Ciberseguridad. La estrategia de la Casa Blanca refleja una creencia ampliamente mantenida en el gobierno de los Estados Unidos de que las fuerzas del mercado no han logrado mantener a salvo a la nación de los cibercriminales y los ataques patrocinados por el estado.

Se citó recientemente al director de la Agencia de Seguridad de Ciberseguridad e Infraestructura de los Estados Unidos: “A menudo culpamos a una empresa hoy que tiene una brecha de seguridad porque no parcheó una vulnerabilidad conocida... ¿Qué pasa con el fabricante que produjo la tecnología que requería demasiados parches en primer lugar?”[5] Muchos entendieron eso como que la responsabilidad de mantener la ciberresiliencia debería ser transferida a los proveedores que necesitan enfrentar el desafío.
Según MITRE, la ciberresiliencia (o ciberresistencia) "es la capacidad de anticipar, resistir, recuperarse y adaptarse a condiciones adversas, estrés, ataques o compromisos en los recursos cibernéticos."[5]
La necesidad de ciberresiliencia surge de la creciente realización de que las medidas de seguridad tradicionales ya no son suficientes para proteger los sistemas, los datos y la red del compromiso. El objetivo de la ciberresiliencia es asegurar que un evento cibernético adverso, ya sea intencional o no intencional, no impacte negativamente en la confidencialidad, la integridad y la disponibilidad de la operación comercial de una organización.

> **"Colectivamente podemos lograr un mejor cumplimiento y una mayor continuidad ante la complejidad: la ciberresiliencia es un deporte de equipo."**
>
> Christy Wyatt
> Presidenta y CEO, Absolute Software

4 MITRE, Cyber Resiliency Overview (Resumen de la Ciberresiliencia), Enero 2020
5 Cyberscoop; Director de la CISA insta al sector tecnológico a dejar de enviar productos inseguros, 27 de febrero de 2023

Absolute Software: Haciendo que la Seguridad Funcione

Absolute es conocida como la pionera en la resiliencia de los endpoints y la red, y nuestra Tecnología Persistence® ha sido adoptada por los principales fabricantes de sistemas del mundo (por ejemplo, Dell, Lenovo, HP, Microsoft, etc.) durante muchos años, proporcionando ciberresiliencia a millones de usuarios.

Incorporada en más de 600 millones de dispositivos, Absolute permite visibilidad y control en los endpoints, las aplicaciones y las conexiones de red. Aprovechando nuestra única capacidad de auto-reparación, los clientes pueden proteger dispositivos, datos y usuarios y asegurar que los controles de seguridad críticos operen con la máxima eficacia, al mismo tiempo que ofrecen una experiencia de usuario remota y móvil óptima.

Como compartimos anteriormente en este informe, nuestra posición única en el firmware de millones de dispositivos activos demuestra cómo Absolute Application Resilience™ proporciona la capacidad de monitorear la salud de las aplicaciones. Podemos reparar y/o reinstalar automáticamente aplicaciones de terceros no saludables listadas en el catálogo de Absolute Application Resilience para restaurarlas a operaciones saludables.

En última instancia, todo se trata de fortalecer la postura de cumplimiento de una organización, asegurar el acceso a la red seguro y confiable, y garantizar que los empleados puedan trabajar con confianza, y seguir trabajando, sin importar donde encuentren el riesgo.

Con Absolute Application Resilience, vemos que las puntuaciones iniciales de salud de la aplicación saltan de menos del 50% a cerca del 100%, sin la asistencia de TI.

Mejorar el tiempo de actividad de seguridad significa cerrar la brecha entre el riesgo cibernético y la ciberresiliencia.

El poder de la ciberresiliencia y Application Resilience

Como saben los profesionales de TI y seguridad, solo se necesita un pequeño número de herramientas para minimizar la exposición al riesgo en el frente de la cadena de ciberataques: EPP o EDR, así como soluciones de acceso remoto. Sin la ayuda de estas herramientas, no puedes mantener la funcionalidad y operatividad que deberías tener. Y no se trata solo de asegurar la capacidad de defensa, sino de aprovechar las mismas herramientas en tus esfuerzos de recuperación en caso de un ataque. Estas actividades a menudo se pasan por alto y se subestiman. Sin embargo, la eficacia de la seguridad juega un papel importante aquí. Para ilustrar el poder de la resiliencia de aplicaciones, evaluamos la salud de las aplicaciones de los principales proveedores de seguridad en EPP/EDR y acceso remoto, que son reconocidos como líderes en informes de la industria y utilizados por los clientes de Absolute: Cisco, Citrix, CrowdStrike, Microsoft, Netskope, Palo Alto Networks, SentinelOne, Sophos, Trend Micro y Zscaler. Luego, comparamos esto con la salud de sus aplicaciones una vez que se aplicaron las políticas de resiliencia de aplicaciones. Los siguientes resultados están anonimizados y en orden aleatorio:

	Aplicaciones No-Resilientes Porcentaje de Dispositivos Saludables*	Aplicaciones Habilitadas para Resiliencia Porcentaje de Dispositivos Saludables*	Incremento de Eficacia en Puntos Porcentuales
Plataforma de Protección de Endpoint / Detección y Respuesta de Endpoint			
Proveedor A	95%	96%	1%
Proveedor B	70%	94%	24%
Proveedor C	47%	99%	52%
Proveedor D	49%	100%	51%
Proveedor E	89%	93%	4%
Acceso Remoto			
Proveedor F	75%	90%	15%
Proveedor G	73%	93%	20%
Proveedor H	85%	97%	12%
Proveedor I	53%	98%	45%
Proveedor J	76%	99%	23%

La salud de una aplicación es una representación de si una aplicación está instalada en absoluto, instalada en el nivel de versión deseado por la organización, y si se están ejecutando servicios que se requieren para permitir que la aplicación funcione como se pretende, así como muchas otras condiciones.

Absolute avanza la ciberresiliencia ante la creciente complejidad de TI y la seguridad,

defendiendo y protegiendo de manera única sus recursos de colaboración, tecnología y seguridad desde el firmware hacia arriba, mientras potencia la agilidad del rendimiento y la continuidad operativa que las empresas líderes requieren hoy. Aprovechando nuestra tecnología de Absolute Persistence® incorporada en los dispositivos y extendiendo sus capacidades de recuperación auto-correctivas a través de Absolute Application Resilience, tanto las empresas como los proveedores de seguridad pueden optimizar la eficacia de las aplicaciones y fortalecer la postura de seguridad y cumplimiento. Con Absolute, neutralizas la disrupción digital y transformas la experiencia del usuario móvil, para que tus personal pueda trabajar con confianza, y seguir trabajando, sin importar donde el riesgo te encuentre.

Metodología del informe

Analizamos datos anónimos de 14 millones de dispositivos habilitados por Absolute activos durante el período de febrero a abril de 2023, en organizaciones de clientes en América del Norte, Europa y APAC, así como datos e información de fuentes terceras de confianza.

Índice de Resiliencia Empresarial

Las empresas pueden evaluar su ciberresiliencia a través de estas tres perspectivas: complejidad, cumplimiento y continuidad.

COMPLEJIDAD

Se enfoca en la salud de la aplicación e incluye el número de controles del endpoint, número de dispositivos y usuarios y número de plataformas de sistemas operativos.

Haz estas preguntas para conocer más sobre tu estado de complejidad.

1. ¿Cuál es el porcentaje de dispositivos por sistema operativo que están atrasados en las actualizaciones de seguridad?
2. ¿Cuál es el número de controles de seguridad por dispositivo?
3. ¿Estamos probando/utilizando las combinaciones óptimas de aplicaciones de antivirus/antimalware y cifrado?

CUMPLIMIENTO

La tarjeta de puntuación que se centra en el riesgo y el cifrado.

Haz estas preguntas para conocer más sobre tu estado de cumplimiento.

1. ¿Están tus datos sensibles cifrados en todos los endpoints, así como durante su tránsito o movimiento?
2. ¿Tienes información sobre la eficacia de tus controles de seguridad en cualquier momento dado?
3. ¿Sabes en cualquier momento dónde se encuentran todos tus dispositivos asignados por la empresa y si contienen algún dato sensible?

CONTINUIDAD

Incluye movilidad, salud de la aplicación y disponibilidad.

Haz estas preguntas para conocer más sobre tu estado de continuidad.

1. ¿Tienes alguna idea sobre la brecha en la cobertura de la red o la calidad de la conexión que te permitiría hacer cumplir los SLAs?
2. ¿Tienes alguna forma de comunicarte con los usuarios finales sin tener que depender de tu sistema de correo electrónico?
3. ¿Tienes formas automatizadas de reparar y/o reinstalar aplicaciones críticas para la misión que podrían prevenir ataques o ayudar con los esfuerzos de recuperación?

/ABSOLUTE®

Absolute Software es el único proveedor de soluciones de seguridad inteligentes y autorreparables. Incrustado en más de 600 millones de dispositivos, Absolute es la única plataforma que ofrece una conexión digital permanente que aplica inteligente y dinámicamente visibilidad, control y capacidades de autorreparación a los endpoints, aplicaciones y conexiones de red, ayudando a los clientes a fortalecer la ciberresiliencia contra la creciente amenaza de ransomware y ataques maliciosos. Confían en Absolute casi 20,000 clientes, G2 reconoció a Absolute como Líder durante el decimotercer trimestre consecutivo en el Informe Grid® de Primavera 2023 para la Gestión de endpoints y como Líder durante el tercer trimestre consecutivo en el Informe Grid para Redes de Zero Trust.

Solicita una Demo

Nasdaq | ABST TSX | ABST