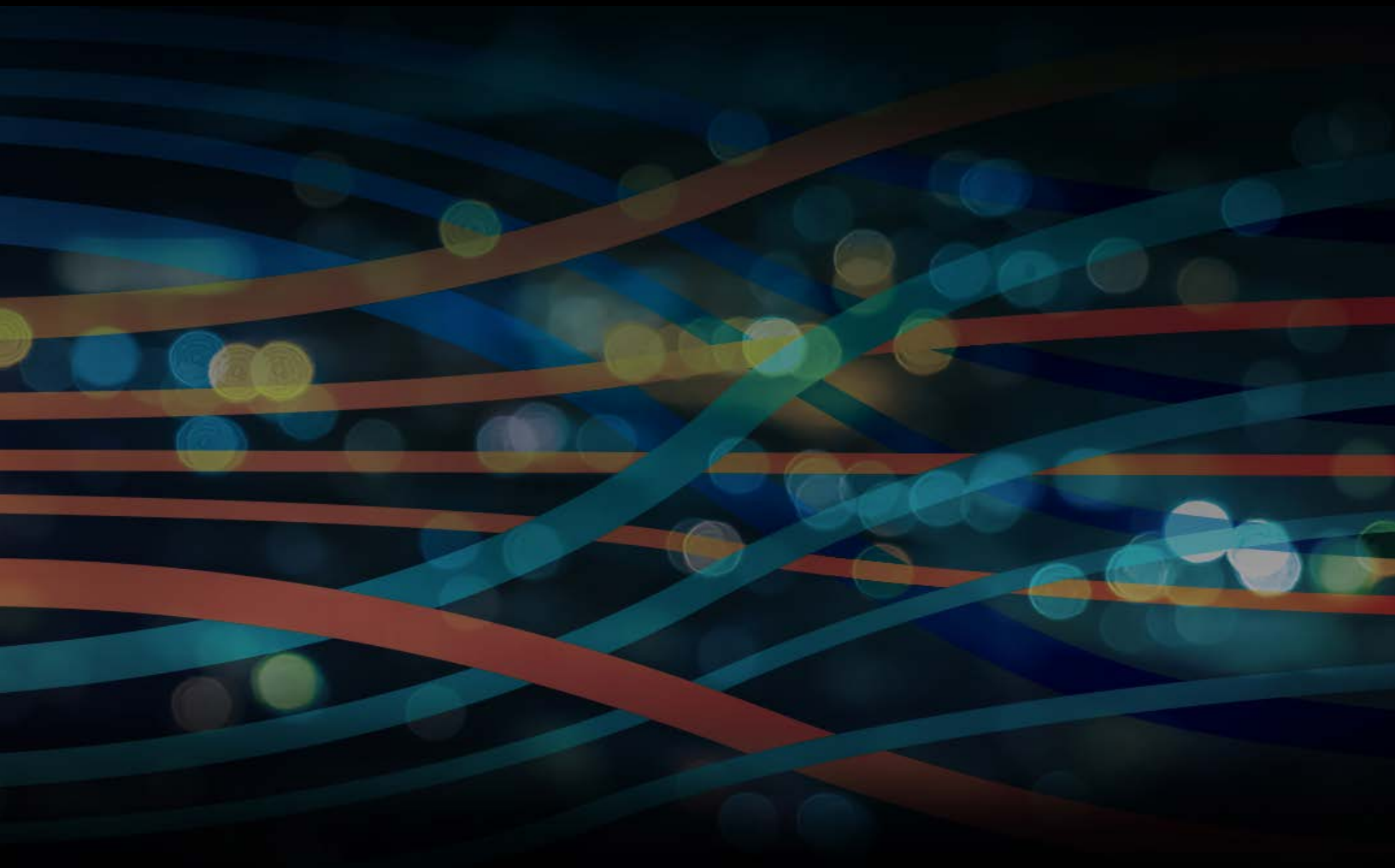
netskope

WHITE PAPER

Cómo adoptar una mentalidad de gestión de los riesgos de seguridad en la nube



A medida que avanzaba el COVID-19, el trabajo remoto se convirtió en la nueva normalidad, acelerando una tendencia que había comenzado hace tiempo. En la actualidad, el 64 % de los empleados de EE.UU. realiza su trabajo fuera de las oficinas corporativas[1] y son pocos los analistas que esperan que esta tendencia cambie su curso cuando la pandemia deje de ser una amenaza para las organizaciones y sus empleados.

Sin embargo, mucho antes de 2020 ya existían problemas de seguridad relacionados con el acceso a la nube y las aplicaciones. La pandemia aceleró esos problemas y en la actualidad existen riesgos generalizados cuando los usuarios acceden a los datos a través de la nube, es decir, en casi todas partes.

Secure Access Service Edge (SASE) surgió como un marco del método que necesitan las empresas y los gobiernos para abordar los factores de riesgo en las aplicaciones en la nube, la información confidencial que circula hacia y entre dichas aplicaciones y los usuarios que actúan de forma peligrosa. La evolución continua de dichos factores de riesgo, incluidas las nuevas aplicaciones, la mayor cantidad de datos y los tipos de datos que se trasladan a la nube, además de una variedad más amplia de usuarios individuales y sus atributos, crean la necesidad de una gestión de riesgos permanente. La gestión de la seguridad no es algo que los equipos puedan "activar y dejar a un lado": los factores de riesgo cambian a cada segundo y los equipos deben poder ajustar continuamente las políticas a los cambios.

Los equipos de seguridad no pueden solucionar el panorama de la nube del mismo modo que protegen los sistemas locales. Y no pueden obligar a hacerlo a productos que no fueron diseñados para la seguridad y conectividad en la nube. El uso de herramientas ineficaces y análisis incompletos constituye un reto para los equipos, que deben evaluar con precisión la posición de riesgo en la nube.

Analicemos cómo hemos llegado a este problema actual y cómo podemos resolverlo hoy.

Enero de 2020 (antes del COVID-19):

El 89% de los usuarios de empresa utilizó aplicaciones y servicios en la nube administrados y no administrados.[2]

Previsión de marzo de 2020:

El 55% de las cargas de trabajo de empresa habrá migrado a la nube en 2022.[3]

Agosto de 2021:

El 83% de los usuarios utiliza instancias de aplicaciones en dispositivos administrados con una media de **20 archivos subidos al mes.**[4]

[1]"Remote Work @ Risk: Cloud and Threat Report," Netskope Threat Labs, agosto de 2020.
[2]"The Dark Side of the Cloud: Cloud and Threat Report," Netskope Threat Labs, febrero de 2020.
[3]Tim Maurer and Garrett Hinck, "Cloud Security: A Primer for Policymakers," Carnegie Endowment for International Peace," 31 de agosto de 2020.
[4]"Cloudy with a Chance of Malice: Cloud and Threat Report," Netskope Threat Labs, febrero de 2021.

Piense de forma creativa

Un responsable de línea descubre una de las muchas herramientas de transferencia de archivos «freemium» o de bajo coste disponibles después de realizar una búsqueda rápida. Es fácil de usar y accesible desde cualquier lugar donde el empleado esté trabajando. El responsable de línea utiliza su tarjeta corporativa y ofrece a sus empleados la solución de productividad que necesitan. Sin embargo, no reflexiona acerca de si esta aplicación en la nube abre una brecha de seguridad que pone en riesgo los datos.

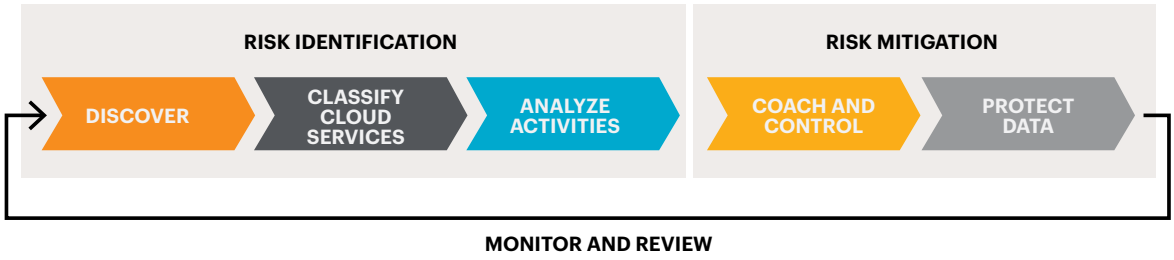
Varios meses más tarde, el equipo de seguridad descubre por casualidad que 50.000 registros de clientes se encuentran en esta herramienta para compartir archivos. No pueden controlar cómo se protegen dichos datos ni tampoco tienen visibilidad de los eventos de seguridad que podrían afectar a esos registros. Esto supone un gran riesgo para la empresa.

La protección de datos debe mantenerse al día

¿Cómo se pueden proteger los datos y las aplicaciones de la empresa si no se implementan ni se configuran los servidores, no se administran las bases de datos o ni siquiera se establecen políticas de seguridad? Se puede adoptar un enfoque de seguridad en la nube que 1.) traslade la seguridad entre los usuarios y las aplicaciones, independientemente de dónde se encuentren, lo cual ayuda a lograr una arquitectura SASE, y 2.) proporcione una gestión de riesgos constante.

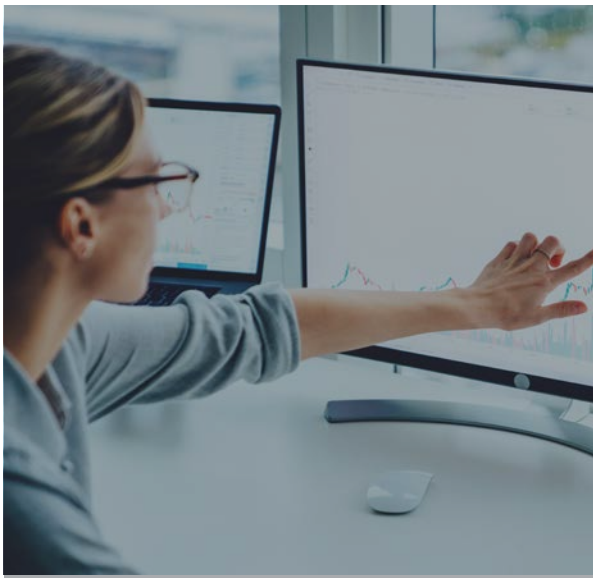
PASAR A UNA MENTALIDAD DE GESTIÓN DE RIESGOS

Hay varios pasos evidentes en el paso a una mentalidad de gestión de riesgos para la seguridad en la nube, que se indican en el siguiente gráfico.



Identificación del riesgo

- Conozca las aplicaciones en la nube que utiliza su organización.
- Clasifique el riesgo asociado con cada aplicación o almacenamiento de datos, y el riesgo organizacional relacionado.
- Identifique a los usuarios que acceden a cada una de esas aplicaciones, cómo se comportan y las actividades asociadas que realizan.



Mitigación del riesgo

- Permita que los usuarios utilicen aplicaciones reduciendo el riesgo para los datos. Informe a los usuarios sobre mejores alternativas cuando el riesgo sea menor y establezca controles para gestionar los factores de riesgo cuando el riesgo sea mayor.
- Proteja la información confidencial mejorando las políticas de protección de datos que supervisan el almacenamiento y controlan el movimiento.

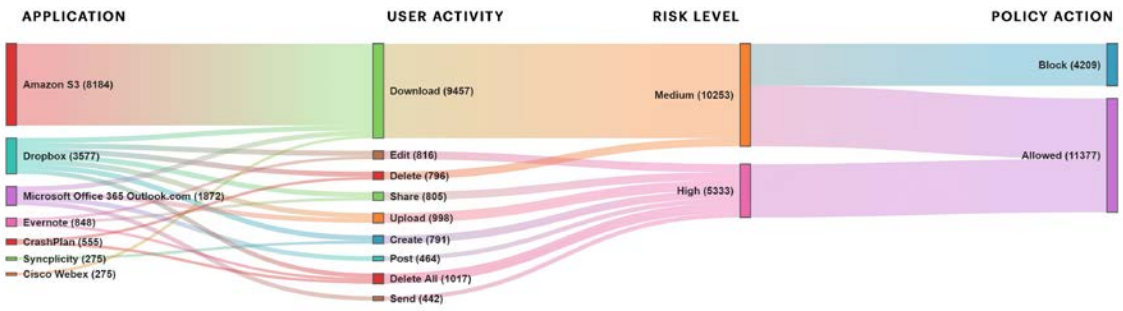
Supervisar y revisar

- Cree un ciclo de realimentación para supervisar el riesgo de la nube de manera continua, proporcionando la información adecuada a todo el mundo, desde los profesionales de seguridad de primera línea hasta los altos ejecutivos y el consejo de administración.

Algunos de estos pasos pueden parecer obvios, pero lo realmente importante aquí es que se trata de un proceso que debe evaluarse continuamente en un ciclo de realimentación, y eso no es sencillo. Si a día de hoy pide a su equipo de seguridad que enumere todas las aplicaciones en la nube que almacenan algunos de los datos de su organización, es poco probable que tengan la respuesta a mano. Puede ser tan complicado como identificar las aplicaciones que usa la organización, y a partir de ahí es aún más difícil. Si les pregunta sobre los riesgos asociados con las aplicaciones, eso es aún más complejo, ya que, ¿cómo se pueden identificar y calificar los factores de riesgo de las aplicaciones que pueden (o no) conocerse?

Visibilidad y control de datos y acceso a la nube

Para elaborar un programa de seguridad eficaz, las organizaciones necesitan visibilidad en las aplicaciones que usan, saber dónde están los datos y hacia dónde se dirigen. Las soluciones de Netskope han sido pensadas para seguir los datos durante su ciclo de vida, dondequiera que vayan. Este enfoque se ha diseñado para crear visibilidad sobre el almacenamiento y el movimiento de los datos en la nube, permitiendo así que los equipos adopten medidas rápidamente en caso de que el acceso o el movimiento supongan algún riesgo.



Netskope Security Cloud combina una pasarela web segura (SWG) de próxima generación, un agente de seguridad de acceso a la nube (CASB) y una prevención de pérdida de datos (DLP) galardonada con microservicios de seguridad, como protección de datos y control de acceso adaptable. La plataforma descubre el uso que una organización hace del software como servicio (SaaS), la infraestructura como servicio (IaaS) y las aplicaciones web. También puede identificar a los usuarios y dispositivos que acceden a cada uno de ellos y proporcionar detalles granulares sobre sus actividades.

La analítica avanzada: una clave para la gestión de riesgos

Cuando se implementa Netskope Security Cloud, Netskope Advanced Analytics cierra el ciclo de la gestión continua de los riesgos.

Esto se debe a que el trabajo más complicado es asegurarse de que su organización tenga en cuenta los nuevos vectores de riesgo y elimine el acceso excesivo allí donde no sea necesario. En otras palabras, la gestión de riesgos exige una adaptación constante para permanecer dentro de un rango aceptable de riesgo que sea tolerable, incluso cuando las aplicaciones, los usuarios y los datos en uso estén cambiando.

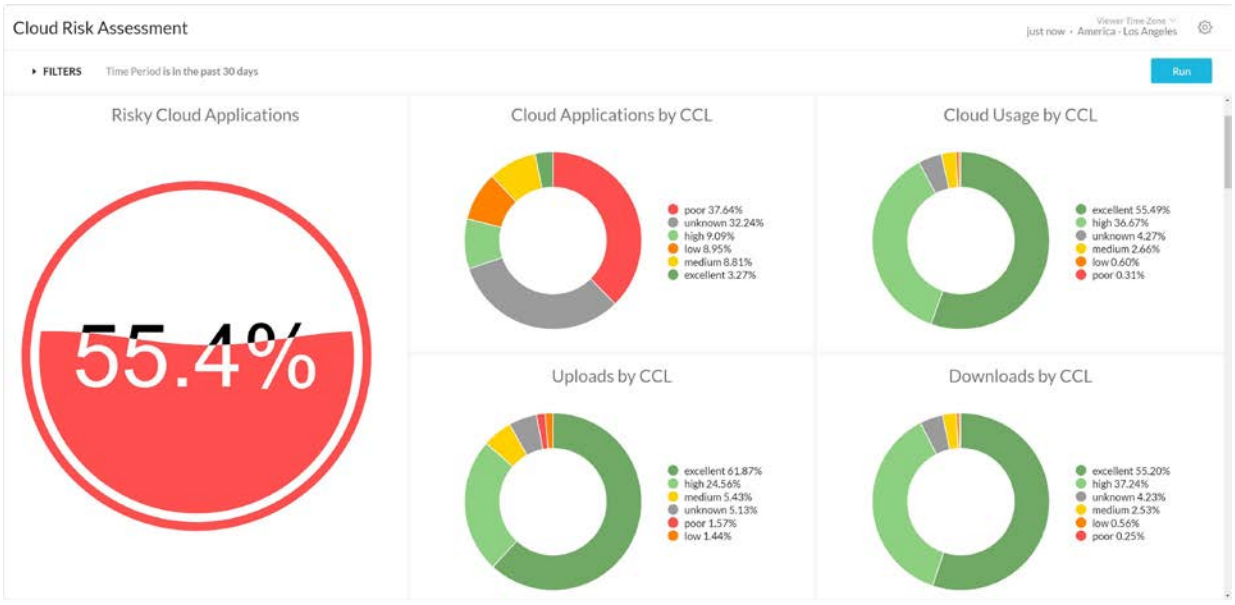
Si cuenta con 10.000 registros de clientes repartidos en 10 aplicaciones en la nube, ¿esto es aceptable o es demasiado arriesgado? ¿Qué sucede si se trata de 10 millones de registros? Necesitará Advanced Analytics, ya que el número en sí no cuenta toda la historia. ¿Cómo pueden los líderes de seguridad de la información corporativa establecer la tolerancia al riesgo de la empresa y crear una política de seguridad que se adapte a las necesidades de los altos cargos y el consejo de administración?

Netskope Advanced Analytics ayuda a los CIO, CISO y a los equipos de TI a dar respuesta a esas preguntas. Debe establecer indicadores clave de rendimiento (KPI) que muestren el estado actual y las tendencias del riesgo para la seguridad de toda la empresa.

Puede hacer uso de Advanced Analytics para establecer la base de cada métrica. Más adelante, puede supervisar cómo está cambiando su exposición al riesgo y adaptar en consecuencia las políticas de seguridad.

En definitiva, Netskope Advanced Analytics respalda a los CISO mediante tres casos de uso de alto nivel:

- Priorizar los esfuerzos de optimización de la seguridad
- Mejorar la eficiencia
- Supervisar la efectividad del programa de seguridad y la posición general de seguridad en la nube



Cloud Risk Assessment de Netskope le permite supervisar el nivel de confianza de la nube (CCL) en toda su organización a fin de identificar los posibles riesgos e implementar políticas de seguridad adecuadas para una adopción segura conforme a sus necesidades comerciales.

1. PRIORIZAR LAS LABORES DE OPTIMIZACIÓN DE LA SEGURIDAD

Desde el punto de vista de una amenaza, su objetivo es interceptar y detener a un posible atacante que pueda poner en peligro a sus usuarios o datos. Pero el escenario de amenazas es inmenso y está creciendo rápidamente. Como sucede con cualquier otra área de TI, la gestión de riesgos exige priorizar los recursos en todas las exposiciones a la nube de la organización.

Netskope Advanced Analytics apoya las decisiones de priorización logrando que las evaluaciones del escenario de seguridad sean fáciles de entender. Los paneles, los informes y las alertas ofrecen información personalizada para grupos específicos de partes interesadas, en un formato diseñado para esas audiencias. Por tanto, el personal de operaciones, la alta dirección y el resto de empleados pueden obtener acceso rápido a la información más relevante para sus cargos. Gracias a las numerosas opciones de visualización de datos, Advanced Analytics permite comprender rápidamente las tendencias de los datos.

VENTAJAS DE NETSKOPE

- Los informes predefinidos incluyen paneles adaptados al personal de operaciones, la dirección y otros trabajadores.
- Capacidad para importar y exportar paneles para colaborar con otros equipos de seguridad.
- Los paneles personalizados se pueden basar en más de 500 campos de datos.
- Las alertas complementan los informes bajo demanda, e indican las métricas que se encuentran fuera de un rango específico.
- Las opciones de visualización incluyen gráficos de barras, gráficos circulares, análisis de tendencias, tablas, gráficos de dispersión, etc.
- Los datos disponibles incluyen detalles sobre el sitio, la aplicación, la instancia, el usuario, la actividad, el archivo, el origen/destino, etc.

2. MEJORAR LA EFICIENCIA DEL PERSONAL DE SEGURIDAD

El personal de seguridad cualificado es uno de los activos de mayor importancia dentro de una organización. Mientras trabajan para proteger a los usuarios y los datos de la organización, necesitan dedicar su tiempo al análisis y la estrategia, no a buscar datos relevantes y apropiados, y filtrar las alertas para hallar las principales causas. Los informes personalizados de Netskope Advanced Analytics proporcionan a los equipos de seguridad visibilidad de lectura rápida sobre cualquier información que necesiten, para identificar la señal a través de todo el ruido superfluo.

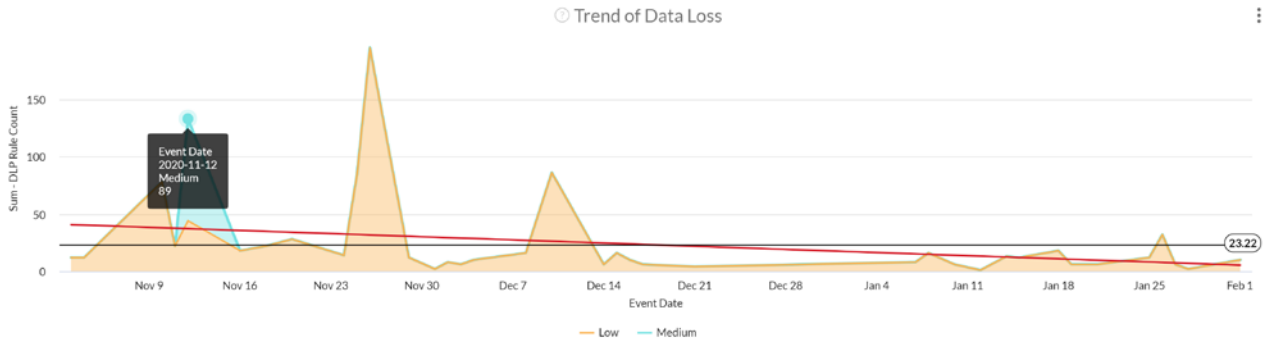
Al mismo tiempo, un paso fundamental para gestionar y controlar el riesgo es investigar las fuentes de riesgos. Además, Netskope Advanced Analytics agiliza el análisis de tendencias de seguridad. Gracias a los *widgets* interactivos, el proceso de investigación es intuitivo, minimizando el esfuerzo de los equipos de seguridad para profundizar en la información granular de Netskope Security Cloud.

VENTAJAS DE NETSKOPE

- La gran biblioteca de informes predefinidos para casos de uso específicos incluye paneles centrados en los CISO, informe de evaluación de riesgos en la nube, panel de protección de datos, informe de cumplimiento del RGPD y muchos otros.
- La personalización permite informes específicos sobre un problema de seguridad concreto, para un cargo determinado, lo que reduce el tiempo necesario para acceder a la información relevante.
- El sencillo generador de informes mejora la eficiencia en la creación de informes personalizados.
- Resultado general: se puede acceder a información de forma más sencilla, con menos esfuerzo, en todos los niveles de la organización.

3. SUPERVISAR LA EFICACIA DEL PROGRAMA DE SEGURIDAD Y EL RIESGO GENERAL

La protección constante de la presencia en la nube de una empresa exige una comprensión actualizada y continua del funcionamiento de las políticas y los programas de seguridad y cómo mejorarlos.



Los informes resumidos de Netskope Advanced Analytics proporcionan datos sobre tendencias que precisan la eficacia del programa de seguridad. ¿Es una política determinada demasiado permisiva? ¿Asume algún usuario concreto cada vez más riesgos en la nube? Manténgase al día sobre los cambios de su política y explique a la dirección que el número de eventos de seguridad aumentará a corto plazo a medida que las políticas se endurezcan, pero las medidas adoptadas reducirán el nivel general de riesgo con el paso del tiempo. Gracias a los informes completos con visualización optimizada de los datos, estas preguntas se pueden responder con facilidad.

El personal de seguridad puede supervisar la efectividad de la seguridad en la nube de una organización en sus paneles y posteriormente analizar en profundidad los detalles para hallar las causas subyacentes en las áreas de interés. Mediante este enfoque, sabrán dónde es necesario realizar modificaciones. Seguidamente, pueden adaptar las políticas y prácticas de seguridad en toda la organización, creando un ciclo de realimentación para actualizar de forma continua la gestión y mitigación de los riesgos de la nube.

VENTAJAS DE NETSKOPE

- La vista de 360 grados ofrece una visibilidad completa sobre la situación frente al riesgo en la nube de la organización a través de todas las aplicaciones, usuarios y datos.
- Análisis de datos resumidos y detallados para destacar las tendencias de seguridad en tiempo real.

«A pesar de los años de inversión y trabajo dedicados a los riesgos cibernéticos, los costes de los incidentes cibernéticos continúan aumentando. Las organizaciones están incrementando su gasto en seguridad cibernética, aunque suelen quedarse cortas».

— Tim Maurer y Garrett Hinck, Carnegie Endowment for International Peace[1]

[1]Tim Maurer y Garrett Hinck, "Cloud Security: A Primer for Policymakers," Carnegie Endowment for International Peace," 31 de agosto de 2020.

CERRAR EL CICLO EN LA GESTIÓN DE RIESGOS

El trabajo remoto es cada vez más habitual. Las tecnologías de la nube están evolucionando aún más rápido. Y las amenazas que sufren las aplicaciones y los datos en la nube se están disparando. Para poder proteger a los usuarios, los datos y las aplicaciones de su organización se necesita una mentalidad de gestión de riesgos y un proceso de mejora continua.

Afortunadamente, Netskope puede ayudarle. Netskope Security Cloud se centra en los datos y la inteligencia en la nube y ofrece la información necesaria para evitar que las amenazas lleguen a los activos que debe proteger. Gracias a Netskope Advanced Analytics, el acceso a dicha información es sencillo y eficiente en todos los niveles de la organización.

Mediante Advanced Analytics, su equipo de seguridad puede obtener la información que necesita, detectar tendencias, centrase en las áreas de interés y abordar los asuntos importantes. Con una analítica mejorada, puede crear un programa de seguridad para protegerse frente a la continua evolución de las amenazas, asegurando de forma eficaz los datos en la nube.

netskope

Netskope Security Cloud ofrece una visibilidad incomparable, datos en tiempo real y protección frente a amenazas cuando se accede a los servicios, los sitios web y las aplicaciones privadas en la nube desde cualquier sitio o dispositivo. Solo Netskope comprende la nube y adopta un enfoque basado en los datos, ofreciendo a los equipos de seguridad la protección y velocidad necesarias para proteger su estrategia de transformación digital.

Para obtener más información, visite https://www.netskope.com.