

APX Módulo Email Encryption

GARANTICE LA ENTREGA SEGURA DE CORREO ELECTRÓNICO CONFIDENCIAL

En el mundo de la conectividad, el correo electrónico sigue dominando las comunicaciones profesionales, lo que lo convierte en el objetivo principal de los delincuentes cibernéticos. Toda organización necesita proteger su propiedad intelectual, sus transacciones comerciales, y la privacidad de sus clientes y de sus empleados, entre otros aspectos.

¿POR QUÉ UTILIZAR EL MÓDULO EMAIL ENCRYPTION DE FORCEPOINT™?

El encriptado de Forcepoint es un servicio basado en políticas que le permite entregar comunicaciones por correo electrónico de forma segura a sus socios comerciales y a particulares. Su fácil administración, con un modo de gestión simple y sin necesidad de utilizar hardware adicional, elimina las tradicionales barreras del costo y la complejidad que impiden el encriptado del correo electrónico. Además, su integración total con TRITON AP-EMAIL y con el Módulo de DLP de correo electrónico implica que no sacrificará la capacidad de inspeccionar el correo electrónico encriptado para detectar la presencia de malware y las violaciones de contenido. El encriptado de Forcepoint ofrece una solución simple y rentable para ayudar a las organizaciones a cumplir rápidamente con los requisitos reglamentarios y proteger la confidencialidad de la información sensible.

- **Las políticas predeterminadas** permiten que su personal de TI actual cumpla en forma rápida y sencilla con los requisitos reglamentarios como PCI y protegen su propiedad intelectual.
- **Una experiencia sin fisuras** al automatizar el encriptado de información confidencial mediante controles de políticas simples pero sumamente efectivos.
- La interfaz de usuario ofrece **una experiencia simple para los terceros destinatarios**, ya que es fácil de usar. Los destinatarios se registran solos y administran sus propias contraseñas, lo que elimina las tareas de administración necesarias para gestionar su acceso.

- **Los correos electrónicos están seguros** y encriptados en la bandeja de entrada del destinatario.
- **Las capacidades de OCR** permiten políticas para encriptar datos identificados con capturas de pantalla, páginas de fax y documentos escaneados como cheques, recibos, documentos legales o archivos legados.
- **La integración** de todos los servicios necesarios y la poderosa automatización reducen los gastos para poder lograr un bajo Costo Total de Propiedad (TOC, Total Cost of Ownership).

PARTE DE UNA COMPLETA DEFENSA DE SEGURIDAD DE CORREO ELECTRÓNICO

La combinación de TRITON AP-EMAIL, el Módulo de DLP de correo electrónico y del Módulo de Encriptado de Correo Electrónico lo defienden de las amenazas entrantes y las comunicaciones salientes a lo largo de toda la cadena de ataque.

- Encripte el correo electrónico en función de una política para proteger así las comunicaciones confidenciales con sus socios comerciales y sus clientes tanto en el caso de los sistemas de correo electrónico tradicionales como en Microsoft Office 365.
- Detenga las amenazas persistentes y otras amenazas avanzadas con objetivos específicos utilizando el análisis en tiempo real de ACE.
- Identifique a los empleados de alto riesgo a través del análisis de actividad comparada con la actividad del grupo de compañeros y con los comportamientos anteriores.
- Agregue el Módulo de Email Sandbox al entorno seguro de comportamiento de archivos y URL a fin de mejorar la detección de amenazas del día cero.
- Agregue el Módulo de Análisis de Imágenes para identificar imágenes explícitas en el correo electrónico que puedan infringir la reglamentación con respecto al acoso sexual y otras normativas.



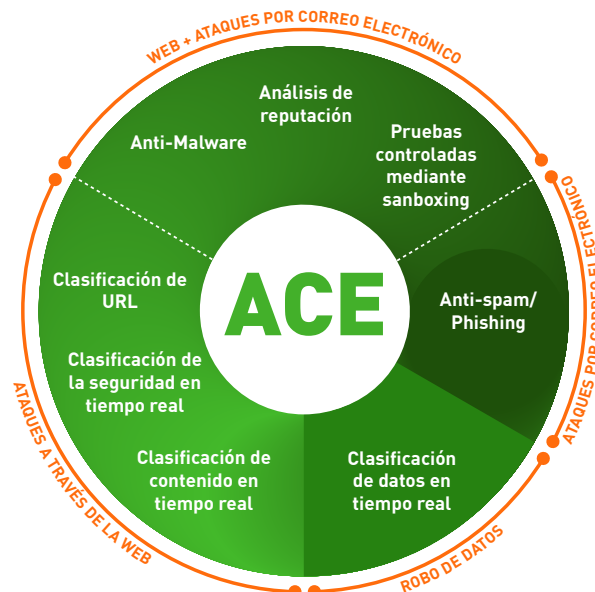
TRITON® AP-EMAIL

Desde señuelos diseñados para las redes sociales hasta phishing con una orientación definida, la mayoría de los ataques cibernéticos comienzan por el correo electrónico. Dado que estas amenazas avanzadas de varias etapas mezclan elementos de la web y del correo electrónico en los ataques, presentan una “cadena de ataque” de oportunidades que deben aprovecharse detenerlos antes de que ocurra la falla de seguridad.

TRITON AP-EMAIL identifica los ataques con una orientación definida, los usuarios de alto riesgo y las amenazas internas y, al mismo tiempo, permite un amplio campo de acción a los trabajadores móviles y permite la adopción segura de nuevas tecnologías como Microsoft Office 365 y Box. Desde la actividad entrante de ataque hasta el robo de datos salientes o los intentos de comunicación botnet, la seguridad que brinda Forcepoint TRITON AP-Email protege las comunicaciones mediante correo electrónico como parte de una completa defensa de TRITON APX contra amenazas avanzadas persistentes (APT, Advanced Persistent Threats) y otras amenazas avanzadas.

▶ TRITON AP-EMAIL RESUELVE DESAFÍOS DE SEGURIDAD DE CORREO ELECTRÓNICO

- Las APT frecuentemente utilizan el correo electrónico en las etapas iniciales de sus ataques avanzados.
- Detenga el robo de datos y las amenazas internas.
- Adopte Microsoft Office 365 y otros servicios para expandirse con seguridad y mantener su nivel de competitividad.
- Los hábitos de los usuarios que implican riesgos pueden generar fallas de seguridad y pérdida de datos.



LA DIFERENCIA DE FORCEPOINT:

Motor De Clasificación Avanzada (ACE, Advanced Classification Engine)

Forcepoint ACE proporciona defensas contextuales en línea, en tiempo real para la seguridad de la web, correo electrónico, de datos y seguridad móvil, utilizando la calificación de riesgos compuesta y el análisis predictivo, para así proporcionar seguridad más eficaz a la que se puede tener acceso actualmente. Brinda también contención a través del análisis del tráfico entrante y saliente con defensas atentas a los datos, proporcionando protección líder en la industria contra el robo de datos. Los clasificadores de seguridad en tiempo real y análisis de contenido y de datos, son el resultado de muchos años de investigación y desarrollo, los cuales permiten que ACE detecte todos los días más amenazas que los motores de antivirus tradicionales (la prueba se actualiza todos los días en <http://securitylabs.forcepoint.com>). ACE es la principal defensa detrás de todas las soluciones Forcepoint TRITON y cuenta con el respaldo de Forcepoint ThreatSeeker Intelligence Cloud.

CONTACTO

www.forcepoint.com/contact

ACERCA DE FORCEPOINT

Forcepoint™ es una marca comercial de Forcepoint, LLC. SureView®, ThreatSeeker® y TRITON® son marcas comerciales registradas de Forcepoint, LLC. Raytheon es una marca comercial registrada de Raytheon Company. Todas las demás marcas comerciales y marcas comerciales registradas son propiedad de sus respectivos dueños.

[DATASHEET_MODULE_EMAIL_ENCRYPTION_ES]-100008ES.011416

FORCEPOINT
TRITON® APX

www.forcepoint.com