La ventaja de Forcepoint

FORCEPOINT

Desafíos actuales de la seguridad cibernética

En la era de la transformación digital, las compañías más exitosas del mundo lideran la industria al monetizar sus datos y su propiedad intelectual. Por eso, proteger estos datos y la propiedad intelectual contra robo cibernético o corrupción resulta crítico; las pérdidas pueden impactar significativamente en los presupuestos y en la reputación de la marca construida con mucho esfuerzo. Los Directores de Seguridad de la Información (CISO, por sus siglas en inglés) y otros ejecutivos responsables de la seguridad comprenden lo que está en juego, pero su trabajo es más difícil que nunca en el modelo operativo de TI actual, que adopta las nubes públicas, la política BYOD (traiga su propio dispositivo) y la movilidad. Los datos ahora están en todas partes y se puede acceder a ellos desde cualquier lugar.

Las superficies de ataque siguen creciendo de manera exponencial, haciendo que sea incluso más difícil bloquear las amenazas. Los métodos de seguridad cibernética tradicionales que dependen de productos independientes no fueron diseñados para este nuevo mundo.

Pero el método centrado en las personas de Forcepoint es diferente. Nuestra seguridad transformadora, centrada en el comportamiento, se adapta en forma dinámica en respuesta al nivel de riesgo que genera el comportamiento de los usuarios, y proporciona a los profesionales de seguridad una nueva ruta para proteger proactivamente sus datos y usuarios en el mundo globalizado actual.

> Los líderes de seguridad y gestión de riesgos deben adoptar un enfoque estratégico continuo de riesgo adaptable y de evaluación de confianza (CARTA). Esto es fundamental para habilitar de manera segura el acceso a las iniciativas comerciales digitales en un mundo de avanzados ataques dirigidos. Facilitará la toma de decisiones en tiempo real, basada en los riesgos y la confianza con respuestas adaptables.[2]
>
> Las 10 principales tendencias tecnológicas estratégicas de Gartner Research para 2018

> El 60% de la TI empresarial está fuera de las instalaciones y en la nube.[1]

1 https://www.idc.com/getdoc.jsp?containerId=US41883016

2 Gartner, Top 10 Strategic Technology Trends for 2018 (Las 10 principales tendencias de tecnología para 2018), por David W Cearley et al., 03 de octubre de 2017.

Los métodos tradicionales se encuentran en un punto de quiebre

El enfoque típico para la seguridad cibernética depende del uso de productos específicos que no se integran. Las distintas tecnologías trabajan para casos de un solo uso, pero la falta de integración entre ellas resulta en una abrumadora cantidad de alertas generadas. Los equipos de seguridad tienen el desafío de intentar distinguir una amenaza real de miles de falsas alarmas. Para el momento en que la encuentren, es posible que ya haya ocurrido un daño importante.

La sobrecarga de alertas es un síntoma de un problema mayor: la dependencia de un método binario centrado en la amenazas donde se pueden abordar las actividades "buenas" y "malas" a través de políticas estáticas, pero la intención resulta desconocida detrás de la vasta mayoría de los eventos restantes que se ubican entre los dos extremos del espectro. Si no se comprende el contexto detrás de la actividad, los equipos de seguridad deberán investigar manualmente cada actividad. Aplicar un método centrado en la amenazas, lleva a una situación en que nadie gana.

Una empresa es víctima de un ataque por ransomware cada 14 segundos.[3]

$3,62 millones de dólares es el costo total promedio de una fuga de datos.[4]

De hecho, los equipos de seguridad cibernética parecen estar destinados a fallar. Se estima que más del 80 % de los incidentes de seguridad cibernética apuntan a vulnerabilidades conocidas.[5]
La manera en que hacemos las cosas hoy simplemente no funcionará en el futuro.

3 https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
4 Ponemon Institute, 2017 Cost of Data Breach Study (Estudio sobre el costo de una fuga de datos)
5 SANS Institute, Cyber Security Trends: Aiming Ahead of the Target to Increase Security in 2017 (Tendencias de la seguridad cibernética: apuntando más allá del objetivo para mejorar la seguridad en 2017)

Por qué utilizar la seguridad cibernética centrada en las personas

Más del 80 % de las brechas relacionadas con piratas informáticos explotan credenciales comprometidas. Los servicios de autenticación y autorización simple de usuarios y dispositivos no son capaces de monitorear el comportamiento y no ofrecen control sobre los datos luego de que se ha otorga el acceso. También resulta casi imposible defenderse contra los hackers que han comprometido a buenos empleados al "apoderarse de sus sistemas" de manera ilícita con métodos de seguridad cibernética tradicionales.

Además, los buenos empleados pueden cometer errores, que inconscientemente conducen a la filtración de información. A veces, es posible que los empleados insatisfechos no tengan las mejores intenciones.

En lugar de intentar proteger completamente las redes administradas y que son propiedad de terceros, bloquear distintos puntos de acceso y encontrarle la lógica a una abrumadora cantidad de eventos de seguridad, es fundamental comprender los comportamientos cibernéticos de todos los usuarios, los empleados, clientes y socios, a medida que interactúan con los datos y los sistemas para evaluar de manera proactiva el riesgo que puede representar su actividad.

Líder en protección adaptable al riesgo

El método antiguo para la seguridad, centrado en los eventos, ya no tiene sentido en el complejo panorama cibernético actual. La seguridad más efectiva es la que se adapta a los riesgos, y proporciona el contexto necesario para aplicar de manera dinámica las políticas relevantes, incluso a nivel de los individuos. Y es solamente a través del contexto que podemos comprender si el comportamiento de una identidad o un usuario en particular es legítimo, riesgoso o malicioso.

El enfoque adaptable a los riesgos de Forcepoint detecta, analiza y aplica políticas; protege a sus usuarios, los datos y sus redes en tiempo real y aumenta la eficacia de sus inversiones en seguridad.

A diferencia de otros sistemas, nuestra solución no inunda su Gestión de Eventos e Información de Seguridad (SIEM) con alertas que deben eliminarse manualmente. En cambio, permite conocer cuál es la actividad normal productiva del empleado y todas las maneras únicas en que las personas interactúan con los datos y aplica automáticamente las políticas adecuadas para sus perfiles de riesgo.

De manera simultánea, brinda visión de dónde se encuentran los datos y dónde viajan, dentro y fuera de la organización. Nuestro modelo se adapta a los riesgos, proporciona mayor visibilidad, brinda una única política para distintos sistemas distribuidos, una rápida aplicación y un alto cumplimiento.

Es hora de pasar a la seguridad cibernética centrada en las personas

¿Quién es Forcepoint?

Forcepoint se creó con el propósito de proporcionar soluciones de seguridad cibernética de vanguardia.

- Una de las compañías de seguridad cibernética más grandes del mundo, con miles de clientes corporativos y gubernamentales, en más de 150 países
- Proveedor líder para la comunidad de inteligencia global y misiones cibernéticas de alta seguridad
- Uno de los portafolios de productos de seguridad más completos de la industria

El factor humano

Al alejarse de un método de seguridad cibernética centrado en las amenazas, puede limitar su enfoque a las dos constantes reales de la seguridad: las personas y los datos.

Proteger el factor humano significa resguardar la intersección entre las personas, los datos críticos y la propiedad intelectual, que comienza con la comprensión del ritmo de las personas y el flujo de los datos. Permite conocer cuál es la actividad normal productiva del empleado y todas las maneras únicas en que las personas interactúan con los datos.

Forcepoint Dynamic Data Protection (DDP) es una solución convergente pionera en la industria para la última generación de DLP que brinda protección adaptable al riesgo. Combina las capacidades de DLP líderes de la industria de Forcepoint con una capacidad de análisis centrado en el comportamiento para brindar protección contra exfiltración de datos. Dynamic Data Protection establece un punto de referencia "normal" de comportamiento del usuario y aplica una serie de medidas correctivas de seguridad automatizadas basadas en las fluctuaciones de la calificación de riesgo de un usuario, todo sin intervención del administrador.

El portafolio de productos de Forcepoint centrado en las personas

Las capacidades de Forcepoint convergen para simplificar la implementación y administración de su capa de seguridad y eliminar las brechas en la seguridad. Cada una de sus capacidades es la mejor de su categoría; puede comenzar con cualquiera y expandirse a medida que aumenten sus necesidades. Nuestra política unificada, análisis común y orquestación optimizan la gestión.

Entre las soluciones de Forcepoint se encuentran:

Análisis conductual de Forcepoint
Análisis de comportamiento de usuarios y entidades para un mundo sin perímetros. El líder en conocimientos factibles basados en una calificación que se adapta a los riesgos.

Forcepoint DLP
Descubrimiento y protección para cumplir con los requisitos regulatorios e industriales.

Forcepoint Insider Threat
Visibilidad del usuario y contexto de los incidentes para datos confidenciales. Comprensión integral de la intención del usuario, elegida por más de 1 millón de puntos finales.

Forcepoint CASB
Visibilidad y control de todo su entorno en la nube. El soporte más amplio para aplicaciones en la nube con evaluación de riesgos personalizada única, basada en el comportamiento del usuario y la clasificación del acceso a los datos.

Forcepoint SD-WAN &
Next Generation Firewall (NGFW)
Seguridad de redes eficiente, disponible y altamente segura. Disminuye los gastos de red en un 50 %, reduce los ataques cibernéticos hasta en un 86 % y recorta el tiempo de respuesta ante incidentes en un 73 %.

Forcepoint Data Guard
Colaboración y uso compartido de la información para las agencias gubernamentales. Elimina las costosas y engorrosas transferencias manuales de datos confidenciales altamente regulados.

Forcepoint Web and Email Security
Protección unificada contra ataques avanzados en cualquier ubicación, en cualquier dispositivo. La detección de amenazas es del 100 % y sin falsos positivos.

Reconocimiento de la industria

Líder en el Cuadrante Mágico de Gartner en Prevención contra la pérdida de datos empresarial en nueve oportunidades consecutivas.*
*Cuadrante Mágico de Gartner para la Prevención contra la pérdida de datos empresarial, 16 de febrero de 2017. Antiguamente figurábamos como Websense en el Cuadrante Mágico para la Prevención contra la pérdida de datos sensible al contenido y en el Cuadrante Mágico para Monitoreo y filtrado de contenido e informes de Prevención contra la pérdida de datos. Gartner no avala a ningún proveedor, producto o servicio descrito en sus publicaciones de investigación, y no expresa ninguna recomendación a los usuarios de herramientas tecnológicas respecto de la elección de los proveedores que tienen las calificaciones más altas o alguna otra designación. Las publicaciones de investigación de Gartner consisten en las opiniones de la organización de investigación de Gartner y no deben considerarse declaraciones de hechos. Gartner rechaza toda garantía, expresa o implícita, en relación con esta investigación, lo que incluye garantías de comerciabilidad o aptitud para un propósito en particular.

Acerca de Forcepoint

Forcepoint está transformando la seguridad cibernética enfocándose en lo que es más importante: el comportamiento de las personas cuando interactúan con sistemas y datos críticos. Este enfoque de la seguridad cibernética centrada en las personas permite que los empleados comprendan el ritmo normal del comportamiento del usuario y el flujo de datos dentro y fuera de una organización. Las soluciones basadas en el comportamiento de Forcepoint se adaptan al riesgo en tiempo real y se entregan mediante una plataforma de seguridad convergente para proteger a los usuarios de la red y el acceso a la nube, evitar que datos confidenciales salgan de la red corporativa y eliminar las fugas causadas por empleados. Con sede en Austin, Texas, Forcepoint protege el factor humano para miles de clientes empresariales y gubernamentales en más de 150 países.

forcepoint.com/contact

[CORPORATE-OVERVIEW-GLOBAL-BROCHURE-ES] 400019.030719

FORCEPOINT