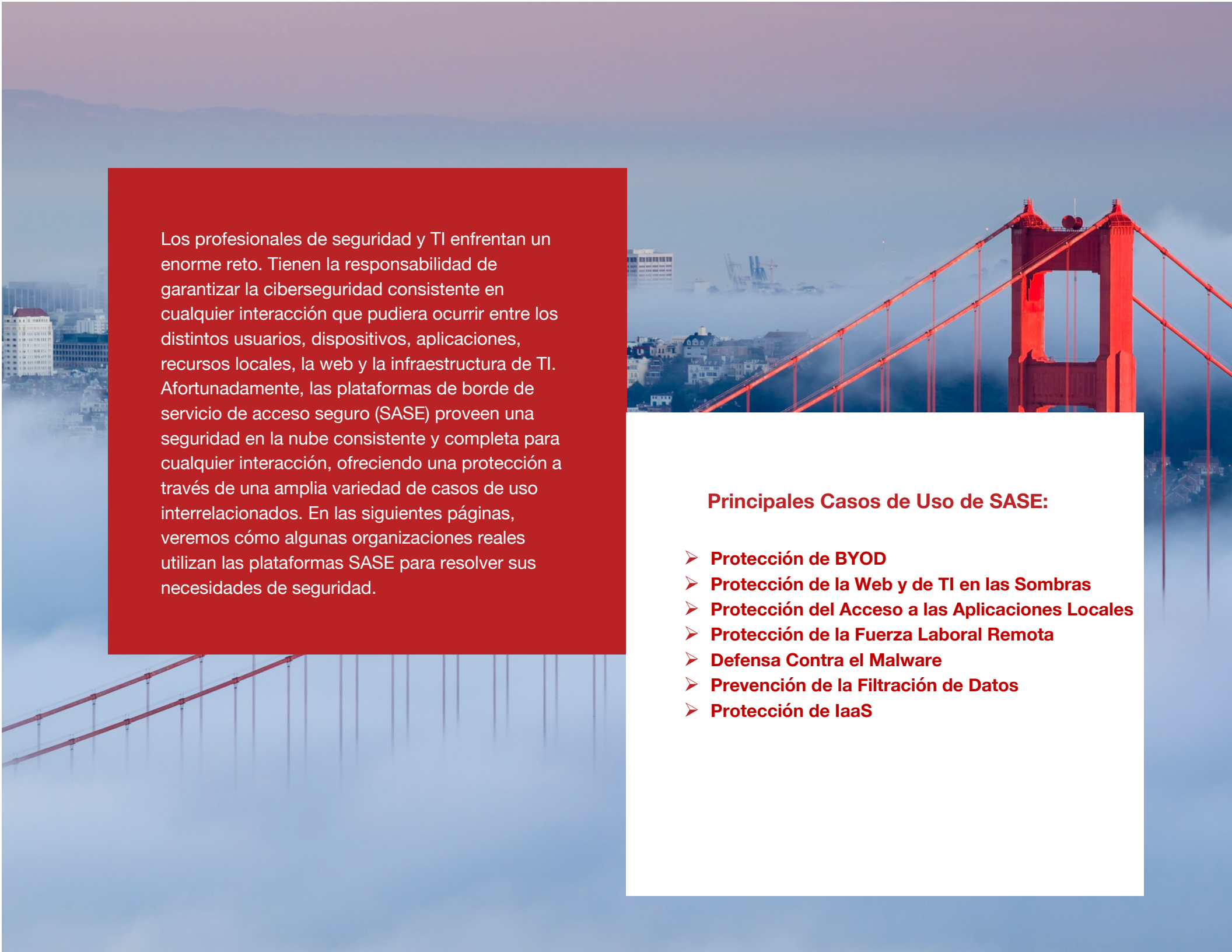
bitglass

Principales Casos de Uso de SASE



Los profesionales de seguridad y TI enfrentan un enorme reto. Tienen la responsabilidad de garantizar la ciberseguridad consistente en cualquier interacción que pudiera ocurrir entre los distintos usuarios, dispositivos, aplicaciones, recursos locales, la web y la infraestructura de TI. Afortunadamente, las plataformas de borde de servicio de acceso seguro (SASE) proveen una seguridad en la nube consistente y completa para cualquier interacción, ofreciendo una protección a través de una amplia variedad de casos de uso interrelacionados. En las siguientes páginas, veremos cómo algunas organizaciones reales utilizan las plataformas SASE para resolver sus necesidades de seguridad.

Principales Casos de Uso de SASE:

- **Protección de BYOD**
- **Protección de la Web y de TI en las Sombras**
- **Protección del Acceso a las Aplicaciones Locales**
- **Protección de la Fuerza Laboral Remota**
- **Defensa Contra el Malware**
- **Prevención de la Filtración de Datos**
- **Protección de IaaS**

Protección de BYOD

El modelo BYOD o "trae tu propio dispositivo" es un sistema mediante el cual los empleados realizan sus funciones de trabajo utilizando sus dispositivos o puntos finales personales. Esto requiere una seguridad exhaustiva, pero las herramientas tradicionales basadas en el monitoreo con agente son poco aptas para este fin. Los equipos de seguridad suelen tener dificultades para acceder a los dispositivos personales de los usuarios y muchos ni siquiera tienen conocimiento de todos los puntos finales personales que se utilizan por cuestiones de trabajo. Además, algunos usuarios temen que el uso de agentes en sus dispositivos personales proporcione al área de TI una visibilidad total de sus aplicaciones y datos personales.

Las plataformas SASE proveen una seguridad en entornos BYOD a través de gestores de seguridad de acceso a la nube (CASB) multimodales, mismos que permiten el despliegue de opciones sin agente. Al prescindir de agentes y utilizar proxies inversos, estos sistemas basados en la nube monitorean el acceso sólo a los recursos de TI administrados, tales como las instancias corporativas de SaaS e IaaS. Esto significa que ofrecen una visibilidad en tiempo real y permiten el control de los datos de la empresa en los dispositivos personales sin monitorear la información personal de los usuarios.

Las plataformas SASE ofrecen funciones de protección de datos, tales como la prevención de la pérdida de datos (DLP) y la encriptación en la nube, además de una protección contra amenazas como el malware o software malicioso y los usuarios internos descuidados o mal intencionados. También facilitan la visibilidad a través del registro exhaustivo de toda la actividad de los usuarios, los archivos y las aplicaciones, además de ofrecer funcionalidades de gestión de acceso e identidad, tales como el inicio de sesión único (SSO), la autenticación multifactorial (MFA) y el control de acceso contextual. De igual manera, disponen de controles no intrusivos a nivel del dispositivo, incluyendo límites de tiempo de bloqueo automático y códigos PIN en vez de patrones de deslizamiento para desbloquear teléfonos.

Escenario del Mundo Real

Un día, la computadora portátil administrada de Travis, un contratista de RH, sufre un desperfecto mientras él se encuentra de viaje. Travis no puede obtener un reemplazo inmediato del área de TI y necesita acceder a Office 365 para realizar sus funciones de trabajo, por lo que comienza a utilizar su iPhone personal. Debido a que su empleador utiliza una plataforma SASE con funcionalidad CASB sin agente, lo único que tiene que hacer es iniciar sesión en Office 365 a través de SSO en su iPhone y el sistema le permite el acceso. El CASB aplica políticas en tiempo real sin agente para proteger los datos sensibles; por ejemplo, negando el acceso a las carpetas altamente confidenciales en OneDrive, o bien, encriptando o aplicando marcas de agua a los archivos descargados. Con una herramienta alternativa como la administración de dispositivos móviles (MDM), el departamento de TI tendría que acceder al dispositivo de Travis e instalar un agente antes de que él pudiera utilizarlo para propósitos de trabajo (sin mencionar las inquietudes que tendría Travis de permitir esto en su iPhone personal por cuestiones de privacidad).

Protección de la Web y de TI en las Sombras

Aunque la web es un activo indispensable para cualquier organización, también puede afectar la productividad de una empresa, facilitar la filtración de datos sensibles y permitir las infecciones de malware. Las puertas de enlace web seguras (SWG), un componente básico de las plataformas SASE, están diseñadas para atender esas necesidades. Las puertas de enlace SWG pueden controlar el acceso a sitios web y a aplicaciones no administradas por categoría (juegos de azar, deportes, streaming, pornografía, malware, phishing y muchas otras) y por confiabilidad del destino. Adicionalmente, las políticas automatizadas pueden prevenir la transmisión de datos sensibles a la web. En otras palabras, estas herramientas bloquean las amenazas, detienen las filtraciones y aumentan la productividad.

Las organizaciones deben considerar la arquitectura de las soluciones al evaluar los componentes SWG de las plataformas SASE. Las puertas de enlace SWG en forma de dispositivos de hardware son costosas, requieren de un servicio VPN para el acceso fuera de las instalaciones y tienen capacidades fijas que dificultan considerablemente su escalabilidad. Las puertas de enlace SWG a través de proxies de nube no requieren de dispositivos, pero sí inducen una latencia debido al salto de la red al proxy. Además, todo el tráfico de red es desencriptado e inspeccionado en el proxy, incluyendo el tráfico personal de los usuarios, por lo que no se respeta la privacidad del usuario. Las puertas de enlace SWG en los dispositivos que realizan la desencriptación e inspección local son ideales. Este método evita la necesidad de dispositivos adicionales, saltos de red y servicios VPN. Esto garantiza la seguridad, el rendimiento y la escalabilidad. Debido a que solamente los eventos de seguridad son registrados y subidos a la nube, también se respeta la privacidad del usuario.

Escenario del Mundo Real

Considere el caso de Jacob, un especialista de mercadotecnia que suele hacer click en los enlaces que recibe por correo electrónico sin tener en cuenta quién es el remitente. Un día, Jacob recibe un mensaje de una cuenta de email falsa que parecer ser de un compañero de trabajo y cuya identidad ha sido suplantada; el mensaje contiene un enlace a un sitio web fraudulento cuyo fin es robar las credenciales de acceso corporativas e infectar los equipos con malware. A pesar de que Jacob hace click en el enlace, su empleador cuenta con una puerta de enlace SWG a nivel del dispositivo, misma que automáticamente evita que él llegue a su destino; el URL es identificado como malicioso y se activa la política de bloqueo adecuada. El empleador de Jacob anteriormente utilizaba una puerta de enlace SWG basada en dispositivos, pero su capacidad fija generaba problemas de escalabilidad y desempeño, lo que afectaba la productividad de los usuarios a medida que la empresa crecía. Con la puerta de enlace SWG a nivel de dispositivo instalada directamente en el punto final de Jacob, su empleador logró garantizar la seguridad en la web y ofrecer una experiencia rápida a los usuarios sin afectar su productividad o privacidad.

Protección del Acceso a las Aplicaciones Locales

Las aplicaciones locales almacenan una gran cantidad de datos sensibles de la organización. Tradicionalmente, el acceso a esos recursos se controlaba requiriendo el uso de una red privada virtual (VPN) por parte de los empleados para establecer túneles seguros a la red; sin embargo, este método se basa en el uso de dispositivos costosos, no es escalable, introduce una latencia que afecta a la experiencia del usuario y ofrece a los empleados un acceso sin restricciones a todo lo que hay en la red, lo que viola los principios básicos del modelo de seguridad de confianza cero.

El acceso a la red de confianza cero (ZTNA) es otro aspecto fundamental de las plataformas SASE. Las plataformas SASE con ZTNA fueron diseñadas para proveer un verdadero acceso seguro de confianza cero a los recursos locales. Idealmente, estas soluciones evitan el uso de centros de datos y dispositivos de hardware privados y se despliegan en la nube pública para ofrecer una escalabilidad y un rendimiento óptimos. Al contar con una solución ZTNA basada en la nube, los usuarios simplemente se autentican a través de SSO para poder tener un acceso seguro a las aplicaciones locales específicas (en vez de acceder a toda la red). La solución aplica políticas de protección de amenazas y datos en tiempo real para proteger la información sensible o regulada, impedir la carga de malware y ofrecer un acceso contextual a los archivos y las carpetas clave.

Escenario del Mundo Real

Al trabajar desde su casa, Samantha, gerente de producto de una compañía de tecnología, se percata de que necesita acceder a la instancia local de Jira de su empleador. Utilizando una solución ZTNA, ella se autentica a través de SSO y accede a la aplicación. Samantha puede visualizar la mayor parte del contenido de la aplicación, pero una política previamente establecida impide que ella pueda acceder a la información crítica de la empresa de forma remota. Adicionalmente, cuando ella intenta descargar archivos altamente sensibles, únicamente obtiene un acceso de 'sólo lectura' en una ventana de navegador que requiere de una autenticación adicional. No es posible tener este tipo de protección granular de los datos con una red privada virtual (VPN). Además, debido a que los dispositivos VPN tienen capacidades fijas y no cuentan con la potencia infinita de la nube, enfrentan limitaciones de escalabilidad considerables a medida que las organizaciones crecen y más usuarios trabajan fuera de las instalaciones. Esto significa que los usuarios de redes VPN se ven en la necesidad de adquirir e instalar dispositivos mejores o adicionales, lo que crea un costoso cuello de botella.

Protección de la Fuerza Laboral Remota

El trabajo remoto es la nueva normalidad y las organizaciones de todo el mundo están aprovechando los beneficios, tales como una mayor productividad y flexibilidad. Sin embargo, resulta altamente problemático proteger a los empleados que trabajan fuera de la oficina y más allá del perímetro tradicional definido los por los firewalls y las puertas de enlace web seguras (SWG) basadas en proxies. Afortunadamente, el uso de una plataforma SASE moderna permite que los empleados accedan de forma segura a aplicaciones administradas y no administradas, servicios en la nube, sitios web y aplicaciones de propiedad exclusiva en la nube pública y en centros de datos privados.

Aunque las herramientas tradicionales orientadas en la red, tales como las redes VPN, alguna vez fueron la norma para proteger a la fuerza laboral remota, su costo, complejidad y falta de escalabilidad las hacen poco ideales para proteger a la fuerza laboral remota en la actualidad. Afortunadamente, las principales plataformas SASE evitan la necesidad de utilizar redes VPN, dispositivos de hardware y tráfico de retorno. Adicionalmente, cuando cuentan con una arquitectura nativa de la nube, proveen una óptima escalabilidad a medida que cambian los perfiles de carga de las organizaciones, ya sea que su fuerza laboral crezca o se desplace geográficamente.

Las plataformas SASE aprovechan la tecnología CASB, SWG y ZTNA para proteger a los trabajadores remotos en instancias Saas e IaaS administradas, destinos web y TI en las sombras y aplicaciones locales, respectivamente. Desde un punto de control único y en tiempo real, pueden detectar datos sensibles, prevenir las filtraciones, detener la propagación del malware, filtrar contenidos inseguros, autenticar a los usuarios y proveer una seguridad granular y consistente para cualquier interacción.

Escenario del Mundo Real

Johan, representante de ventas de una importante compañía aseguradora, trabaja a distancia desde su casa. Para desempeñar eficazmente su trabajo, él necesita un acceso continuo a Salesforce. Su empleador, consciente de la información sensible de los clientes que contiene su instancia de Salesforce, encripta los datos inactivos a través de SASE y requiere que los empleados remotos realicen una autenticación multifactorial (MFA) antes de poder visualizarlos. Un día, Johan decide almacenar algunas de las cotizaciones de sus clientes en su cuenta personal de Google Drive para facilitar el acceso; sin embargo, la puerta de enlace SWG de su dispositivo (un componente básico de las principales plataformas SASE) instantáneamente evita que él pueda subir los archivos, mismos que contienen información de identificación personal (PII). Este enfoque en la seguridad web desde el dispositivo es ideal para trabajadores remotos, ya que no implica saltos de red que induzcan la latencia, cuellos de botella que afecten el rendimiento de los dispositivos locales o la necesidad de utilizar un servicio VPN que inhiba la productividad. Con la plataforma SASE, la organización de Johan puede detectar y evitar en tiempo real la carga y descarga inapropiada de la PII en cualquier lugar donde se encuentre su fuerza laboral.

Defensa Contra el Malware

Las amenazas como el malware son el flagelo de las empresas modernas. En años recientes, las infestaciones de ransomware como WannaCry y Petya han puesto de rodillas a innumerables organizaciones a nivel mundial. Los equipos de seguridad requieren de soluciones de protección avanzada contra amenazas (ATP) para cada vector de ataque que pudiera ser el blanco del malware. Dada la realidad de la nube, el modelo BYOD ("trae tu propio dispositivo") y el trabajo remoto, las soluciones ATP ya no son solamente para el perímetro o el punto final. Puesto que las plataformas SASE garantizan una seguridad consistente para cualquier interacción en la nube, en la web y en los recursos locales, son las herramientas ideales para una solución ATP integral. Estas plataformas utilizan un enfoque triple para bloquear el malware con funcionalidades CASB, SWG y ZTNA, además de que suelen aprovechar las integraciones con los principales proveedores de AV como CrowdStrike y Cylance para identificar las amenazas de día cero.

Las plataformas SASE impiden que el malware se propague a través de las aplicaciones administradas SaaS, IaaS y locales de la organización. Tienen la capacidad de bloquear las amenazas en tiempo real a medida que son cargadas a las aplicaciones o descargadas a los dispositivos y eliminan las amenazas en los datos inactivos al analizar el contenido de las aplicaciones. Algunas plataformas SASE pueden hacer esto sin el uso de un agente, lo que significa que pueden proteger contra el malware incluso en dispositivos personales. A fin de hacer frente a otro eslabón clave en la cadena de ataque, las plataformas SASE también están diseñadas para bloquear las amenazas en la web. Si los usuarios intentan hacer click en un URL malicioso que conduzca a sitios web diseñados para infectar sus dispositivos con malware, la plataforma bloqueará el acceso a dichos sitios web.

Escenario del Mundo Real

Christina trabaja en el área de finanzas de una gran empresa farmacéutica. Su organización utiliza diversas aplicaciones web y en la nube, incluyendo Office 365, Snack y G Suite. Una mañana, ella decide trabajar desde casa en su computadora portátil personal sin saber que está infectada con malware. Cuando ella intenta compartir un archivo infectado con un compañero de trabajo a través de Slack, la plataforma SASE de su empleador automáticamente bloquea el proceso de carga del archivo hacia la aplicación y le explica que el archivo contiene malware. Ese mismo día, mientras Christina trabaja en su computadora portátil administrada, ella recibe un email falsificado cuyo remitente parece ser un empleado de TI, informándole que sus credenciales de acceso a Office 365 han expirado. Sin pensarlo, ella hace click en el URL que aparece en el email para restablecer su contraseña. Afortunadamente, la plataforma SASE de su empleador incluye una puerta de enlace SWG a nivel de dispositivo, misma que evita que Christina acceda al sitio web malicioso e infecte su equipo con malware. En un mundo lleno de dispositivos personales, amenazas interminables y fuerzas laborales dinámicas y remotas, las organizaciones requieren una seguridad sin agente para el modelo BYOD, así como la funcionalidad de puertas de enlace SWG a nivel de dispositivo que eviten el uso de servicios VPN y dispositivos especializados.

Prevención de la Filtración de Datos

Las organizaciones suelen manejar una gran cantidad de datos sensibles y reglamentados; desde información de identificación personal (PII) y datos de la industria de tarjetas de pago (PCI) hasta información protegida sobre la salud (PHI) y demás. Si esta información llega a filtrarse, puede perjudicar a los titulares de los datos (exponiéndolos al robo de identidad y a los ataques de spear phishing), ocasionar el incumplimiento con la reglamentación y la subsiguiente aplicación de sanciones, generar pleitos legales costosos con penalidades elevadas y causar perjuicios a la reputación de las marcas, lo que afecta el éxito general de la empresa.

Uno de los principales propósitos de las plataformas SASE es prevenir la fuga de datos de forma consistente e integral sin importar la aplicación, el dispositivo o la acción intentada. Esto se logra mediante un enfoque integral que incorpora las capacidades de las tecnologías complementarias, tales como CASB, SWG y ZTNA. Por consiguiente, las plataformas SASE ofrecen un panel único para configurar las políticas que se implementan de manera consistente donde sea que vayan los datos—en aplicaciones administradas, la web y los recursos locales. Estas plataformas protegen los datos inactivos en aplicaciones administradas en la nube mediante el uso de sistemas de DLP, tales como la puesta en cuarentena y la encriptación de archivos, además de evitar filtraciones en el acceso utilizando funciones en tiempo real como la gestión de derechos digitales (DRM) y la redacción electrónica. En caso de que algún usuario intente exflitrar los datos a través de un sitio web (ya sea su correo electrónico personal, su cuenta de Dropbox o cualquier otra cosa), el sistema impedirá la carga en tiempo real. Finalmente, cuando se trata de proteger la seguridad de las aplicaciones locales, las plataformas SASE pueden evitar que los usuarios filtren o accedan a los archivos sensibles aplicando políticas precisas como las anteriormente mencionadas.

Escenario del Mundo Real

Kaito es un médico que trabaja para una empresa de salud. Al colaborar con un colega, Kaito decide descargar parte de la información protegida sobre la salud (PHI) de un paciente desde una aplicación interna y bajarla a su dispositivo personal, de manera que pueda enviarla al email personal de su colega para su inspección. Sin embargo, la empresa de salud cuenta con una plataforma SASE que identifica la información sensible, determina que dichos datos no deben transmitirse a un punto final no administrado y bloquea la descarga. A continuación, Kaito utiliza un dispositivo administrado e intenta subir el expediente del paciente a su cuenta de Dropbox para poder acceder a él con su teléfono personal. Al acceder a Dropbox, le aparece un recordatorio de TI solicitando que utilice la instancia OneDrive segura de su organización. Kaito ignora el mensaje e intenta subir la información, pero la plataforma SASE detecta una vez más el patrón de datos sensibles y evita la fuga de datos en tiempo real. Solamente las plataformas SASE pueden prevenir las fugas de datos de forma consistente y completa.

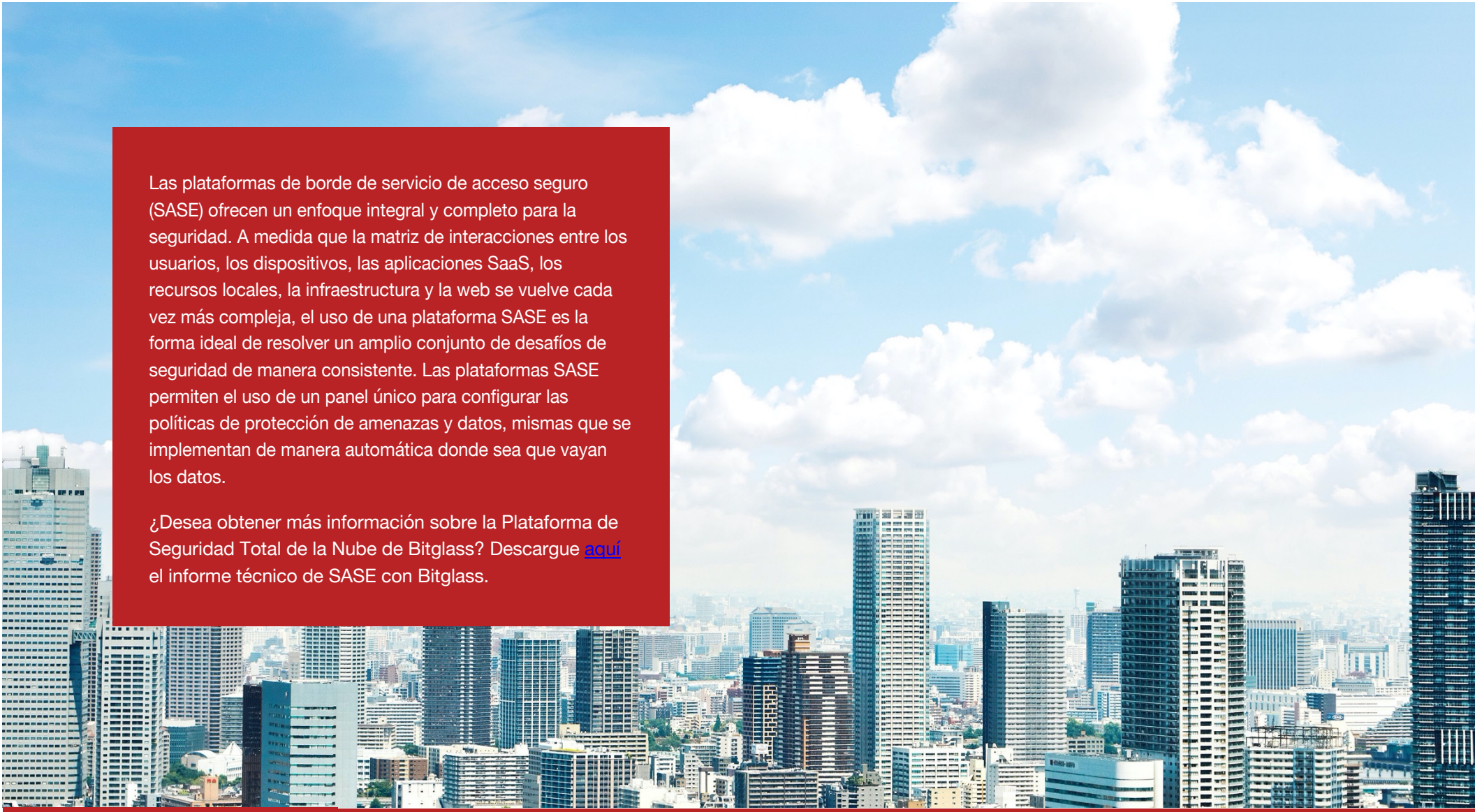
Protección de IaaS

La infraestructura como servicio (IaaS) es uno de los segmentos de más rápido crecimiento de la computación en la nube. Gracias a las plataformas de IaaS como Amazon Web Services (AWS), Microsoft Azure y Google Cloud Platform (GCP), las organizaciones están aprovechando la infraestructura basada en la nube que se encuentra fuera del alcance de las herramientas tradicionales de seguridad perimetral. Aunque que las plataformas de IaaS proveen algunas funciones nativas de seguridad y cumplimiento (tales como el registro de transacciones administrativas), existen múltiples deficiencias. La buena noticia para las empresas es que las plataformas SASE son ideales para proteger la seguridad de las instancias de IaaS. Esto se logra principalmente a través de funciones que se originan en la tecnología de gestores de seguridad de acceso a la nube (CASB).

Las plataformas SASE tienen un enfoque triple en cuanto a la seguridad de IaaS. Primero, analizan los datos inactivos en servicios como AWS S3 a fin de identificar la información sensible que haya logrado llegar a la plataforma. Los datos sensibles que sean descubiertos pueden ser encriptados según las políticas preestablecidas para evitar su visualización y uso no autorizados. Además de los datos inactivos, las plataformas SASE también protegen el acceso a las aplicaciones personalizadas desarrolladas en plataformas de IaaS. Es posible controlar el acceso por variables contextuales, tales como grupo, dispositivo, ubicación e incluso factores personalizados. Finalmente, las herramientas de gestión de la postura de seguridad en la nube (CSPM) escanean las instancias IaaS para detectar errores en la configuración definidos en los marcos de cumplimiento (incluyendo CIS Benchmark, HIPAA y PCI DSS) a fin de prevenir las filtraciones y el incumplimiento; por ejemplo, detectando buckets o sectores de almacenamiento que contengan información confidencial y estén expuestos el público. Una vez que se identifican los problemas, estas herramientas ofrecen soluciones de remediación personalizadas e incluso se encargan automáticamente de resolverlos.

Escenario del Mundo Real

En su prisa por llegar a casa, Sawraj, quien trabaja como administrador de AWS para una empresa de seguridad, accidentalmente crea un bucket S3 expuesto al público con información confidencial de su empleador. Mientras corre hacia su automóvil, se le cae al suelo una nota adhesiva con sus credenciales de acceso al servicio AWS que estaba adherida a su computadora portátil. El empleado de un competidor encuentra la nota y se la lleva consigo. Afortunadamente, el empleador de Sawraj cuenta con una plataforma SASE. Las herramientas de gestión de la postura de seguridad en la nube (CSPM) detectan y corrigen automáticamente el error en la configuración del bucket. Por la noche, cuando el competidor intenta utilizar las credenciales de Sawraj para iniciar una sesión, la plataforma identifica que el acceso proviene de un dispositivo nuevo desde una ubicación nueva y a una hora inusual del día. En respuesta, aplica una autenticación multifactorial reforzada, solicita un token por SMS que es enviado al teléfono real de Sawraj y evita exitosamente el acceso del intruso malicioso.



Las plataformas de borde de servicio de acceso seguro (SASE) ofrecen un enfoque integral y completo para la seguridad. A medida que la matriz de interacciones entre los usuarios, los dispositivos, las aplicaciones SaaS, los recursos locales, la infraestructura y la web se vuelve cada vez más compleja, el uso de una plataforma SASE es la forma ideal de resolver un amplio conjunto de desafíos de seguridad de manera consistente. Las plataformas SASE permiten el uso de un panel único para configurar las políticas de protección de amenazas y datos, mismas que se implementan de manera automática donde sea que vayan los datos.

¿Desea obtener más información sobre la Plataforma de Seguridad Total de la Nube de Bitglass? Descargue aquí el informe técnico de SASE con Bitglass.

bitglass

Principales Casos de Uso de SASE

Phone: (408) 337-0190
Email: info@bitglass.com

www.bitglass.com

About Bitglass

Bitglass' Total Cloud Security Platform is the only SASE offering that combines a Gartner-MQ-Leading cloud access security broker, the world's only on-device secure web gateway, and zero trust network access to secure any interaction. Its Polyscale Architecture boasts an industry-leading uptime of 99.99% and delivers unrivaled performance and real-time scalability to any location in the world. Based in Silicon Valley with offices worldwide, the company is backed by Tier 1 investors and was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution.