Solución de gestión de la posición de **seguridad en la nube** ayuda a Sophos a tomar el control de su infraestructura en la nube

Sophos defiende la infraestructura y los datos de sus más de 3000 usuarios y 400 000 clientes en todo el mundo. Los equipos internos de TI y seguridad de Sophos utilizan múltiples productos propios para las operaciones de seguridad diarias de la empresa. Este entorno real sirve como un valioso campo de pruebas, que proporciona a la empresa conocimientos clave que inspiran mejoras y avances continuados en la cartera de productos de Sophos.

Sophos
Abingdon, Reino Unido

Sector
Proveedor de software de seguridad de la información

Sitio web
www.sophos.com

Número de usuarios
3.000 y posteriores

Soluciones de Sophos
Sophos Cloud Optix

"Con Sophos Cloud Optix, minimizamos notablemente la fatiga por alertas. La potente inteligencia artificial integrada en Sophos Cloud Optix correlaciona los datos y nos muestra aquello que es verdaderamente importante y procesable".

Ross McKerchar
CISO
Sophos

Desafíos

- Conseguir visibilidad de toda la infraestructura en la nube
- Evitar la fatiga por alertas y garantizar que las alertas son válidas y procesables
- Gestionar las cuentas y la seguridad en la nube desde una ubicación centralizada
- Reafirmar que los controles de seguridad ya implementados funcionan como deben

Sophos defiende la infraestructura y los datos de sus más de 3000 usuarios y 400 000 clientes en todo el mundo. Los equipos internos de TI y seguridad de Sophos utilizan múltiples productos propios para las operaciones de seguridad diarias de la empresa. Este entorno real sirve como un valioso campo de pruebas, que proporciona a la empresa conocimientos clave que inspiran mejoras y avances continuados en la cartera de productos de Sophos.

¿Cómo consigue Sophos una visibilidad sin precedentes de la totalidad de su entorno en la nube pública?

Los equipos de seguridad TI y de ciberseguridad de Sophos buscaban una herramienta de visibilidad, seguridad y cumplimiento para toda su infraestructura en la nube, que consta de más de 200 cuentas en la nube pública, usando Amazon Elastic Compute Cloud (Amazon EC2), que forma parte de Amazon Web Services (AWS) y Microsoft Azure. Andy Joel, director de operaciones globales de CIS de Sophos, y Dave Davison, jefe sénior del equipo rojo de Sophos, han liderado las tareas de evaluación y llevado a cabo evaluaciones de prueba de concepto exhaustivas de múltiples productos.

Algunas de las herramientas que evaluaron eran soluciones de administración en la nube con solo un número limitado de funciones de seguridad. Otras carecían de escalabilidad: disponían de consolas de administración únicas e intuitivas bien diseñadas, pero solo podían gestionar media docena de cuentas a la vez. "Si miramos lo que hay disponible en el mercado, la principal conclusión es que las empresas podrían pensar que las soluciones de administración en la nube incluyen seguridad en la nube, pero esto no es así en absoluto. Incluir una sencilla serie de comprobaciones de configuración no es seguridad en la nube. En el actual entorno dinámico en que los ciberdelincuentes utilizan automatización e inteligencia artificial para atacar, se necesita una solución sofisticada que analice el tráfico de red y los registros de actividad de los usuarios para informar de forma proactiva de posibles filtraciones. Para nosotros, es Cloud Optix", apunta Davison.

El equipo descubrió que la única solución que realmente cumplía cada uno de sus requisitos era Sophos Cloud Optix. En Sophos, todo funciona deprisa y cambia rápido y, a menudo, los equipos de producto crean nuevas cuentas en la nube con fines de desarrollo. Para Joel, la herramienta resuelve una de sus mayores preocupaciones: tener visibilidad de todos estos entornos de producción tan variables y garantizar que permanecen seguros.

El centro de administración centralizada, intuitivo y fácil de utilizar, ofrece una visión global del terreno en la nube sumamente dinámico de Sophos. Incorpora paneles de control con vistas de la arquitectura en la nube, incluidos flujos de tráfico, resúmenes y datos de alertas y estados de cumplimiento.

"Sophos Cloud Optix nos proporciona una visibilidad de primer nivel sin precedentes de toda nuestra infraestructura, mucho más de lo que la mayoría de herramientas de administración en la nube afirman ofrecer", explica. Sophos Cloud Optix posibilita la detección automática de los recursos de la empresa en todos los entornos en la nube. Gracias a la visualización de la topología de la red y la supervisión continua de los recursos, el equipo de seguridad puede responder a los riesgos de seguridad y solucionarlos rápidamente.

¿Cómo ayuda Sophos Cloud Optix a mejorar los procesos de seguridad al tiempo que ofrece una medida de confianza adicional?

Un ejemplo de Sophos Cloud Optix en acción es la reciente detección de una serie de cuentas de usuario que no tenían habilitada la autenticación multifactor, un conflicto directo con la política de la empresa. Esta infracción de la política se produjo a pesar del hecho de que Sophos tenía un proceso implementado para habilitar la autenticación multifactor. Gracias a Sophos Cloud Optix, Joel descubrió que el proceso no estaba funcionando exactamente como debía, así que lo modificó en consecuencia.

"Si no se tiene una visibilidad completa y continuada de lo que ocurre en el entorno, es imposible ver las actividades potencialmente sospechosas, maliciosas o no conformes. Sophos Cloud Optix nos ayuda a verlo todo, protegerlo todo y tomar las medidas adecuadas", concluye Joel.

Otra realidad que se puso de manifiesto como resultado del despliegue de Sophos Cloud Optix es que Sophos tenía un número reducido de alertas de alta prioridad y ninguna alerta crítica en toda la infraestructura en la nube, incluida la cuenta de producción para la plataforma de administración de Sophos Central. Como Joel indica, "esto dice mucho de las personas que han diseñado y creado el entorno de producción. Sophos Cloud Optix nos da una sensación de confianza y seguridad de que tenemos todos los controles correctos en los sitios correctos y que están funcionando como deben".

¿Qué hace destacar las alertas de Sophos Cloud Optix entre las tecnologías de la competencia?

Davison también apunta que, a diferencia de los productos de la competencia que bombardean a los equipos de seguridad con miles de alertas, Sophos Cloud Optix utiliza inteligencia artificial para potenciar las analíticas de supervisión, detección y seguridad. Todo esto se traduce en una serie de "pequeñas alertas" priorizadas y correlacionadas que son precisas a la vez que procesables. Ayuda al equipo de Sophos a solucionar riesgos de seguridad más rápido mediante la clasificación automatizada de alertas combinada con información contextual. Esto evita la fatiga por alertas y ayuda al equipo de seguridad a centrarse en lo más relevante.

"He constatado que algunos proveedores tratan de convencer a los clientes de que cuantas más alertas, mejor, pero esto no es en absoluto cierto. No nos conviene tener que filtrar cientos de elementos de baja prioridad. Creo que Sophos Cloud Optix realmente ha tomado la dirección correcta en este sentido. Las alertas críticas suelen apuntar a las situaciones que necesitamos gestionar", afirma.

La flexibilidad de configurar las alertas y las medidas correctivas de forma personalizada es otra gran ventaja para una empresa como Sophos que tiene tantos grupos distintos (cada uno con sus propios requisitos de seguridad) creando flujos de trabajo en la nube. Por ejemplo, en determinadas cuentas una alerta podría clasificarse como "crítica", mientras que en otras podría clasificarse como "media".

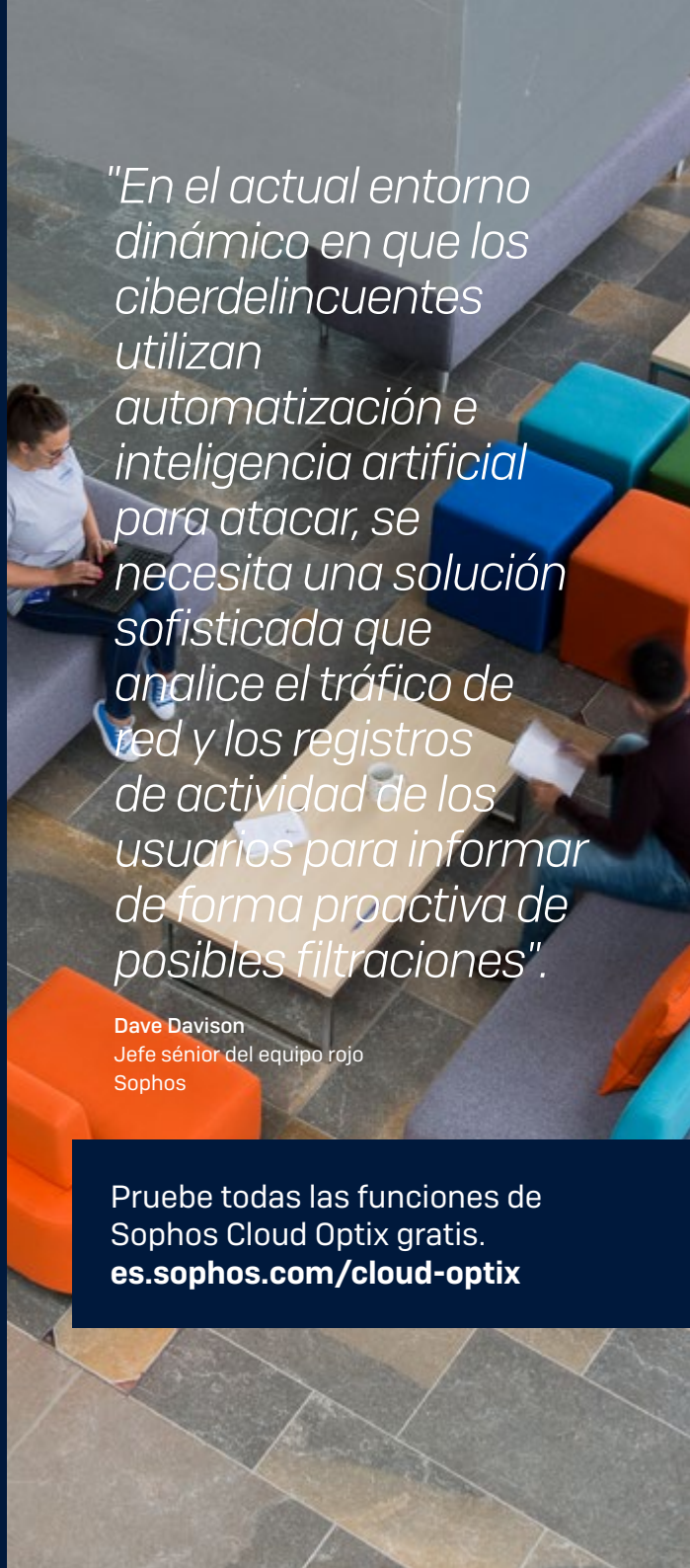
Ross McKerchar, CISO de Sophos, explica este punto en mayor detalle: "Con Sophos Cloud Optix, minimizamos notablemente la fatiga por alertas. Otras soluciones actúan conforme a los números, bombardeando a los equipos de seguridad con una enorme cantidad de alertas indiscriminadas. La potente inteligencia artificial integrada en Sophos Cloud Optix correlaciona los datos y nos muestra aquello que es verdaderamente importante y procesable. Esto nos da una idea muy precisa de nuestra posición de seguridad y nivel de riesgo, lo que nos permite priorizar y solucionar de forma proactiva mediante procesos automatizados. Es un producto de seguridad creado por personal de seguridad para personal de seguridad. Utilizaríamos esta tecnología aunque no fuera nuestra".

En entornos en la nube en constante evolución, ¿cómo ayuda Sophos Cloud Optix a mantener un cumplimiento continuo?

El cumplimiento es el tercer requisito que Sophos Cloud Optix satisface para Sophos. Con plantillas predefinidas, automatización, políticas personalizadas y herramientas de colaboración, permite ajustarse tanto a normativas de cumplimiento externas estándar como al gobierno interno para garantizar la aplicación continuada de las prácticas recomendadas en todas las cuentas en la nube de la empresa. Cuando se crean cargas de trabajo en la nube, suele ser un reto determinar qué procesos de cumplimiento son aplicables y cómo deben implementarse. Davison y su equipo esperan poder utilizar Sophos Cloud Optix en un futuro muy cercano como forma de reducir el coste y la complejidad del gobierno, el riesgo y el cumplimiento en sus entornos en la nube pública.

09-09-2020 CS-ES (DD)

SOPHOS



"En el actual entorno dinámico en que los ciberdelincuentes utilizan automatización e inteligencia artificial para atacar, se necesita una solución sofisticada que analice el tráfico de red y los registros de actividad de los usuarios para informar de forma proactiva de posibles filtraciones".

Dave Davison
Jefe sénior del equipo rojo
Sophos

Pruebe todas las funciones de Sophos Cloud Optix gratis.
es.sophos.com/cloud-optix