Cómo Migrar de un Enfoque Reactivo a uno Preventivo

5 pasos críticos

EN SU ESTRATEGIA DE SEGURIDAD DE ENDPOINTS

BeyondTrust

CONTENIDO

*Paso ignorado

SEGURIDAD de los ENDPOINTS

Descripción general y beneficios

En 2019, el 70% de las infracciones exitosas comenzaron en los endpoints. * Y ahora, con el cambio a gran escala al trabajo remoto debido a COVID 19, la explosión de dispositivos de usuario final, BYOD y endpoints que trabajan fuera de la red, muchas organizaciones están todavía tratando de determinar las mejores estrategias de seguridad, dando a los atacantes tiempo para aprovechar y capitalizar la incertidumbre.

La seguridad en endpoints tradicional busca proteger dispositivos móviles, computadoras portátiles, *desktops*, servidores, IoT y POS y garantiza que ellos cumplan con ciertos criterios antes de que se les otorgue acceso a los recursos de la red. El objetivo de la seguridad de endpoints es limitar la superficie de ataque bloqueando la entrada no autorizada y protegiendo la red de amenazas maliciosas.

Las amenazas a los endpoints pueden presentarse en forma de ataques externos, así como amenazas internas, que pueden ser de naturaleza malintencionada o no intencional. **Un endpoint comprometido puede dar a un atacante un punto de apoyo dentro de un entorno, lo que le permite lanzar más ataques a los sistemas para acceder a datos y comprometer endpoints adicionales a través del movimiento lateral.**

Dado que una red de TI corporativa es esencialmente un enlace de endpoints, la integridad y la seguridad de los endpoints deben priorizarse antes de implementar otras soluciones de seguridad en la capa de aplicación. A medida que evolucionamos hacia la gestión moderna de endpoints, el enfoque debe cambiar al acceso a datos corporativos y aplicaciones en la nube que pueden no estar conectadas a un entorno corporativo.

*IDC, "Do You Think Your Seguridad de los Endpoints Strategy Is Up to Scratch?", Octubre 2019

Hemos visto un aumento del **30,000%** *en malwares atribuidos directamente a COVID 19*

*—Zscaler**

*www.zscaler.com/blogs/research/30000-percent-increase-covid-19-themed-attacks

Eliminar los privilegios de administrador no se trata solo de seguridad, sino que también permitirá que sus computadoras funcionen más rápido, mejor y por más tiempo.

—SAMI LAIHO
Microsoft MVP & Ethical Hacker

Beneficios de la seguridad en endpoints

- **Seguridad mejorada:** la eliminación de los privilegios de administrador, la aplicación de privilegios mínimos y del control de acceso "Just-In-Time (JIT)", y el empleo de herramientas basadas en firmas como antivirus reducen el riesgo de incidentes de seguridad y violaciones de datos de amenazas dirigidas a endpoints.

- **Rendimiento mejorado del endpoint:** la eliminación de privilegios superfluos y el refuerzo de los dispositivos se traduce en menos configuraciones erróneas, incompatibilidades, incidentes de seguridad y otros problemas que pueden causar interrupciones y protege contra la inestabilidad del endpoint.

- **Cumplimiento y auditorías simplificados:** cuanto más estrictamente esté integrado, administrado y controlado un sistema de endpoint, y cuanto mejor sea la visibilidad en toda la empresa, más sencillo será el camino hacia el cumplimiento normativo.

- **Excelencia operativa:** las herramientas de seguridad adecuadas permiten a TI soportar y administrar más tipos de endpoints y perseguir con confianza cambios favorables para el negocio en el entorno, incluida la implementación de nuevas tecnologías y garantizar la estandarización para la supervisión y el control de cambios.

DESAFÍOS

tradicionales en la seguridad de endpoints

En el entorno de amenazas actual, las infracciones parecen inevitables. Si bien el riesgo de una infracción se puede mitigar significativamente con medidas de detección, el riesgo nunca se puede reducir a cero. Tener soluciones para evitar que los usuarios realicen acciones que podrían resultar en malwares, ransomwares y phishing son igualmente importantes. **Dado que el 70% de las infracciones comienzan en los endpoints, la seguridad del endpoint tradicional debe evolucionar para gestionar de forma más proactiva las amenazas modernas.**

La evolución de las ciberamenazas, los entornos de endpoints cada vez más complejos y diversos, la desalineación corporativa de las tecnologías de seguridad con las amenazas y los equipos de TI e InfoSec cada vez más escasos de recursos son solo algunos de los muchos factores convergentes que ponen en riesgo el universo de endpoints de una organización y, por lo tanto, toda la red.

Las herramientas de seguridad de endpoints tradicionales como el antivirus previenen ataques *conocidos*, pero **pierden un promedio del 60% de los ataques de endpoints modernos y más avanzandos**. Y, mientras que las soluciones de Endpoint Detection and Response (EDR) sean una valiosa estrategia de seguridad de defensa en capas, se basan en análisis estadísticos y modelos que no siempre reconocen correctamente la diferencia entre las amenazas y el comportamiento aceptable que conduce a falsos positivos o retrasos inaceptables en el tiempo de respuesta.

Por otro lado, las soluciones Gestión de Privilegios en los Endpoints (EPM) evitan que los ataques infrinjan los endpoints utilizando una estrategia diferente. Evitan que los actores de amenazas penetren en un entorno al eliminar los privilegios necesarios para comprometer un host. Esto mitiga los riesgos en la capa de aplicación al controlar qué aplicaciones están realmente autorizadas a ejecutarse y, lo que es más importante, con qué privilegios. Este modelo resuelve un problema crítico al prevenir el movimiento lateral a través de las redes en busca de datos sensibles para comprometer.

350,000

de nuevos programas maliciosos se detectan a cada día*

*www.av-test.org/en/statistics/malware/

¿Cómo pueden las organizaciones cambiar a un enfoque ***más preventivo*** *de seguridad en endpoints?*

Evolucionando hacia un

ENFOQUE DE GESTIÓN MODERNO

Seguridad en Endpoints es un Ecosistema, no una Solución Única

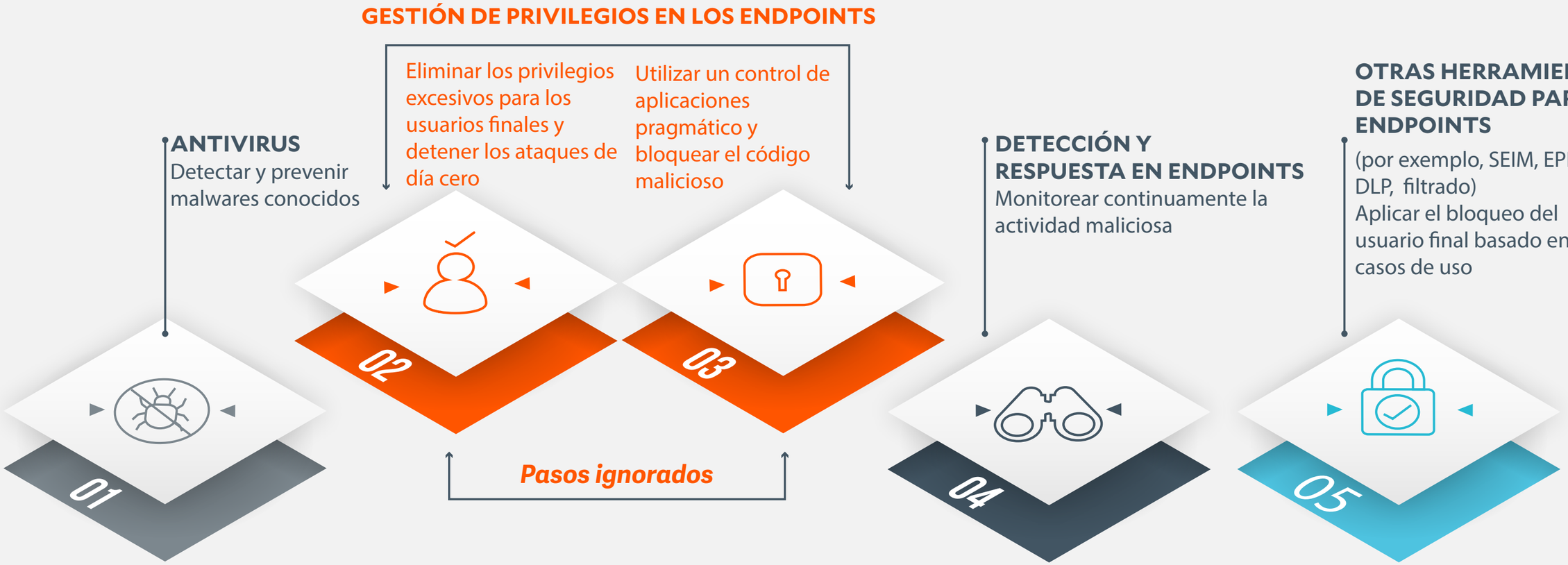
La seguridad en los endpoints ha evolucionado considerablemente en las últimas décadas, desde un simple software de antivirus basado en firmas hasta un enfoque holístico de tecnologías diseñadas para proteger contra amenazas conocidas o desconocidas para los endpoints. Hoy en día, la seguridad de los endpoints es necesaria para prevenir, detectar, responder y mitigar las amenazas internas y externas, y escalar para satisfacer la creciente diversidad de dispositivos utilizados por empleados, proveedores y terceros, ya sea en las instalaciones o de forma remota.

También debe ser adaptable y alcanzable para que pueda adaptarse a un entorno de amenazas en evolución. La seguridad de endpoints no es solo una solución, es un ecosistema que debe tener la prevención como un principio fundamental en lugar de solo una actitud reactiva.

Esta Guía rápida describe **5 pasos críticos** para habilitar un enfoque preventivo integral para proteger todos los endpoints de su organización.

5 PASOS CRÍTICOS A CONSIDERAR EN SU ESTRATEGIA DE SEGURIDAD DE ENDPOINTS

Un enfoque preventivo para la seguridad de los endpoints



Antivirus

DETECTAR Y PREVENIR

malwares conocidos

Antivirus

* Ponemon Institute, *"El tercer estudio anual sobre el estado de los riesgos de seguridad de endpoints"*, enero de 2020

Por lo general, el software antivirus (AV) es la primera herramienta de seguridad implementada en endpoints, ya que defiende contra amenazas comunes y conocidas. **Sin embargo, el antivirus claramente no está diseñado a prueba de** balas, ya que más del 60% de los ataques no son detectados por el antivirus, debido a amenazas *desconocidas* o técnicas evasivas que explotan aplicaciones "confiables". Por lo tanto, según el cumplimiento normativo y las mejores prácticas de seguridad bien definidas, el antivirus debe considerarse solo un componente de una estrategia de seguridad de endpoints más completa.

Se deben utilizar medidas mucho más efectivas, que tradicionalmente no se consideran parte de la seguridad de los endpoints, para complementar soluciones de AV y mejorar estadísticamente la eficacia de la seguridad de los endpoints. Esto incluye restringir el uso de privilegios de administrador y controlar qué aplicaciones se pueden ejecutar. La combinación de gestión de privilegios y control de aplicaciones bloqueará los ataques tradicionales de malwares y ransomwares.
Esto se convierte en una parte fundamental del paso 2.

Gestión de Privilegios en los Endpoints

ELIMINAR LOS PRIVILEGIOS EXCESIVOS

Paso ignorado

para los usuarios finales y detener los ataques de día cero

Paso ignorado

Con la seguridad del perímetro ahora más fuerte que nunca, los dispositivos de los usuarios finales son atacados en gran medida por los actores de amenazas. La mayoría de los usuarios tienen acceso sin restricciones a través de navegadores web y pueden ser manipulados a través del correo electrónico, lo que facilita que un pirata informático "los atraiga" mediante técnicas de ingeniería social. Si el usuario tiene privilegios de administrador local cuando abre un adjunto o enlace infectado, la "carga útil" puede ejecutarse con sus privilegios, dando al pirata informático el control de la máquina, instalando puertas traseras silenciosamente y reconfigurando (o deshabilitando) otros controles de seguridad.

Muchos usuarios finales todavía tienen privilegios administrativos completos, credenciales de administrador secundario o incluso cuentas de administrador temporales/compartidas para hacer su trabajo. Los usuarios administradores también pueden desinstalar o deshabilitar otras herramientas de seguridad en sus sistemas que, intencionalmente o no, podrían presentar un riesgo mayor.

Al eliminar los privilegios de administrador, el usuario ya no puede descargar ni ejecutar software malicioso que desencadena ataques de ransomwares o malwares. Esto reduce drásticamente la superficie de ataque y limita en gran medida lo que pueden hacer los actores de amenazas que evaden el AV: la gran mayoría de exploits y cargas útiles fallará. Sin infección presente, no tienen la capacidad de moverse lateralmente para comprometer datos confidenciales. **La eliminación de los privilegios de administrador habría mitigado el 77% de las vulnerabilidades de Microsoft.***

Con la administración de privilegios, los usuarios pueden realizar tareas de administración sin usar credenciales de administrador o root, otorgando los privilegios a la aplicación y no al usuario. Este enfoque de administración "sin contraseña" permite a las organizaciones dar a los usuarios los privilegios suficientes para hacer sus trabajos.

*BeyondTrust, "*2020 Microsoft Vulnerabilities Report*"

> ***Eliminar los privilegios de administrador de los usuarios finales es una de las formas más efectivas de mejorar la postura de seguridad general.***
>
> ***—DAN BLUM***
>
> *Cybersecurity Strategist y Autor de Rational Cybersecurity for Business*

03

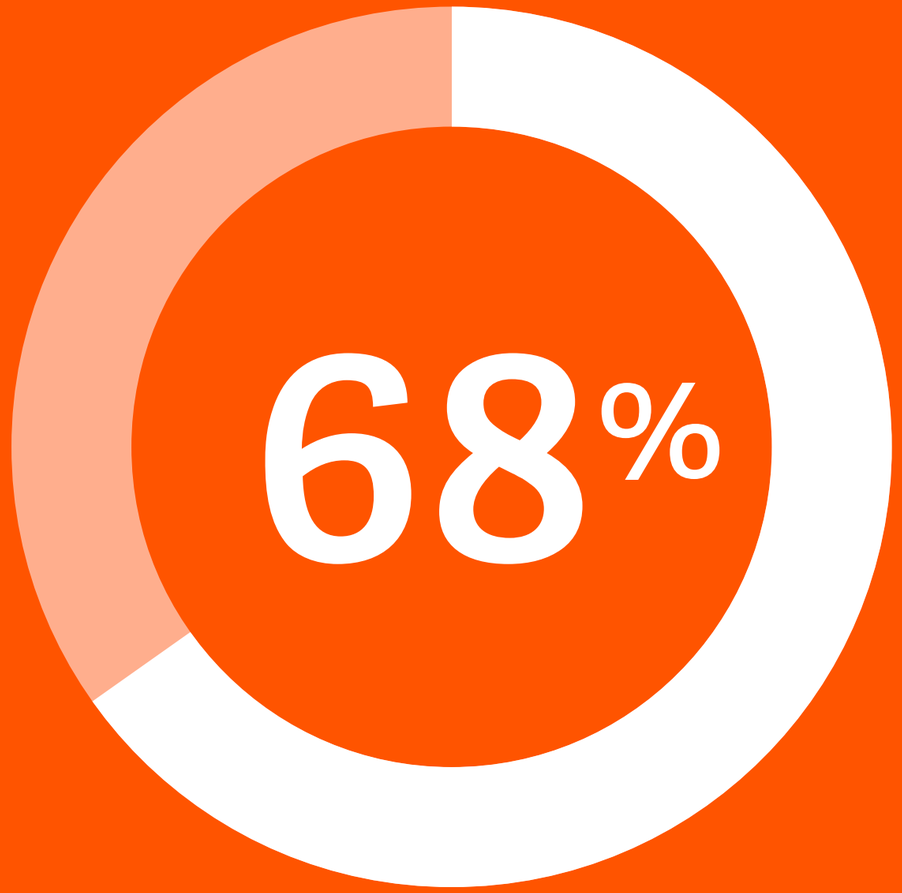
Gestión de Privilegios en los Endpoints

Paso ignorado

UTILIZAR UN CONTROL DE APLICACIONES PRAGMÁTICO

y bloquear el código malicioso

Gestión de Privilegios en los Endpoints



de las organizaciones se han visto afectadas por uno o más ataques en endpoints en el último año*

* Ponemon Institute, *"El tercer estudio anual sobre el estado de los riesgos de seguridad de endpoints"*, enero de 2020

Paso ignorado

No todos los ataques a endpoints necesitan aprovechar los privilegios para comprometer una máquina, y aquí es donde interviene el control de aplicaciones. Los controles de aplicaciones impiden que los usuarios, los actores de amenazas y otras aplicaciones ejecuten comandos o aplicaciones inapropiados en un terminal.

Los atacantes suelen apuntar y explotar aplicaciones confiables para permitir el acceso a largo plazo a un sistema. Al comprometer las aplicaciones clave, el código malicioso se puede inyectar o vincular a las aplicaciones sin ser detectado. Las aplicaciones de correo electrónico y basadas en la web a menudo son atacadas de esta manera.

El Control de aplicaciones decide qué aplicaciones puede ejecutar un usuario, independientemente de los privilegios, y permite a las organizaciones definir aplicaciones buenas y malas en función de las necesidades del negocio y los modelos basados en la reputación. Al utilizar el control de aplicaciones, los equipos de seguridad pueden reforzar la seguridad del sistema, lo que dificulta mucho más que un adversario cause daños.

Tradicionalmente, el control de aplicaciones se consideraba difícil y estaba reservado solo para los entornos más estáticos. Sin embargo, al superponer el Control de aplicaciones sobre la Gestión de privilegios, se confía en la funcionalidad crítica del sistema operativo de forma predeterminada (los usuarios sin privilegios no pueden introducir código nuevo en directorios como Archivos de programa, Windows, System32 o Controladores). Esto lo convierte en un enfoque pragmático porque solo debe aplicarse a directorios y archivos específicos, donde los actores de amenazas suelen "soltar" y ejecutar sus cargas útiles.

El uso de una solución de Gestión de Privilegios en los Endpoints como segunda y tercera capa de seguridad del endpoint proporciona no solo un modelo para la gestión de privilegios, sino también para un control de aplicaciones sólido. El resultado combinado es una reducción drástica en la superficie de riesgo del endpoint. Además, el control de aplicaciones es un requisito de varios marcos y mandatos de cumplimiento.

Detección y respuesta en endpoints

MONITOREAR CONTINUAMENTE

la actividad maliciosa

Dado que no todos los riesgos serán mitigados por antivirus o restricción de privilegios, ni por control aplicaciones, es muy importante tener una solución EDR para garantizar la seguridad de los endpoints.

Las soluciones de Endpoint Detection and Response (EDR) están diseñadas para ayudar a las organizaciones a identificar y reaccionar ante amenazas que han pasado por alto sus otras defensas. EDR se ejecuta localmente en estaciones de trabajo o servidores de usuarios para monitorear procesos, tareas programadas, aplicaciones, usuarios registrados y, lo que es más importante, para determinar si hay actividad maliciosa o no autorizada en el sistema. Esto complementa a la solución EPM al reconocer y alertar sobre la posible actividad de un atacante en un sistema fuera del alcance de EPM como una herramienta de administración de privilegios. Las alertas de EDR pueden incluir actividad relacionada con la red, aplicaciones maliciosas conocidas, intentos de usar programas integrados de manera maliciosa y otras actividades. Y, si EDR detecta un evento, la confianza del ataque es mucho mayor porque los privilegios y las aplicaciones potencialmente maliciosas han visto mitigado su ejecución por EPM. La cantidad de falsos positivos disminuirá, lo que reducirá el tiempo necesario para revisar los datos de eventos y los análisis.

Es importante recordar que una solución EDR por sí sola no brinda a su organización capacidades de monitoreo completas. Se necesitan profesionales de seguridad bien capacitados y procesos sólidos para maximizar su inversión en EDR y mejorar realmente tu seguridad. Sin el equipo y el compromiso de tiempo adecuados, los productos EDR pueden acumular datos y alertas, lo que a su vez puede aumentar los costos de recursos.

*EDR por sí solo **no** brinda a su organización capacidades de monitoreo completas.*

05

Otras herramientas de seguridad para endpoints

APLICAR BLOQUEO DE USUARIO FINAL

según los casos de uso

La Gestión de Privilegios en los Endpoints hace que todas las demás herramientas de Seguridad de los Endpoints sean más efectivas al reducir el ruido y minimizar la superficie de ataques

Las estrategias de seguridad de endpoint no son todas iguales. Una vez que su organización ha implementado los pasos **1 a 4**, es imperativo revisar casos de uso específicos y evaluar otras soluciones de endpoint según las necesidades.

Algunos tipos de herramientas de seguridad de endpoints a considerar incluyen:

- Las soluciones de análisis de endpoints, como la evaluación de vulnerabilidades, el monitoreo de registros y las soluciones de administración de eventos e información de seguridad (SIEM), se mejoran con Gestión de Privilegios en los Endpoints al garantizar que solo las aplicaciones aprobadas y parcheadas se ejecuten, lo que reduce el ruido en los registros y enriquece los datos con actividad privilegiada.
- Las soluciones de detección y respuesta, incluidas las plataformas de protección de endpoints (EPP) y las aplicaciones de filtrado de correo electrónico y web, también se complementan con EPM al evitar que una parte significativa de la actividad maliciosa ocurra, lo que permite que estas herramientas se concentren en una menor cantidad de actividad.

Además, existen muchos tipos diferentes de herramientas de prevención de Seguridad de los Endpoints que las organizaciones también podrían considerar en su camino para asegurar sus endpoints. Estos incluyen prevención de pérdida de datos, cifrado (seguridad de endpoints y datos), endpoint hardening, administración de parches, configuración segura, acceso remoto y proxy web, por nombrar solo algunos. Y, al igual que todas las demás soluciones de seguridad en endpoints, EPM reduce drásticamente la superficie de ataque al eliminar los privilegios de administrador y prevenir las amenazas de día cero.

BeyondTrust Gestión de Privilegios en los Endpoints

REDUCCIÓN PREVENTIVA DEL RIESGO

BeyondTrust Privilege Management para Windows y MacOS

Una solución preventiva de seguridad en endpoints que elimina los privilegios administrativos, brinda a los usuarios los privilegios suficientes para hacer su trabajo y ser productivos, y ofrece un potencial de reducción de riesgos rápido e inigualable. Los modelos de implementación simplificados disponibles on-premise o mediante SaaS impulsan el retorno a la inversión y la adopción rápida.

Principales recursos

Habilitación de privilegios mínimos: restrinja los privilegios de administrador para usuarios, cuentas, aplicaciones y procesos informáticos a solo aquellos recursos absolutamente necesarios para actividades legítimas.

Administración sin contraseña: realice funciones administrativas en un endpoint sin necesidad de credenciales con privilegios o de administrador con la administración Just-in-Time (JIT).

Control de aplicaciones: obtenga un control total sobre lo que los usuarios pueden instalar o ejecutar con un automatizado manejo de excepciones.

Plantillas de inicio rápido: las plantillas de estilo de trabajo flexibles y listas para usar le permiten implementar políticas de privilegios en días, no en meses, trabajando de manera efectiva para cada función y en múltiples sistemas operativos.

Protección de aplicaciones confiables: las plantillas prediseñadas detienen los ataques que involucran aplicaciones confiables, detectan scripts incorrectos y archivos adjuntos de correo electrónico infectados, deteniendo inmediatamente ataques sin archivos y más.

Power Rules: usa scripts de PowerShell para automatizar flujos de trabajo, crear comportamientos personalizados o crear integraciones con ITSM y otras herramientas; los ecosistemas integrados significan mejores posiciones de seguridad.

Auditoría e informes empresariales: proporcione una única pista de auditoría de toda la actividad de los usuarios para optimizar los análisis forenses y simplificar el cumplimiento, y utiliza paneles e informes gráficos para un acceso rápido.

Tenemos un equipo de seis ingenieros que administran todo el entorno de desktops y dispositivos móviles, por lo que necesitábamos algo que realmente los capacitara para hacer el trabajo de la manera más rápida y eficiente posible, y el uso de Gestión de Privilegios en los Endpoints realmente les permitió hacer eso.

—RYAN POWELL
Gerente del Centro de Respuesta y Operaciones

Conclusión

Los 5 pasos críticos para la seguridad de endpoints permiten un enfoque integral y preventivo para proteger todos los endpoints de su organización, ya sean de oficina o remotos. La habilitación de privilegios mínimos y el control pragmático de las aplicaciones a menudo se pasan por alto, pero son cruciales para lograr una seguridad completa en los endpoints.

Las soluciones de BeyondTrust Gestión de Privilegios en los Endpoints reducen significativamente su superficie de ataque y mitigan las posibilidades de una infracción al eliminar los privilegios de administrador y adoptar un enfoque sin contraseña. A través de listas blancas inteligentes y reglas de energía personalizadas, esto se puede lograr sin obstaculizar la productividad del usuario final ni afectar su ecosistema de seguridad existente.

El uso de BeyondTrust como parte de un enfoque preventivo en capas para su estrategia de seguridad de endpoints garantiza una experiencia de usuario sin fricciones al brindar el nivel adecuado de acceso en el momento justo.

Recursos adicionales

- Glosario de BeyondTrust: Seguridad de los Endpoints
- Guía para la gestión de privilegios en endpoints
- Informe de vulnerabilidades de Microsoft 2020
- Guía rápida: habilita y proteja a su fuerza laboral
- Demo: Privilege Management para Windows y Mac
- Cuadrante mágico de Gartner de 2020 para la gestión de acceso privilegiado

BeyondTrust

Acerca de BeyondTrust

BeyondTrust es el líder mundial en gestión de accesos privilegiados (PAM) y permite a las organizaciones proteger y administrar todo su universo de privilegios. Nuestros productos y plataforma integrados ofrecen la solución PAM más avanzada de la industria, lo que permite a las organizaciones reducir rápidamente su superficie de ataque en entornos tradicionales, de nube e híbridos.

El enfoque de BeyondTrust Universal Privilege Management asegura y protege los privilegios a través de contraseñas, endpoints y accesos, brindando a las organizaciones la visibilidad y el control que necesitan para reducir el riesgo, lograr el cumplimiento y aumentar el rendimiento operativo. Nuestros productos permiten el nivel adecuado de privilegios solo por el tiempo necesario, creando una experiencia sin fricciones para los usuarios que mejora la productividad.

Con un legado de innovación y un firme compromiso con los clientes, las soluciones de BeyondTrust son fáciles de implementar, administrar y escalar a medida que las empresas evolucionan. Contamos con la confianza de 20.000 clientes, incluido el 70 por ciento de Fortune 500, y una red global de socios.

Obtenga más información en www.beyondtrust.com/es

V2020_09_ENG