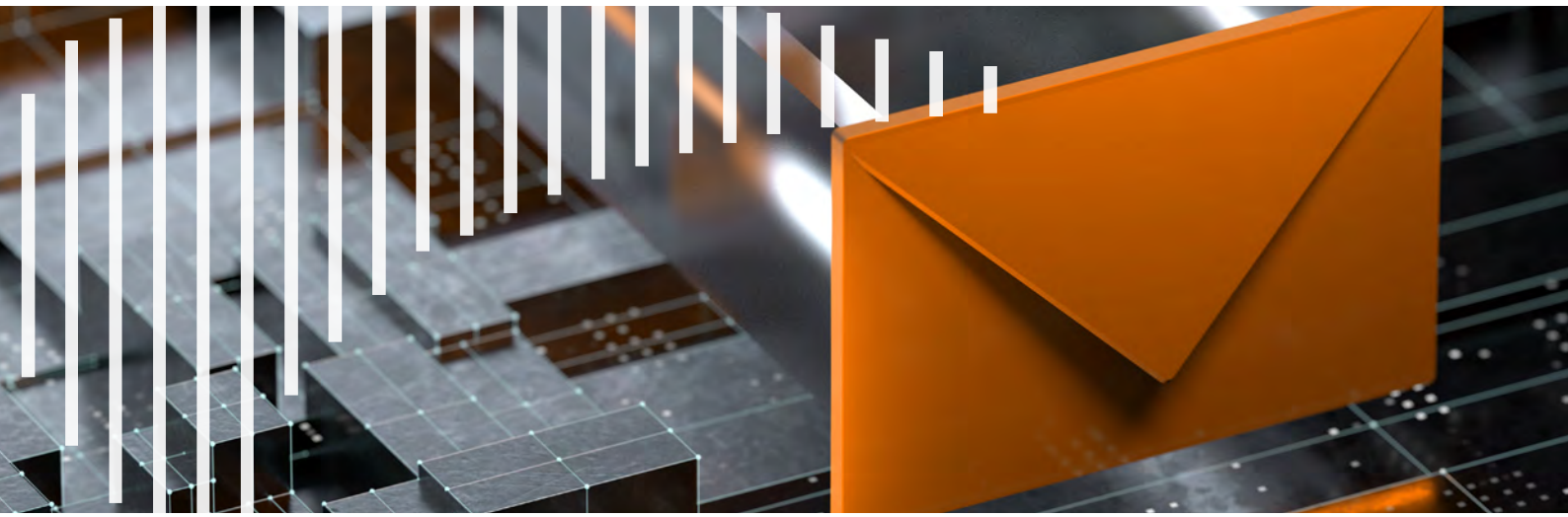
SONICWALL



Seguridad de correo electrónico adaptable en la era de la nube

Prestaciones esenciales para evitar que las amenazas que viajan por e-mail lleguen a los buzones.

RESUMEN

La nube es un agente de cambios imparable. Su eficiencia, elasticidad y escalabilidad urgen a las empresas a sustituir sus herramientas de productividad y oficina locales —como el e-mail y las herramientas de colaboración y de compartición de archivos— por las nuevas versiones en la nube. Pero existen dos grandes preocupaciones respecto a la adopción de esas aplicaciones: la seguridad y la disponibilidad del servicio.

Este informe examina cómo la solución SonicWall Email Security reúne lo último en tecnologías de seguridad de correo electrónico para combatir las amenazas crecientes, como el phishing dirigido, el compromiso del correo electrónico de negocio (BEC), el fraude por correo electrónico, la filtración de datos y el ransomware.

Introducción

Cuando se trata de amenazas que llegan por correo electrónico, los atacantes tardan poco en adaptarse a las megatendencias. El cambio al trabajo desde casa y la pandemia por COVID-19 son dos de las últimas tendencias que han hecho de la comunicación por e-mail un vector de ataque más lucrativo para el phishing dirigido y el ransomware. En el pasado, las filtraciones de datos nos han enseñado que estos ataques a menudo utilizan diversidad de tácticas, técnicas y procedimientos (TTP) para comprometer completamente al usuario.

Lo que se ha probado repetidamente es que el correo electrónico constituye la principal puerta de entrada, ya que:

- Contiene la URL inicial que enlaza a unas páginas de phishing ocultas o a una descarga maliciosa.
- Introduce el adjunto que contiene una carga útil maliciosa.
- Inicia ataques de ingeniería social (p. ej., fraude de correo electrónico o recolección de credenciales).

Para detener esas sofisticadas amenazas, las organizaciones deben implementar un sistema de filtrado de contenido de e-mail constantemente actualizado, que aprenda y se adapte a nuevos TTP de phishing. Al mismo tiempo, el análisis avanzado de amenazas del sistema puede bloquear con eficacia, precisión y menos falsos positivos hasta el phishing personalizado de gran calidad y bajo volumen, así como los ataques por compromiso del correo electrónico de negocio, suplantación y día cero.

Es imprescindible que la solución...

- Analice todo el tráfico de correo electrónico, y no solo los mensajes entrantes y salientes, ya que las amenazas y las filtraciones por correo electrónico pueden suceder a través de cuentas comprometidas o difundirse entre los empleados.
- Aplique funcionalidades de aprendizaje automático e inteligencia artificial para revelar los ataques de phishing mejor escondidos, diseñados para engañar a los usuarios y evadir los filtros de seguridad. Debería detectar anomalías, fraude y BEC, contar con procesamiento de lenguaje natural, detectar los indicadores clave de compromiso y los ataques multifaceta dirigidos a las vulnerabilidades pinhole en las capas de seguridad conocidas.
- Analice los correos electrónicos en la nube antes de que lleguen al buzón. Eso permite a las organizaciones disfrutar de lo mejor de ambos mundos y lleva hasta el buzón de cada usuario el concepto de seguridad sin perímetro.

SOLUTION BRIEF

Arquitecturas de Email Security de SonicWall

La solución Email Security de SonicWall ofrece un stack de seguridad que es a la vez profundo y ancho, y que proporciona una cobertura de protección óptima en entornos tanto de Exchange local como de oficina en la nube (es decir, Microsoft 365 o Google Workspace).

Puede elegir entre una arquitectura basada en pasarela o en API, según sus requisitos de implementación particulares. Ambas proporcionan lo último en tecnología capaz de atrapar formas complejas de phishing, compromiso del correo electrónico de negocio (BEC), fraude de correo electrónico y ataques por suplantación de identidad, antes de que lleguen al buzón. Además de evitar que los usuarios caigan en la trampa de esos fraudes, la solución también ayuda a reducir el riesgo por error humano, al evitar que las decisiones o acciones erróneas de los usuarios sean las causantes de infecciones por ransomware, filtración de datos o infracciones en el cumplimiento.

Seguridad de correo electrónico basada en API

SonicWall Cloud App Security (CAS) es una solución de protección de e-mail basada en API y nativa de nube, diseñada para atajar ataques complejos y de alta calidad de phishing y día cero. Estos ataques dirigidos y de bajo volumen están probados sobre el terreno específicamente para evadir los filtros de seguridad que incorporan Microsoft y Google.

A través de APIs, la solución se integra fácilmente en los flujos de seguridad de los sistemas de oficina en la nube, donde se ajusta para identificar los ataques que evaden los filtros de seguridad de oficina en la nube. Además, su sistema inline multicapa para la prevención de amenazas es invisible

NINGÚN E-MAIL, ENLACE O ADJUNTO PUEDE LLEGAR AL BUZÓN HASTA QUE CAS LO HAYA EXAMINADO Y HAYA DETERMINADO QUE ES 100 % INOFENSIVO.

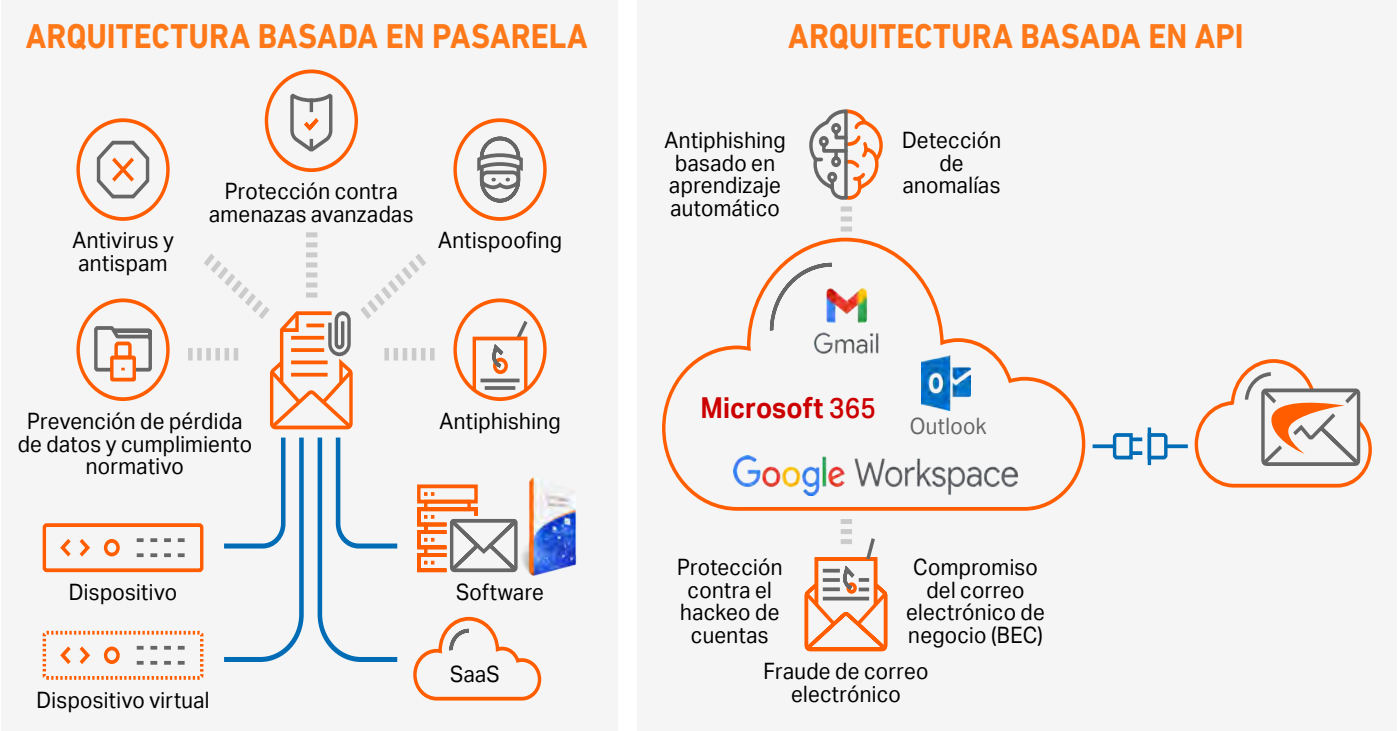
para los atacantes y permite una protección en toda la suite para las aplicaciones de correo y SaaS en la nube.

CAS se instala en minutos y emplea las últimas innovaciones en tecnologías de aprendizaje automático e inteligencia artificial, combinadas con análisis de Big Data. La inteligencia artificial entrena de forma dinámica y continua a múltiples motores de aprendizaje automático y de emulación de amenazas para que reconozcan y detecten nuevas conductas de phishing y sus tácticas, técnicas y procedimientos.

Juntos, analizan cientos de indicadores de amenaza únicos, lo que proporciona una protección efectiva contra phishing, BEC, sandboxing de archivos adjuntos, análisis de URL de tiempo de clic y fraudes.

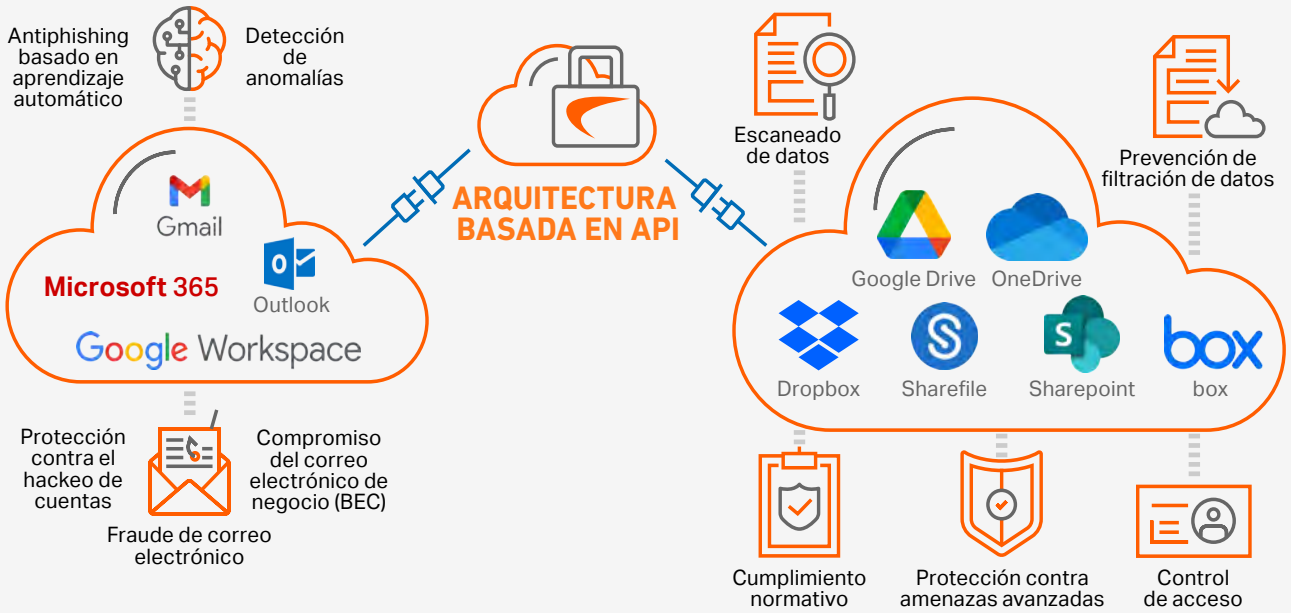
Se personaliza un motor de aprendizaje automático específicamente para la organización. Dicho motor se entrena en el entorno particular del cliente para identificar

Tecnologías Email Security de SonicWall



SONICWALL

SonicWall Cloud App Security



Protección en toda la suite para las aplicaciones de correo y SaaS en la nube

Detenga las amenazas avanzadas y evite la filtración de datos al controlar con quién se comparten los datos de su empresa

amenazas dirigidas contra esa organización en particular y permite una respuesta personalizada.

Otro motor de aprendizaje automático se ajusta específicamente para detectar anomalías y obtener analíticas de la conducta del usuario. Este motor exclusivo detecta conductas o acciones que no parecen «normales» cuando se observan en el contexto de las actividades históricas de una organización y un usuario. El motor analiza el comportamiento mediante algoritmos de aprendizaje automático, que crean un perfil basándose en información sobre eventos históricos, incluidas las localizaciones y las horas de los inicios de sesión, las transferencias de datos y los patrones de los e-mails. Cuando se detecta una anomalía, se genera un evento de seguridad y se proporciona el contexto y otra información necesaria para las investigaciones.

Antes de que lleguen al buzón, CAS realiza un análisis de todos los mensajes (entrantes, salientes e internos). Ningún e-mail, enlace o adjunto puede llegar al buzón hasta que CAS lo haya examinado y haya determinado que es 100 % inofensivo. Las alertas mantienen informado al personal relevante, como el administrador o los analistas de seguridad, sobre los potenciales compromisos, para las resoluciones o recuperaciones posteriores a la entrega.

Seguridad de correo electrónico basada en pasarela

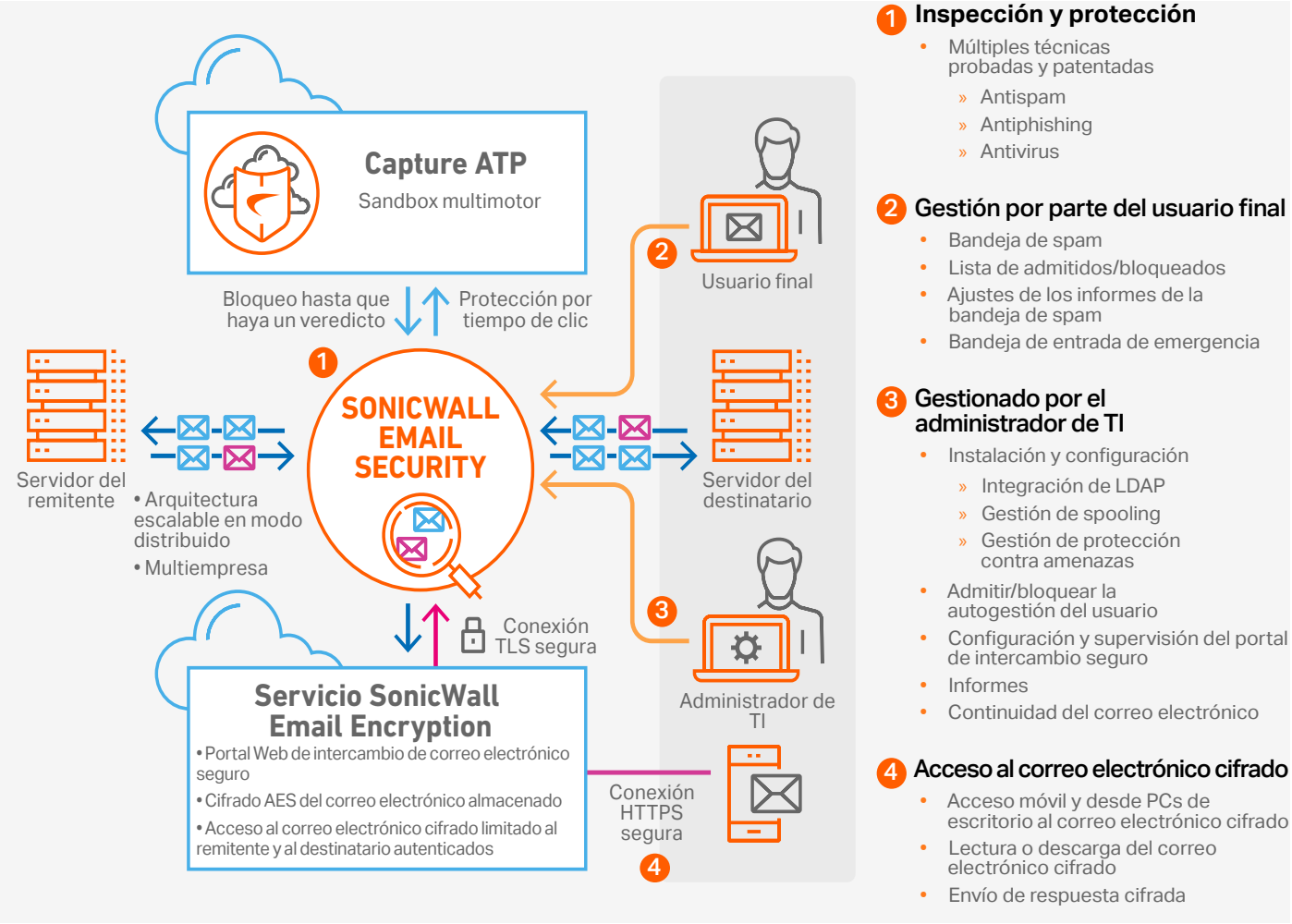
La solución basada en pasarela de SonicWall Email Security combina la inteligencia artificial y las técnicas de aprendizaje automático con funcionalidades de heurística, reputación y análisis del contenido para proporcionar una protección completa contra los ataques de phishing dirigido, spoofing y ransomware.

La línea inicial de defensa elimina hasta el 99 % del spam fácil de detectar a nivel de conexión, antes de que tenga oportunidad de entrar en la red. A continuación, la Gestión avanzada de contenidos (ACM) de SonicWall analiza y filtra cualquier e-mail restante dañino. El sistema de escaneado de ACM detiene con efectividad las campañas más avanzadas de phishing y suplantación, al aprovechar los análisis Adversarial Bayesian™. Las técnicas utilizan motores de análisis avanzados de texto e imágenes; distanciamiento lexicográfico; análisis de imágenes (blanco sobre blanco, fuentes pequeñas, etc.) y detección de mensajes ininteligibles para ver a través del TTP que utilizan las campañas de phishing para ocultar sus intenciones maliciosas.

ACM escanea todos los componentes del correo electrónico (metadatos, cuerpo, asunto, archivos adjuntos, URLs, etc.) para garantizar el cumplimiento de las políticas corporativas. A continuación, la solución bloquea o reenruta los e-mails que no cumplan las normas a los grupos o personas correspondientes, basados en LDAP.

Además, Email Security se integra con el LDAP de su organización para evitar ataques por recolección automática de direcciones (DHA). Asimismo, aprovecha unas definiciones antivirus líderes en el sector que se actualizan continuamente para proporcionar lo último en protección contra el malware. Al mismo tiempo, incluye SPF (Marco de directivas de remitente), DKIM (Correo identificado por claves de dominio) y autenticación de mensajes, informes y conformidad basada en dominios (DMARC), con el fin de detener los ataques de spoofing, el compromiso del correo electrónico de negocio y el fraude de correo electrónico.

Protección con Email Security basada en pasarela



Compromiso del correo electrónico de negocio y detección del fraude de correo electrónico

La ciencia que está detrás del reconocimiento y la detención de los ataques por compromiso del correo electrónico de negocio, fraude y suplantación de personalidad se basa en el contexto interno. Uno de los principales beneficios de implementar la arquitectura basada en API de CAS dentro del servicio de correo en la nube es que se tiene acceso inmediato al historial de conversaciones. A las pocas horas de su instalación, la inteligencia artificial de CAS escanea hasta cinco días de diálogos del correo electrónico para establecer la confianza y la autenticidad de los remitentes.

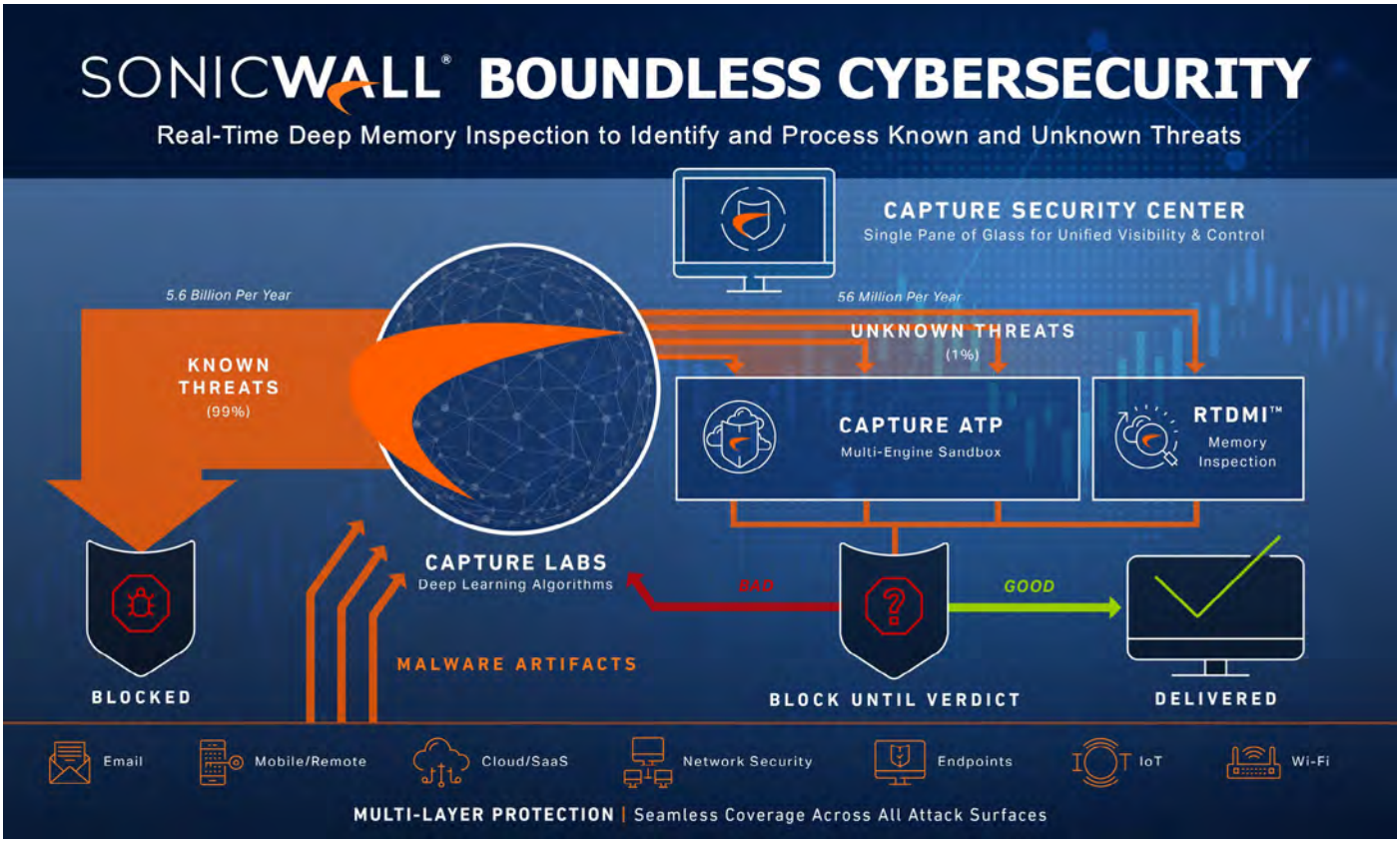
Al mismo tiempo, construye una red de reputación para el aprendizaje continuado de las relaciones y las conductas de los remitentes. Esto proporciona una detección precisa del compromiso del correo electrónico de negocio y reduce el número de falsos positivos que plagan la mayoría de las otras soluciones de correo electrónico. El ajuste, que con otras soluciones de seguridad suele tardar meses, sucede inmediata y automáticamente al utilizar millones de conversaciones históricas de e-mail. La solución también puede reconocer las comunicaciones de usuarios que se salen de lo normal, mientras que otras simplemente lo verían por primera vez.

Detección de anomalías y de hackeo de cuentas

Las anomalías son probables indicadores de que una cuenta está comprometida. CAS tiene un motor específico de detección de anomalías que supervisa las conductas o acciones que parecen atípicas cuando se observan en el contexto de las actividades históricas de un usuario. Mediante algoritmos de aprendizaje automático, analiza esas irregularidades y crea perfiles basándose en la información sobre los eventos históricos de cada usuario, incluyendo las localizaciones y las horas de los inicios de sesión, los datos transferidos y los patrones de los e-mails. Cuando se observan anomalías se generan eventos de seguridad, y se envían alertas con contexto y otra información necesaria a los analistas y a los encargados de la respuesta ante incidentes, para las labores de investigación y toma de medidas.

Protección contra amenazas avanzadas

Los productos de seguridad de correo electrónico de SonicWall son componentes del entorno de la plataforma SonicWall Capture Cloud. Eso permite que trabajen directamente en todo el stack de seguridad de SonicWall, incluidos firewalls, protección de endpoints y productos de seguridad de acceso para la gestión sincronizada de las amenazas.



Además, aprovechan el servicio Capture ATP de SonicWall con la tecnología SonicWall Real-Time Deep Memory Inspection™ (RTDMI), el único sistema galardonado de detección de amenazas avanzadas que utiliza un sandbox multimotor para analizar los archivos adjuntos y las URLs sospechosos que contienen los mensajes de correo.

El motor de análisis de archivos RTDMI patentado de SonicWall analiza los archivos sospechosos al monitorizar la conducta maliciosa de una aplicación en la memoria. RTDMI ve lo que hay detrás de cualquier técnica de ocultación o cifrado que el malware moderno pueda utilizar para evadir el análisis de sandbox. Así, proporciona una detección extremadamente precisa de los ataques contenidos en documentos, ejecutables, elementos archivados y otros tipos de archivos.

Asimismo, RTDMI trabaja conjuntamente con las comprobaciones de reputación, los análisis estáticos y las verificaciones de hash globales del sector de la inteligencia de amenazas, para proporciona un veredicto rápido. Cuando se detectan variantes de malware y ransomware novedosas, se utilizan para crear definiciones para una parte de la cadena de defensa. No obstante, esto también beneficia al instante y en tiempo real al resto del ecosistema de protección multicapa de SonicWall. **Todo el proceso se realiza en cuestión de segundos, lo que reduce significativamente la ventana de exposición.**.

Protección después de la entrega en el buzón

En 2020, la pandemia de COVID-19 creó la plantilla distribuida más extensa de la historia, con miles de millones de personas que utilizaban a diario el correo electrónico desde la comodidad de sus casas. Desgraciadamente, muchas de esas personas no han recibido la preparación adecuada para distinguir los mensajes de correo electrónico legítimos de los falsos, ni saben reconocer un enlace sospechoso. Lo que más miedo da es que ahora los e-mails de phishing pueden estar tan bien hechos que parecen genuinos incluso para los usuarios más conscientes de la seguridad.

Sabemos que los buenos empleados no son perfectos. Basta con hacer clic en el sitio equivocado o descargar algo que no se debe, un solo descuido, y el proceso de infección se despliega a toda velocidad. Para mitigar de forma efectiva el factor humano, SonicWall ha añadido **Click-Time Protection (CTP)**. Esta característica de seguridad llamada «protección en el momento del clic» se ha diseñado especialmente como medida de seguridad adicional para proteger de ellos mismos a los usuarios «inocentes» y por consiguiente salvar a la organización de un desastre potencial.

La principal función de CTP consiste en examinar cada URL y adjunto cuando el usuario hace clic en un enlace o se descarga un archivo dentro de un correo electrónico, aunque se reenvíe a otra persona. Un análisis en tiempo real detecta y pone en cuarentena la URL maliciosa y después informa a los usuarios a través de una notificación en pantalla. Además, si la URL sospechosa enlaza a una campaña de phishing, CTP puede retirar y eliminar los mensajes de correo dañinos que utiliza la propia campaña.

Prevención de filtración de datos

Las soluciones de pasarela y CAS de Email Security vienen cada una con su respectivo módulo de cumplimiento de seguridad, lo que permite controlar con quién y cómo se comparten los datos de la compañía. Ambas permiten establecer y sincronizar políticas unificadas de cifrado y prevención de filtración de datos (DLP) entre los usuarios y las aplicaciones de oficina en la nube. Asimismo, aprovechan más de cien tipos de información y son compatibles con clasificadores de datos que abarcan más de 40 países.

La solución examina todas las partes del e-mail y de las aplicaciones populares para compartir en la nube, incluidos los archivos adjuntos, para asegurarse de que la propiedad intelectual, la información personal identificable (PII) y otros datos que afectan al cumplimiento normativo no salgan de la red de su organización de forma accidental o voluntaria. Además, como preparación para el cumplimiento normativo y las auditorías, la solución proporciona plantillas de políticas que se corresponden con HIPAA, SOX, PCI, RGPD y otras leyes de obligado cumplimiento.

Conclusiones

Las soluciones SonicWall Email Security aplican las últimas tecnologías de inteligencia artificial y aprendizaje automático ajustadas para atrapar los ataques de phishing dirigido, BEC y suplantación de identidad por e-mail, antes de que lleguen al buzón.

Obtenga más información sobre cómo las soluciones SonicWall Email Security pueden proteger a su organización de las amenazas avanzadas que llegan por correo electrónico.

www.sonicwall.com/email-security

Acerca de SonicWall

SonicWall proporciona ciberseguridad sin límites, sin perímetro, para una era hiperdistribuida y una realidad laboral caracterizadas por la movilidad, el trabajo remoto y la inseguridad. Al detectar amenazas desconocidas, proporcionar visibilidad en tiempo real y ofrecer una alta rentabilidad, SonicWall cierra la brecha de la seguridad cibernética para empresas, gobiernos y pymes en todo el mundo. Si desea obtener más información, visite www.sonicwall.com o síganos en Twitter, LinkedIn, Facebook e Instagram.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Si desea obtener más información, consulte nuestra página Web.
www.sonicwall.com

SolutionBrief-AdaptiveEmailSecurity-COG-5189