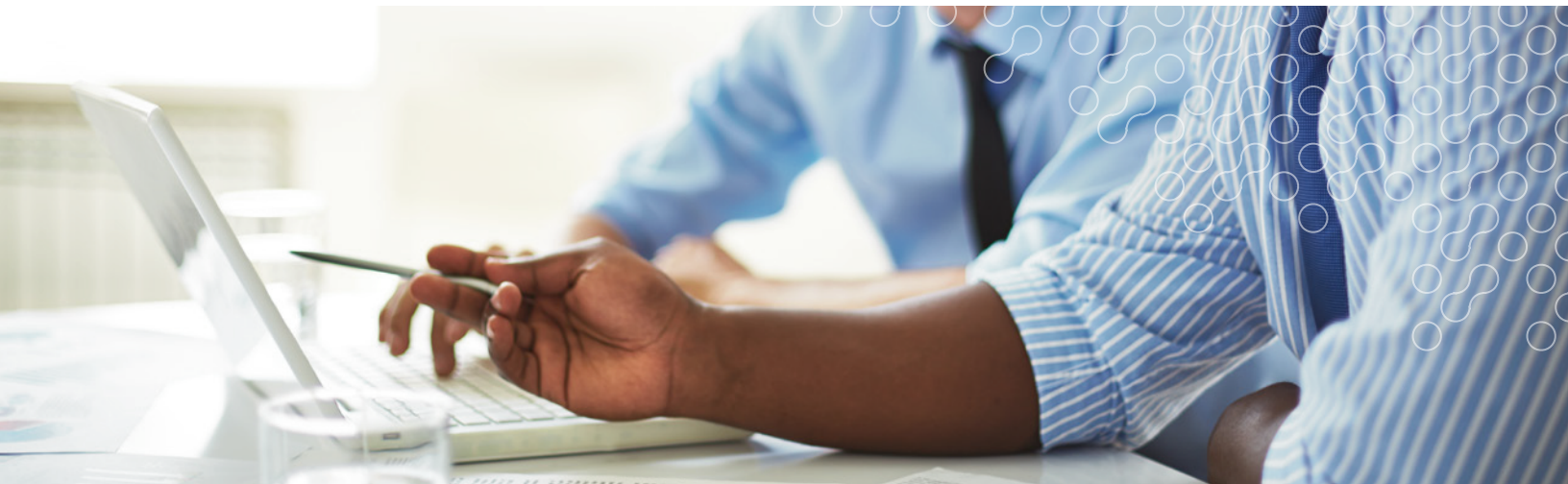


# Netskope y CrowdStrike

El uso cada vez mayor de servicios en la nube y la capacidad de acceder a ellos desde cualquier dispositivo hace que la nube y los endpoints sean puntos críticos para la seguridad. Netskope y CrowdStrike crean juntas una solución de defensa en profundidad, que amplía la detección de amenazas avanzadas a los endpoints y a las aplicaciones en la nube. El intercambio automatizado de información sobre amenazas entre Netskope y CrowdStrike reduce el tiempo necesario para la detección, el análisis forense y la prevención de amenazas en la nube.



## MIRADA RÁPIDA

- Intercambio forense automatizado entre la nube y las soluciones de protección de endpoints
- Respuesta acelerada en el bloqueo de actores maliciosos
- Visibilidad y corrección integrales de amenazas en la nube y los endpoints
- Política de acceso adaptativo para la nube basada en la postura de seguridad de endpoints

## VISIÓN GENERAL DE NETSKOPE Y CROWDSTRIKE

El uso cada vez mayor de los servicios en la nube, junto con la capacidad de acceder a estos servicios en la nube desde cualquier lugar y desde cualquier dispositivo, ha disuelto el perímetro empresarial tradicional. Las organizaciones consideran cada vez más los servicios en la nube y los endpoints como los puntos de control más críticos. Netskope ofrece visibilidad y control integrales de los servicios en la nube, incluida la protección avanzada y de varios niveles contra las amenazas. La plataforma Falcon - nativa de la nube de CrowdStrike, detiene las infracciones al aprovechar el antivirus de próxima generación, la detección y respuesta de endpoints y la inteligencia de amenazas.

Juntas, Netskope y CrowdStrike ofrecen una visión integral de las amenazas tanto en la nube como en los endpoints y colaboran para responder de forma más rápida y eficaz a esas amenazas. Al compartir el análisis forense de amenazas, Netskope y CrowdStrike pueden garantizar que las amenazas recién descubiertas se identifiquen rápidamente, los endpoints se protejan y se neutralice la amenaza en toda la organización. Además, Netskope puede identificar los dispositivos de endpoint que están protegidos por CrowdStrike y controlar granularmente el acceso a la nube y las actividades de los endpoints donde el agente de CrowdStrike no está instalado.

# Netskope y CrowdStrike



## PRINCIPALES CASOS DE USO

### Intercambio de información forense sobre amenazas entre la nube y el endpoint

La plataforma de protección de endpoints CrowdStrike Falcon se une a la perfección con el motor de protección contra amenazas nativo de la nube de Netskope y comparte los indicadores de compromiso (IOC, por sus siglas en inglés) detectados para reforzar la ya robusta detección de malware de Netskope. Juntas, la capacidad mejorada de CrowdStrike y de Netskope proporcionan a los clientes conjuntos un aumento procesable y en tiempo real de los análisis forenses de las amenazas, además de una protección mejorada contra malware tanto en el endpoint como en la nube. Netskope puede enriquecer CrowdStrike al compartir datos sobre nuevas amenazas descubiertas dentro de los servicios en la nube y desde sitios web visitados por los endpoints. A cambio, CrowdStrike puede aprovechar esta información para proporcionar a Netskope detalles de los endpoints que ya pueden estar comprometidos por la amenaza.

### Corrección de ciclo cerrado entre la nube y los endpoints

Netskope puede detectar y remediar amenazas, como malware, que se envían o residen en servicios en la nube. Para cerrar el ciclo de las amenazas recién descubiertas

en la nube, Netskope se integra con CrowdStrike para impulsar el descubrimiento y la prevención en los endpoints. Cuando se descubre un nuevo malware en la nube, Netskope puede pasar el hash del archivo malicioso a CrowdStrike y, basándose en este hash del archivo, CrowdStrike puede alertar sobre los endpoints afectados y/o evitar que se ejecute el archivo malicioso.

### Acceso adaptativo para la nube basado en la postura de seguridad de endpoint

Una de las principales ventajas de los servicios en la nube es la posibilidad de acceder a ellos desde cualquier lugar y desde cualquier dispositivo. Sin embargo, el acceso ilimitado a servicios en la nube no autorizados (Shadow IT) suele ser un vector para que el malware o las amenazas más avanzadas ingresen a una organización. Para solucionar esto, Netskope proporciona capacidades de clasificación de dispositivos que permiten identificar los procesos que se ejecutan en los dispositivos que acceden a los servicios en la nube. Netskope puede evaluar si los procesos del agente de CrowdStrike se están ejecutando en endpoints de Windows y macOS y aplicar políticas de control de acceso adaptativas basadas en el resultado. Por ejemplo, Netskope puede permitir cargas a servicios en la nube solo desde dispositivos endpoints que estén protegidos por CrowdStrike.



Netskope es líder en seguridad en la nube. Ayudamos a las organizaciones más grandes del mundo a aprovechar las ventajas de la nube y la web sin sacrificar la seguridad. Nuestra tecnología patentada Cloud XD apunta y controla las actividades en cualquier servicio en la nube o sitio web. Así los clientes obtienen una protección integral de datos y contra amenazas que funciona en todas partes. A esto le llamamos seguridad inteligente en la nube.

© 2019 Netskope, Inc. Todos los derechos reservados. Netskope es una marca comercial registrada y Netskope Active, Netskope Discovery, Cloud Confidence Index y SkopeSights son marcas comerciales de Netskope, Inc. Todas las demás marcas comerciales son marcas comerciales de sus respectivos propietarios. 07/19 SB-329-1