FIREEYE™

FICHA TÉCNICA

FireEye Email Security Cloud Edition

Protección basada en la nube que identifica, analiza y bloquea los ataques de correo electrónico

ASPECTOS DESTACADOS

- Ofrece la seguridad completa para los correos electrónicos entrantes y salientes
- Consolida la pila de seguridad del correo electrónico con una solución completa de un proveedor único
- Admite las reglas YARA personalizadas para mejorar la eficacia en la detección de amenazas
- Permite la corrección automática de Office 365 para eliminar los correos electrónicos que se vuelven maliciosos después de la entrega
- Se integra con cualquier proveedor de correo electrónico de terceros
- Proporciona conocimientos extensos de los ataques y atacantes a partir de investigaciones de vanguardia y de las observaciones de adversarios
- Cumple con los requisitos de seguridad FedRAMP

"Dado que el correo electrónico es fundamental para todos los entornos de colaboración, la implementación de FireEye Email Security nos permite mitigar los riesgos de compromiso de este canal altamente explotado con una solución única".

Nils Göldner
Socio director y asesor de la nube
Blackboat GmbH

Descripción general

El correo electrónico es el factor más vulnerable para los ataques cibernéticos ya que es el punto de ingreso de datos de mayor volumen. Las organizaciones enfrentan un número en constante crecimiento de amenazas por el correo electrónico no deseado, malware y amenazas avanzadas. La mayoría de estas amenazas avanzadas llega por correo electrónico en la forma de URL vinculadas a sitios de suplantación de identidad de credenciales, solicitudes fraudulentas de transferencia electrónica y archivos adjuntos armados. La naturaleza muy específica y altamente personalizable del correo electrónico permite que los ciberdelincuentes lo ataquen de manera exitosa, haciendo del correo electrónico la opción principal para realizar delitos cibernéticos.

FireEye Email Security puede reducir los costos y aumentar la productividad de los empleados a través de una solución de seguridad de correo electrónico única que minimiza el riesgo de que ocurran brechas costosas a causa de ataques avanzados por correo electrónico. Implementado en la nube, FireEye Email Security es una puerta de enlace de correo electrónico segura y con funciones completas que lidera la industria en cuanto a la identificación, aislamiento y detención inmediata de los ataques basados en archivos adjuntos, URL y suplantación, antes de que los mismos ingresen al entorno de la organización. Con la corrección automática de Office 365 (O365), se pueden extraer los correos electrónicos que se vuelven maliciosos retroactivamente después de la entrega a la bandeja de entrada del usuario. FireEye Email Security también analiza el tráfico de correo electrónico saliente en busca de amenazas avanzadas, correos electrónicos no deseados y virus.

Mediante una convergencia de complementos de detección y contexto basado en la información, las URL maliciosas se revelan en una verdadera plataforma escalable de grandes datos. Los nombres de los remitentes y las direcciones de correo electrónico se verifican para comprobar su autenticidad y el contenido se examina para detectar prácticas de suplantación a fin de detener el fraude del director ejecutivo (CEO Fraud) y otros ataques sin malware. El motor Multi-Vector Virtual Execution™ (MVX) sin firma analiza archivos adjuntos de correo electrónico y URL en función de una matriz cruzada integral de los sistemas operativos, aplicaciones y navegadores web. Las amenazas se identifican con un ruido mínimo y los falsos positivos son prácticamente inexistentes.

FireEye recopila amplia inteligencia sobre amenazas relativas a adversarios, a través de investigaciones directas de las brechas de seguridad y millones de sensores. Email Security utiliza esta evidencia real y la inteligencia contextual sobre ataques y atacantes para priorizar alertas y bloquear amenazas en tiempo real.

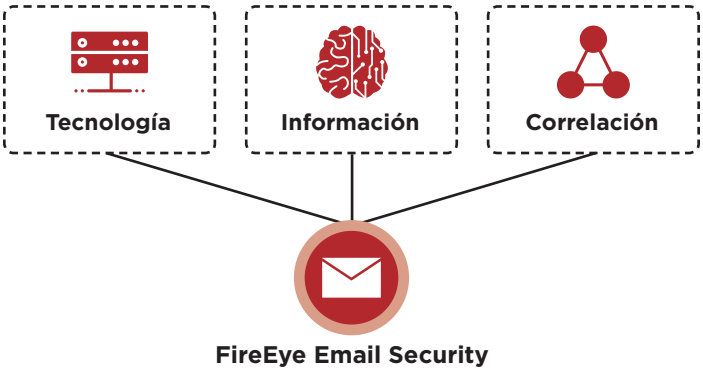

Figura 1. Una puerta de enlace de correo electrónica segura.

Al integrarse con FireEye Network Security las organizaciones pueden obtener una mayor visibilidad con respecto a ataques combinados de vectores múltiples y coordinar protección en tiempo real.

Defensa contra amenazas en el correo electrónico
Con información personal fácilmente disponible en línea, un delincuente cibernético puede utilizar técnicas de ingeniería social para convencer a prácticamente cualquier usuario de hacer clic en una URL o abrir un archivo adjunto.

Email Security proporciona detección y protección en tiempo real contra ataques de phishing selectivo, recopilación de credenciales y suplantación que por lo general eluden los servicios de seguridad del correo electrónico tradicional. Los correos electrónicos se analizan y ponen en cuarentena (bloquean) si se detectan amenazas desconocidas y avanzadas que estén ocultas en:

- Todos los tipos de archivos adjuntos, como archivos EXE, DLL, PDF, SWF, DOC/ DOCX, XLS/XLSX, PPT/PPTX, JPG, PNG, MP3, MP4 y ZIP/RAR/TNEF
- Archivos adjuntos protegidos por contraseña y cifrados.
- URL incluidas en correos electrónicos, archivos PDF y documentos de Microsoft Office
- URL de suplantación de identidad de credenciales y errores tipográficos
- Vulnerabilidades desconocidas del sistema operativo, explorador y aplicación
- Código malicioso integrado en correos electrónicos de suplantación de identidad selectiva

Si bien los ataques de ransomware comienzan con un correo electrónico, se requiere una devolución a un servidor de comando y control para cifrar los datos. Email Security identifica y detiene estas campañas de malware de etapas múltiples difíciles de detectar.

Detección de amenazas superior

Email Security ayuda a mitigar el riesgo de costosas brechas de seguridad al identificar y aislar los ataques avanzados, selectivos y otros tipos de ataques evasivos que se ocultan como tráfico normal. Una vez que se detectaron estos ataques se interceptan, analizan y almacenan en la memoria para identificar más rápidamente las amenazas futuras.

La parte central de Email Security se encuentran Advanced URL Defense y el motor MVX. Estas tecnologías utilizan análisis y aprendizaje automático de vanguardia a fin de identificar los ataques que eluden las defensas tradicionales basadas en firmas y políticas.

PhishVision es una parte integral de Advanced URL Defense, ya que es un motor de clasificación de imágenes que utiliza el aprendizaje profundo para recopilar y comparar capturas de pantalla de marcas confiables y comúnmente atacadas con respecto a las páginas web y de inicio de sesión a las que se hace referencia en las URL. Trabajando en combinación con PhishVision, Kraken es un complemento de detección de suplantación de identidad que aplica análisis de dominio y de contenido de la página para aumentar el aprendizaje automático. Otro avance en cuanto a la detección de URL es Skyfeed, un sistema de recopilación de información sobre malware de diseño específico y totalmente automatizado. A fin de descubrir falsos negativos se recopilan cuentas de redes sociales, blogs, foros y envíos de información sobre amenazas. La naturaleza multifacética de Advanced URL Defense ofrece a las organizaciones que están protegidas por Email Security una defensa incomparable contra los ataques de phishing selectivo y recopilación de credenciales.

Un correo electrónico puede comenzar siendo benigno para burlar las defensas de seguridad. Solo después de haber sido entregado a la bandeja de entrada de un destinatario, el correo electrónico se vuelve malicioso. Email Security – Cloud Edition analiza y alerta retroactivamente cuando un correo electrónico se vuelve malicioso después de la entrega. A través de la API de O365, los correos electrónicos que se vuelven retroactivamente maliciosos se pueden extraer de forma automática de la bandeja de entrada al crear una política de corrección automática para O365.

El motor MVX detecta ataques de día cero, flujo múltiple y otros ataques evasivos a través de un análisis dinámico sin firma en un entorno seguro y virtual. Detiene la infección y las fases de compromiso de la cadena letal de ataque cibernético al identificar ataques y malware no vistos anteriormente.

Protección AVAS mejorada

Email Security–Cloud Edition está disponible con protección antivirus y contra el correo no deseado (Anti-Spam and Antivirus, AVAS) para detectar ataques comunes que usan correspondencia convencional de firmas además de las técnicas de suplantación.

Los ataques de suplantación, como el fraude del director ejecutivo (CEO Fraud) (que a menudo se denominan compromisos de correos electrónicos empresariales) siguen teniendo un impacto financiero considerable en las empresas. Esto se debe, en parte, a la falta de indicadores de amenazas tradicionales, como enlaces o archivos adjuntos maliciosos, ya que los ataques no contienen malware y se basan en técnicas de ingeniería social. A fin de combatir estos ataques y proteger a los clientes, FireEye desarrolló algoritmos, sistemas y herramientas innovadores que se especializan en detectar la suplantación y defenderse de la misma.

Indicador común de un ataque por correo electrónico es la antigüedad del dominio del remitente. Al crear una campaña de suplantación, los criminales envían correos electrónicos de ataque desde un dominio similar al de la persona o compañía que están suplantando, por lo general, algunas horas después de la creación de ese dominio.

Email Security es capaz determinar con precisión la antigüedad y desarrollo de un dominio mediante las herramientas Newly Existing Domains (NED) y Newly Observed Domains (NOD) que se desarrollaron de forma interna. Los dominios que se determinaron como creados recientemente se tratan como sospechosos y se inspeccionan de manera extensiva para detectar otros indicadores de ataque, como errores tipográficos y falsificación del nombre para mostrar del remitente o del nombre de usuario.

El lugar de llevar a cabo el proceso de comprar y registrar un dominio, los ciberdelincuentes pueden sencillamente cambiar el nombre para mostrar o nombre de usuario del remitente a fin de aparentar que el correo electrónico proviene de una fuente confiable. Email Security se defiende contra esta falsificación informática (spoofing) del remitente determinando la autenticidad del nombre para mostrar y del nombre de usuario mediante la autenticación del nombre descriptivo.

Análisis de correos electrónicos salientes

Email Security detecta amenazas avanzadas desconocidas, incluidos archivos adjuntos maliciosos y URL de suplantación de identidad que se envían a través de correos electrónicos salientes. El tráfico de correo electrónico saliente también se analiza en busca de malware y correos electrónicos no deseados para evitar que los dominios de una organización se incluyan en una lista negra.

Integración para mejorar las eficiencias en el manejo de alertas.
Email Security analiza todos los adjuntos de correo electrónico y las URL para identificar con precisión los ataques avanzados actuales. Las actualizaciones en tiempo real de todo el ecosistema de seguridad de FireEye, combinadas con la atribución de alertas de perpetradores conocidos, proporcionan contexto para priorizar y actuar en caso de alertas críticas y bloquear los ataques por correo electrónico avanzados. Las amenazas conocidas, desconocidas y no basadas en malware se identifican con un ruido y falsos positivos mínimos, de forma tal que los recursos se enfoquen en ataques reales para reducir los gastos operativos.

Adaptación rápida al cambiante panorama de las amenazas

Email Security ayuda a su organización a adaptar continuamente su defensa proactiva contra amenazas en el correo electrónico. Email Security genera su propia información sobre amenazas en lugar de recurrir a envíos de información de terceros que pueden sufrir demoras. La información sobre amenazas interna y específica para correos electrónicos (o DNS inteligente [Smart DNS]), las capacidades de recopilación de datos, los expertos en seguridad para el correo electrónico y los analistas de amenazas proporcionan la infraestructura subyacente de las tecnologías contra correo no deseado mejoradas y la detección de suplantación. La inteligencia profunda sobre las amenazas y atacantes combina inteligencia de adversarios, máquinas y víctimas para:

- Brindar una visibilidad mayor y oportuna ante las amenazas
- Identificar capacidades y funciones específicas del malware y los archivos adjuntos maliciosos detectados
- Proporcionar información contextual para priorizar y acelerar la respuesta
- Determinar la probable identidad y los motivos de un atacante, y realizar un seguimiento de sus actividades dentro de su organización
- Identificar retroactivamente ataques de suplantación de identidad selectiva y prevenir el acceso a sitios de suplantación de identidad mediante la reescritura de URL maliciosas

Las organizaciones tienen acceso al portal de Email Security para ver alertas en tiempo real, crear reglas inteligentes personalizadas (Smart Custom Rules) y generar informes. Las reglas inteligentes personalizadas permiten que su organización cree políticas y reglas basadas en varias condiciones concretas.

Integración del flujo de trabajo de respuesta

Email Security funciona con otras soluciones de FireEye para ayudar a automatizar los flujos de trabajo de respuesta de alertas:

La administración central correlaciona las alertas de Email Security y Network Security de FireEye para obtener una vista más amplia de un ataque y establecer reglas de bloqueo a fin de evitar que el ataque se propague.

La plataforma FireEye Helix funciona sin interrupciones con Email Security y está específicamente diseñada para simplificar, integrar y automatizar las operaciones de seguridad.

Implementación sencilla y protección en toda la empresa

Email Security–Cloud Edition está basado en la nube, sin hardware o software para instalar. Es ideal para las organizaciones que migran su infraestructura de correo electrónico a la nube. Este cambio elimina la complejidad de comprar, instalar y mantener una infraestructura física.

Email Security–Cloud Edition se integra sin interrupciones con sistemas de correo electrónico basados en la nube, como Microsoft Office 365 con Exchange Online Protection y G Suite.

Para protegerse contra los correos electrónicos maliciosos y fraudulentos, las organizaciones simplemente envían los mensajes a Email Security, que primero analiza los correos electrónicos para detectar correo no deseado, malware conocidos y tácticas de suplantación. Luego usa tecnología de defensa de URL y la cámara de detonación sin firma, el motor MVX, para analizar cada archivo adjunto y URL para detectar amenazas y detener los ataques avanzados en tiempo real.

Capacidades adicionales

Personalización mediante reglas basadas en YARA

Email Security permite que los analistas utilicen las reglas YARA personalizadas para gestionar y mejorar las detecciones, detener las amenazas más recientes e identificar las campañas en curso.

Protección activa o modo de solo supervisión

Email Security puede analizar los correos electrónicos y poner en cuarentena amenazas para una protección activa. Las organizaciones simplemente actualizan sus registros de MX para enviar mensajes a FireEye. Para implementaciones solo de supervisión, las organizaciones simplemente deben configurar una regla BCC transparente para enviar copias de los correos electrónicos a FireEye para el análisis de MVX.

Autorización y certificaciones de cumplimiento

ISO 27001
Email Security–Cloud Edition cumple con el estándar de seguridad de la información ISO 27001 que garantiza que los centros de datos se gestionan de manera segura.

FedRAMP
Email Security–Cloud Edition con protección AVAS cumple con los requisitos de seguridad FedRAMP para servicios en la nube operados por entidades del gobierno y de educación pública.

SOC 2 Tipo 2
Email Security–Cloud Edition cumple con la Certificación de Seguridad y Confidencialidad del Servicio de Controles de Organizaciones de Tipo 2 (SOC 2) del Instituto Estadounidense de Contadores Públicos Certificados (American Institute of Certified Public Accountants, AICPA).

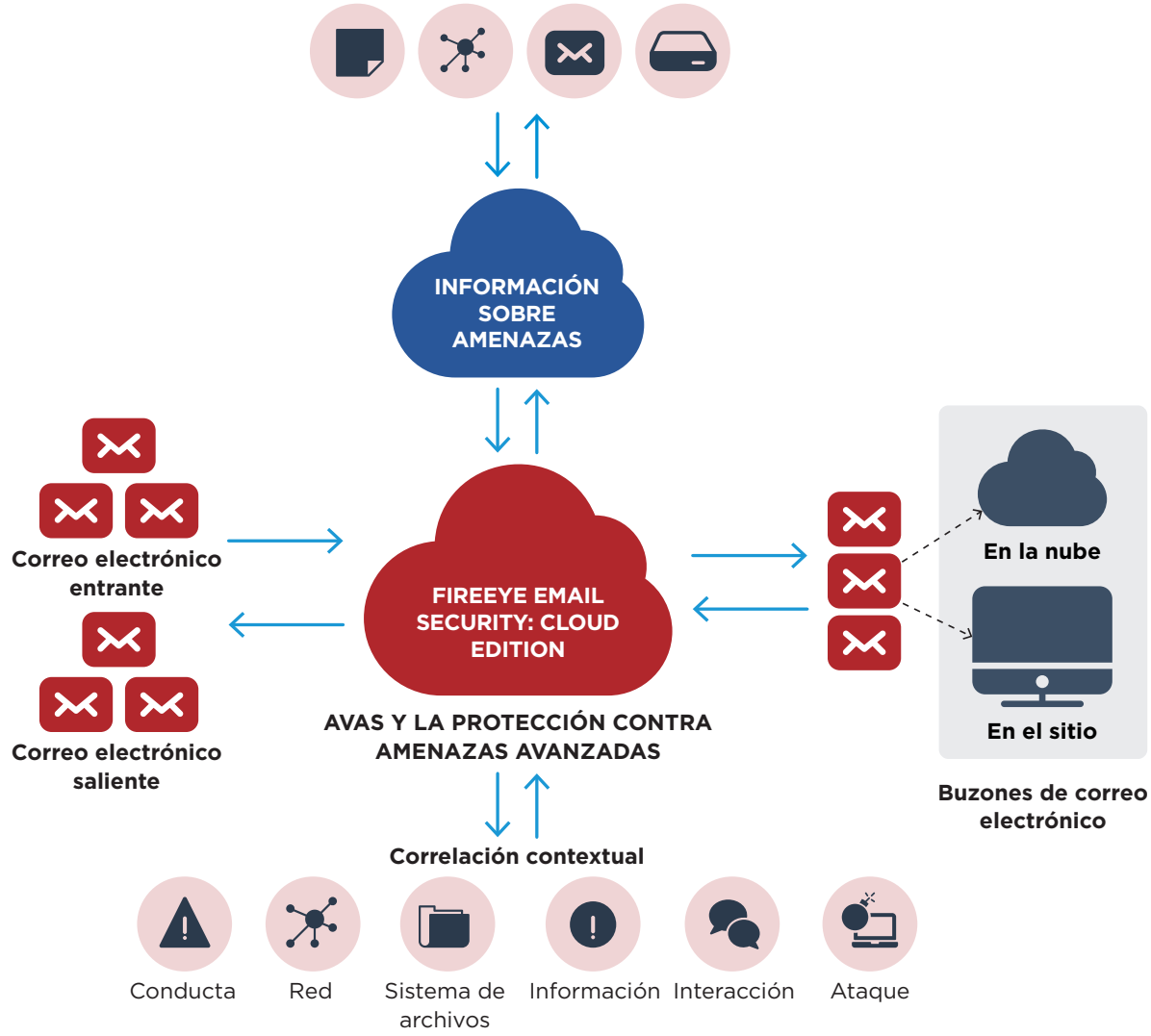

Figura 2. FireEye Email Security – Cloud Edition.

Para obtener más información sobre FireEye, visite: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

Acerca de FireEye, Inc.
FireEye es una empresa de seguridad basada en inteligencia. FireEye, que funciona como una extensión escalable y transparente de las operaciones de seguridad del cliente, ofrece una sola plataforma que combina tecnologías innovadoras de seguridad, inteligencia sobre amenazas similar a los de una Nación y los servicios de consultoría de fama mundial de Mandiant®. Gracias a este enfoque, FireEye elimina la complejidad y la carga de la seguridad cibernética para las organizaciones que desean estar preparadas y responder ante los ataques cibernéticos, además de prevenirlos.