Nuevas ideas sobre la protección de datos y frente a las amenazas

+ eBook

Lo que los proveedores tradicionales tratan de ocultar

netskope

Índice

Introducción

Las prácticas tradicionales en materia de amenazas y protección de datos pueden estar haciendo más mal que bien. Esta prácticas antiguas también permiten a los proveedores de seguridad ocultar problemas que prefieren que no salgan a la luz. La pandemia aceleró la adopción de sistemas SaaS y en la nube, situando a más usuarios y más datos dejando más usuarios y datos fuera de los perímetros y del alcance de las solucios de seguridad tradicionales. Al trabajar con empresas y mutinacionales en la implantación de Plataformas de servicio de seguridad (SSE), hemos recopilado diez ideas sobre controles de las políticas, buenas prácticas y cómo descubrir puntos ciegos. Recomendamos actualizar sus requisitos de Solicitud de información (RFI) al plantearse una solución SSE o una Plataforma de servicio de acceso seguro (SASE) teniendo en cuenta estos conocimientos adquiridos sobre el terreno.

¿Quién debería conocer estas ideas?

Arquitectos, directores y gestores de seguridad y redes

¿Cuándo se han de leer?

Antes de iniciar un proyecto SSE/SASE y de emitir una solicitud RFI.

¿Por qué se deben leer?

Para comprender los cambios significativos detectados en el panorama de la protección.

Idea 1

Eludir la inspección de tráfico de Microsoft 365 es un punto ciego

Las mejores soluciones SSE de su categoría ahora eliminan la necesidad de elegir entre el rendimiento y la seguridad para eludir la inspección de tráfico de Microsoft 365 (M365); además de que este punto ciego en la protección de los datos y frente a las amenazas ha crecido demasiado como para ignorarlo. Deberá cuestionar a cualquier proveedor de seguridad inline que eluda la inspección del tráfico M365 en su entorno.

Puntos clave

- **Más de un tercio de las amenazas en la nube proceden de OneDrive y SharePoint.** Esta tendencia ha sido uniforme en los últimos cinco años y se puede ver en el informe Netskope Threat Labs 2024 en que estas aplicaciones se sitúan en el primer y tercer puesto en popularidad, respectivamente.
- **Más de la mitad del tráfico web codificado está relacionado con la nube, y M365 puede ocupar la porción mayor.** Hemos superado un punto de inflexión con más tráfico por servicios en la nube y SaaS que tráfico web tradicional. Las aplicaciones M365 pueden representar entre el 35 y el 40% del tráfico SaaS relacionado con la nube ya que los usuarios IT pasan sus días de trabajo en estas aplicaciones, creando y gestionando contenidos.
- **La inspección del tráfico M365 con soluciones de seguridad tradicionales afecta a la experiencia del usuario.** El tráfico de los usuarios que trabajan en remoto y en modalidad híbrida con redes de retorno a un centro de datos en las propios dispositivos de seguridad de las instalaciones puede afectar a la experiencia del usuario. Por otro lado, el acceso directo por parte de los usuarios que traspasan estas puertas de enlace de seguridad crea un punto ciego para la protección de los datos y frente a las amenazas. Las soluciones SSE están reemplazando a estos dispositivos de seguridad y a las VPN tradicionales por una experiencia de usuario más segura, granular y rápida.
- **Los certificados de socios de Microsoft suponen un procedimiento predeterminado que no incluye una inspección o evaluación detallada, a menos que se indique lo contrario.** En retrospectiva, la certificación tenía su justificación, dado el punto anterior sobre las soluciones de seguridad tradicionales que afectaban a la experiencia del usuario. No obstante, las soluciones SSE actuales aportan una serie de accesos globales con una experiencia del usuario eficaz, sin tener que sacrificar la seguridad ni el rendimiento. La tendencia debe cambiar y pasar a inspeccionar el tráfico M365 como fuente principal de amenazas en la nube y posible robo de datos.
- **Consulte el certificado de conexión segura de su navegador web para validar la inspección.** Haga clic en el icono delante de la URL al trabajar con una aplicación M365 para ver la conexión segura del navegador web y su certificado. Si ve un certificado de Microsoft para el túnel TLS, entonces está eludiendo la inspección y existe un punto ciego. Una solución SSE incluye la inspección y utiliza su certificado (o un certificado emitido por una autoridad de certificación) para el túnel TLS seguro desde el usuario hasta la plataforma en la nube SSE. De modo que podrá ver el certificado de la solución SSE para la conexión segura, no el certificado de Microsoft.

Idea 2

Ahora la primera línea de defensa actúa en tiempo real en T+0 para las amenazas frente a la respuesta generalizada

La protección frente a amenazas en el momento T+0 es la primera línea; no hay que dejarse confundir con tasas de detección más altas, horas o días después tras conocer la información sobre las amenazas amenazas compartida entre un grupo más amplio de usuarios. Se trata de un área en la que debe presionar a los proveedores de seguridad inline para que ofrezcan unas tasas de eficacia de la detección T+0 con un bajo porcentaje de falsos positivos.

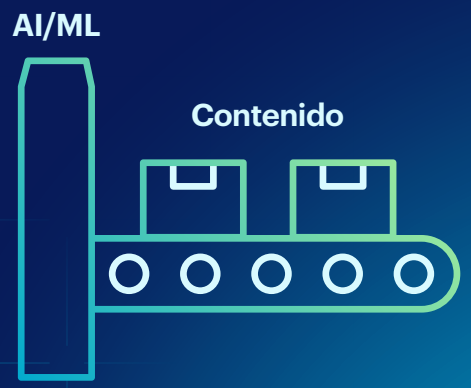
Puntos clave

- **Los ataques tienen ciclos de vida más rápidos, se pueden tratar específicamente y utilizan apps/dominios de confianza.** El paciente cero es la primera persona infectada por una nueva amenaza y con ataques dirigidos, podría ser el único. Determinados ataques utilizan aplicaciones de confianza y servicios en la nube para alojar y poner en marcha la amenaza, estos dominios suelen estar permitidos y como hemos indicado anteriormente, a menudo se eluden evitando su inspección.
- **Validar la protección frente a amenazas en tiempo real T+0 en lugar de T+4-horas o más.** Al revisar los informes de laboratorio sobre la eficacia de la protección frente a amenazas inline, hay que revisar los resultados de T+0 en tiempo real y, si no se suministran, solicitarlos. Numerosos informes documentarán la mayores tasas de eficacia horas o días más tarde, cuando la inteligencia de amenazas generalizada haga que todos parezcan tener un buen desempeño en términos de seguridad.
- **Prestar atención a la tasa de falsos positivos en los informes de las pruebas, es mejor un porcentaje más bajo.** Un truco conocido para probar la protección frente a amenazas es aumentar la capacidad de detección a expensas de los fasos positivos. Mientras que una solución podría obtener tasas del 98% y el 99% de eficacia a lo largo de varias horas de pruebas, hay que comprobar si la tasa de falsos positivos es del 2% o superior. Es poco probable que se obtengan los mismos resultados de alta detección cuando la protección frente a amenazas se active a una tasa de falsos positivos más baja hasta un nivel aceptable por debajo del 1% para los clientes.
- **Solicitar un informe de las pruebas de eficacia frente a amenazas recientes para líneas de defensa inline.** Los ataques cambian y no todas las amenazas suponen archivos ejecutables, ya que aumentan los ataques sin archivos, y los formularios falsos y los ataques por phishing se enfocan en comprometer las credenciales de acceso. Los formularios de acceso falsos, alojados en servicios en la nube de confianza para aplicaciones a las que los usuarios acceden cada día por su trabajo, requieren protección en tiempo real para proteger al paciente cero y a otros usuarios que están expuestos por primera vez a estos ataques. Los informes de las pruebas deben incluir los archivos PE (ejecutables), los ataques no-PE (sin archivos) y los ataques por «phishing». La mayoría de las comprobaciones de los «endpoints» no abarcan a los tres, de modo que se deben buscar soluciones SSE para cubrir esas lagunas. Opcionalmente, cabe considerar las mejores herramientas de prueba de penetración de su categoría si no se puede ofrecer un informe de las pruebas.
- **T+0 es la primera línea de defensa; todos parecen tener un buen desempeño en seguridad horas después, al intercambiarse información sobre las amenazas.** No se conforme con echar un vistazo rápido o buscar los informes de las pruebas de laboratorio de protección frente a las amenazas y conozca los datos de los resultados en tiempo real de T+0, en lugar de horas o días después. También se ha de estar seguro de que la tasa de falsos positivos es aceptable para las pruebas y que cumple con sus expectativas. Es fundamental la protección contra amenazas en tiempo real en T+0 y la rapidez con que las soluciones pueden detectar nuevos ataques en menos de una hora.

Idea 3

La visibilidad del contenido permite implantar líneas de defensa AI/ML con una protección en tiempo real

La inteligencia artificial generativa se expande con perspectivas de transformar numerosas áreas de nuestro día a día, tanto a nivel profesional como personal. Para que la inteligencia artificial y el aprendizaje automático funcionen en tiempo real necesitan contenidos, y ahí es donde las soluciones SSE difieren de la protección de los datos y frente a las amenazas.



Puntos clave

- **Las defensas AI/ML en tiempo real solamente funcionan si incluyen el contenido.** Asumir que los ataques se basan en archivos ignora los formatos de acceso y otras tácticas alojadas en los servicios en la nube utilizadas en los ataques. La detección del «phishing» en tiempo real con defensas AI/ML es viable teniendo en cuenta el contenido que se puede exponer inline durante la transacción comercial para proteger al usuario. Las defensas AI/ML que solamente se utilizan en segundo plano no protegen en tiempo real.
- **Las defensas inline deben aportar visibilidad al contenido para las aplicaciones SaaS.** No todas las soluciones de seguridad SSE inline pueden exponer el contenido para las aplicaciones SaaS gestionadas y no gestionadas y los servicios en la nube, de modo que se ha de inventariar el contenido que se puede inspeccionar. Además, tenga en cuenta que la mayoría de las amenazas proceden de áreas que no pertenecen a la compañía y de instancias personales de aplicaciones SaaS populares en que la inspección inline es su primera línea de defensa, ya que los «endpoints» y la seguridad en el correo electrónico carecen de la capacidad para descodificar el contenido de las aplicaciones SaaS en tiempo real para el análisis AI/ML.
- **Ambos sistemas de protección de los datos y frente a las amenazas utilizan defensas inline basadas en AI/ML.** Los archivos ejecutables portátiles (PE) se pueden detectar inline con clasificadores ML en que 6 de cada 10 archivos PE maliciosos no incluyen una firma conocida en el momento de su detección, según el análisis de las amenazas llevado a cabo por Netskope. Los ataques de «phishing» también se pueden detectar en los casos en que las defensas AI/ML analizan formularios falsos para proteger en tiempo real mucho antes de que las URL afectadas por el «phishing» se compartan en los feeds de inteligencia sobre amenazas. He aquí algunos ejemplos de ataques de «phishing» detectados usando defensas AI/ML en tiempo real.
- **El código fuente es el contenido más popular utilizado en ChatGPT.** Como la aplicación de IA generativa más popular hasta la fecha, ChatGPT está siendo utilizado principalmente para optimizar el código fuente. Los clasificadores de datos AI/ML de Netskope pueden detectar más de 20 tipos de código fuente inline sin la clasificación de datos tradicional, su registro o identificadores de datos de DLP. Así, las soluciones SSE con conectores app GenAI pueden implantar inmediatamente la protección de los datos del código fuente de la compañía e informar a los usuarios en tiempo real para que utilicen aplicaciones y áreas de GenAI aprobadas por la compañía.
- **Las defensas AI/ML deben ser inline, no solo en segundo plano.** Las funciones AI/ML se han utilizado durante años en segundo plano para la detección, optimización, clasificación e incluso para operaciones. El uso extraordinario de las apps GenAI ha supuesto un exceso de uso de la inteligencia artificial en los mensajes y contenidos de marketing. Debemos centrarnos en lo que las soluciones SSE están aportando al primer plano con funciones AI/ML en tiempo real frente al segundo plano.

Idea 4

El «phishing» no se limita al correo electrónico y se adentra en todas las comunicaciones

La llegada masiva de nuevos canales de comunicación a los usuarios está permitiendo el «phishing», el fraude y el acceso comprometido a los negocios, sin limitarse al correo electrónico. Aprovechándose de las SaaS y los servicios de alojamiento en la nube, los ataques de «phishing» pueden moverse por estos dominios populares y evitar la detección por parte de los métodos de seguridad tradicionales, incapaces de descodificar y analizar contenidos SaaS con líneas de defensa en tiempo real. En el futuro, la visibilidad del contenido es un requisito indispensable para que las soluciones SSE puedan habilitar líneas de defensa en tiempo real.

Puntos clave

- **El método de «phishing» es un punto de entrada primario del ransomware.** Cada semana surgen nuevas historias que exponen el impacto del ransomware, con informes de investigación que destacan puntos de entrada clave del «phishing» como paquetes de software y parches, accesos no autorizados, descargas automáticas, publicidad maliciosa y ataques sin archivos. En la cadena de búsqueda y eliminación de los ataques de ransomware, la visibilidad de contenidos permite que la protección de los datos y frente a las amenazas incluya la detección de anomalías, accesos no autorizados y exfiltración de datos.
- **Las redes sociales, la mensajería instantánea, los chats y las comunicaciones personales sufren phishing.** Las instituciones financieras han sido el principal objetivo de los ataques de «phishing», pero las redes sociales han crecido hasta casi alcanzarlas, ocupando el segundo plano a solo un punto porcentual, seguidas de SaaS/webmail en tercer puesto según las **últimas tendencias**.
- **Los usuarios esperan poder disfrutar de un equilibrio profesional/personal y el acceso a apps personales.** El trabajo híbrido y en remoto plantea nuevas formas de gestionar los dispositivos de los usuarios que acceden a sus comunicaciones personales. Incluso al volver a la oficina, los usuarios esperan encontrar una conciliación de la vida laboral y personal. Se debe trabajar para limitar el acceso a las aplicaciones que entrañan un alto riesgo, controlar las actividades de las aplicaciones para proteger los datos, y considerar el aislamiento remoto del navegador (RBI) de las aplicaciones personales SaaS y webmail para proteger los datos. Bloquear el acceso solamente frustra a los usuarios y que los usuarios trabajen al más alto nivel supone una ventaja competitiva.
- **Las apps SaaS contienen formularios de acceso falsos en dominios de confianza para los usuarios.** La adopción de SaaS continúa aumentando año tras año con una tasa de crecimiento superior al 20%, donde más del 98% de las nuevas aplicaciones SaaS son adoptadas por unidades de negocio y usuarios, no por el departamento informático. Hay que mirar por encima de las aplicaciones SaaS gestionadas y concentrarse en las áreas no gestionadas y las instancias personales de las aplicaciones como puntos ciegos con referncia a los ataques de phishing que alojan formularios de acceso falsos.
- **Los ataques ya no se limitan al correo tradicional, por lo tanto, se deberá inspeccionar los sistemas SaaS inline.** Un factor significativo oculto entre la puerta de enlace web segura (SWG) tradicional y el agente de seguridad de acceso a la nube (CASB) es la inspección inline de las aplicaciones SaaS y los servicios en la nube, donde se estima la presencia de cientos de compañías y organizaciones. Conviene evitar los estereotipos de CASB como DLP para SaaS gestionadas y SWG tradicionales para todo lo relacionado con la web y la nube.

Idea 5

Preocupación por las instancias de apps personales como fuente de amenazas y exfiltración de datos

Una nueva zona de alto riesgo para la propagación de amenazas y el robo de datos reside en el punto ciego de las instancias SaaS personales (frente a las de la compañía). Aunque usted puede suministrar a sus usuarios aplicaciones de productividad ofimática SaaS gestionadas, ellos también pueden disponer de su propia versión de instancia personal. Ello posibilita la exfiltración de datos de instancias de la compañía a instancias personales en aplicaciones con suma facilidad, y bajo el mismo dominio que usted autoriza y puede no inspeccionar inline.

Puntos clave

- **El robo de datos aumenta en un 300% en los últimos 30 días de trabajo de los usuarios que abandonan la compañía.** En los dos primeros años de pandemia, el análisis por parte de Netskope de la migración de datos y su expansión observó un rasgo interesante. En el caso de los empleados que abandonaban la empresa, los investigadores buscaron sus últimos 30 días de actividad en materia de datos y detectaron un aumento de más del 300% en la exfiltración de datos en comparación con los usuarios activos. Trabajando en remoto, los usuarios recopilaban datos e información que consideraban valiosa para su siguiente trabajo unas semanas antes de irse.
- **Durante esos 30 días, el 74% del robo de datos implicaba el uso de apps personales de almacenamiento en la nube.** No sorprende que los usuarios recopilasen datos y los desviasen a un almacenamiento personal en la nube durante los últimos 30 días de trabajo, en los que la aplicación más utilizada era Google Drive. Las aplicaciones y los servicios en la nube que ofrecen almacenamiento gratuito favorecen la exfiltración de datos y la presencia de amenazas, teniendo en cuenta lo sencillo que resulta su uso y su acceso.
- **Supervisar y controlar los movimientos de datos entre las instancias corporativas y personales.** Más de 480 aplicaciones cuentan con instancias corporativas y personales, en que el movimiento de los datos y la actividad deben supervisarse, controlarse y analizarse en busca de conductas anómalas. Y en el caso de aplicaciones sin reconocimiento de las instancias, su solución SSE debería poder mapear las identidades de los usuarios para aplicar controles de las políticas por área de aplicación.
- **La abrumadora mayoría de amenazas basadas en la nube proceden de instancias personales.** El primer punto clave en este eBook determinó que OneDrive y SharePoint suponían un tercio del malware transmitido a través de la nube. Lo especial de este punto clave es que las amenazas principalmente proceden de instancias personales y fraudulentas, no de instancias gestionadas por la compañía. Los atacantes crean y utilizan fácilmente aplicaciones gratuitas públicas fraudulentas o cuentas comprometidas para enviar amenazas y exfiltrar datos, por eso es necesario inspeccionar el tráfico SaaS inline con líneas de defensa en tiempo real.
- **Evitar el bloqueo y las restricciones por áreas y habilitar el reconocimiento de instancias en las apps SaaS**. Las soluciones SSE sin reconocimiento de las instancias para cientos de aplicaciones sugerirán el bloqueo de áreas no gestionadas, y solo permitirán el acceso a SaaS gestionadas inline. Esto resulta frustrante para las unidades de negocios y los usuarios, con más del 98% de las aplicaciones usadas no siendo gestionadas por el departamento de informática, lo que elimina una resiliencia viable y la posibilidad de hacer una copia de seguridad si sus apps gestionadas se quedan sin conexión por algún motivo.

Idea 6

Los usuarios necesitan recomendaciones y pautas en tiempo real, no transparencia

Los programas formativos en materia de seguridad pueden cumplir con las normativas una vez al año, pero los conocimientos se olvidan fácilmente y prevalecen las viejas costumbres. Aunque sigue vigente la antigua práctica de seguridad de la transparencia para los sistemas de defensa, ahora nos encontramos en un entorno creciente de SaaS y servicios en la nube en el que los usuarios necesitan asesoramiento en tiempo real durante las transacciones comerciales para proteger los datos. Imagínese conducir en la oscuridad de la noche hacia una nueva ciudad sin navegación GPS en busca de su destino.

Puntos clave

- **Las recomendaciones y las pautas en tiempo real ayudan a los usuarios durante las transacciones comerciales.** Ayudar a los usuarios durante las transacciones comerciales con las aplicaciones de riesgo y recomendar alternativas más seguras. O advertir sobre las actividades de riesgo dentro de las aplicaciones al compartir datos fuera de la compañía. Las recomendaciones en tiempo real, como la navegación por GPS mientras se conduce, están disponibles y debe sacarse el mayor partido rápidamente en las implantaciones SSE nuevas para guiar a los usuarios.
- **Más del 95% del tiempo los usuarios hacen lo correcto cuando se les indica y evitan riesgos.** Cuando se muestra a los usuarios una alerta en tiempo real durante una transacción comercial, referida a una aplicación o actividad de riesgo, nuestras investigaciones y los comentarios de los clientes reflejan que más del 95% de las veces cancelan la transacción comercial para evitar el riesgo.
- **En el otro 5% de los casos, se recogen sus justificaciones para aprender y perfeccionar los controles de las políticas de acceso**. En el caso de los usuarios advertidos sobre una actividad de riesgo con recomendaciones en tiempo real, se puede conocer su justificación para continuar con la transacción comercial. Así podrá perfeccionar aún más los controles de las políticas con un conocimiento más profundo de más casos de uso y escenarios.
- **El bloqueo de las actividades frustra a los usuarios, aumenta las solicitudes de ayuda y reduce la agilidad empresarial**. Los controles de políticas de granularidad gruesa que bloquean las transacciones comerciales deben sustituirse por controles de en tiempo real y para recoger justificaciones. Se genera así un escenario en que todo el mundo gana, donde la mayoría de los usuarios cancelan la transacción de riesgo y los pocos que completan la transacción le informan de por qué lo hacen, aumentando así la agilidad empresarial.
- **Evitar el bloqueo cuando se puedan integrar recomendaciones en tiempo real y educar sobre actividades de riesgo.** Las opiniones de los CIO y los CISO muestran que aprovechar las recomendaciones en tiempo real también supone menos consultas al servicio de asistencia relacionadas con las políticas de bloqueo. La experiencia del usuario, el acceso rápido y la transparencia siguen siendo importantes, pero como ocurre con la navegación GPS, los usuarios aprecian tener pautas para proteger los datos y a la compañía.

Idea 7

Protección de datos frente a DLP formal, cuál es la diferencia

Si trabaja en redes o seguridad y surge el tema de la protección frente a la pérdida de datos (DLP) en una reunión, es probable que piense que es hora de irse o de consultar sus mensajes. Reducir la superficie de ataque con la protección de datos antes de una DLP formal resulta sumamente valioso para los equipos de redes y de seguridad. Los controles de las políticas y el acceso funcionan a modo de embudo para la protección de datos, de manera que cuando se utilizan DLP el esfuerzo resulta más eficiente y específico.

Puntos clave

- **Una DLP formal requiere la clasificación y el registro de los datos, y eso lleva tiempo**. En el caso de los datos estructurados, la DLP formal es la respuesta para todos los canales de actividad con datos, tanto web, SaaS, nube, como para correo electrónico y "endpoint". Sí, lleva tiempo encontrar fuentes de datos sensibles, clasificar los datos y registrarlos para que correspondan exactamente o utilizar una identificación especial en que el rendimiento y la escala son vitales para millones, incluso miles de millones de registros.
- **La protección de datos supervisa y controla el movimiento de los datos por aplicación e instancia.** Antes de la DLP formal, se deberían implementar controles de las políticas de protección de datos que incluyan el acceso a apps de riesgo, actividades en las apps y movimientos de datos por aplicación e instancia. Se deberían instaurar defensas laterales con seguridad de red SSE entorno al movimiento de los datos para que los usuarios reduzcan la superficie de riesgo y la exposición de los datos.
- **Recomendar alternativas más seguras para las apps y las actividades de riesgo, además de pautas en tiempo real**. Parte de la protección de los datos antes de la DLP consiste en el uso de recomendaciones en tiempo real durante las transacciones comerciales. Como ocurre con la navegación GPS y el hecho de saber si se ha producido un accidente en la carretera, puede ofrecer alternativas más seguras para proteger a los usuarios, los datos y a su empresa.
- **Recopilar las justificaciones para avanzar y perfeccionar los controles para el movimiento de los datos.** Conocer nuevos ejemplos y escenarios a través de los usuarios para perfeccionar los controles de las políticas de protección de datos que podrían requerir o no políticas y normas DLP. Una solución SSE aporta visibilidad y control de los contenidos al margen de las soluciones de seguridad tradicionales, dedicando el tiempo necesario para aprender estas nuevas competencias.
- **Reducir la superficie de ataque con un enfoque de embudo para implantar controles de protección de los datos.** Al trabajar con sus requisitos de RFI y una prueba de concepto, debería haber una estructura de embudo para los controles de las políticas, que permita reducir la superficie de ataque mucho antes de que se invoquen las políticas y las normas de la DLP. Todo un conjunto de controles de las políticas debería centrarse en la actividad y el movimiento de los datos, recomendaciones, justificaciones y alternativas más seguras.

Idea 8

La existencia de apps gestionadas frente a no gestionadas redefine las defensas inline

El departamento de seguridad se desvanece junto con la perspectiva del departamento de informática de gestionar solamente lo que adoptan y a lo que acceden. La trasformación digital está avanzando y llevando a las unidades de negocio y los usuarios a adoptar servicios SaaS y en la nube sin implicación del departamento de informática. Mientras que este departamento gestiona 40-60 aplicaciones SaaS y servicios en la nube, probablemente hay miles de aplicaciones en uso dentro de una compañía u organización. Si no se conocen, el primer paso sería una evaluación de riesgos en la nube.

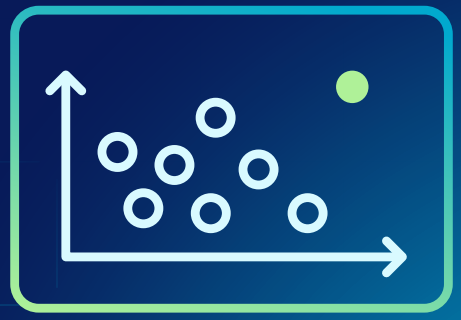
Puntos clave

- **Más del 97% de las aplicaciones que se utilizan no han sido adoptadas y gestionadas por el departamento de informática.** Es la velocidad de adopción la que lleva a SaaS a experimentar un crecimiento superior al 20% año tras año. A medida que las empresas adoptan una estrategia que da prioridad en la nube, buscan apps SaaS para reemplazar a los sistemas que usan en sus centros de datos. Algunos países cuentan con una estrategia de prioridad en la nube, como ocurre en Australia.
- **Las unidades de negocio y los usuarios son los primeros que adoptan apps no gestionadas.** Las unidades de negocio y los usuarios tienen objetivos y plazos que les llevan a la transformación digital, y es una cuestión de supervivencia para algunas compañías. Son los primeros en adoptar aplicaciones SaaS no gestionadas y servicios en la nube ajenos al departamento de informática. Una solución SSE puede habilitar de manera segura áreas no gestionadas e instancias personales con controles de las políticas inline y asesoramiento.
- **La inspección de las APIs solo es válida para apps gestionadas y servicios en la nube.** Mejor juntos es la actitud preponderante, teniendo en cuenta que la inspección de las APIs se limita a aplicaciones gestionadas y servicios en la nube y el factor determinante que mencionamos anteriormente para la inspección inline cubre tanto instancias como aplicaciones personales, gestionadas y no gestionadas. ¿Desea controlar cómo se comparten los archivos e implantar una inspección de las APIs? ¿Desea limitar las apps de riesgo y hacer recomendaciones a los usuarios? Implante la inspección inline con controles de las políticas en tiempo real.
- **Su almacenamiento en la nube probablemente esté limpio, el resto contiene amenazas maliciosas.** No pasa nada, el almacenamiento en la nube gestionado por la empresa probablemente esté limpio y bien protegido. Por eso los atacantes utilizan el alojamiento gratuito en la nube con cuentas falsas e instancias personales para introducir amenazas y «phishing». Aparece entonces el factor determinante, también en esta ocasión, al margen de lo que se puede ver en las áreas e instancias gestionadas.
- **Inspeccionar las apps no gestionadas y las instancias personales inline.** Su RFI debería abarcar la capacidad de incluir la inspección inline para miles de apps no gestionadas y cientos de aplicaciones para el reconocimiento de las instancias. La capacidad para inspeccionar este contenido inline es un factor clave para la protección de los datos y frente a las amenazas, que ayuda a detectar conductas anómalas y a utilizar la analítica para descubrir riesgos y movimientos de datos desconocidos.

Idea 9

La detección de conductas anómalas ya no es opcional

Durante años, la detección de conductas anómalas de usuarios y entidades (UEBA) ha tenido que superar dificultades para encontrar eventos y registros adecuados para los casos de infiltración, accesos comprometidos y exfiltración de datos. La incorporación de registros y eventos SSE, que facilitan información sobre los usuarios, las aplicaciones y la actividad de los datos, ha abierto las puertas para gestionar estos casos con una gran eficacia.



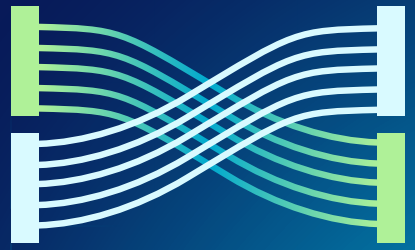
Puntos clave

- **Los usuarios son más descuidados con los datos si trabajan en remoto o en modalidad híbrida.** Unos meses después del inicio de la pandemia las tendencias eran muy claras, con los usuarios en remoto asumiendo más riesgos al acceder a sitios web, contenidos y al compartir dispositivos gestionados. Los usuarios también encontraron vías ajenas a los recorridos conocidos para compartir datos y actividades mientras trabajaban en remoto con múltiples aplicaciones SaaS y servicios en la nube, incluyendo sus propias instancias personales. A medida que avanzaba la pandemia, los usuarios también aumentaron su productividad, quizás por la falta de conversaciones junto a la máquina de café y las distracciones.
- **Un acceso comprometido genera una economía subyacente.** Aumentar la adopción de servicios SaaS con acceso directo desde una ubicación remota y en formato híbrido también abrió la puerta a ataques que comprometen el acceso y una economía subyacente para vender estas credenciales. Para evitarlo, su solución SSE debe incluir direcciones IP de salida específicas para el acceso SaaS que sean exclusivas de su compañía u organización. Se evita así el uso de credenciales comprometidas y problemas reputacionales con direcciones IP compartidas.
- **Use la inspección inline para crear líneas de referencia para las actividades grupales de usuarios y compañeros.** Las soluciones SSE inspeccionan miles de aplicaciones SaaS y cientos de instancias, y ofrecen un registro de eventos y datos excelente. De este modo, se pueden crear las tan deseadas líneas de actividad de usuarios y grupos de compañeros de UEBA para detectar conductas anómalas que van más allá de lo que las reglas sobre anomalías secuenciales y las consultas pueden detectar con precisión. Además, los grupos de compañeros evitan cualquier conducta anómala existente previamente dentro de una referencia de usuario individual.
- **Aprovechar el UEBA basado en el aprendizaje automático (ML) para detectar anomalías.** Teniendo en cuenta los controles granulares de las políticas de una solución SSE, las alertas, registros y eventos habilitan múltiples modelos de aprendizaje automático (ML) y detectores únicos. Una solución SSE debe contar con más de 50 modelos ML y con más de 100 detectores para la detección de anomalías, para tener un grado aceptable de madurez y experiencia.
- **Clasificar y supervisar a los usuarios en función de sus conductas de riesgo y de la exfiltración de datos.** Las soluciones SSE abren la puerta al Índice de confianza del usuario (UCI) para usarse en los controles de las políticas de acceso y para señalar investigaciones en los casos de correlación de eventos para actividades de riesgo y movimientos de datos. Visite nuestro **blog sobre cómo poner en práctica la UEBA** para conocer más detalles.

Idea 10

Analizar para descubrir las amenazas desconocidas en la analítica y las visualizaciones

Comparable a utilizar AI/ML a modo de defensa es el uso de la analítica y las visualizaciones avanzadas para comprender tendencias de aplicación, conductas y anomalías conocidas o desconocidas. Un análisis de riesgos en la nube puede sentar las bases para comenzar a implementar controles de las políticas y supervisar los cambios en la conducta y las actividades, con objeto de lograr los resultados deseados. Las recomendaciones en tiempo real y la recopilación de justificaciones se pueden mostrar en visualizaciones gráficas, así como en nubes de palabras. Es necesario considerar opciones más allá de los SWG tradicionales y los filtros web, documentando la visibilidad SSE para apps, usuarios y actividades de datos.



Puntos clave

- **La visibilidad es fundamental para los usuarios, las aplicaciones y la actividad de los datos para encontrar amenazas desconocidas.** ¿Cuántas aplicaciones de almacenamiento en la nube se usan en su compañía u organización? ¿Cuántas de ellas son gestionadas respecto a las no gesetionadas y se comparten datos con terceros, colaboradores y consultores? Lo mismo se puede decir de las apps de inteligencia artificial generativa, además de una amplia gama de aplicaciones utilizadas en los departamentos de marketing, ventas y recursos humanos que trabajan con datos sensibles.
- **Eliminar puntos ciegos para instancias M365 y aplicaciones no gestionadas.** Las soluciones SSE eliminan el punto ciego de no inspeccionar el tráfico M365 y las instancias personales ocultas o las áreas no gestionadas, a menudo relacionadas con la presencia de amenazas y la exfiltración de datos. Los días en que se filtraba por dominio y categoría web para las aplicaciones primarias y los servicios en la nube más utilizados pertenecen al pasado. Ahora los datos se encuentran dentro de las instancias, la actividad y el movimiento de los datos.
- **Aprovechar los paneles y las visualizaciones gráficas (es decir, gráficos Sankey).** Los seres humanos son muy efectivos con las visualizaciones para detectar anomalías y áreas de interés para conocer más detalles y profundizar. Las soluciones SSE deben ofrecer una amplia variedad de paneles y visualizaciones además de los informes tradicionales, además de la capacidad de almacenar eventos y registros durante 3, 6 o 13 meses, para permitir así su análisis con el paso de los años. Se recomienda el uso de plataformas SSE con desconexión de acceso en tiempo real, aunque el destino podría no contar con elementos visuales analíticos avanzados y paneles listos para usar.
- **Controlar la exfiltración de flujos de datos por los usuarios, las aplicaciones y las instancias.** Los datos son el componente de confianza cero que conecta a usuarios, dispositivos, aplicaciones y redes. Los datos fluyen entre estos componentes y son el núcleo de lo que hay que proteger. Las soluciones SSE con control y visibilidad granular habilitan un acceso con privilegios mínimos y supervisan de manera constante para perfeccionar y madurar los controles de las políticas y lograr unos principios de confianza cero. Ofrecer un acceso de confianza cero con un punto ciego para usuarios, apps y actividad anula la estrategia y los objetivos del proceso de confianza cero.
- **Descubrir las amenazas desconocidas con análisis a partir del contexto y las visualizaciones.** Los usuarios adoptan y encuentran nuevas vías desconocidas y no autorizadas para enviar datos cada día. La analítica puede descubrir estas amenazas desconocidas y plasmarlas en visualizaciones gráficas de manera rápida y eficaz. Salvo que una nueva actividad con datos genere una alerta, debería permanecer oculta para los infiltrados, usuarios de riesgo o empleados abandonan la empresa y recopilan información sensible para su próximo trabajo.

Resumen

Estos 10 puntos ponen de manifiesto nuevas capacidades y requisitos para una solicitud RFI de SSE o SASE y para futuros proyectos. La opinión de los clientes recomienda una transformación SSE, partiendo de las funciones existentes de las soluciones de seguridad tradicionales. Entonces comienza el proceso SSE desarrollando nuevas habilidades y capacidades dentro de la organización, añadiendo nuevas líneas de defensa como las direcciones IP de salida específicas, ayudando a los usuarios con recomendaciones en tiempo real, eliminando puntos ciegos y compensaciones, añadiendo barreras de seguridad y protección de los datos antes de la DLP, aprovechando las líneas de defensa en tiempo real (T+) incluyendo la detección basada en AI/ML, y supervisando las conductas anómalas mientras se usa la analítica para mostrar gráficamente las amenazas desconocidas.

- **Más información sobre la Plataforma de servicio de seguridad de Netskope**
- **Estudios de casos de clientes**
- **Funciones críticas de Gartner para SSE**