Gran Fabricante Mexicano Implementa una estrategia de ciberseguridad basada en la nube con Sophos como base

Fundada en 1982 y con sede en Mérida, en el estado de Yucatán, México, Infra del Sur es una empresa fabricante de gases industriales y medicinales, incluyendo oxígeno, utilizado para soporte vital, cirugía, congelación y preservación de tejidos, laparoscopia, regulación del flujo sanguíneo, estimulación respiratoria y otros tratamientos médicos. La empresa opera a nivel internacional y también suministra a los clientes con gases medicinales e industriales. Uno de nuestros socios comerciales, Air Products, está ubicado entre los mayores fabricantes de gases industriales del mundo.

Edgar Sánchez González dirige el departamento de TI de la organización y Supervisa la tecnología y la infraestructura de seguridad de la organización. "Nuestra misión es proteger con éxito la infraestructura y, en ciberseguridad, nuestra visión es establecer un conjunto de estrategias y soluciones para prevenir acceder y garantizar la continuidad y resiliencia de nuestro negocio y la seguridad de nuestros datos", afirma.

CLIENTE EN UN VISTAZO

INFRA DEL SUR

Infra del Sur

Industria
Fabricante de gases industriales y medicinales

Número de usuarios
Más de 300

Soluciones de Sophos

Sophos Intercept X Avanzado con MDR para servidor: 50 licencias

Sophos Intercept X Avanzado con MDR para Endpoint: 305 licencias

"Identificamos a Sophos como el único proveedor que ya contaba con la integración total de sus soluciones."

Edgar Sánchez González, Gerente de TI en Infra del Sur

Desafío

- Priorizar una avalancha constante de alertas de seguridad.
- Proporcionar protección integral con Telemetría e inteligencia de redes.
- Ahorro de tiempo, mejora de la eficiencia y simplificar la gestión de la seguridad.

¿Qué impulsa la necesidad de un sistema totalmente integrado basado en la nube?

El equipo de TI estaba teniendo dificultades para mantenerse al tanto del alto volumen de alertas provenientes de múltiples herramientas de seguridad. El tiempo y el esfuerzo dedicados a priorizar las alertas estaban restando valor a su trabajo en otras iniciativas y tareas importantes. González y su equipo se dispuso a encontrar una solución basada en la nube que integraría su firewall, endpoints, Wi-Fi, switches, protección de dispositivos móviles, informes, y cualquier otras necesidades futuras en un portal de administración central. También quería que la solución tuviera telemetría integrada para proporcionar protección e inteligencia de red.

¿Cuáles son los criterios más importantes en la selección de proveedores?

En 2020, González y su equipo tomaron la iniciativa de revisar las necesidades de seguridad de la organización y requisitos, definieron un plan para el futuro desarrollo de TI y analizaron soluciones de varios proveedores. Durante una fase de prueba de valor (POV), el equipo comparó varias soluciones. Estaban especialmente interesados en las capacidades de integración, el filtrado de contenido, las protecciones contra bots, la aplicación controles y otros aspectos de las posibles soluciones. El equipo también consideró cómo las soluciones afectarían el rendimiento del equipo y experiencia de usuario. "Nos enfocamos en asegurar que los usuarios empresariales no se verían afectados en sus tareas diarias", dice González.

"Decidimos hacer nuestra primera inversión protegiendo los endpoints con Sophos Intercept X Advanced, sabiendo que podríamos expandir nuestras protecciones más adelante dentro de la misma plataforma."

Edgar Sánchez González Gerente de TI en Infra del Sur

¿Cómo se destaca Sophos entre el resto?

González y su equipo eligieron Sophos por varias razones. "Identificamos a Sophos como el único proveedor que ya tenía una integración completa de sus soluciones", dijo. explica. También le gusta cómo la plataforma escalable de Sophos incorpora múltiples productos avanzados y servicios y puede crecer con la organización. "Decidimos hacer nuestra primera inversión en proteger endpoimts con Sophos Intercept X Advanced, sabiendo que podríamos expandir nuestras protecciones más adelante dentro de la misma plataforma", agrega.

Otra razón por la que Sophos encaja a la perfección es que la plataforma se alinea con la estrategia general de ciberseguridad del equipo. González y su equipo pretenden aprovechar Sophos como su base de tecnología de seguridad, ya que cumple sus requisitos como una solución integrada y completamente basada en la nube.

González también ve el valor añadido en Sophos Detección y respuesta gestionadas (MDR). Sophos MDR es un servicio 24/7 completamente administrado que brinda expertos que detectan y responden a los ataques cibernéticos, tomando medidas en nombre de los clientes para detener las amenazas a medida que ocurren. "El equipo de MDR no solo notifica conmigo, toman medidas proactivas y responden como un equipo de servicios completamente administrado", dice González.

¿Qué resultados puede esperar una gran empresa después de implementar Sophos?

González dice que él y su equipo encontraron que el proceso de implementación de Sophos fue rápido y fácil: y han cosechado muchos beneficios desde la implementación. Un gran ahorro de tiempo ha sido la limpieza y las alertas. Sophos Intercept X advanced aísla automáticamente los dispositivos comprometidos y realiza la limpieza sin necesidad de intervención humana. Utiliza aprendizaje profundo artificial inteligencia (AI) para detectar y bloquear conocidos y malware desconocido. "Las alertas se clasifican según su prioridad, y la mayoría de las alertas, si no todas, son de carácter informativo ya que la herramienta ya ha contenido las peores amenazas", explica González.

Desde la implementación de Sophos, González y su equipo ha ganado considerablemente más tiempo para dedicarse a obras de infraestructura y a prestar servicios de alta calidad a los clientes. González aprecia especialmente las capacidades de generación de informes de la solución "Los informes de activos que provienen de Los MDR sin ninguna interacción humana son realmente buenos informes ejecutivos que son fáciles de interpretar y presentar en las reuniones", dice.

¿Qué nivel de ROI se puede esperar de una inversión en Sophos?

El equipo hizo una gran cantidad de diligencia debida antes tomando su decisión sobre Sophos, para que tuvieran una línea de base contra la cual pudieran medir el ROI. Miraron cuánto costaría personal de una entrada de operaciones de seguridad (SOC) con seis analistas, un ingeniero dedicado y un gerente encargado de supervisar y analizar el trabajo del equipo. Tomaron en cuenta la disponibilidad las 24 horas del día, los 7 días de la semana, una solución de gestión de eventos e información de seguridad (SIEM) y el costo de los conectores y el software para endpoints.

"Para nosotros armar un SOC costaría $518,000 anuales", dice González. "Eso es poco atractivo y una gran inversión, y no veríamos un ROI en ella hasta muy lejos en el futuro." Tomando en cuenta que el costo promedio de recuperación de un ciberataque en México es de $880,000 dólares, el equipo determina que el ROI de su inversión en Sophos es superior al 100%. "Nuestra inversión en la compra de Sophos MDR ha sido rentable", confirma González. Agrega que su propia carga de trabajo en realidad ha sido reducida a la mitad en general, y ha ganado una paz significativa de la mente. "Te puedo decir que me siento mucho más tranquilo delegando el 20% de mis tareas de seguridad al MDR equipo", informa. González resume los factores que influyeron en su decisión de elegir Sophos: "...gestión de costes, integraciones de terceros, cumplimiento y gestión de riesgos, amplitud de capas de seguridad, funcionalidad, rendimiento del producto y servicios sólidos".

"Los informes de activos que provienen de MDR sin ninguna interacción humana son realmente buenos informes ejecutivos que son fácil de interpretar y presentar en las reuniones."

Edgar Sánchez González IT Manager at Infra del Sur

Obtenga más información sobre MDR hoy.
www.sophos.com/mdr

SOPHOS

23-04-14 CCS-ES (NP)