RESUMEN DE LA SOLUCIÓN

Protección de usuarios remotos con Netskope

Cada vez más empleados trabajan fuera del tradicional entorno de red corporativo. Estos usuarios remotos obvian los controles de seguridad perimetral tradicionales, de modo que dejan a las organizaciones expuestas y vulnerables ante pérdidas de datos y amenazas. Por lo tanto, es preciso una nueva solución de seguridad basada en la nube que proporcione protección, visibilidad y acceso remoto para toda la empresa.

PRINCIPALES CASOS DE USO

- **Obtenga una mayor visibilidad de la actividad de los usuarios remotos.** Comprenda las acciones de los usuarios, así como los riesgos asociados a los sitios web y las aplicaciones en la nube.
- **Mejore la experiencia de usuario final de los usuarios remotos.** Conecte los usuarios a la nube, la web y las aplicaciones privadas con una infraestructura de red global, escalable y de alto rendimiento.
- **Aplique políticas granulares de prevención de pérdida de datos (DLP) y de protección frente a amenazas.** Establezca políticas DLP para proteger los datos sensibles y detectar las amenazas alojadas dentro de los entornos de los sitios web o la nube.
- **Sustituya las soluciones VPN obsoletas por acceso a red Zero Trust.** Proporcione un acceso remoto directo, seguro y sin interrupciones a las aplicaciones alojadas en centros de datos y nubes públicas.
- **Consolide la seguridad de sus usuarios remotos.** Combine Netskope Next Generation Secure Web Gateway (NG SWG) con Netskope Private Access (NPA) para ofrecer una plataforma de seguridad moderna, unificada y basada en la nube.

EL DESAFÍO

Trabajar fuera de la oficina se ha convertido en una práctica común. Sin embargo, las compañías se encuentran con dificultades a la hora de garantizar la seguridad de sus usuarios remotos. Las soluciones de seguridad obsoletas, que suelen ubicarse en centros de datos, resultan costosas y complejas, y además son sorteadas por los usuarios remotos que se conectan directamente a Internet. Esto deja a los usuarios remotos expuestos a amenazas y permite la exfiltración de datos a la nube y a la web. Por otro lado, los servicios VPN de acceso remoto que utilizan los usuarios remotos para conectarse a las aplicaciones en los centros de datos a nivel de red ofrecen pocas garantías, y no pueden dar acceso de forma efectiva a las aplicaciones alojadas en los entornos de la nube pública.

NETSKOPE PARA USUARIOS REMOTOS

Netskope proporciona una plataforma mundial de seguridad basada en la nube para dar un acceso seguro a los usuarios remotos a la web, la nube y las aplicaciones privadas en centros de datos o en la nube pública. La solución de Netskope es la única capaz de decodificar el tráfico de las aplicaciones en la nube y del sitio web para visibilizar las actividades de los usuarios remotos, inspeccionar el movimiento de datos y detectar amenazas ocultas en el tráfico SSL/TLS. Netskope ofrece a los usuarios remotos una mejor experiencia de usuario ya que permite que se conecten sin interrupciones y de forma segura a las aplicaciones privadas mediante el acceso a red Zero Trust (ZTNA). Netskope solo necesita un único cliente ligero instalado en un dispositivo para gestionar el tráfico en la web y la nube, además de canalizar el tráfico de aplicaciones privadas.

CAPACIDADES

PROTECCIÓN DE DATOS

Los datos están cada vez más expuestos a riesgos ya que transitan fuera del perímetro de la empresa y, por lo tanto, se escapan a la visibilidad y el control de las medidas de seguridad tradicionales. En la actualidad, es obligatorio contar con políticas de protección de datos consistentes en los servicios IT gestionados, como Salesforce, Microsoft Office 365 y AWS, así como en miles de servicios en la nube no gestionados y sitios web que permiten subir datos. Con los servicios en la nube, resulta demasiado fácil que los empleados compartan datos sensibles en un lugar poco seguro o con la persona equivocada. Es más probable que usuarios malintencionados o empleados descontentos intenten llevar a cabo una exfiltración de datos sensibles de la compañía cuando se encuentran fuera del entorno de la oficina. Por ello, es fundamental proporcionar una protección de datos sólida a los usuarios que trabajan en remoto.

Netskope DLP protege los datos sensibles de ser subidos por usuarios remotos a aplicaciones en la nube (SaaS), entornos de la nube pública (IaaS) o cualquier sitio web. Netskope también es capaz de identificar y prevenir el movimiento de datos sensibles que pueda indicar que un usuario interno malintencionado está intentando robar datos. Netskope cuenta con las capacidades DLP más avanzadas, diseñadas para llevar a cabo una fácil implementación, obtener una tasa menor de falsos positivos y ofrecer una investigación de incidentes detallada.

PROTECCIÓN FRENTE A AMENAZAS

Cuando los usuarios remotos se conectan directamente a Internet y obvian los controles de seguridad *on-premise* tradicionales, dejan a las organizaciones expuestas a importantes riesgos. Además, el teletrabajo aumenta la superficie de ataque de una empresa, ya que el tamaño y la extensión de la red, así como el número de dispositivos expuestos ante amenazas evasivas, son mayores.

Netskope es capaz de decodificar sitios web y servicios en la nube con cifrado TLS para identificar y reducir la oleada actual de amenazas capacitadas para la nube a las que deben hacer frente las organizaciones. Los cibercriminales utilizan los servicios en la nube como infraestructura escalable y fiable para implementar el ciclo de vida de su ciberataque en la nube. Varios ejemplos de ello son las páginas de *phishing* alojadas en los servicios de almacenamiento en la nube

Con Netskope, los usuarios remotos tienen acceso seguro gracias a Secure Access Service Edge (SASE), término acuñado por Gartner. La solución SASE engloba Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) y acceso a red Zero Trust Network Access (ZTNA) en una misma plataforma con controles de política unificados.

como OneNote, las redes de mando y control que utilizan las aplicaciones de colaboración como Slack o GitHub, o las cargas útiles de malware alojadas en *buckets* de AWS S3 o Microsoft Azure.

Gracias a Netskope Threat Research Lab, equipo especializado en descubrir y analizar las nuevas amenazas en la nube, Netskope ofrece defensas multicapa que incluyen antivirus, heurística y análisis del script en fase de preejecución, *bare-metal sandboxing,* detección de anomalías mediante *machine learning*, además de numerosas fuentes de inteligencia de amenazas de terceros.

ZERO TRUST NETWORK ACCESS

El servicio ZTNA de Netskope permite que las organizaciones puedan empezar a sustituir las soluciones de hardware con VPN obsoletas por una arquitectura de acceso remoto segura y basada en la nube. Al adoptar la solución ZTNA para sus usuarios remotos, podrá olvidarse de las grandes inversiones, la renovación de ciclos y los constantes costes de mantenimiento de los *appliances* VPN.

Netskope proporciona una alternativa al *backhauling* de los usuarios remotos mediante la red corporativa para acceder a las aplicaciones en los entornos de la nube pública, una arquitectura obsoleta e ineficaz que suele afectar a la experiencia de usuario. Además, Netskope reduce la posibilidad de poner en peligro las aplicaciones frente a accesos no autorizados ya que no deja expuestas públicamente estas aplicaciones en entornos de nube pública.

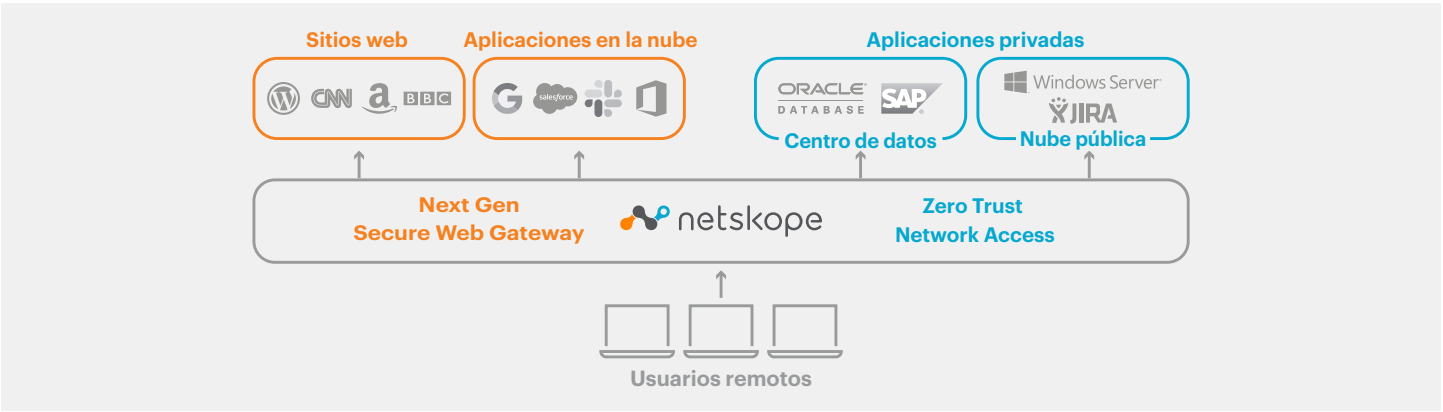

IMAGEN 1: Protección de usuarios remotos con Netskope

Netskope conecta a los usuarios remotos de forma directa y sin interrupciones a aplicaciones privadas alojadas en centros de datos privados o nubes públicas. La conexión entre los usuarios remotos y las aplicaciones se mantiene segura gracias a un túnel con cifrado TLS de extremo a extremo y tiene un enrutamiento óptimo mediante NewEdge, la infraestructura de red global, escalable y de alto rendimiento de Netskope. Al integrar una autenticación e inspección sólidas de la postura de seguridad de los dispositivos se garantiza que solo tengan acceso a las aplicaciones los usuarios autorizados con dispositivos seguros.

«El 62 % de las organizaciones considera que el mayor desafío para la seguridad de las aplicaciones es garantizar el acceso seguro a las aplicaciones privadas que están distribuidas en el centro de datos y en los entornos cloud».

Cybersecurity Insiders, 2019 Zero Trust Adoption, noviembre de 2019

VISIBILIDAD

Netskope proporciona un conocimiento experto, detallado y valioso de las aplicaciones en la nube y los sitios web que visitan los usuarios remotos de la compañía. Además, la tecnología Cloud XD™ de Netskope es capaz de decodificar el tráfico de la nube y la web para comprender qué actividades están llevado a cabo los usuarios y diferenciar entre instancias corporativas y personales en las aplicaciones en la nube. Con Netskope, podrá obtener una visibilidad granular de la actividad en las aplicaciones de la nube y de la difusión de datos sensibles tanto dentro como fuera de su organización. No obstante, para poder ofrecer una solución de seguridad sólida, los equipos de seguridad deben realizar controles de seguridad granulares del uso de las aplicaciones en la nube gestionadas y no gestionadas. El punto ciego más relevante para los equipos de seguridad es el uso no oficial de las aplicaciones no gestionadas que suele ser muy común en las organizaciones.

CONTROL GRANULAR

Netskope Cloud XD es el «motor» de la plataforma de Netskope. Se encarga de dar sentido a los servicios de la nube, las aplicaciones y el tráfico de la web para ofrecer contexto y contenido a las políticas de protección de datos y frente a amenazas. Cloud XD comprende el lenguaje de la nube (APIs, JSON, etc.) para proporcionar visibilidad granular de los usuarios, dispositivos, aplicaciones, instancias, evaluación de riesgos, categorías URL y categorías en los entornos de la nube y la web. Después, lleva a cabo acciones inteligentes de acuerdo con sus políticas de aplicación como por ejemplo permitir, bloquear, eliminar, codificar, poner en cuarentena, etc.

La visibilidad y los controles granulares de las actividades que llevan a cabo los usuarios remotos cuando utilizan las aplicaciones en la nube o visitan sitios web desempeña un papel fundamental a la hora de reducir el riesgo de pérdidas de datos y de aumentar la protección frente a amenazas. Las políticas de NG SWG de Netskope son capaces de distinguir entre instancias personales y corporativas dentro de las aplicaciones en la nube. Entre los posibles usos de esta capacidad de discernir las instancias se incluyen la habilidad de prevenir el movimiento de datos sensibles a instancias personales del almacenamiento en la nube, o la de prevenir el acceso de instancias solitarias de entornos de la nube pública que se utilizan para alojar páginas de *phishing* o malware.

BENEFICIOS	DESCRIPCIÓN
PROTECCIÓN AVANZADA FRENTE A AMENAZAS	**PROTEJA A SUS USUARIOS REMOTOS DE AMENAZAS BASADAS EN LA NUBE Y LA WEB. MANTENGA SU NEGOCIO PROTEGIDO FRENTE A USUARIOS INTERNOS MALICIOSOS:** • Detecte automáticamente las cuentas comprometidas mediante un análisis del comportamiento de los usuarios: por ejemplo, la frecuencia con la que inician sesión en aplicaciones en la nube, accesos desde ubicaciones geográficas sospechosas, ataques de fuerza bruta o patrones de inicio de sesión inusuales. • Detecte y detenga las amenazas procedentes de las aplicaciones en la nube y los sitios web en tiempo real gracias a múltiples motores antimalware, fuentes de inteligencia de amenazas (>40), heurísticas en fase de preejecución, *sandboxing* y aprendizaje automático. • Detecte y alerte acerca de comportamientos anómalos mediante la identificación de cantidades de datos cargados, descargados o eliminados que resulten inusuales. • Maximice la inversión de sus tecnologías ya existentes mediante la integración de Netskope con soluciones de Detección y Respuesta en Endpoints (EDR, por sus siglas en inglés), gestión de información y eventos de seguridad (SIEM), orquestación, automatización y respuesta de seguridad (SOAR) y aislamiento de navegador remoto (RBI).
PROTECCIÓN DE DATOS AVANZADA	**DESARROLLE POLÍTICAS DE DLP GRANULARES CON PLANTILLAS SENCILLAS O CON REGLAS PERSONALIZADAS:** • Implemente de forma rápida políticas de DLP capacitadas para la nube mediante las numerosas plantillas de políticas predefinidas que permiten identificar los datos sensibles de acuerdo con regulaciones comunes. • Detecte los datos sensibles de forma precisa mediante el análisis de etiquetas de clasificación de datos, la inspección de datos que usen expresiones regulares, la aplicación de la gestión de los datos de la empresa (EDM, en inglés) o la detección de documentos con huella digital. • Aplique las políticas de DLP de forma selectiva a los datos según el contexto de una transacción. Analice actividades, usuarios, aplicaciones, instancias o dispositivos específicos para desarrollar políticas que generen menos falsos positivos. • Tome medidas correctivas adecuadas cuando se activen las políticas de DLP, como bloquear las transferencias de datos, alertar, avisar a los usuarios, o cifrar o poner en cuarentena un archivo. • Las herramientas de investigación nativas de Netskope simplifican el análisis de incidentes DLP ya que proporcionan información forense, como por ejemplo fragmentos de los datos relacionados con una infracción, y permiten priorizar los incidentes y asignarlos a los investigadores.
ZERO TRUST NETWORK ACCESS	**PERMITA UN ACCESO REMOTO SIN INTERRUPCIONES A LAS APLICACIONES ALOJADAS EN CENTROS DE DATOS Y NUBES PÚBLICAS:** • Proporcione un acceso a red Zero Trust (ZTNA) a las aplicaciones privadas. Proteja los datos y los recursos con controles de acceso a nivel de las aplicaciones que se basen en la identidad del usuario y la postura de seguridad del dispositivo. • Ofrezca un acceso directo y sin interrupciones a nubes públicas para que los usuarios remotos se conecten directamente a las aplicaciones alojadas en dichos entornos, sin necesidad de emplear *backhauling* con la infraestructura corporativa para acceder a ellas. • Evite que las aplicaciones privadas queden expuestas públicamente en entornos de nube pública, como AWS o Azure, para así no correr el riesgo de tener usuarios no autorizados externos. • Simplifique las operaciones informáticas, modernice la arquitectura de redes, mejore la experiencia de usuario final y aumente la seguridad en el uso de Internet mediante una plataforma escalable basada en la nube que unifica las soluciones ZTNA, CASB, SWG y DLP.
VISIBILIDAD Y CONTROL	**OBTENGA UNA VISIBILIDAD EN PROFUNDIDAD DEL USO QUE REALIZAN LOS USUARIOS REMOTOS DE LAS APLICACIONES EN LA NUBE Y DE LA WEB, Y DEFINA LAS POLÍTICAS PARA CONTROLAR LAS ACTIVIDADES:** • Descubra todas las aplicaciones de la nube gestionadas y no gestionadas (*shadow IT*) que utilizan los usuarios remotos y evalúe su potencial de riesgo. • Identifique los comportamientos y actividades de alto riesgo por parte de los usuarios remotos dentro de las aplicaciones en la nube gestionadas y no gestionadas. • Utilice la capacidad de Netskope para distinguir instancias para prevenir la pérdida de datos corporativos a instancias personales en aplicaciones en la nube. • Gestione las actividades compartidas y posteriores de forma granular en las aplicaciones de la nube para prevenir que los datos sensibles queden expuestos. • Detecte amenazas de cuentas comprometidas y de usuarios internos o con privilegios. • Registre una pista de auditoría de la actividad de los usuarios remotos dentro de las aplicaciones de la nube y los sitios web para las investigaciones forenses.

SOLICITE UNA DEMO EN DIRECTO:
https://www.netskope.com/request-demo

netskope

Netskope Security Cloud proporciona una visibilidad incomparable, así como protección de datos y amenazas en tiempo real durante el acceso a servicios en la nube, sitios web o aplicaciones privadas desde cualquier parte y desde cualquier dispositivo. Solo Netskope entiende la nube y adopta un enfoque centrado en los datos que otorga a los equipos de seguridad el equilibrio adecuado entre la protección y la velocidad que necesitan para asegurar su viaje de transformación digital. Reimagine su perímetro con Netskope.