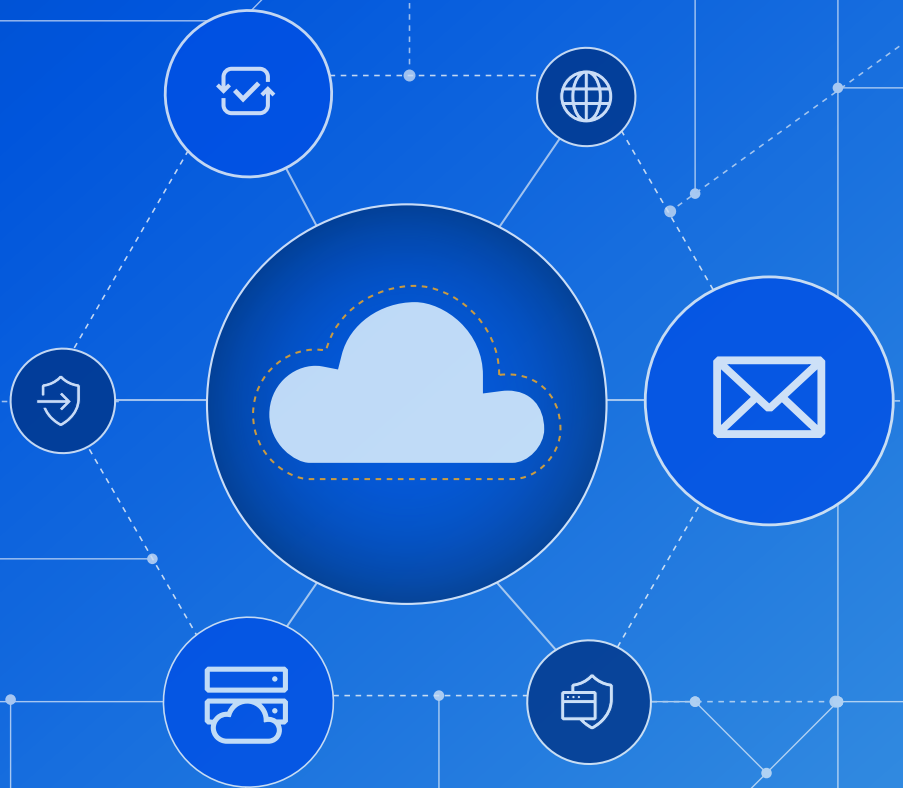
CLOUDFLARE

DOCUMENTO TÉCNICO

Simplificamos la protección de las aplicaciones SaaS

Cómo proteger a los usuarios y los datos con un enfoque Zero Trust



Contenido

Introducción

En el entorno distribuido actual, las aplicaciones de software como servicio (SaaS) han brindado a las organizaciones una mayor flexibilidad para dar soporte a los usuarios corporativos y proveedores de todo el mundo. Algunos de los conjuntos de aplicaciones SaaS más destacados actualmente incluyen la comunicación (envío de correo electrónico, plataformas de chat), la productividad (documentos, hojas de cálculo) y la colaboración (almacenamiento en línea). Para 2025, Gartner prevé que el 85 % de las empresas dirigirán sus negocios bajo el principio de "prioridad por la nube", y SaaS será la herramienta preferida para las implementaciones de gestión de acceso[1].

Si bien las aplicaciones SaaS permiten a las organizaciones ser más ágiles, el cambio a la nube conlleva riesgos de seguridad y rendimiento, especialmente para las organizaciones que combinan varias soluciones específicas diseñadas para funcionar de manera independiente. Los equipos de seguridad, redes e informática, encargados de implementar y gestionar docenas, si no cientos, de estas aplicaciones, a menudo tienen poco tiempo, tienen dificultades para conseguir visibilidad en toda la organización y lidian con brechas de seguridad y conectividad provocadas por los servicios que no están diseñados intrínsecamente para trabajar juntos.

Como resultado, muchas organizaciones se ven obligadas a buscar mejores formas de consolidar los productos de seguridad en todo su entorno SaaS, para aumentar la eficiencia, reducir la complejidad de la gestión y la implementación, y recibir soporte consolidado.

Gartner estima que, para 2025, el 80 % de las empresas recurrirán a soluciones de un único proveedor que unifiquen el acceso a la web, los servicios en la nube y las aplicaciones privadas desde una plataforma de servicios de seguridad en el perímetro (SSE)[2].

El recorrido hacia la seguridad SaaS simplificada conlleva varias consideraciones importantes. La forma en que los equipos de trabajo se comunican y operan hoy en día exige un enfoque simple y escalable de la seguridad, uno que esté diseñado para anticiparse a los riesgos emergentes, que reduzca los incidentes que provienen de las aplicaciones SaaS y que facilite a los equipos de seguridad supervisión y prevención de las amenazas a sus organizaciones.

Sigue leyendo para descubrir cómo una plataforma Zero Trust, que integra capacidades de agente de seguridad de acceso a la nube (CASB) y seguridad del correo electrónico en la nube (CES), facilita el camino para detener la pérdida de datos, el phishing, el ransomware, el Shadow IT y el movimiento lateral en toda tu organización.

[1] Gartner, "Forecast Analysis: Information Security and Risk Management, Worldwide". Analistas: Shailendra Upadhyay, Mark Driver, Christian Canales, Ruggero Contu, Lawrence Pingree, Elizabeth Kim, John A. Wheeler, Nat Smith, Rahul Yadav, Swati Rakheja, Dave Messett, Mark Wah, Shawn Eftink. 12 de agosto de 2021. Gartner. [2]Gartner, "Predicts 2022: "Consolidated Security Platforms Are the Future". Analistas: Charlie Winckless, Joerg Fritsch, Peter Firstbrook, Neil MacDonald, Brian Lowans. 1 de diciembre de 2021. Gartner.

La evolución de CASB

La seguridad integral de SaaS requiere varias tecnologías fundamentales para que los equipos de seguridad puedan obtener visibilidad de todo su entorno SaaS, supervisar y mitigar fácilmente las amenazas, y proteger el acceso a los sistemas y datos confidenciales. Uno de los componentes más importantes de cualquier estrategia de seguridad SaaS es un agente de seguridad de acceso a la nube (CASB) que ofrece controles de seguridad de datos y visibilidad de los servicios y aplicaciones alojados en la nube de una organización.

Seguridad SaaS 101: CASB

El CASB de SaaS permite a los equipos informáticos y de seguridad ver toda la configuración de los datos y la actividad de los usuarios desde un único panel de control. Sus capacidades varían según el proveedor, pero suelen incluir las siguientes características[3]:

- **Protección de datos:** los CASB protegen los datos confidenciales e impiden que salgan de los sistemas controlados por la empresa.
- **Control de acceso:** los CASB ayudan a controlar lo que los usuarios pueden ver y hacer dentro de las aplicaciones controladas por la empresa. También pueden proporcionar capacidades de verificación de la identidad para garantizar que los usuarios son quienes dicen ser.
- **Detección de Shadow IT:** los CASB ayudan a identificar los sistemas y servicios no autorizados (comúnmente denominados "Shadow IT") que los usuarios utilizan con fines empresariales. Al clasificar estos sistemas, pueden detectar y mitigar riesgos de seguridad previamente desconocidos.
- **Protección frente a amenazas:** los CASB utilizan la detección antimalware, el espacio seguro, la inspección de paquetes y otras tecnologías para ayudar a bloquear las fugas de datos y los ataques externos.
- **Gestión de la postura:** los CASB ofrecen a los equipos de seguridad información sobre el análisis del comportamiento de los usuarios y el control del estado de las aplicaciones, de modo que puedan inspeccionar fácilmente el movimiento y el seguimiento de las amenazas en su entorno SaaS.
- **Conformidad:** los CASB ayudan a las organizaciones a cumplir con los requisitos normativos (por ejemplo, SOC 2, HIPAA, RGDP, etc.) mediante la identificación de las configuraciones erróneas, evitando así las sanciones y multas asociadas por el incumplimiento de normativa.

[3] Esta no es una lista exhaustiva de las capacidades que puede incluir una oferta de CASB.

Desafíos actuales de CASB

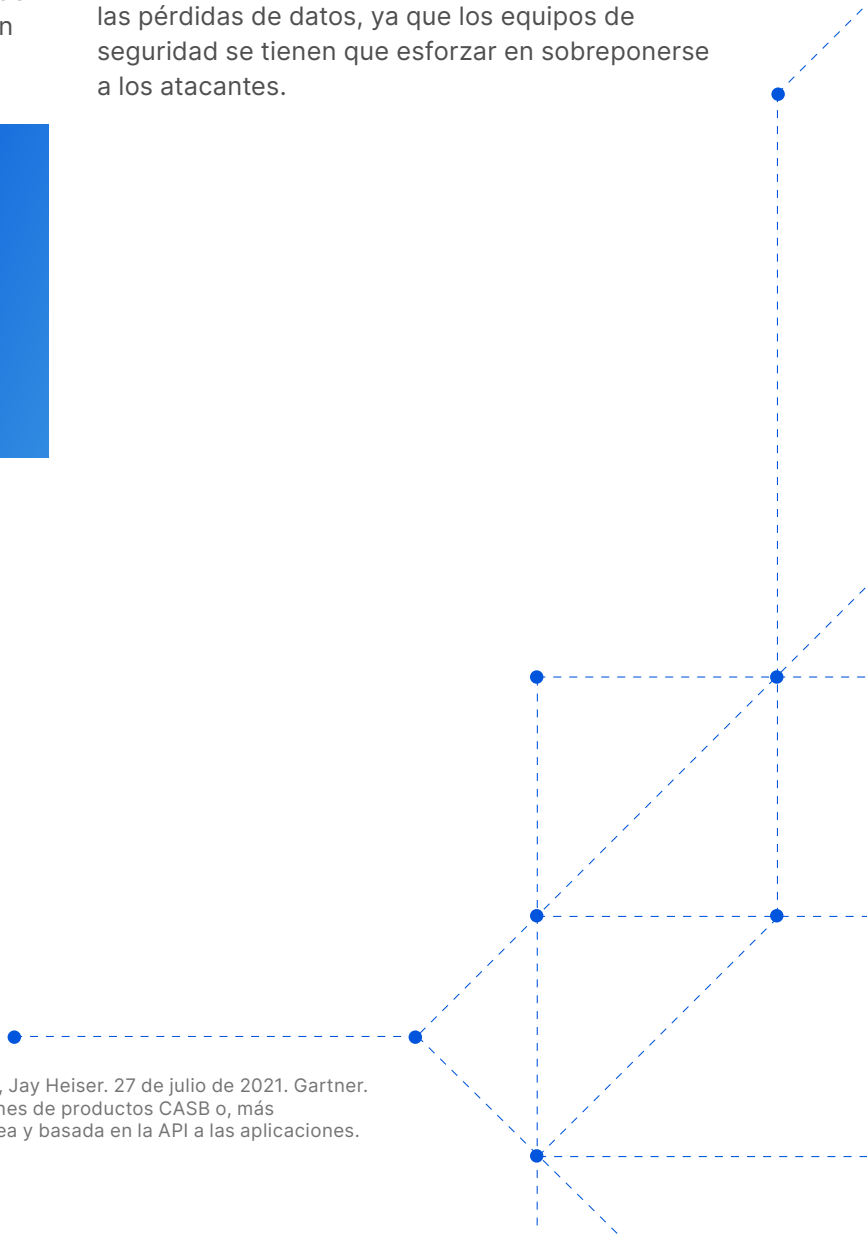
Conforme aumenta la adopción de SaaS, también lo hace la superficie de ataque que las organizaciones necesitan proteger. En lugar de una única base de datos que contenga datos útiles, esos datos están ahora dispersos en aplicaciones que son gestionadas por terceros (p. ej. Dropbox, Google Drive, etc.), independientemente de que las hayas puesto en espacios aislados para uso corporativo.

Si bien los CASB ayudan a proteger los datos corporativos y a los usuarios dentro de las aplicaciones SaaS, todavía no capturan todas las amenazas. Dado que se procesa un mayor volumen de datos útiles mediante aplicaciones SaaS, los atacantes se dirigen cada vez más a estas aplicaciones para materializar fugas de datos y otras amenazas. Además, errores de configuración y de usuario sencillos también pueden dejar la puerta abierta a estos ataques:

Gartner prevé que más del 99 % de las filtraciones en la nube hasta 2025 se originarán por errores de configuración evitables o fallos de usuarios[4].

Cuando se trata de anticipar y remediar errores de configuración de los usuarios y modernos ataques a las aplicaciones SaaS, muchos CASB se quedan cortos. Para solucionarlo, algunos proveedores han empezado a ofrecer servicios de gestión de la postura de seguridad en la nube o SaaS (CSPM o SSPM[5]), que están diseñados para rastrear errores de configuración y cumplimiento en el plano de control. Sin embargo, este no es el caso en general, lo que deja a muchas organizaciones sin las capacidades de detección y corrección que necesitan.

Además, algunas soluciones de CASB no identifican las fugas de datos antes de que se produzcan, lo que encarece los costes de corrección y aumenta las pérdidas de datos, ya que los equipos de seguridad se tienen que esforzar en sobreponerse a los atacantes.



[4] Gartner, "Hype Cycle for Cloud Security, 2021". Analistas: Tom Croll, Jay Heiser. 27 de julio de 2021. Gartner.
[5] Estos servicios y funciones se ofrecen a menudo junto a las soluciones de productos CASB o, más comúnmente, como parte de ellas, proporcionando protección en línea y basada en la API a las aplicaciones.

Problemas de implementación e integración de CASB

Conforme los proveedores de SaaS refuerzan las capacidades de sus soluciones de seguridad integradas, quedan dos grandes escollos: la integración y la visibilidad. Estos proveedores hacen que los datos sean accesibles y fáciles de usar, pero el peso sigue recayendo en las organizaciones que deben consolidar las capacidades de seguridad de una manera que sea fácil de gestionar. Para las organizaciones que adoptan varias soluciones específicas, el seguimiento de las amenazas a través de diferentes plataformas resulta más difícil cuando esas soluciones no están diseñadas para integrarse entre sí o vienen con diferentes niveles de visibilidad.

Este enfoque aumenta la complejidad del entorno de las aplicaciones, por lo que incluso los ataques básicos se vuelven más difíciles de anticipar y mitigar, ya que los atacantes solo necesitan identificar las fugas de las plataformas de seguridad para llevar a cabo los ataques sin ser detectados. Con un CASB, las organizaciones pueden acceder a los productos de seguridad desde el mismo lugar, lo que les ofrece mejor visibilidad y capacidad de mitigación en toda su pila de seguridad.

Aun así, los CASB son solo una pieza de una estrategia de seguridad SaaS más amplia. Para cubrir todo el entorno SaaS, las organizaciones necesitan converger las capacidades del CASB con otras tecnologías Zero Trust, sin añadir una complejidad innecesaria ni obligar a los equipos de seguridad a configurar y mantener manualmente cada herramienta. Controlar con éxito el SaaS a escala no puede ser un proceso manual. Se requiere un proceso de automatización para complementar las plataformas de gestión del SaaS y las herramientas CASB, permitiendo a las organizaciones mitigar eficazmente una amplia gama de amenazas sin el riesgo de desgastar a sus equipos o a que los usuarios cometan errores de configuración, entre otros.

La evolución de la seguridad del correo electrónico

Como ocurre con la mayoría de los servicios SaaS, la comunicación por correo electrónico ha evolucionado como una aplicación empresarial esencial para organizaciones de todos los tamaños. Con el cambio a la nube y el trabajo remoto, más organizaciones están recurriendo a soluciones de correo electrónico en la nube dentro de Microsoft 365 y Google Workspace, en concreto, hasta el 70 % de las organizaciones en todo el mundo, según Gartner[6].

En consecuencia, el correo electrónico es ahora la aplicación SaaS más adoptada y constituye una de las mayores superficies de ataque para el phishing, el malware, la suplantación de identidad, los ataques al correo electrónico corporativo y otras amenazas modernas.

Sin embargo, la protección contra los ataques al correo electrónico puede ser una tarea tediosa y abrumadora para los equipos de seguridad, especialmente porque los atacantes siguen empleando tácticas más sofisticadas contra usuarios confiados. Para salvaguardar a los usuarios y los datos de estas amenazas, los responsables de seguridad deberían considerar la integración del correo electrónico en su plataforma de seguridad SaaS de forma que mejore la visibilidad y proporcione una protección más sólida y simplificada.

Seguridad SaaS 101: seguridad del correo electrónico

La seguridad moderna del correo electrónico abarca un conjunto de herramientas, procesos y técnicas para proteger las cuentas y el contenido del correo electrónico contra ataques maliciosos y accesos no autorizados. Algunos de los tipos más comunes de tecnologías de seguridad del correo electrónico son los siguientes:

- **Puertas de enlace de correo electrónico seguras (SEG):** procesan y filtran el tráfico SMTP, y requieren que las organizaciones cambien su registro MX para que apunte a su agente de transferencia de correo.
- **Seguridad del correo electrónico en la nube (CES):** analiza el contenido del correo electrónico (mediante el acceso a la API de los proveedores de correo electrónico en la nube) sin necesidad de cambiar el registro MX. (Nota: Gartner se refiere a esta categoría como "ICES" o "CES integrada".)
- **Domain-based Message Authentication Reporting and Conformance (DMARC):** autentifica los mensajes de correo electrónico mediante la comprobación de los registros del marco de política de remitente (SPF) y DomainKeys Identified Mail (DKIM). Dentro de este sistema, los correos electrónicos que no superan las comprobaciones SPF o DKIM se marcan como spam o se bloquean para que no lleguen a su destinatario.
- **Protección de datos del correo electrónico (EDP):** las soluciones EDP utilizan el cifrado para evitar la pérdida accidental de datos y el acceso no autorizado al contenido del correo electrónico.

---

[6] Gartner, "Market Guide for Email Security". Analistas: Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer. 7 de octubre de 2021. Gartner.

Desafíos actuales de la seguridad del correo electrónico

El correo electrónico, que originariamente se entregaba a través de plataformas de software locales, se ha ido desplazando cada vez más hacia sistemas de entrega nativos de la nube. Muchas organizaciones han recurrido a conjuntos de servicios de productividad con muchas funciones, como Microsoft 365 y Google Workspace, que permiten a los usuarios trabajar y colaborar de forma más eficaz.

Dado que el correo electrónico existe desde hace mucho tiempo, incluso los usuarios esporádicos son conscientes de algunas de las amenazas más frecuentes que pueden encontrar, como correos electrónicos sospechosos, enlaces maliciosos, etc. Como resultado, los atacantes han desarrollado sus estrategias para dificultar la identificación entre mensajes legítimos y maliciosos. Estas amenazas combinadas recorren varios canales de comunicación para parecer más legítimas (p. ej. vishing, smishing, etc.), y a menudo consiguen engañar a los usuarios para que faciliten información confidencial.

El aumento del uso del correo electrónico también expone a las organizaciones a fugas. Una vez que un atacante obtiene acceso a la cuenta de correo electrónico de un usuario, a menudo le resulta fácil moverse lateralmente dentro de una organización y poner en riesgo o robar datos confidenciales. Además, si bien los proveedores de correo electrónico en la nube ofrecen capacidades limitadas de seguridad integradas, diseñadas para mitigar amenazas comunes como el spam, el malware y el phishing, son notablemente deficientes contra los ataques de remitentes internos comprometidos que se mueven lateralmente de una bandeja de entrada a otra.

Para combatir estas amenazas, las soluciones de seguridad del correo electrónico también están evolucionando. Las plataformas de correo electrónico nativas de nube ofrecen un nivel básico de capacidades de seguridad integradas que pueden hacer frente a los ataques comunes de spam y malware.

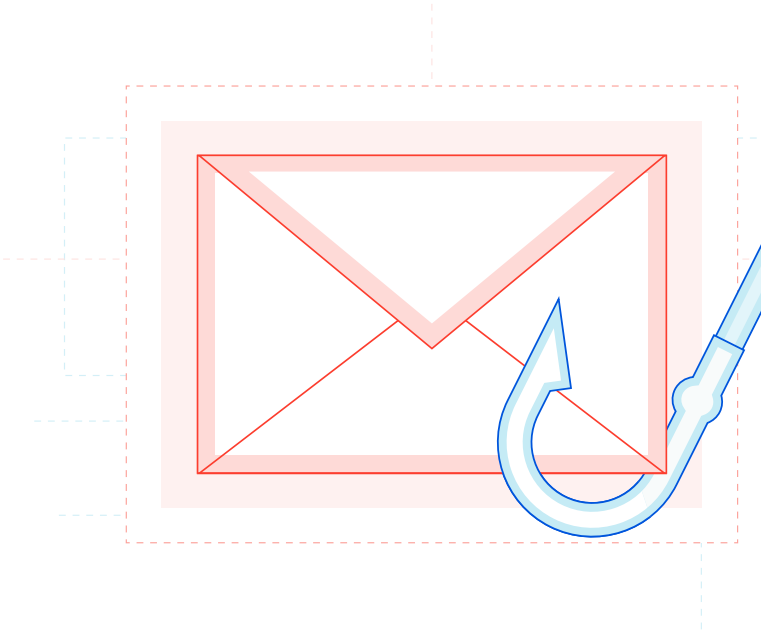
Para 2023, Gartner estima que al menos el 40 % de las organizaciones se apoyarán en esta protección integrada en lugar de adoptar herramientas independientes como las SEG[7].

Muchas organizaciones optan por simplificar su pila de seguridad del correo electrónico renunciando a las SEG, y buscando en su lugar ofertas de seguridad que detengan los ataques avanzados de phishing y ataques al correo electrónico corporativo mientras se integran estrechamente con su entorno de correo electrónico en la nube a través de la API. Para 2023, Gartner estima que el 20 % de las soluciones contra el phishing se suministrarán a través de la integración de la API con plataformas de correo electrónico[8].

[7] Gartner, "Market Guide for Email Security". Analistas: Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer. 7 de octubre de 2021. Gartner. [8] Gartner, "Market Guide for Email Security".

Problemas de implementación e integración de la seguridad del correo electrónico

Aunque estas capacidades integradas proporcionan a las organizaciones cierta tranquilidad, no son ni mucho menos suficientes para combatir las modernas amenazas del correo electrónico. Categorías completas de ataques, como el phishing de objetivo definido, los ataques al correo electrónico corporativo, entre otros, requieren plataformas de seguridad específicas que no ofrecen los proveedores de correo electrónico. Además, las soluciones de seguridad del correo electrónico heredadas no están diseñadas para escalar, combatir los desafíos nativos de la nube o detectar ataques muy específicos.



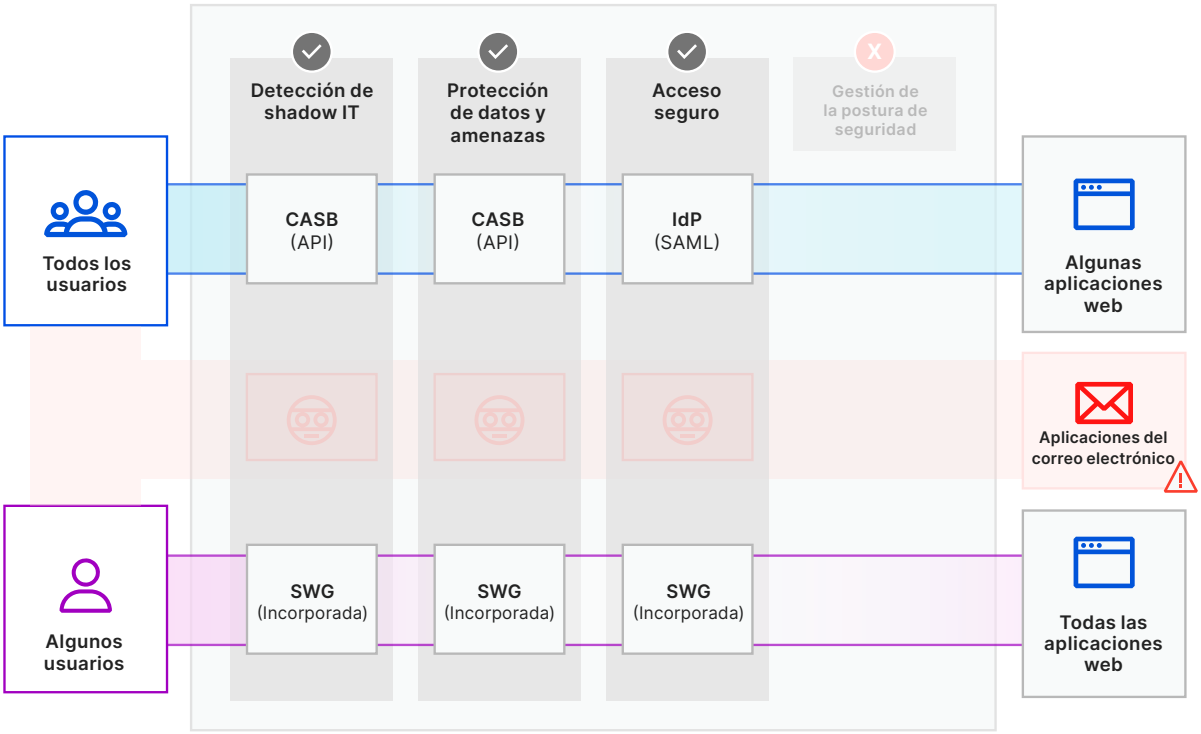
Incluso cuando los equipos de seguridad localizan herramientas de seguridad para el correo electrónico que están diseñadas para detectar las amenazas modernas, se pueden topar con otros problemas: requisitos de configuración complejos, largos procesos de implementación y tediosos problemas de mantenimiento de políticas. Por ejemplo, los productos SEG son muy difíciles de implementar contra los ataques al correo electrónico, ya que no es viable (o escalable) mantener una lista cada vez más larga de políticas para detener cada variante de ataque. La detección de ataques avanzados requiere el uso de algoritmos a escala que solo los servicios nativos de la nube pueden gestionar.

Para proteger los sistemas de correo electrónico corporativos de estos ataques, sin desbordar a los equipos de seguridad, sin superponer productos de hardware heredados ni confiar en que los usuarios detecten cada mensaje malicioso, las organizaciones necesitan un enfoque Zero Trust que integre las capacidades de seguridad del correo electrónico nativo de la nube y reduzca la confianza implícita en las comunicaciones basadas en el correo electrónico.

Un enfoque mejor para la seguridad SaaS

Las aplicaciones SaaS, desde las plataformas de comunicación hasta los sistemas de entrega de correo electrónico, constituyen una parte importante de las operaciones empresariales actuales. Sin embargo, la protección de estas aplicaciones contra las amenazas cada vez más complejas puede ser un suplicio para los equipos de seguridad, que a menudo tienen que lidiar con diversas herramientas que no están diseñadas para integrarse de forma nativa o que no son capaces de proporcionar visibilidad en todo el entorno SaaS de una organización.

Seguridad tradicional en SaaS

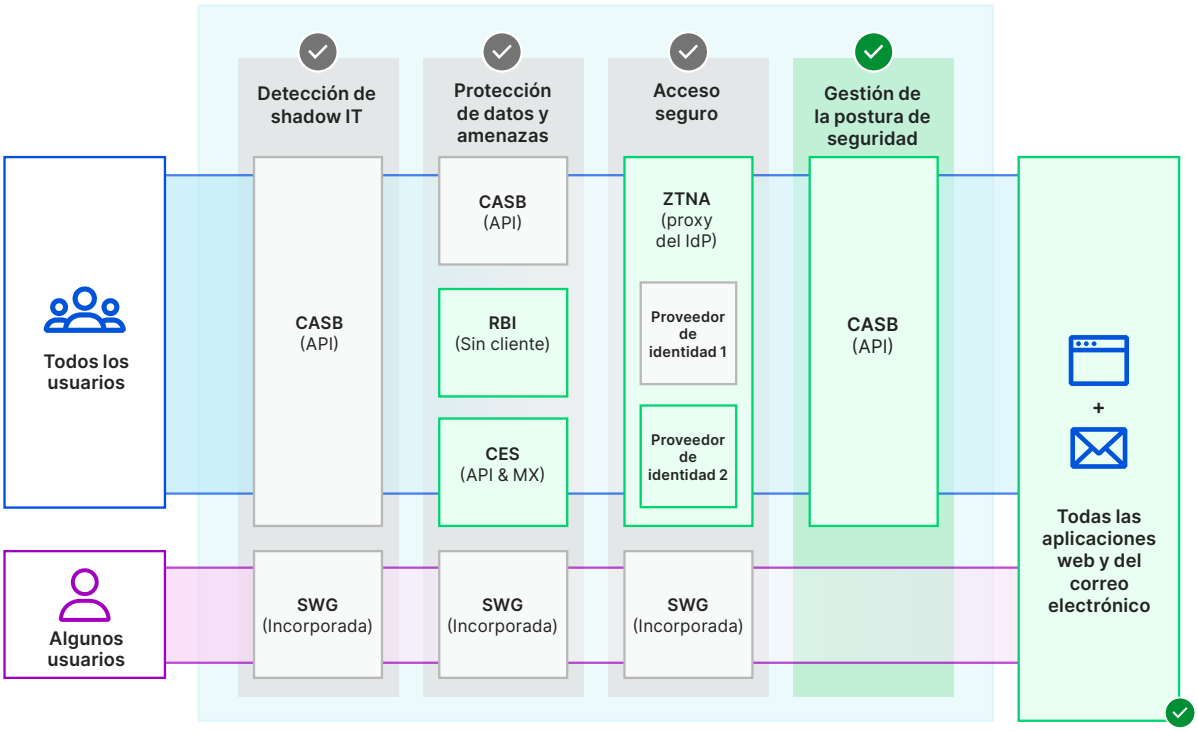


SWG = puerta de enlace web segura | CASB = agente de seguridad de acceso a la nube | IdP = proveedor de identidad

Conforme los proveedores creaban herramientas de seguridad SaaS más potentes, los equipos informáticos y de seguridad tuvieron que reunir estas soluciones líderes para proteger sus aplicaciones y datos. Este proceso a menudo requería tiempo y unos recursos internos considerables para su implementación y gestión y, aunque las soluciones específicas eran capaces de abordar amenazas a nivel individual, no existía una plataforma global que proporcionara soporte y visibilidad de varios proveedores en toda la organización.

A menudo, las medidas de seguridad tradicionales de SaaS tampoco ampliaban completamente sus protecciones a las plataformas de correo electrónico, exponiendo a las organizaciones vulnerables a ataques específicos que replicaban los flujos de trabajo esenciales de las empresas, se hacían pasar por socios y usuarios de confianza y eludían fácilmente los sistemas de clasificación de correo electrónico existentes y los controles integrados. Además, sin la integración nativa entre estas soluciones, o la visibilidad de todo el panorama de amenazas, la protección de las aplicaciones contra las amenazas modernas dejó aún más lagunas que los equipos de seguridad debían solucionar.

Seguridad moderna en SaaS



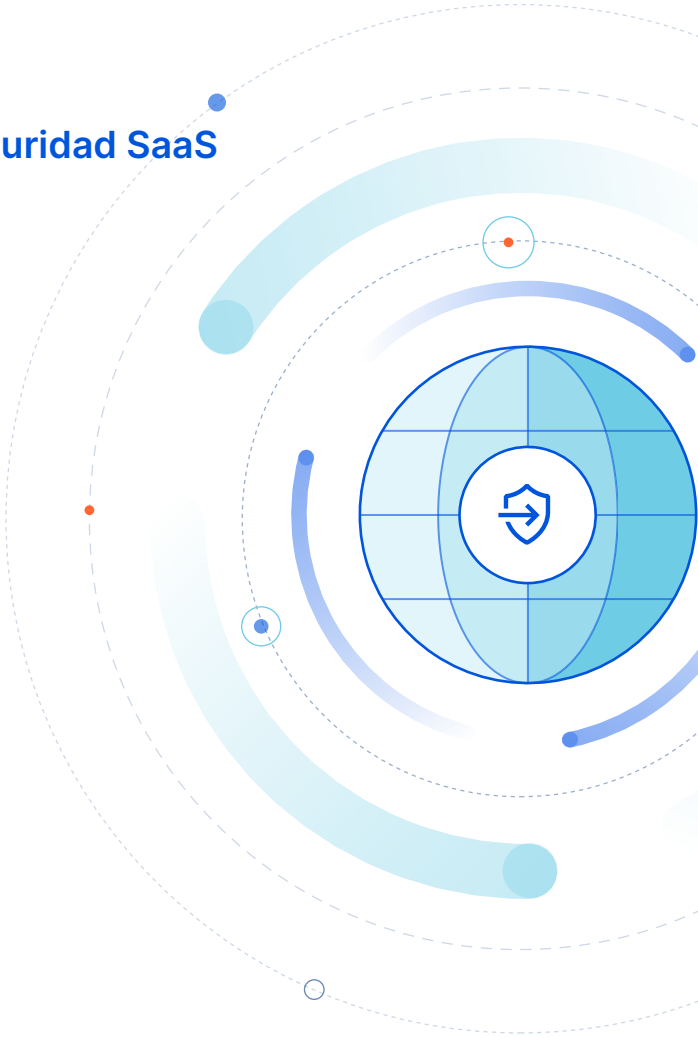
SWG = puerta de enlace web segura | CASB = agente de seguridad de acceso a la nube | IdP = proveedor de identidad | RBI = aislamiento remoto del navegador CES = seguridad del correo electrónico en la nube | ZTNA = acceso a la red Zero Trust

Para solucionar las lagunas de las soluciones tradicionales de seguridad y gestión de SaaS, las organizaciones necesitan una protección moderna contra las amenazas que esté diseñada para proteger las aplicaciones y los datos desde una única plataforma nativa de Internet. Un componente fundamental de este enfoque moderno es la gestión de la postura de seguridad, que permite a los equipos de seguridad determinar mejor cómo acceden los usuarios a los recursos críticos y obtener visibilidad y control sobre las amenazas externas e internas.

En lugar de exigir a las organizaciones que utilicen herramientas de una solución concreta para remediar las amenazas individuales, una plataforma de seguridad SaaS puede analizar las aplicaciones para detectar anomalías en la configuración, los permisos y el uso compartido, y luego permitir a los equipos de seguridad gestionar el acceso a las aplicaciones, mitigar los ataques por correo electrónico, bloquear las amenazas internas y el uso compartido de datos peligrosos, y mucho más.

Este enfoque no solo proporciona una protección más sólida y completa a las aplicaciones SaaS, sino que permite a las organizaciones ahorrar tiempo en la clasificación de las incidencias, automatizar los procesos de seguridad y centrarse en las iniciativas estratégicas en lugar de preocuparse por la fuga de datos, los ataques, y las configuraciones y el mantenimiento manuales.

Cómo aplicar un enfoque Zero Trust a la seguridad SaaS



Desarrollar el enfoque adecuado para la seguridad SaaS requiere visibilidad de las amenazas modernas basadas en SaaS y en la nube, pero adaptar las soluciones existentes a las necesidades de una organización puede ser una carga para los equipos informáticos y de seguridad. En lugar de combatir las amenazas a nivel individual, o de confiar en una combinación de herramientas aisladas, las organizaciones necesitan una plataforma de seguridad simplificada, fácil de gestionar y capaz de anticipar y mitigar las amenazas modernas.

Si bien tanto las funcionalidades de CASB como las de la seguridad del correo electrónico en la nube son componentes esenciales de una estrategia de seguridad SaaS, están diseñadas para funcionar mejor dentro de una arquitectura Zero Trust, en la que cada pieza de tecnología funciona mejor en conjunto que por separado. Cuando se implementa correctamente, esta disposición en capas también ayuda a mitigar los problemas adyacentes al eliminar las brechas de seguridad, conservar el ancho de banda del equipo de seguridad y automatizar la vigilancia de las amenazas.

Cómo protege Cloudflare las aplicaciones SaaS

Cloudflare ofrece el camino más fácil para proteger todo tu entorno SaaS, permitiendo a las organizaciones controlar cómo sus usuarios acceden a los recursos esenciales, cómo mantener esos recursos a salvo de ataques externos o internos, y cómo supervisar y mitigar los riesgos en tiempo real.

* Regístrate en nuestra lista de espera DLP

Cómo proteger las aplicaciones SaaS con Cloudflare Zero Trust

Para proteger los datos en tránsito, Cloudflare Zero Trust coloca funciones de control de acceso (ZTNA), puerta de enlace (SWG) y aislamiento del navegador (RBI) delante de las aplicaciones en la nube y SaaS para apoyar y operar como una arquitectura de implementación CASB en línea.

Para proteger los datos en reposo dentro de las aplicaciones SaaS, las integraciones fáciles de configurar y basadas en la API analizan continuamente las aplicaciones más utilizadas en busca de vulnerabilidades y amenazas potenciales.

Cómo combinar la seguridad del correo electrónico de Cloudflare Area 1 con Cloudflare Zero Trust

La seguridad del correo electrónico de Cloudflare Area 1 es representativa de la seguridad integrada del correo electrónico en la nube que ofrece a las organizaciones más flexibilidad en función de sus necesidades de seguridad del correo electrónico. Para ello, se integra a través de la API y actúa como puerta de enlace para verificar, filtrar, inspeccionar y aislar el tráfico de correo electrónico en línea a través de los cambios de registro MX.

Area 1 rastrea preventivamente Internet para detectar infraestructuras de ataque y campañas de phishing, protegiendo a los clientes de los ataques de phishing días antes de que lleguen a las bandejas de entrada de los destinatarios.

Para obtener más información sobre cómo Cloudflare ayuda a proteger las aplicaciones SaaS, visita https://www.cloudflare.com/products/zero-trust.

Fuentes

1. Gartner, "Forecast Analysis: Information Security and Risk Management, Worldwide". Analistas: Shailendra Upadhyay, Mark Driver, Christian Canales, Ruggero Contu, Lawrence Pingree, Elizabeth Kim, John A. Wheeler, Nat Smith, Rahul Yadav, Swati Rakheja, Dave Messett, Mark Wah, Shawn Eftink. 12 de agosto de 2021. Gartner.

2. Gartner, "Predicts 2022: Consolidated Security Platforms Are the Future". Analistas: Charlie Winckless, Joerg Fritsch, Peter Firstbrook, Neil MacDonald, Brian Lowans. 1 de diciembre de 2021. Gartner.

4. Gartner, "Hype Cycle for Cloud Security, 2021". Analistas: Tom Croll, Jay Heiser. 27 de julio de 2021. Gartner.

6. Gartner, "Market Guide for Email Security". Analistas: Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer. 7 de octubre de 2021. Gartner.

7. Gartner, "Market Guide for Email Security". Analistas: Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer. 7 de octubre de 2021. Gartner.

8. Gartner, "Market Guide for Email Security". Analistas: Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer. 7 de octubre de 2021. Gartner.

+34 518 880 290 | enterprise@cloudflare.com | www.cloudflare.com/es-es/

REV:BDES-3303.24JUN2022