Forcepoint

CLOUD SEGURITY

1.1.- Email Security

Forcepoint Cloud Email Security (anteriormente TRITON AP-EMAIL Cloud)

Protección contra ataques de spam, phishing y ransomware desde cualquier lugar donde se acceda al correo electrónico

Las amenazas avanzadas combinan elementos de la web y del correo electrónico en todos los ataques cibernéticos de múltiples etapas para buscar el canal de ataque más débil, pero esta estrategia también presenta múltiples oportunidades para detener esos ataques antes de que se produzcan posibles fallas. Forcepoint Cloud Email Security asegura el canal de comunicación utilizado con más frecuencia en las primeras etapas de una APT y otros ataques avanzados, al mismo tiempo que permite un amplio campo de acción a los trabajadores móviles y la adopción segura de nuevas tecnologías como Microsoft Office 365.

En un mundo en el que todo pasa por la nube, los avances en tecnología modifican constantemente la manera en que nos comunicamos y colaboramos. Con el paso de los años, el correo electrónico ha sido, y continúa siendo, el eje central de la productividad; de manera que la seguridad del correo electrónico es esencial para el éxito a largo plazo y la reputación de su organización.

Forcepoint Cloud Email Security brinda protección contra amenazas avanzadas en etapas múltiples que suelen aprovecharse del correo electrónico para atravesar sus defensas de TI. Aplica miles de análisis de amenazas en tiempo real, sandboxing y otras tecnologías de defensas avanzadas para identificar ataques dirigidos.

Solida protección para usuarios, donde quiera que vayan.

Forcepoint Cloud Email Security está potenciada por Advanced Classification Engine (ACE) y ThreatSeeker Intelligence Cloud de Forcepoint, que trabajan juntos en tiempo real para identificar y clasificar con precisión el tráfico del correo electrónico, aplicar políticas y detectar amenazas. Hospedado en la infraestructura de centro de datos en la nube global de Forcepoint, TRITON le ofrece funciones de generación de informes y administración unificada que simplifican el trabajo de su equipo de seguridad, dándoles el contexto y el conocimiento que necesitan para reducir al mínimo el tiempo de permanencia de los ataques.

La arquitectura TRITON simplifica la implementación de Forcepoint Cloud Email Security por separado o en cualquier combinación con Forcepoint Cloud Web Security (anteriormente TRITON AP-WEB Cloud). La arquitectura TRITON unifica las implementaciones completas de seguridad para la web y el correo electrónico en la nube y también las opciones de implementación híbrida y en las instalaciones, mientras mantiene el control central.

Beneficios:

Detenga los ataques dirigidos y las etapas tempranas de las amenazas avanzadas persistentes.

Proteja la información sensible contra el robo, ataques externos y amenazas internas.

Adopte de manera segura tecnologías en la nube, como Microsoft Office 365.

Identifique comportamientos de "alto riesgo" por parte de los usuarios y enséñeles a mejorar el reconocimiento de amenazas.

Características:

Identificación de alta precisión en tiempo real y clasificación de amenazas con Forcepoint Advanced Classification Engine (ACE).

Inteligencia sobre amenazas en tiempo real de Forcepoint ThreatSeeker Intelligence (anteriormente ThreatSeeker Intelligence Cloud), que ofrece visibilidad de la actividad de amenazas cibernéticas actuales a nivel global.

Administración unificada, generación de informes y panel en los diversos productos Forcepoint.

Empaquetamiento de adjuntos en archivos para brindar protección adicional contra adjuntos potencialmente maliciosos.

Cloud Data Security es protección contra la pérdida de datos (DLP) en la nube para el tráfico de correo electrónico saliente.

1.2.- Linux Security

Forcepoint Threat Protection for Linux:

Mejore su capacidad de respuesta ante incidentes de Linux para malware y otras amenazas.

La visibilidad que necesita para malware y otras amenazas que afectan sus servidores basados en Linux de manera que pueda mantener el curso normal de los procesos comerciales vitales.

En muchas organizaciones, Linux es la plataforma elegida para las implementaciones en la nube, la infraestructura web y otros servicios de soporte. Los ataques no detectados de estos sistemas pueden costarle muy caro a su organización en términos de tiempo de inactividad de los negocios, daño a la reputación, menores ingresos y multas reglamentarias.

Forcepoint Second Look le brinda las capacidades que necesita para detectar riesgos dentro de su implementación de Linux de manera que pueda minimizar el tiempo de permanencia de los atacantes en sus sistemas y pueda reanudar las operaciones normales de forma rápida y segura. Utiliza una combinación de análisis de memoria y verificación de integridad para ayudar a su equipo de seguridad a determinar exactamente dónde deben concentrar sus esfuerzos, destacando malware furtivo, programas desconocidos o no autorizados y otros indicadores de compromiso potenciales que podrían haber penetrado en las otras defensas.

Forcepoint Second Look automatiza los análisis de memoria de Linux para verificar la integridad de kernel y procesa miles de estaciones de trabajo y servidores Linux distribuidos geográficamente. Detecta rootkits, puertas traseras o backdoors, procesos no autorizados y otros signos de intrusión y sus alertas de análisis de memoria se pueden integrar fácilmente con cualquier sistema existente de Gestión de eventos e incidentes de seguridad (SIEM) de manera que su equipo pueda desarrollar una investigación y una respuesta rápidas y exhaustivas.

Beneficios:

Detecta amenazas de Linux conocidas y desconocidas, como malware, sin confiar en las firmas que otras soluciones generalmente omiten escanea rápidamente miles de sistemas con cientos de gigabytes de memoria.

Verifica la integridad del código kernel y ejecutable de un sistema remoto en todos los procesos sin requerir un completo vaciado de memoria.

Crea un impacto lo más bajo posible en los sistemas supervisados.

Aprovecha la infraestructura de SSH para la comunicación en red, eliminando la necesidad de tener un agente en continua ejecución.

Proporciona flexibilidad y facilidad de implementación para permitirle a su equipo de seguridad de TI evaluar e interpretar los resultados con rapidez.

Características:

Compatible con las distribuciones de kernel Linux versión 2.6 y superior para sistemas de 32 bits y 64 bits x86

Motor de escaneo configurable para escaneos automatizados de sistemas remotos

Se integra con sistemas de administración de eventos de información de seguridad (SIEM)

Extensa colección de software de referencia tanto para kernels como para aplicaciones

Interfaz gráfica de usuario fácil de usar

Salida en formato de datos estructurados JSON

1.3.- Web Security

Forcepoint Cloud Web Security (anteriormente TRITON AP-WEB Cloud)

Seguridad en la nube de primer nivel para proteger a usuarios y datos en todas partes

Solida protección para usuarios, donde quiera que vayan

Las amenazas avanzadas incluyen ataques sofisticados en etapas múltiples, con técnicas incorporadas que eluden la detección mientras roban sus datos sensibles. Las amenazas internas, como el robo de empleados y el malware al que se tiene acceso desde la misma organización, son tan perjudiciales como las amenazas externas.

Forcepoint Cloud Web Security ofrece capacidades, líderes de la industria, para la prevención contra la pérdida de datos (DLP), sandboxing y generación de informes, detiene más amenazas avanzadas sin firma que ponen en peligro sus datos que cualquier otra solución, incluyendo: Blue Coat, Cisco y Zscaler.

Forcepoint Cloud Web Security se basa en una plataforma unificada que permite que los productos Forcepoint trabajen juntos y proteger los datos en todas partes: en la nube, en el camino, en la oficina. Simplificando el cumplimiento y permitiendo tener mejor toma de decisiones y una seguridad más eficiente.

Adopte la protección líder en la industria contra amenazas avanzadas y robo de datos:

Los avances en la tecnología de la nube han proporcionado a las organizaciones una mayor flexibilidad y capacidades rápidas de colaboración. Para obtener estos beneficios, su organización debe simplificar la seguridad con una solución inteligente, con prioridad en la nube, que brinde protección en tiempo real, además que permita lograr su misión a largo plazo y proteger su reputación.

Forcepoint Cloud Web Security brinda protección en línea contra amenazas avanzadas que utilizan técnicas sofisticadas para evadir la detección, robar sus datos sensibles y también contra amenazas internas, como robos perpetrados por empleados y malware. Forcepoint Cloud Web Security es líder acreditado en seguridad de contenidos web SaaS, y detiene más amenazas avanzadas sin firma que ponen en riesgo sus datos que cualquier otra solución.

Dashboard fáciles de usar:

- Vea los niveles de amenazas, productividad y ancho de banda en un instante.
- Cambio rápido de programas para análisis veloces

Generación de informes:

- Más de 80 informes predefinidos.
- Cree informes personalizados ilimitados arrastrando y soltando 70 atributos.
- Historial de informes extendido opcional durante un máximo de 18 meses para ajustarse a los requisitos reguladores y de cumplimiento.

Sandbox integrado en la nube:

- Análisis de código en tiempo real para la identificación de amenazas avanzadas.
- Ejecución segura de códigos sospechosos ajenos a los recursos de su red.

Inteligencia integrada sobre amenazas:

- Brinda información de más de 155 países a Forcepoint Cloud Web Security.
- Tasa promedio de actualización de 3.2 piezas de inteligencia sobre amenazas por segundo.

1.4.- Forcepoint CASB (Cloud Access Security Broker)

Forcepoint CASB proporciona visibilidad y control sobre las aplicaciones de nubes autorizadas y no autorizadas para permitir su uso seguro y productivo.

Discover Shadow IT & Risk

La adopción no sancionada de las aplicaciones en la nube es un problema de seguridad para las empresas. El enfoque seguro y no intrusivo de Forcepoint CASB para el descubrimiento de aplicaciones en la nube y la puntuación de riesgos garantiza que la TI puede eliminar puntos ciegos descubriendo qué aplicaciones de nube son utilizadas por los empleados y sus perfiles de riesgo.

Prevenir Fugas de Datos Sensibles:

Inspeccione los archivos y el contenido de la nube en tiempo real para evitar la filtración malintencionada o no intencional de información confidencial. Identificar y analizar datos sensibles o regulados almacenados en los servicios de sincronización de archivos en la nube para comprender la exposición a los permisos compartidos y garantizar el cumplimiento de regulaciones como PCI, SOX y HIPAA.

Controlar el acceso BYOD:

Minimizar el riesgo de proliferación de datos a dispositivos no administrados o no confiables mediante la aplicación de reglas de acceso basadas en dispositivos. Impedir la descarga o sincronización de datos a dispositivos no administrados mientras se permite el acceso en línea sólo a los datos en la nube.

Detectar y bloquear ataques cibernéticos:

Forcepoint CASB monitorea toda la actividad del usuario y analiza patrones de uso para detectar rápidamente anomalías que pueden indicar una toma de cuenta. El tablero proporciona una gran cantidad de análisis en la nube, destacando las actividades sospechosas y los intentos de comprometer las cuentas.

Identificar brechas de seguridad:

Forcepoint CASB utiliza API de nube para analizar sus inquilinos de la nube, ayudando a los usuarios y administradores de la revisión de TI a detectar cuentas inactivas, usuarios externos y ex empleados que todavía pueden tener acceso a sus aplicaciones en la nube. Además, Forcepoint CASB inspecciona las configuraciones de seguridad de sus inquilinos para detectar deficiencias y para recomendar las configuraciones de mejores prácticas para una gestión eficaz de la nube.

Optimizar la detección de anomalías y amenazas:

Forcepoint CASB es el único agente de seguridad de acceso a la nube que protege los datos de la empresa contra robos y pérdidas debido a usuarios maliciosos y descuidados, que correlaciona anomalías de actividad con direcciones IP de riesgo.

Network Security

1.5.- Forcepoint NGFW (anteriormente Stonesoft Next Generation Firewall)

Protección flexible, escalable y de alta disponibilidad contra amenazas avanzadas.

Optimice y escale la seguridad de redes para su empresa distribuida con menores costos de infraestructura y mucho menos tiempo de inactividad.

Seguridad altamente escalable:

A medida que aumenta la dependencia de las redes, también lo hacen los costos y las complejidades de la conectividad y la infraestructura de redes. Una red compleja y distribuida es difícil de administrar y está propensa a tiempo de inactividad.

Forcepoint NGFW utiliza un enfoque único e incorporado para optimizar la disponibilidad, la escalabilidad y el costo de las redes. El agrupamiento para la alta disponibilidad y un alto rendimiento, pueden utilizarse para centros de datos y otros casos de uso intenso de computadoras, lo que permite la escalabilidad de la administración de la red.

Eficiencias operativas:

Los analistas sugieren que el 80% de los costos totales de TI se producen después de la compra inicial. El monitoreo diario, el mantenimiento regular, la respuesta a incidentes y otras realidades operativas, requieren recursos que podrían interrumpir las operaciones críticas de una organización. Forcepoint NGFW actúa como el centro de la seguridad de sus redes, centralizando el monitoreo, la administración y la elaboración de informes en diversos dispositivos virtuales, físicos y en la nube, así como dispositivos de terceros. Los flujos de trabajo optimizados simplifican las tareas administrativas diarias y la gestión de la seguridad para lograr una mayor eficiencia y un bajo costo total de propiedad (TCO).

Permita la transformación de su negocio:

Las presiones extraordinarias impulsan a las organizaciones a crecer, adoptar nuevas tecnologías y respaldar la fuerza de trabajo, cada vez más móvil y distribuida. La complejidad de estos cambios representa un desafío para los equipos de TI que deben respaldar y asegurar estas iniciativas con recursos limitados. Los que actualmente utilizan un surtido de soluciones de punto encontrarán alivio en la visibilidad en toda la empresa, el control y la alta disponibilidad que proporciona la solución Forcepoint NGFW.

Características:

Soporte para Amazon Web Services

Gestión centralizada de hasta 2000 firewalls

Opciones de software, implementación física, virtual y en la nube, que incluyen Amazon Web Services (AWS)

Agrupamiento activo incorporado que escala a 16 nodos para alta disponibilidad

Instalación plug-and-play de firewalls de redes remotas

Redes privadas virtuales (VPN) de enlaces múltiples, escalables y resilientes para conectividad de un lugar a otro.

Data & Insider threat

1.6.- DLP Web Forcepoint DLP (antes TRITON AP-DATA)

Obtenga la visibilidad y los controles de datos necesarios para mantener sus datos esenciales seguros.

Proteja sus datos con visibilidad y control inigualables en cualquier lugar que estén, en la oficina, viajes o en la nube.

Forcepoint DLP y Forcepoint DLP Endpoint (antes TRITON AP-ENDPOINT) extienden los controles de seguridad de datos a las aplicaciones empresariales en la nube y a sus dispositivos finales. Aproveche de manera segura los potentes servicios en la nube como Microsoft Office 365, Google for Work y SalesForce.com y proteja sus datos confidenciales y su propiedad intelectual en computadoras portátiles Windows y Mac, tanto dentro como fuera de la red.

Caracteristicas:

Nuestra impresión digital PreciseID única detecta hasta una impresión parcial de datos estructurados (registros de bases de datos) o no estructurados (documentos) en dispositivos finales Mac y Windows – ya sea que un empleado esté trabajando en la oficina o fuera de ella.

Calificación de riesgo de incidentes los análisis de datos avanzados proporcionan un informe calificado por niveles de los principales riesgos a la seguridad de datos dentro de su organización.

Vea texto dentro de una imagen con OCR el reconocimiento óptico de caracteres (OCR) integrado identifica los datos confidenciales dentro de imágenes como diseños CAD, documentos escaneados, MRI y capturas de pantalla.

Prevención de la pérdida de datos por goteo (Drip DLP) evalúa la actividad de transmisión acumulativa de datos en el transcurso del tiempo para identificar fugas de pequeñas cantidades de datos.

Políticas basadas en comportamiento combinan el reconocimiento de contenido y contexto para identificar en forma automática cuando los usuarios están poniendo en riesgo los datos confidenciales.

Cifrado de datos cifra automáticamente los datos que se transfieren a dispositivos de almacenamiento extraíbles para permitir el intercambio seguro de datos con socios.

Flujo de trabajo de incidentes basado en el correo electrónico facilita la distribución de un incidente a los dueños de los datos y partes interesadas de la empresa para revisión y reparación, sin necesidad de otorgar acceso al sistema de gestión de DLP.

Controles de DLP empresarial extendidos le permiten configurar una vez para detectar y evitar que los datos confidenciales se envíen fuera de la organización a través del correo electrónico, las cargas en la web, mensajería instantánea y clientes de servicios en la nube.

Implementación segura de componentes de DLP de Microsoft Office 365 en Microsoft para aplicar las políticas de DLP en Microsoft Office 365.

1.7.- DLP EndPoint Forcepoint (antes TRITON AP-ENDPOINT)

Detenga amenazas avanzadas y proteja la información confidencial de los usuarios móviles.

Defienda a sus usuarios del robo de datos y ataques sofisticados cuando están en sus escritorios o en movimiento.

Sus empleados cuentan con máxima flexibilidad cuando trabajan en la oficina, en sus hogares o en la calle, pero sus computadoras portátiles también son vulnerables a las serias amenazas resultantes de sus propios comportamientos riesgosos o de explotaciones diseñadas por atacantes externos ambiciosos.

Forcepoint DLP Endpoint: Protege a sus usuarios del robo de datos, ya sea que estén dentro o fuera de la red corporativa. Sus poderosas capacidades de prevención de la pérdida de datos (DLP) le permiten asegurar sus datos personales, la propiedad intelectual y otra información confidencial en dispositivos finales MacOS, Linux o Windows; y sus políticas pre-configuradas le permiten cumplir con los requisitos reglamentarios con rapidez y facilidad.

Integración perfecta para una mejor protección en la nube:

Forcepoint DLP Endpoint está potenciado por la arquitectura TRITON, que hace más fácil la tarea del personal de TI al incluir en una sola consola herramientas administrativas y de elaboración de

informes, unificadas para nuestras soluciones para dispositivos finales, la web, el correo electrónico y DLP.

Adopte de manera segura servicios en la nube, como Microsoft® Office 365™ y Box, y obtenga visibilidad y control completos de los datos en la nube.

Cumpla rápidamente con los requisitos de cumplimiento y de regulación con una amplia selección de políticas pre-elaboradas, y satisfaga a los auditores con informes estandarizados o personalizados.

Características:

Soporte para MacOS X

Impresión digital precisa de datos para identificar incluso fragmentos de datos confidenciales

Gestión, elaboración de informes y consolas unificadas en los productos Forcepoint.

1.8.- Forcepoint Insider Threat (antes SureView Insider Threat)

La visibilidad y el contexto que necesita para eliminar amenazas internas

Empodere a su organización para proteger mejor la información de sus clientes, ciudadanos u otras partes interesadas le han confiado a través de la detección de sus usuarios más riesgosos y el seguimiento de las actividades de los empleados que podrían perjudicar a su organización.

La visibilidad inigualable de la actividad temprana en las computadoras de los usuarios previene el robo y la perdida de datos de sistemas usurpados, empleados maliciosos o usuarios finales negligentes.

Forcepoint Insider Threat: Es una herramienta de monitoreo del comportamiento de los usuarios que ha estado protegiendo las redes de organizaciones y gobiernos más confidenciales del planeta durante más de 15 años.

Forcepoint Insider Threat: Detecta actividad sospechosa, ya sea que se trate de un sistema usurpado, un empleado malicioso o simplemente un usuario que está cometiendo un error. Garantiza que su propiedad intelectual o sus datos relacionados con el cumplimiento de normativas no corran riesgos.

Identifica en forma automática a los usuarios más riesgosos y proporciona contexto del comportamiento inusual, incluida una visión “por encima del hombro” que les permite a las organizaciones combatir las amenazas provenientes del interior de la organización de manera proactiva y con autoridad.