RESUMEN DE LA SOLUCIÓN

Netskope para Microsoft Teams

Netskope para Microsoft Teams ayuda a las organizaciones a colaborar de forma segura desde cualquier lugar para aumentar la productividad mientras protege los datos confidenciales de usos indebidos y accesos no autorizados.

«En el contexto empresarial actual, el 33 % de los empleados trabajan a distancia. De media, están repartidos en más de 8 ubicaciones».

Informe sobre amenazas en la nube de Netskope
Febrero de 2020

PRINCIPALES CASOS DE USO

- **Perfeccione los controles de colaboración.** Aplique políticas de acceso granulares y limite el intercambio de datos confidenciales en Microsoft Teams a terceros no autorizados o dispositivos no gestionados.
- **Aplique políticas de prevención de pérdida de datos.** Evite que se descarguen o se carguen archivos y datos confidenciales en Microsoft Teams.
- **Detecte y evite amenazas.** Detecte *malware* y riesgos en la nube, como amenazas internas, cuentas comprometidas y comportamientos anómalos de usuarios.
- **Supervise, investigue y audite.** Analice una pista de auditoría completa de toda la actividad de usuarios y aplicaciones en Microsoft Teams.

EL DESAFÍO

Microsoft Teams es una solución de colaboración que se ha consolidado en el mundo empresarial. Esta herramienta, que forma parte del conjunto de aplicaciones de Office 365, ayuda a aumentar la productividad y la colaboración en empresas de todos los tamaños al ofrecer un espacio único donde conversar con compañeros/as, organizar videoconferencias y almacenar archivos. Si bien esta colaboración innovadora resulta muy atractiva para los usuarios, también presenta nuevos retos para los equipos del departamento de seguridad informática a la hora de identificar, controlar y proteger los datos que se comparten entre usuarios y empleados. Los responsables de seguridad deben garantizar que solo las personas autorizadas puedan ver y acceder a datos confidenciales, para evitar exfiltraciones o usos compartidos fuera de la organización, para cumplir con las normativas y, por último, para detectar y detener amenazas que quieran ingresar al sistema.

Las organizaciones necesitan una estrategia global y uniforme para controlar y proteger usuarios y datos en Microsoft Teams, así como todas las demás aplicaciones de Office 365.

DESCRIPCIÓN DE NETSKOPE PARA MICROSOFT TEAMS

Netskope para Microsoft Teams es una solución CASB (Cloud Access Security Broker) avanzada que protege datos y archivos confidenciales en entornos de Microsoft Teams. Netskope ofrece a las organizaciones un enfoque integral de la seguridad en la nube, ya que les permite tener visibilidad y control exhaustivos de todas las cuentas de Microsoft Teams de la empresa. El equipo

de operaciones de seguridad obtiene información detallada y contexto sobre la actividad de colaboración en Microsoft Teams con controles de acceso a archivos y datos granulares, y puede detectar comportamientos anómalos que podrían suponer una amenaza grave para la organización. Los controles de seguridad en tiempo real pueden bloquear actividad maliciosa o no autorizada al instante con protecciones de seguridad entre su implementación de Microsoft Teams y los usuarios, sin importar dónde se encuentren.

Netskope para Microsoft Teams cuenta con la certificación de Microsoft, ya que Netskope forma parte del programa de certificación y licencias de Microsoft Teams y cumple con todos los requisitos.

FUNCIONALIDADES CLAVE

ADMINISTRACIÓN CENTRALIZADA Y UNIFORME

Netskope ofrece un único punto de control para administrar la seguridad de la nube y el cumplimiento en la web y en miles de aplicaciones en la nube. El área de seguridad informática ahora puede ver en detalle las actividades de sus instancias de Microsoft Teams desde un solo panel, lo que le permite definir controles granulares y contextuales para proteger datos confidenciales. Netskope unifica la gestión de políticas en Microsoft Teams y otras aplicaciones de Office 365, como OneDrive, Outlook y SharePoint, y en entornos de nube pública como Azure, lo que facilita flujos de trabajo e informes homogéneos e intuitivos para proteger los entornos de Microsoft.

CONTROL Y VISIBILIDAD GRANULARES

Netskope le permite ver todo lo que sucede en Microsoft Teams y en otras aplicaciones de Office 365, además de cómo interactúan estas aplicaciones en la nube. Los administradores de seguridad obtienen información basada en riesgos que identifica archivos confidenciales y expone cómo se comparten. Con Netskope para Microsoft Teams, el área de seguridad informática define políticas muy específicas para controlar actividades y garantizar la protección. Gracias a Cloud XD™, Netskope puede aplicar políticas de seguridad detalladas a partir de información contextual, como aplicaciones en la nube, usuarios, instancias, actividades y dispositivos. Cloud XD™ decodifica en tiempo real el tráfico de aplicaciones en la nube y descubre información contextual que puede usarse para controlar aplicaciones en la nube gestionadas y no gestionadas. Al distinguir instancias empresariales y personales de una aplicación en la nube, los equipos de seguridad informática pueden bloquear la carga de un documento confidencial de Microsoft Teams a una aplicación en la nube no gestionada. Cuando los empleados usan sus dispositivos personales para acceder a datos corporativos almacenados en aplicaciones de Microsoft relacionadas, como OneDrive o SharePoint, Netskope puede aplicar políticas condicionales que limitan el acceso a solo lectura y evitan la descarga de archivos confidenciales a dispositivos personales no gestionados. Las políticas personalizadas también detectan y restringen actividades, como el intercambio de información de identificación personal (PII) en canales de Microsoft Teams, y los mensajes de advertencia personalizados alertan a los empleados de ciertas actividades de alto riesgo.

> **«El 20 % de los usuarios mueve datos sensibles entre aplicaciones en la nube, y el 37 % de esos datos incurre en violaciones de DLP».**
>
> **Informe sobre amenazas en la nube de Netskope**
> **Febrero de 2020**

PROTECCIÓN DE DATOS AVANZADA

Netskope ofrece funciones avanzadas de prevención de pérdida de datos (DLP) para identificar y proteger datos confidenciales, más allá de dónde se encuentren o a qué lugar vayan, como aplicaciones SaaS, servicios IaaS o la web. Esto incluye proteger datos en reposo y en tránsito. Los equipos de seguridad pueden inspeccionar los mensajes y archivos de Microsoft Teams en tiempo real. Esto les permite detectar exfiltración de datos confidenciales y reducir el riesgo de amenazas internas en momentos de mayor colaboración. Netskope cuenta con las funcionalidades de DLP más avanzadas del sector, diseñadas para ofrecer una gran precisión y una tasa baja de falsos positivos. Al admitir más de 3000 identificadores de datos, más de 1000 tipos de archivos, expresiones regulares personalizadas, análisis de proximidad, *fingerprinting*, correspondencia exacta y reconocimiento óptico de caracteres (OCR),

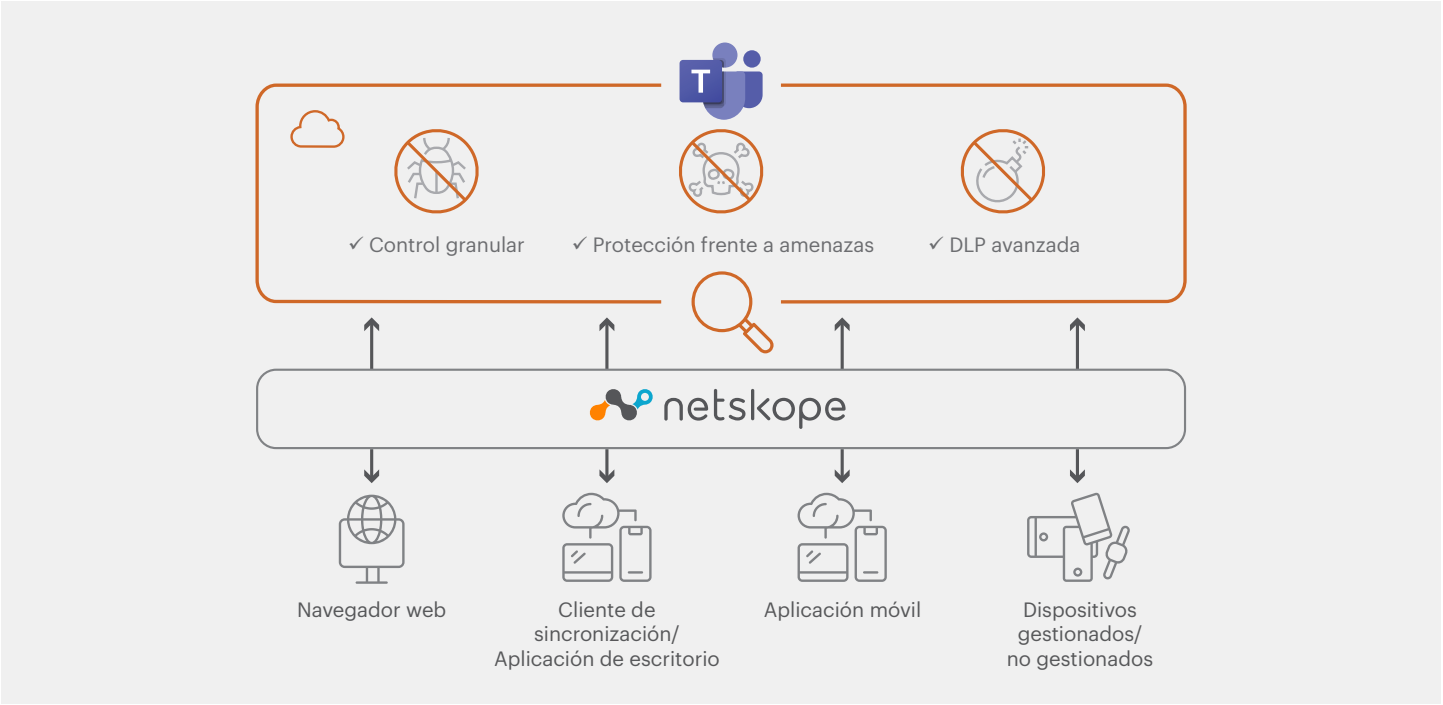

IMAGEN 1: Netskope para Microsoft Teams

Netskope DLP protege eficazmente los datos en todas sus aplicaciones de Office 365. Netskope también ayuda a cumplir las normativas facilitando más de 40 plantillas de políticas predefinidas (por ejemplo, PCI, HIPAA o RGPD), así como plantillas personalizables para responder a los requisitos únicos de cada sector.

PROTECCIÓN FRENTE A AMENAZAS EN LA NUBE Y MALWARE

Netskope ofrece protección avanzada frente a amenazas en la nube y *malware* para que nada vulnere su entorno ni afecte la productividad. Netskope detecta amenazas en datos en reposo, pero también controla el tráfico en la nube y los datos en tránsito. Con un motor de protección en múltiples capas y 40 fuentes diferentes de inteligencia de amenazas, logra exponer amenazas nuevas en la nube que suelen esquivar los controles de soluciones anticuadas. Netskope ofrece análisis de comportamiento de usuarios y entidades (UEBA) que aprovecha el aprendizaje automático para supervisar la conducta de los usuarios. Además, el motor de detección de anomalías basado en reglas avisa al equipo de operaciones de seguridad si hay inicios de sesión sospechosos, demasiada actividad, exfiltración de datos o credenciales comprometidas para resolver incidentes lo más rápido posible, al tiempo que ofrece opciones de reparación flexibles.

Los administradores de seguridad pueden detectar y resolver fácilmente *malware* en la nube o en archivos compartidos con Microsoft Teams. Los archivos que contienen *malware* se ponen en cuarentena y se reemplazan por archivos de marcador de exclusión que se propagan por toda la organización para reducir el riesgo de infección. Con la ayuda de la visibilidad granular de Cloud XD, el área de operaciones de seguridad también puede prevenir que instancias personales o no autorizadas hagan un ataque de *phishing* o distribuyan amenazas en la nube, que son los principales desafíos a los que se enfrentan las empresas hoy en día. Por último, Netskope permite que los equipos de respuesta frente a incidencias recopilen metadatos completos durante 90 días, y hasta por 1 año, del tráfico de la web y de la nube para realizar investigaciones y análisis adicionales.

BENEFICIOS	DESCRIPCIÓN
GRAN VISIBILIDAD Y CONTROL	**CONSIGA UNA MAYOR VISIBILIDAD Y CONTROL DE MICROSOFT TEAMS:** • Detecte la creación de nuevos Teams • Detecte cambios en los ajustes de privacidad en Teams (por ejemplo, de «Privado» a «Público») • Detecte si se incorporan o quitan usuarios en Teams • Detecte y examine contenido (mensajes y archivos adjuntos) en los equipos • Bloquee, permita y alerte cuando haya una actualización, carga o descarga de contenido en Teams • Reemplace mensajes incorrectos o que no cumplen la normativa con una advertencia (extinción)
POLÍTICAS DETALLADAS DE ACCESO DE SEGURIDAD	**CREE POLÍTICAS DE SEGURIDAD GRANULARES EN MICROSOFT TEAMS** • En función del usuario, dispositivo, aplicación en la nube, actividad, instancia y mucho más con Cloud XD™ • Examine determinados tipos de Teams • Examine mensajes de chat directos, en canales y en reuniones
PROTECCIÓN DE DATOS AVANZADA	**DESARROLLE POLÍTICAS DE DLP GRANULARES:** • Defina palabras clave y frases para detectar datos confidenciales o regulados • Cree expresiones regulares personalizadas y granulares para identificar patrones alfanuméricos • 3000 identificadores de datos predefinidos (como número de tarjeta de crédito, nombres personales y direcciones) • Más de 40 plantillas de políticas y cumplimiento (como PCI-DSS e HIPAA) • *Fingerprinting* de archivos no estructurados y estructurados con correspondencia exacta o parcial • Reconocimiento óptico de caracteres (OCR) con clasificación y escaneo de imágenes gracias a la tecnología de aprendizaje automático **ACCIONES DE DLP:** • Alertas de infracciones de DLP • Bloqueo de mensajes o archivos adjuntos que infringen las políticas
PROTECCIÓN FRENTE A AMENAZAS EN LA NUBE Y MALWARE	**PROTÉJASE DE LAS AMENAZAS DE LA NUBE MÁS RECIENTES:** • **Análisis de comportamiento de usuarios y entidades (UEBA):** Ofrece análisis de aprendizaje automático por lotes y en tiempo real, y reglas secuenciales predefinidas y personalizables para detectar cargas, descargas y eliminaciones masivas de datos, inicios de sesión incorrectos, etc. • **Amenazas internas:** Detecte comportamientos anómalos identificando cantidades inusuales de datos cargados y cambios en el comportamiento de usuarios y la frecuencia de inicios de sesión en servicios en la nube. • **Cuentas comprometidas:** Evalúe intentos de acceso identificando inicios de sesión desde ubicaciones geográficas sospechosas, ataques de fuerza bruta y patrones de acceso inusuales. • **Integración con herramientas de terceros:** Conecte Netskope con soluciones de EPP (plataforma de protección de endpoints), EDR (detección y respuesta en endpoints), SIEM (gestión de información y eventos de seguridad), *sandboxing* y con muchas herramientas más. • **Amenazas de usuarios con privilegios:** Identifique elevaciones de privilegios repentinas, cuentas inactivas y accesos al sistema de usuarios inusuales. • ***Malware*:** Bloquee *malware* conocido, descubra archivos desconocidos e identifique exfiltraciones de datos por actividades de comando y control (C2). • **Inteligencia de amenazas:** Recopile y use más de 40 fuentes de inteligencia de amenazas. Cloud Threat Exchange (CTE) de Netskope le permite compartir información de amenazas con EPP, EDR, SIEM, etc.

SOLICITE UNA DEMOSTRACIÓN EN VIVO:

https://www.netskope.com/es/request-demo

netskope

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