Netskope CASB para Microsoft 365

Microsoft 365 está siendo adoptado por organizaciones de todos los tamaños. Como el único CASB con el estado de Microsoft Gold Cloud Productivity Partner, Netskope CASB para Microsoft 365 brinda a los usuarios productividad con las herramientas que necesitan mientras mantienen la visibilidad y los controles para proteger los datos confidenciales, evitar pérdidas y garantizar el cumplimiento.

CASOS DE USO CLAVE

• **Aplique políticas granulares de protección contra la pérdida de datos en todas las aplicaciones de Microsoft 365:** Evite que se descarguen o carguen datos confidenciales en todas las aplicaciones de Microsoft 365.

• **Construir controles de colaboración y uso compartido:** Restrinja el uso compartido de datos confidenciales o regulados en Microsoft 365 a terceros no autorizados.

• **Administre la descarga y sincronización de datos a dispositivos no administrados:** Aplique políticas de acceso granular en dispositivos no administrados mediante políticas de usuario específicas del contexto.

• **Realice investigaciones con registros de auditoría detallados:** Examine una pista de auditoría completa de toda la actividad de los usuarios y las aplicaciones.

• **Detecte y administre las amenazas y el malware de los empleados:** Detecte amenazas internas, cuentas comprometidas, amenazas en la nube, malware malicioso y comportamiento anómalo del usuario.

EL RETO

La colaboración y la comunicación son componentes clave de la productividad en las organizaciones modernas. Microsoft 365 proporciona el entorno necesario para facilitar esta colaboración y comunicación, ofreciendo la suite de productividad de facto para muchas organizaciones de todos los tamaños. Microsoft 365 se creó desde cero para adaptarse a una fuerza de trabajo más móvil, lo que ayuda a realizar el trabajo en cualquier lugar y en cualquier momento. Sin embargo, esta flexibilidad también puede facilitar los desafíos de seguridad. Aunque Microsoft 365 proporciona controles de seguridad nativos, las organizaciones a menudo descubren que necesitan un enfoque más amplio de la seguridad que tenga en cuenta el uso de aplicaciones empresariales y la movilidad de los trabajadores móviles.

NETSKOPE CASB PARA MICROSOFT 365

Netskope CASB para Microsoft 365 proporciona una solución de seguridad sólida que ayuda a los equipos de seguridad a comprender y controlar las actividades de riesgo en el conjunto de aplicaciones de Microsoft 365 y permite la protección de datos confidenciales y el bloqueo de amenazas en la nube. Netskope brinda una visibilidad profunda de la actividad y el uso del nivel de datos dentro de cada aplicación de Microsoft 365 y cualquier otra aplicación en la nube que use su organización, administrada o no administrada. En cada aplicación, los equipos de seguridad pueden observar violaciones de datos corporativos y amenazas cibernéticas potenciales que pueden poner en peligro la seguridad y el cumplimiento de su organización.

CAPACIDADES

UNA VISTA COMPLETA DE MICROSOFT 365 Y TODAS LAS APLICACIONES

Netskope puede revelar una visibilidad profunda de su Microsoft 365 y todas las aplicaciones en uso dentro de su organización. Los equipos de seguridad pueden analizar cada aplicación individual de Microsoft 365 u obtener una vista consolidada del uso.

Las aplicaciones de Microsoft 365 como Exchange, SharePoint y OneDrive pueden revelar actividades críticas y uso de datos previamente desconocidos, información que los equipos de seguridad simplemente desconocían antes. Con Netskope, puede obtener una visibilidad granular de la actividad de Microsoft 365 y la difusión de datos confidenciales dentro y fuera de su organización. Sin embargo, para proporcionar una solución de seguridad más sólida, los equipos de seguridad deben implementar controles de seguridad granulares en el uso de aplicaciones en la nube tanto administradas como no administradas. El punto ciego más grande para los equipos de seguridad es el uso no oficial de aplicaciones no administradas que a menudo proliferan en las organizaciones.

Con Netskope, puede obtener una visibilidad granular de la actividad de Microsoft 365 y la difusión de datos confidenciales dentro y fuera de su organización.

La seguridad más robusta de Microsoft 365 se puede eludir por completo con TI en la sombra o aplicaciones de consumo que pueden proporcionar una puerta de enlace para filtrar datos confidenciales. Sin el conocimiento de los equipos de seguridad, un empleado podría descargar correctamente datos confidenciales de una instancia administrada de Microsoft 365 y luego cargar los mismos datos confidenciales en su instancia personal de Microsoft 365.

Netskope proporciona una sólida plataforma de seguridad en la nube que descubre todas las aplicaciones, administradas o no administradas. A través de Cloud XD, Netskope puede distinguir granularmente entre instancias corporativas y personales de cualquier aplicación en la nube, lo que ayuda a bloquear todas las vías que pueden permitir que los datos confidenciales se exfiltren fuera de una organización.

Con la tecnología de Cloud XD, la plataforma de seguridad de Netskope ayuda a definir un control contextual granular profundo en sus políticas de seguridad.

POLÍTICAS DE ACCESO DE SEGURIDAD GRANULAR

Los empleados de hoy exigen la libertad de usar activamente sus propios dispositivos personales en el lugar de trabajo, mientras acceden a recursos corporativos confidenciales basados en la nube. Sin embargo, el fácil acceso puede permitir la descarga de datos confidenciales en dispositivos personales que pueden aumentar el riesgo organizacional, ya que un empleado puede cargar los mismos datos confidenciales en su aplicación personal basada en la nube, todo bajo la supervisión del equipo de seguridad.

Netskope puede aplicar políticas de seguridad granulares en las aplicaciones de la suite de Microsoft 365, los dispositivos de los empleados y los datos confidenciales, instalando medidas de seguridad que evitan que los datos confidenciales vayan a donde no deberían. Con la tecnología de Cloud XD, la plataforma de seguridad de Netskope ayuda a definir un control contextual granular profundo en sus políticas de seguridad. Cloud XD proporciona una inspección profunda de paquetes en tiempo real en el tráfico de aplicaciones en la nube, descubriendo información contextual que pueden utilizar los equipos de seguridad para definir controles de seguridad ultra estrictos que están diseñados específicamente para cada aplicación en la nube en uso activo, independientemente de si son administradas o no administrado.

Dotados de nuevos y potentes controles de seguridad, los equipos de seguridad pueden alejarse de las políticas de seguridad de "permitir" o "denegar" de grano grueso que a menudo proporcionan una aplicación primitiva que no puede distinguir entre una instancia corporativa o personal de la misma aplicación en la nube. Al habilitar de forma segura las aplicaciones en la nube con barandillas de seguridad, se garantiza que los usuarios y los departamentos puedan continuar usando las aplicaciones en la nube, pero sin afectar la postura de seguridad de la organización.

PROTECCIÓN AVANZADA CONTRA LA PÉRDIDA DE DATOS

Los datos están en riesgo a medida que desaparece el perímetro de la empresa, lo que hace que las aplicaciones y los usuarios de la empresa vayan más allá de sus líneas de seguridad tradicionales. Nacido en la nube, Netskope proporciona protección contra pérdida de datos (DLP) nativa de la nube que protege los datos confidenciales dondequiera que viajen; a cualquier aplicación SaaS, servicio IaaS o a la web.

Construido desde cero, Netskope tiene la capacidad DLP más avanzada de la industria, diseñada para una alta precisión y un bajo número de falsos positivos. Con más de 3000 identificadores de datos, compatibilidad con más de 1000 tipos de archivos, expresiones regulares personalizadas, análisis de proximidad, huellas dactilares, coincidencia exacta y reconocimiento óptico de caracteres (OCR).

Netskope ayuda a los clientes a automatizar configuraciones de políticas complejas y manuales al proporcionar más de 40 plantillas de políticas prediseñadas (PCI, HIPAA, GDPR, etc.), que luego pueden acelerar las implementaciones al personalizar rápidamente las plantillas para que se ajusten a sus requisitos únicos.

Netskope CASB para Microsoft 365 permite a los administradores de seguridad definir reglas granulares de DLP que garantizan que, a medida que los empleados colaboran, no transmiten sin darse cuenta datos confidenciales que infringen claramente la política de seguridad corporativa; protegiendo su organización mientras asegura que los empleados experimenten el máximo nivel de productividad.

PROTECCIÓN CONTRA AMENAZAS EN LA NUBE Y MALWARE

Los ciberdelincuentes han trasladado sus vectores de ataque a la nube, adaptándose a la forma en que las organizaciones ahora implementan sus aplicaciones y datos. Buscan eludir los débiles controles de seguridad. Las soluciones de seguridad heredadas que se implementan en las instalaciones a menudo nunca analizan el tráfico en la nube, ya que la empresa moderna está dispersa entre los usuarios móviles, que acceden directamente a las aplicaciones en la nube desde sus dispositivos finales.

Nacido en la nube, Netskope puede proteger Microsoft 365 examinando directamente el tráfico en la nube, exponiendo las amenazas en la nube que a menudo eluden las soluciones de seguridad heredadas. Con el respaldo de Netskope Threat Labs, un equipo dedicado centrado en el descubrimiento y análisis de nuevas amenazas en la nube, Netskope proporciona una defensa integral contra amenazas para los servicios en la nube, combinando una visibilidad de la nube de 360° con prevención de amenazas de múltiples capas y capacidades flexibles de remediación. Netskope puede proporcionar una visibilidad profunda del tráfico en la nube que otras soluciones de seguridad simplemente no pueden, deteniendo las nuevas amenazas en la nube que con demasiada frecuencia eluden las soluciones de seguridad existentes.

Netskope recopila datos de eventos de Microsoft 365. Mediante el uso de aprendizaje automático avanzado, Netskope puede marcar actividades de comportamiento anómalo en las cuentas de usuario que pueden indicar intentos de exfiltración de datos por parte de ciberdelincuentes que han eludido sus defensas de seguridad.

BENEFICIOS	DESCRIPCIÓN

DEEP MICROSOFT 365 Y VISIBILIDAD Y CONTROL DE LA APLICACIÓN EN LA NUBE

OBTENGA VISIBILIDAD PROFUNDA Y CONOCIMIENTO DE LA APLICACIÓN MICROSOFT 365 Y TODO EL USO DE LA APLICACIÓN EN LA NUBE

- Descubra todas las aplicaciones en la nube administradas y no administradas (Shadow IT)
- Evite la pérdida de datos corporativos de Microsoft 365 por el uso de instancias personales de Microsoft 365
- Evite la pérdida de datos corporativos de Microsoft 365 por el uso de aplicaciones en la nube no administradas.
- Evite que los datos no autorizados se compartan externamente
- Evite que los datos regulados de alto valor se almacenen en la nube
- Bloquear la descarga de datos de Microsoft 365 a dispositivos personales
- Detectar cuentas comprometidas y amenazas internas/de usuarios privilegiados
- Capture un registro de auditoría de actividad para investigaciones forenses

POLÍTICAS DE ACCESO DE SEGURIDAD GRANULAR

CREE FÁCILMENTE POLÍTICAS DE CUMPLIMIENTO GRANULAR BASADAS EN UN CONTEXTO ESPECÍFICO PARA PROTEGER DATOS CONFIDENCIALES DEL ACCESO NO AUTORIZADO:

Cree un control de acceso granular a Microsoft 365 basado en:

- Tipo de dispositivo (administrado, no administrado)
- Tipo de actividad (descarga, carga)
- Usuario específico (John Smith)
- Atributos de usuario (rol, departamento)
- Rango de direcciones IP (por ejemplo, red, proxy)
- Ubicación geográfica (por ejemplo, Rusia)

Aplique políticas de acceso granular como:

- Permitir/denegar el acceso a aplicaciones específicas dentro de Microsoft 365
- Permitir/denegar acciones específicas del usuario dentro de cada aplicación de Microsoft 365
- Forzar autenticación intensificada

PROTECCIÓN AVANZADA CONTRA LA PÉRDIDA DE DATOS

DESARROLLE POLÍTICAS DE DLP GRANULARES A TRAVÉS DE PLANTILLAS FÁCILES DE USAR.

Cree un control de acceso granular a Microsoft 365 basado en:

- Defina palabras clave y frases para detectar datos confidenciales o regulados.
- Cree expresiones regulares personalizadas para patrones alfanuméricos
- Metadatos de archivo (nombre de archivo, tamaño y tipo)
- Huella digital de archivos no estructurados
- Huella digital de archivos estructurados con coincidencia exacta o parcial
- Diccionarios de palabras clave de términos específicos de la industria

Opciones de corrección de DLP:

- Notificar al usuario final
- Notificar a un administrador
- Poner en cuarentena el archivo
- Eliminar el archivo

AMENAZAS EN LA NUBE Y PROTECCIÓN CONTRA MALWARE

OBTENGA UNA VISIÓN DE 360 GRADOS DE TODAS LAS AMENAZAS BASADAS EN LA NUBE:

- **Amenazas internas:** detecte comportamientos anómalos por cantidades inusuales de datos cargados/datos, cambios en el comportamiento del usuario y frecuencia de inicio de sesión en la cuenta de servicios en la nube
- **Cuentas comprometidas:** evalúe los intentos de acceso mediante la identificación de accesos de inicio de sesión geográficos sospechosos, ataques de fuerza bruta y patrones de inicio de sesión inusuales
- **Amenazas de usuarios privilegiados:** identifique aumentos repentinos de privilegios de usuarios, cuentas inactivas y acceso inusual al sistema.
- **Malware:** bloquee el malware conocido, descubra archivos desconocidos e identifique el comportamiento de comando y control que indica la filtración de datos

Cibercorp

¡CONTÁCTATE CON NOSOTROS!

(55) 5089 0510 ext. 803

5548401400

www.cibercorp.com.mx

mkt@cibercorp.com.mx