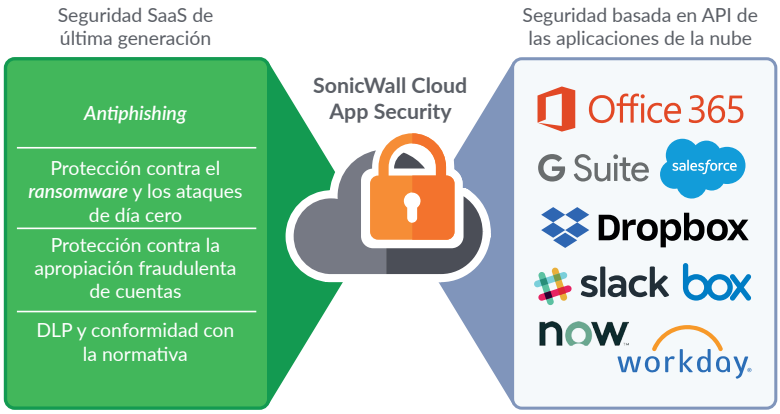
SONICWALL

SonicWall Cloud App Security

SonicWall Cloud App Security ofrece seguridad de última generación para aplicaciones SaaS como Office 365 y G Suite, protegiendo el correo electrónico, los datos y las credenciales de usuario frente a amenazas avanzadas y garantizando al mismo tiempo el cumplimiento normativo en la nube. Si quiere pasar a trabajar en la nube, SonicWall le ofrece la mejor seguridad basada en API con un TCO reducido, gastos generales de implementación mínimos y una experiencia del usuario perfecta.



Visibilidad: Identifique todos los servicios en la nube (autorizados y no autorizados) que utilizan los empleados de una organización. Esto incluye la visibilidad del tráfico este-oeste (nube a nube) ya que los usuarios pueden autenticarse en aplicaciones no autorizadas mediante TI autorizada, como Office 365.

Seguridad para el correo electrónico de última generación: Dado que el correo electrónico se ha convertido en la aplicación SaaS más utilizada, proteger este popular vector de amenaza es clave para la seguridad SaaS. La solución incluye *sandboxing* para archivos adjuntos, protección avanzada de URL y protección contra ataques Business Email Compromise (BEC).

Protección avanzada ante amenazas: Evite la propagación del *malware* a través de aplicaciones como OneDrive, Box y Dropbox con análisis antivirus en tiempo real de amenazas conocidas y *sandboxing* Capture ATP para los ataques de día cero y amenazas desconocidas.

Protección de datos: Aplique políticas de seguridad centradas en los datos ofreciendo controles de acceso granular y evitando la carga de archivos sensibles o confidenciales. La solución incorpora herramientas de políticas basadas en funciones, así como tecnologías de clasificación de datos y prevención de pérdidas de datos que permiten monitorizar la actividad de los usuarios y bloquear o limitar el acceso.

Conformidad: La solución recopila un amplio registro de auditoría de cada acción, incluidos los eventos en tiempo real e históricos, y proporciona plantillas DLP sencillas para imponer controles de políticas y la conformidad con la normativa en tiempo real.

Ventajas:

Seguridad para el correo electrónico de última generación

- Detenga el *ransomware*, los ataques de día cero y el correo electrónico de *phishing* selectivo antes de que lleguen a la bandeja de entrada de los usuarios
- Obtenga protección avanzada frente a las amenazas con *sandboxing* de archivos adjuntos y protección avanzada de URL
- Analice el correo electrónico entrante, saliente e interno en Office 365 y G Suite
- Bloquee los ataques de suplantación de identidad mediante el aprendizaje automático y la inteligencia artificial (IA)
- Retire correos electrónicos maliciosos de las bandejas de entrada de los usuarios después de la entrega

Seguridad SaaS de última generación (CASB)

- Obtenga visibilidad y control granular de las TI aprobadas y en la sombra
- Consiga una cobertura global para el tráfico entre el usuario y la nube y entre nubes
- Evite las cargas de datos sensibles y el uso compartido de archivos sin autorización
- Defina unas políticas de seguridad coherentes para las aplicaciones aprobadas
- Ofrezca protección frente a la apropiación indebida de cuentas (ATO), las amenazas internas y las credenciales comprometidas
- Detenga la propagación del *ransomware* y *malware* de día cero en la nube
- Haga cumplir las políticas de conformidad con la normativa mediante plantillas DLP sencillas
- Identifique violaciones y brechas de seguridad mediante el análisis de eventos históricos y en tiempo real

Seguridad simplificada y asequible

- Brinde una experiencia de usuario fluida para el acceso desde cualquier dispositivo y ubicación
- Elimine puntos de fallo, problemas de latencia y la necesidad de redirigir el tráfico a través de un proxy
- Automatice el descubrimiento de aplicaciones en la nube cuando se implementan con SonicWall NGFW
- Logre un bajo coste total de propiedad (TCO) con una implementación rápida y facilidad de uso

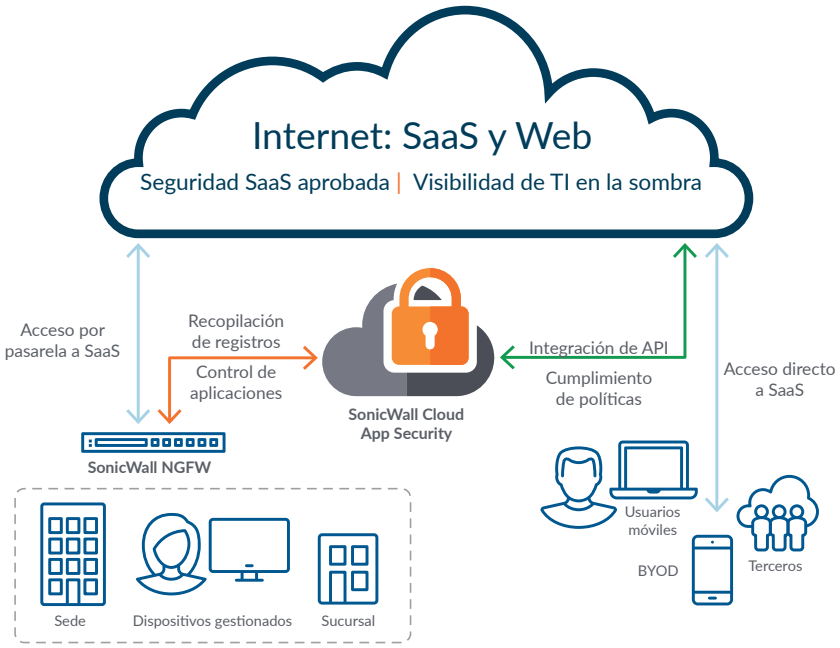
Generalidades de la solución

Descripción de la solución de SonicWall

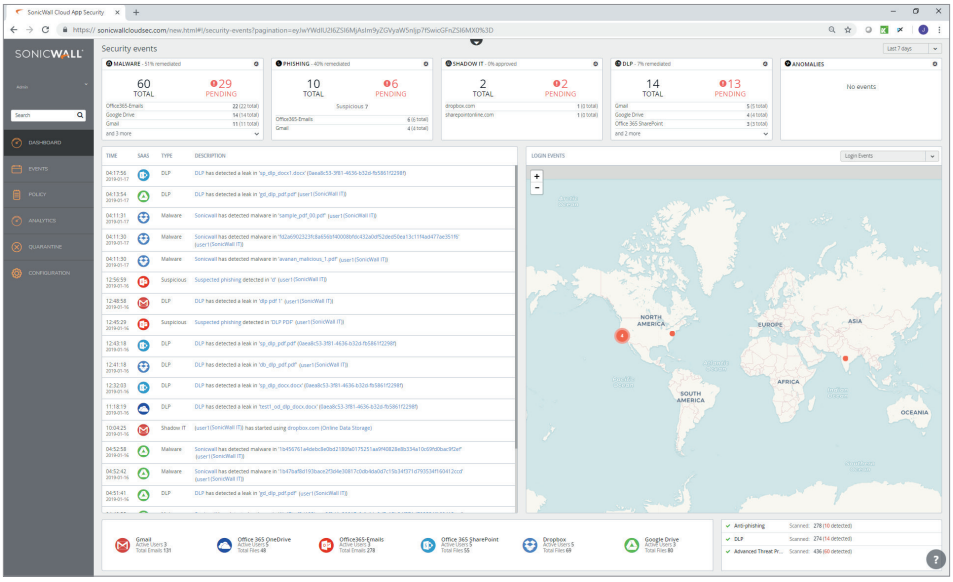
La solución SonicWall Cloud App Security ofrece análisis fuera de banda del tráfico para aplicaciones SaaS aprobadas o no mediante interfaces API y análisis de registro del tráfico.

La solución se integra sin problemas con las aplicaciones SaaS aprobadas a través de interfaces API, ofreciendo funcionalidades CASB: visibilidad, protección avanzada de amenazas, prevención de pérdidas de datos (DLP) y conformidad con la normativa. Al instalarse con un firewall de última generación SonicWall (NGFW), Cloud App Security ofrece visibilidad y control de las TI en la sombra para el uso de la nube en la red.

La solución permite a los departamentos de TI implementar las aplicaciones SaaS sin poner en peligro la seguridad ni la conformidad. Los administradores pueden definir políticas coherentes en todas las aplicaciones SaaS implementadas dentro de la organización desde una sola consola. Use las plantillas disponibles de generación de informes DLP y de conformidad para cerrar rápidamente las brechas de seguridad y establecer políticas personalizadas con el fin de satisfacer las necesidades del negocio y de la normativa. Si ya dispone de unos cientos de usuarios o cientos de miles de empleados distribuidos por todo el mundo, puede ampliar la solución para satisfacer sus necesidades sin necesidad de instalar y gestionar hardware.



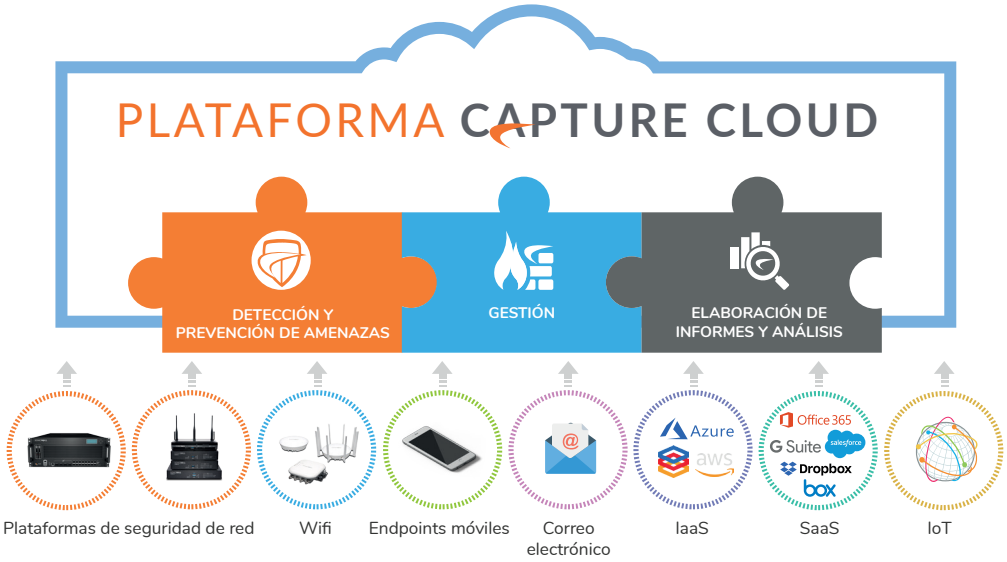
Seguridad SaaS basada en API que ofrece funcionalidades CASB



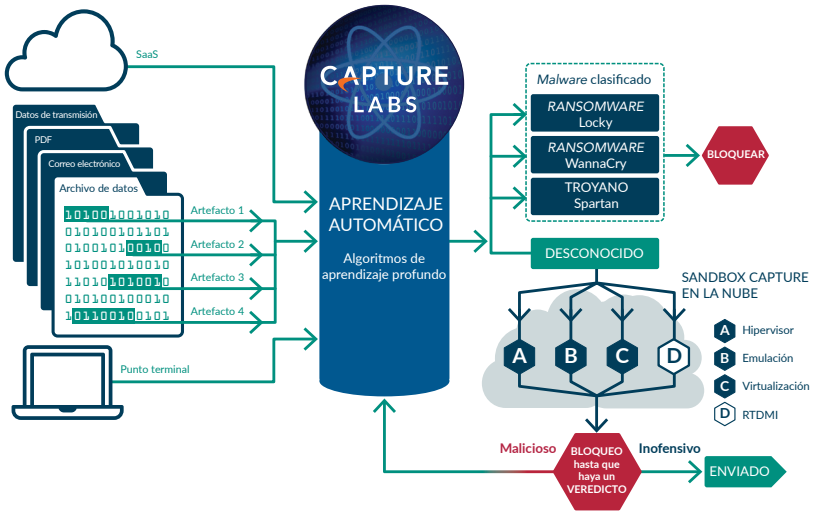
El cuadro de mando en tiempo real permite a los administradores monitorizar el uso de las aplicaciones de riesgo y hacer un seguimiento de la actividad del usuario, del volumen de transacciones y de la ubicación en la que se usa la aplicación. La solución garantiza una adopción segura de las aplicaciones SaaS sin afectar a la productividad de los empleados.

Integración con la plataforma Capture Cloud de SonicWall

SonicWall Cloud App Security es un servicio de seguridad nativo de la nube diseñado a través de la plataforma Capture Cloud y que se ofrece a través de Capture Security Center. La plataforma Capture Cloud de SonicWall proporciona funciones de prevención de amenazas y gestión de red basadas en la nube, así como informes y análisis, para organizaciones de cualquier tamaño. La plataforma consolida la inteligencia de amenazas recopilada de diversas fuentes, incluidos nuestro galardonado servicio de *sandboxing* de red multimotor, Capture Advanced Threat Protection, así como más de 1 millón de sensores de SonicWall situados en todo el mundo. Además, Capture Security Center ofrece gestión a través de un único panel y facilita a los administradores la elaboración de informes históricos y en tiempo real sobre la actividad de la red y de la nube.



Para proteger las aplicaciones SaaS, SonicWall Cloud App Security aprovecha la plataforma SonicWall Capture Cloud, que combina la inteligencia de seguridad global de Capture Threat Network y la prevención avanzada frente a amenazas del *sandbox* multimotor Capture ATP. Este enfoque permite a SonicWall ampliar sus capacidades de prevención automatizada y en tiempo real de violaciones de seguridad en los entornos SaaS, lo cual permite a los administradores trasladarse a la nube. Las API nativas se integran directamente con los servicios de nube, lo que permite a la solución analizar los archivos de aplicaciones como OneDrive o Dropbox mediante el servicio Capture ATP con Real-Time Deep Memory Inspection™ (RTDMI™), evitando que el *ransomware* y el *malware* de día cero penetren en la red.



Seguridad integral para Office 365 y G Suite

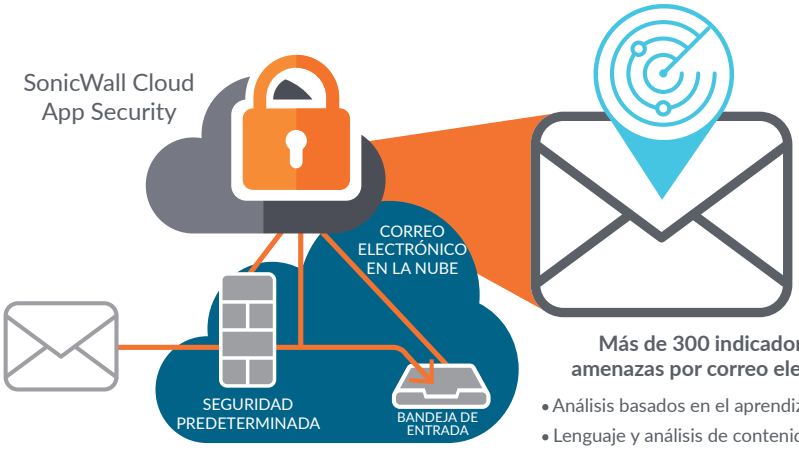
Seguridad de última generación para el correo electrónico en la nube

SonicWall Cloud App Security incluye seguridad del correo electrónico de última generación diseñada para las plataformas de correo electrónico en la nube. Por lo general, cuando las organizaciones trasladan su correo electrónico a la nube, confían exclusivamente en la seguridad integrada del proveedor de correo o la complementan con un proxy MTA tradicional. Las puertas de enlace externas para el correo, sin embargo, quizá no sean suficientes para detectar y bloquear las amenazas actuales.

Además de las tradicionales capas de seguridad para el correo electrónico que ofrecen el SPF, el DKIM y la DMARC, así como la filtración de URL empleando las tres principales fuentes de datos de listas negras de URL, la arquitectura única de Cloud App Security ofrece una protección que ninguna otra solución para la pasarela externa puede dar:

- Añade una capa de protección avanzada frente a amenazas: Cloud App Security bloquea los mensajes de *phishing* no detectados por Office 365 y G Suite. La solución hace uso del aprendizaje automático, la inteligencia artificial y el análisis de *big data* para ofrecer potentes medidas *antiphishing*, entornos aislados para archivos adjuntos, protección avanzada de URL y protección frente a la suplantación de identidad.
- Supervisa los correos entrantes, salientes e internos: La integración con el SaaS de Cloud App Security permite analizar y poner en cuarentena todos los correos electrónicos antes de que estos lleguen a la bandeja de entrada del usuario, ya procedan de fuera de la organización o de una cuenta interna que entrañe riesgo.
- Analiza los mensajes históricos en busca de amenazas: Al conectarse por primera vez, Cloud App Security analiza los mensajes históricos (incluso de cuentas cerradas) para encontrar posibles violaciones de datos o cuentas comprometidas.
- Retirada global de correos electrónicos: Los mensajes pueden editarse o retirarse en cualquier momento si son maliciosos, contienen información confidencial o el empleado ha pulsado «responder a todos» por error.

La protección del correo electrónico de Cloud App Security se aplica antes de la bandeja de entrada, pero después de los filtros nativos de Microsoft o Google (y cualquier pasarela de MTA externa que pueda haberse implementado), por lo que sus algoritmos de aprendizaje automático son capaces de identificar todas las amenazas que estos pasen por alto. Cloud App Security también puede incorporar los resultados de los análisis nativos a sus propios algoritmos de detección.



- Plena integración con Office 365 o G Suite
- Control total del buzón de correo: mensajes entrantes, salientes, internos

Más de 300 indicadores de amenazas por correo electrónico

- Análisis basados en el aprendizaje automático
- Lenguaje y análisis de contenido
- *Sandboxing* de Capture ATP
- Protección avanzada de URL

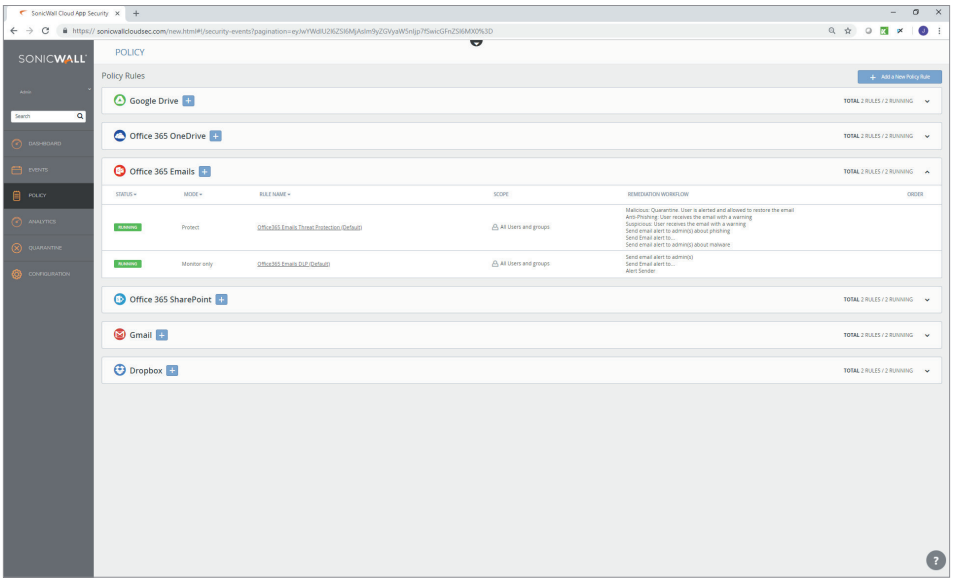
La protección virtual en línea detiene los mensajes maliciosos antes de que lleguen a la bandeja de entrada de los usuarios

Seguridad de última generación para todo el paquete de productividad

Cloud App Security ofrece una seguridad completa y profunda para Office 365 o G Suite. Tanto si utiliza correo electrónico como unidades compartidas, mensajería instantánea (IM) o todo el entorno colaborativo, la solución le ayuda a:

- Prevenir la propagación del *phishing* y el *malware* en su organización y su difusión entre clientes y *partners*.
- Comprobar la presencia de contenido malicioso en todos los archivos utilizando el análisis de contenido activo y el *sandboxing* de Capture ATP para poner en cuarentena las amenazas antes de que sus usuarios las descarguen.
- Identificar información confidencial y aplicar políticas de preparación para la nube que la mantengan dentro de la organización o el grupo de trabajo. Sus usuarios pueden sacar partido de toda la potencia del paquete de productividad basado en la nube mientras los flujos de trabajo automatizados permiten cumplir con las normas, garantizando que los datos de PCI, HIPAA, PII u otros datos confidenciales no se compartan externamente.

Protección integral del paquete Office en la nube



Cada aplicación SaaS tiene un motor de políticas totalmente diferente, cada una de ellas con sus propias reglas y capacidades de cumplimiento. Las soluciones de SonicWall las asignan a todas las aplicaciones SaaS aprobadas y proporcionan más controles granulares. De este modo, Cloud App Security le permite crear una única política que se aplica de manera coherente en todas las aplicaciones.

Además, las políticas contextuales permiten crear flujos de trabajo de cumplimiento que informan del problema al usuario, ofrecen opciones de políticas seguras y auditan las respuestas por encima y más allá de lo que normalmente permiten los controles de permisos integrados en cada SaaS.

Seguridad SaaS

Para proteger el uso de SaaS dentro de las organizaciones, SonicWall Cloud App Security ofrece:

Seguridad de TI aprobada: se integra directamente con los servicios de nube mediante interfaces API para brindar una protección avanzada ante amenazas y prevención de pérdidas de datos dentro de los entornos SaaS.

Visibilidad y control informáticos en la sombra: integración fluida con SonicWall NGFW para el descubrimiento automatizado de aplicaciones de la nube y la evaluación de riesgos mediante análisis del registro de tráfico.

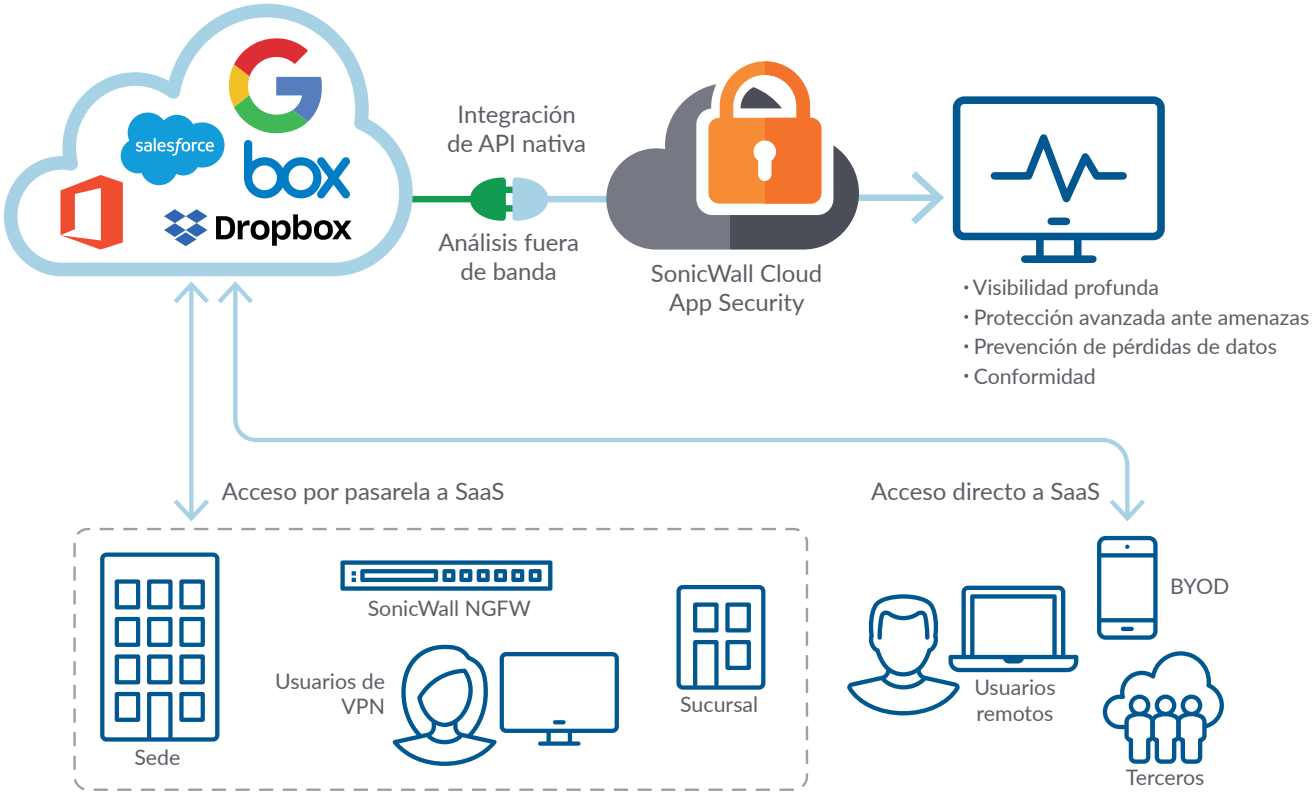
Seguridad de TI aprobada

Cuando se adoptan aplicaciones SaaS como Box y Dropbox, la responsabilidad de garantizar la seguridad de los datos recae en la organización y no en el proveedor de servicios de la nube (CSP). Esta información se suele divulgar en letra pequeña y los CSP no rinden cuentas por las fugas de datos o la infección y propagación de *malware*. De ahí que las organizaciones que decidan usar estas aplicaciones deben considerar la implementación de una solución que permita inspeccionar los datos en las aplicaciones de la nube.

Solo las soluciones basadas en API son capaces de inspeccionar datos en reposo dentro de las aplicaciones SaaS, ya que las soluciones en línea basadas en proxy inspeccionan únicamente los datos cargados en la nube desde detrás de un firewall. Dado que muchas organizaciones disponen ya de un gran volumen de datos almacenados en la nube, las API sirven para aplicar políticas a estos datos. Entre otras funciones (solo posibles con conexión directa a una aplicación a través de API), se encuentra la capacidad de analizar los ajustes de configuración de seguridad en la aplicación y sugerir cambios que la refuercen, además de la posibilidad de analizar los permisos de uso compartido de archivos y carpetas para evaluar el riesgo de acceso externo o de terceros a los datos de la empresa.

La solución ofrece visibilidad profunda, protección avanzada contra amenazas mediante el *sandbox* Capture ATP y prevención contra pérdida de datos para aplicaciones SaaS, como el correo basado en la nube, junto con aplicaciones de uso compartido de archivos y almacenamiento en la nube como Google G Suite y Microsoft Office 365.

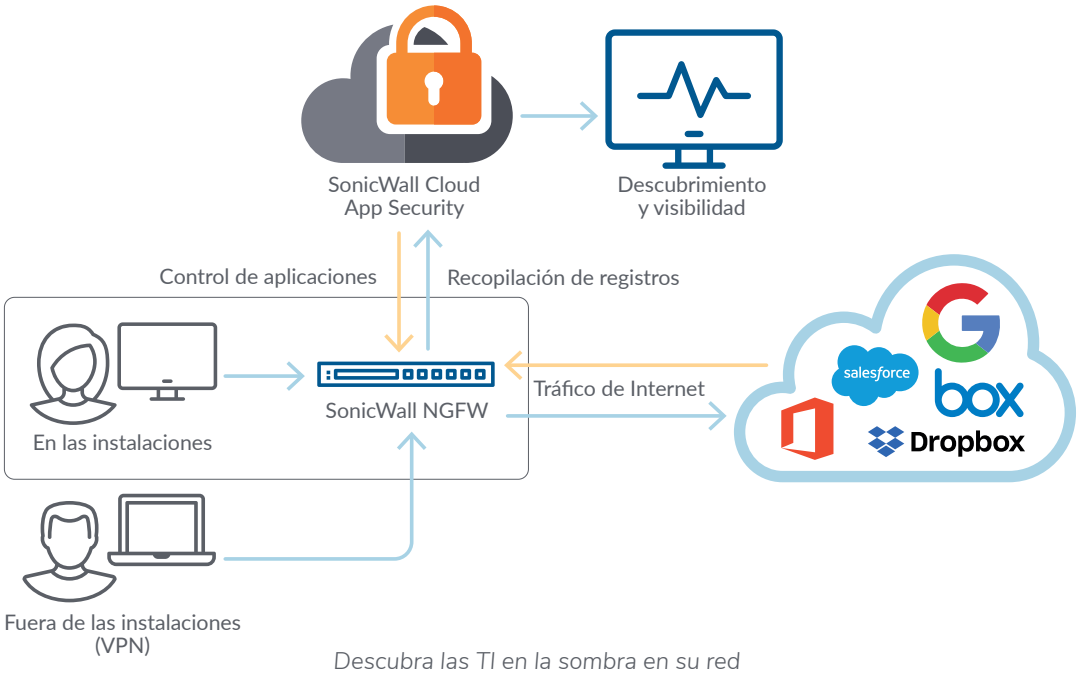
SonicWall Cloud App Security analiza todo el tráfico (eventos de registro, actividades de los usuarios, archivos y objetos de datos, estado de la configuración, etc.) y aplica las políticas de seguridad necesarias a través de integraciones directas con API nativas del servicio en la nube. La solución saca partido de las API nativas, por lo que no utiliza un proxy ni se inserta entre el usuario y la nube. De este modo, la solución proporciona cobertura para esas aplicaciones, con independencia del dispositivo o de la red del usuario. Además, la estrategia basada en API permite una fácil implementación, un control granular y un impacto nulo en la experiencia del usuario.



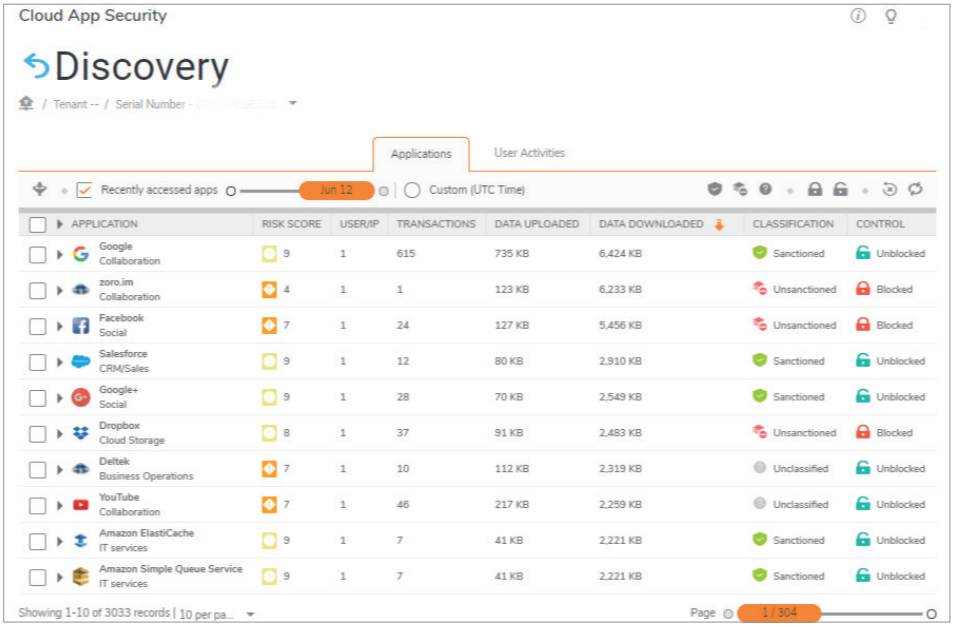
Aplicaciones SaaS aprobadas seguras

Visibilidad y control informáticos en la sombra

Los NGFW de SonicWall analizan y registran todo el tráfico que entra y sale de la red. Los registros generados para el tráfico saliente no distinguen claramente las aplicaciones de nube utilizadas y tampoco proporcionan una puntuación de riesgo para cada aplicación utilizada por los usuarios. Para los empleados remotos redireccionados por los NGFW que utilizan VPN, la solución utiliza estos registros con el fin de recopilar información adicional sobre las acciones realizadas por los usuarios en los servicios de nube. Cloud App Security procesa los archivos de registro de los NGFW de SonicWall y revela qué servicios en la nube están siendo utilizados por qué usuarios, los volúmenes de datos cargados y descargados de y hacia la nube, y el riesgo y la categoría de cada servicio en la nube. De hecho, Cloud App Security se encarga de preparar la infraestructura existente para la nube. A medida que los empleados cada vez utilizan más aplicaciones en la nube para el trabajo, Cloud App Security permite a los administradores detectar brechas en la seguridad, clasificar las aplicaciones de nube en aplicaciones de TI autorizadas y no autorizadas, y reforzar políticas de acceso para bloquear las aplicaciones que impliquen riesgos. Cloud App Security es una parte fundamental de la visión de SonicWall de ofrecer funciones de prevención y detección de violaciones de datos en tiempo real para los usuarios que adoptan tecnologías en la nube.



Descubra las TI en la sombra en su red



SonicWall Cloud App Security descubre y notifica servicios de TI en la sombra de riesgo mediante una base de datos de reputación exclusiva de servicios basados en la nube mantenida por SonicWall.

A las aplicaciones descubiertas se les asigna una puntuación de riesgo derivada de un algoritmo basado en la reputación y en las certificaciones de seguridad y conformidad. Los administradores de TI pueden clasificar las aplicaciones en función de la puntuación de riesgo como aplicaciones de TI aprobadas o no aprobadas para su uso. A través de Capture Security Center, la solución capacita a los administradores a establecer políticas de bloqueo/desbloqueo y controlar las actividades de las TI en la sombra en la red.

Prestaciones

PRESTACIÓN		VENTAJAS
Visibilidad	Descubrimiento de aplicaciones de la nube	Automatice el descubrimiento de aplicaciones de la nube aprovechando los archivos de registro de su firewall SonicWall para identificar las actividades de las TI en la sombra en la red
	Visibilidad del uso de la nube	Obtenga una representación visual en tiempo real de las aplicaciones que se utilizan, volumen de tráfico, actividad del usuario y ubicación de uso
	Evaluación de riesgos de las aplicaciones	Tome decisiones informadas para bloquear/desbloquear las aplicaciones según la evaluación del riesgo
	Supervisión de eventos	Monitorice cada acción, incluidos los eventos históricos y en tiempo real, que se lleva a cabo en su entorno SaaS
Seguridad para el correo electrónico de última generación	*Antiphishing*	Detenga los ataques selectivos de *phishing* que están diseñados para evadir la seguridad predeterminada que ofrece Office 365 o G Suite
	Antispoofing	Proteja su marca corporativa y a los usuarios contra fraudes de correo electrónico y ataques de suplantación de identidad
	Sandboxing de archivos adjuntos	Bloquee los archivos adjuntos de correos electrónicos maliciosos para que no lleguen a las bandejas de entrada de los usuarios
	Protección avanzada de URL	Asegúrese de que los usuarios están protegidos frente a URL embebidas maliciosas
Protección avanzada ante amenazas	Protección contra el *malware* de día cero	Evite que el *malware* se almacene y propague a través de aplicaciones como Box, Dropbox, OneDrive y G Drive
	Protección contra la apropiación fraudulenta de cuentas	Proteja las credenciales SaaS detectando comportamientos anómalos de los usuarios, violaciones de permisos o cambios de configuración
Seguridad de datos	Clasificación de datos	Identifique los datos sensibles o confidenciales y aplique políticas en todas las aplicaciones SaaS para controlar cómo se puede compartir dicha información
	Control de acceso centrado en los datos	Gestione los permisos de archivos de acuerdo con el rol del usuario y el tipo de datos que contiene el archivo
	Flujos de trabajo de corrección	Asegúrese de que los datos no afecten al negocio a través del cumplimiento de las políticas en tiempo real
Conformidad	Plantillas de conformidad	Reduzca los gastos administrativos utilizando plantillas de conformidad sencillas para satisfacer los requisitos de SOX, PCI, HIPAA y GDPR
	Registro de auditoría	Acceda a los datos de eventos históricos para una auditoría de conformidad retrospectiva así como una elaboración de informes en tiempo real
	Cumplimiento de políticas	Haga cumplir en tiempo real las políticas de cada SaaS para controlar los permisos de acceso, traslado de archivos, bloqueo y edición de correo electrónico y comuníquese tanto con usuarios como con administradores

SonicWall Cloud App Security	CLOUD APP SECURITY - BÁSICO	CLOUD APP SECURITY - AVANZADO
Unified Cloud Management (Capture Security Center)	●	●
Aplicaciones de la nube compatibles	Seleccione 1 aplicación SaaS (Office 365 o G Suite)	Elija hasta 10 aplicaciones SaaS
Antiphishing para O365 Mail o Gmail	●	●
Capture ATP* para archivos adjuntos de correo electrónico	●	●
Protección avanzada de URL	●	●
Capture ATP* para los archivos almacenados en SaaS	●	●
Protección contra la apropiación fraudulenta de cuentas	●	●
Protección contra pérdidas de datos	—	●
Visibilidad de TI en la sombra**	—	●

SonicWall Capture ATP incluye Real-Time Deep Memory Inspection™ (RTDMI™)
***Requiere SonicWall NGFW*

Información de pedido de Cloud App Security:

Para saber cómo hacer un pedido de Cloud App Security y obtener información sobre los precios, póngase en contacto con su distribuidor o con el departamento de ventas de SonicWall aquí.

Haga clic aquí para obtener una versión de prueba gratuita de 30 días de SonicWall Cloud App Security - Avanzada

Para obtener más información sobre Cloud App Security, visite www.sonicwall.com/casb.

Servicios habilitados por partners

¿Necesita ayuda para planificar, implantar u optimizar su solución de SonicWall? Los partners de servicios avanzados de SonicWall están formados para prestarle servicios profesionales de primera clase. Obtenga más información en www.sonicwall.com/PES.

Acerca de SonicWall

SonicWall lleva más de 27 años combatiendo el crimen cibernético y defendiendo a pequeñas y medianas empresas, así como a grandes compañías y agencias gubernamentales de todo el mundo. Con el respaldo de SonicWall Capture Labs, nuestras galardonadas soluciones de detección y prevención de violaciones de seguridad en tiempo real protegen más de un millón de redes, sus correos electrónicos, aplicaciones y datos, en más de 215 países y territorios. Estas organizaciones funcionan con mayor eficacia y menos temor a la seguridad. Si desea más información, visite www.sonicwall.com o síganos en Twitter, LinkedIn, Facebook e Instagram.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
(Estados Unidos)
Encontrará más información en nuestro sitio web.
www.sonicwall.com

Datasheet-CloudAppSecurity-US-VG-MKTG5359

SONICWALL®