

Guía de ciberseguridad para el sector de la fabricación

La información sobre amenazas líder en el mundo y los expertos analistas de amenazas de Sophos le ayudan a identificar y responder a las amenazas avanzadas más rápido 24/7.

La Industria 4.0 y las «fábricas inteligentes» están transformando el sector de la fabricación. Los sistemas de control industrial (ICS) como SCADA, los dispositivos del Internet industrial de las cosas (IIoT), la robótica y los análisis avanzados están revolucionando el funcionamiento de las fábricas en la actualidad. Pero la amplia transformación digital, la convergencia de TI/TO y la tolerancia extremadamente baja del sector al tiempo de inactividad operativa están agrandando la superficie de ataque, aumentando los riesgos de los fabricantes de que se exploten vulnerabilidades, se filtren datos, se sabotee la producción, etc.

Sophos protege a las organizaciones de fabricación de una amplia variedad de ciberataques, incluidos los perpetrados por humanos que la tecnología por sí sola no puede detener. Gracias a la detección y respuesta gestionadas (MDR) y a la seguridad para endpoints y redes, Sophos permite a las organizaciones de fabricación optimizar sus defensas y libera a los equipos de TI para que se centren en el negocio.

Retos de ciberseguridad en el sector de la fabricación

Los retos de ciberseguridad para el sector de la fabricación siguen creciendo debido a la rápida digitalización y la falta de normas de ciberseguridad igual de sofisticadas, lo que hace que los responsables de TI y TO no estén preparados para responder a las nuevas ciberamenazas. Además, las ciberamenazas en este sector siguen creciendo tanto en volumen como en complejidad.

Una encuesta de Sophos realizada en 2022 a 419 profesionales de TI que trabajan en el sector de la fabricación y la producción reveló que el 55 % de las organizaciones se habían visto afectadas por el ransomware en 2021, lo que supone un aumento del 52 % en el índice de ataques de ransomware con respecto al año anterior.

El coste medio para remediar un ataque de ransomware fue de 1,23 millones de USD para las organizaciones de fabricación. Además, un porcentaje significativo de los encuestados, el 77 %, afirmaron que el ataque afectó a su capacidad de operar, mientras que el 71 % reconocieron haber sufrido pérdidas de negocio/ingresos.

No se trata solo de ransomware. El entorno de TI general de las organizaciones de fabricación se ha vuelto aún más complejo: a lo largo del año, el 61 % de las organizaciones indicó que había aumentado el volumen de los ataques, el 66 % vio aumentar la complejidad de los ataques, y el 51 % afirmó que había aumentado su impacto.



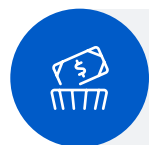
55 %

de las organizaciones de fabricación se vieron afectadas por el ransomware en 2021



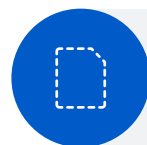
66 %

de los profesionales de TI del sector de la fabricación observaron un aumento de la complejidad de los ataques



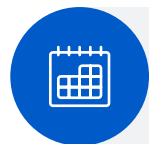
1,23 M USD

coste medio de remediación tras un ataque



59 %

datos que recuperaron las organizaciones de fabricación tras pagar el rescate



>1 mes

El 10 % de las organizaciones de fabricación tardaron más de un mes en recuperarse tras un ataque



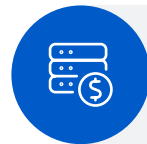
57 %

de los ataques al sector de la fabricación comportaron el cifrado de datos



77 %

de las organizaciones de fabricación afectadas por el ransomware afirmaron que afectó a su capacidad operativa



7 %

de las organizaciones de fabricación recuperaron TODOS los datos tras pagar el rescate

Fuente: Encuesta mundial de Sophos El estado del ransomware 2022

Tras estas estadísticas se esconden varios cambios en el panorama de las amenazas:

La profesionalización de la ciberdelincuencia

En el último año, uno de los acontecimientos más significativos ha sido el desarrollo y la profesionalización de la economía de la ciberdelincuencia. Cada vez más, los grupos delictivos se especializan en un componente concreto de un ataque, por ejemplo, acceso inicial, ransomware, malware para robar información, etc., y lo ofrecen como servicio a otros delincuentes. Estos modelos «como servicio» reducen el umbral de habilidades necesario para llevar a cabo un ataque, lo que aumenta el volumen de adversarios y amenazas.

Estos servicios especializados ofrecen orientación y recursos de ejecución a sus clientes delincuentes, lo que aumenta la eficacia de los ataques. Para ilustrar este punto, en marzo de 2022, un asociado del grupo de ransomware como servicio Conti publicó un archivo que incluía una gran cantidad de documentación y pautas de gran valor diseñadas para enseñar a un «afiliado» hostil los pasos necesarios para llevar a cabo un ataque de ransomware.

Los atacantes también están adoptando muchos de los comportamientos de los proveedores legítimos de servicios de TI, como pedir a las víctimas de ransomware que «puntuén su servicio» una vez que han descifrado los archivos tras el pago.

La evolución de las tácticas, técnicas y procedimientos de los atacantes

Con frecuencia, los delincuentes aprovechan las debilidades en la postura de seguridad de las organizaciones para evitar que las soluciones de seguridad los detengan. Entre otras:

- **Explotar vulnerabilidades sin parchear:** este fue el método más utilizado por los adversarios para penetrar en las organizaciones en los ataques para los que los especialistas en respuesta a incidentes de Sophos tuvieron que intervenir el año pasado, habiéndose utilizado en el 47 % de los incidentes.
- **Explotar herramientas de TI legítimas:** los adversarios también se aprovechan de muchas de las herramientas utilizadas por los profesionales de TI, como PowerShell, PsExec y PowerSploit, para usar credenciales y datos de acceso robados. Haciéndose pasar por usuarios legítimos, los atacantes pretenden entrar sigilosamente en un entorno.

Los retos de ciberseguridad para este sector no acaban aquí. Las organizaciones de fabricación también tienen que lidiar con amenazas internas (tanto maliciosas como accidentales), estrictos requisitos de cumplimiento normativo y riesgos relacionados con proveedores externos, entre otros retos.

Soluciones de seguridad de Sophos para el sector de la fabricación

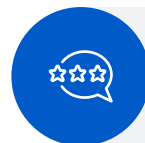
Sophos ofrece soluciones de ciberseguridad avanzadas que permiten a las organizaciones de fabricación gestionar y reducir los ciberriesgos. Nuestro ecosistema de ciberseguridad adaptativa ofrece una cartera completa de servicios y productos líderes en el mercado que elevan las defensas de nuestros clientes incluso contra las amenazas más avanzadas, todo ello basado en los incomparables conocimientos sobre amenazas, IA y operaciones de seguridad de Sophos X-Ops.



Sophos ofrece resultados líderes en ciberseguridad a más de **530 000 clientes** en todo el mundo.



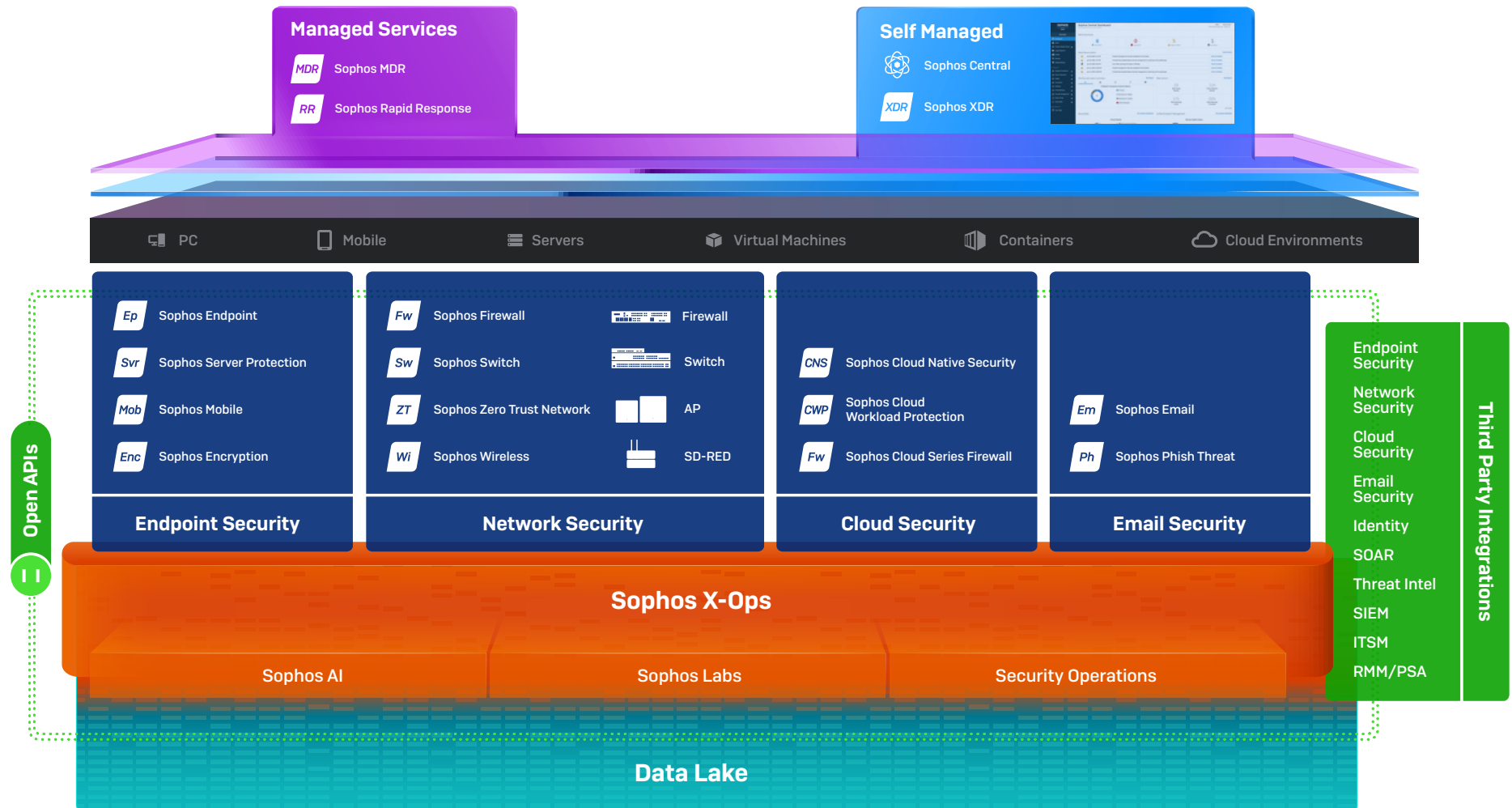
Ningún proveedor ha sido **nombrado líder de Gartner** en seguridad para endpoints más veces que Sophos.



El servicio MDR y protección para endpoints y firewalls **mejor valorados** y con **más reseñas** en Gartner Peer Insights.

A fecha de 1 de agosto de 2022

Sophos Adaptive Cybersecurity Ecosystem



Casos de uso

Sophos puede ayudar a resolver los problemas de ciberseguridad más comunes a los que se enfrentan las organizaciones de fabricación.

Detener los ataques avanzados perpetrados por humanos, incluido el ransomware

Sophos MDR es un servicio 24/7 totalmente gestionado prestado por expertos especializados en detectar y responder a los ciberataques que las soluciones tecnológicas por sí solas no pueden detener. Nuestro equipo de expertos detiene por usted los ataques avanzados dirigidos por humanos, neutralizando las amenazas antes de que puedan interrumpir las operaciones de su negocio o vulnerar los datos confidenciales de los clientes.

«Con Sophos MDR, hemos reducido drásticamente nuestro tiempo de respuesta a amenazas».

Tata BlueScope Steel

«La capacidad de Sophos MDR para remediar o eliminar amenazas de forma rápida y alertarnos sobre ellas nos libera para que podamos centrarnos en tareas de alto valor».

Tomago Aluminium

«Sophos libera a los equipos de TI para que puedan dedicarse a tareas más proactivas en lugar de verse arrastrados a la gestión de los retos de seguridad».

AG Barr

Con Sophos MDR, nuestros analistas expertos detectan y responden a las amenazas en minutos, utilizando la tecnología que prefiera, tanto si necesita una respuesta a incidentes integral como si prefiere recibir ayuda para tomar decisiones más acertadas.

Utilizamos:

- ▶ Soluciones galardonadas de Sophos, que incluyen nuestra protección para endpoints, firewalls, la nube y el correo electrónico.
- ▶ Productos de otros proveedores como Microsoft, CrowdStrike, Palo Alto Networks, Fortinet, Check Point, Rapid7, Amazon Web Services [AWS], Google, Okta, Darktrace y muchos más.
- ▶ Cualquier combinación de nuestra tecnología y tecnología de otros proveedores.

Sophos MDR protege su organización de ataques avanzados que las soluciones tecnológicas por sí solas no pueden detener, a la vez que aumenta el retorno de sus inversiones actuales. Como proveedor del servicio MDR en el que más confía el mundo, aportamos una experiencia con una profundidad y amplitud sin precedentes sobre las amenazas a las que se enfrenta el sector de la fabricación. Sirviéndonos de esta extensa telemetría, podemos generar «inmunidad comunitaria», aplicando lo aprendido al proteger a una organización de fabricación a todos los demás clientes del sector, reforzando así las defensas de todos.

EL MÁS UTILIZADO
**Proveedor
n.º 1**

Más organizaciones confían en Sophos para la MDR que en cualquier otro proveedor.

EL MEJOR
VALORADO
4,8/5

Gartner Peer Insights

Solución MDR mejor valorada y con más reseñas a fecha de 1 de agosto de 2022

LA MEJOR
PROTECCIÓN
38 min

para detectar, investigar y responder

Nuestros analistas son más de 5 veces más rápidos que los equipos de SOC internos más rápidos

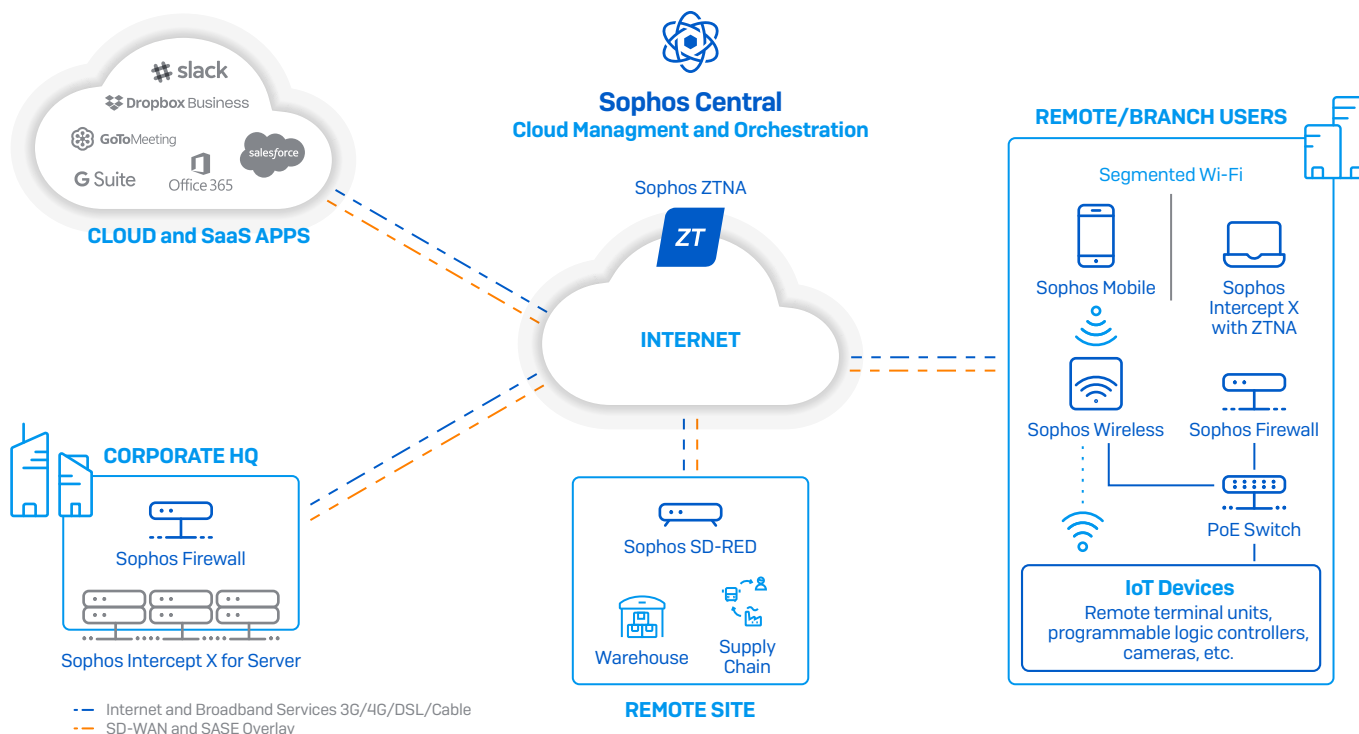
A fecha de septiembre de 2022

Proteger el acceso a datos y sistemas de control industrial críticos

Las organizaciones de fabricación necesitan adoptar un enfoque Zero Trust, consistente en no confiar en nada y verificarlo todo, para proteger el acceso a sus infraestructuras críticas y a su información con derecho de propiedad registrado. La solución Sophos Zero Trust Network Access valida continuamente la identidad del usuario, el estado de seguridad del dispositivo y el cumplimiento antes de conceder acceso a sus aplicaciones y datos.

ZTNA protege sus sistemas RDP (el Protocolo de escritorio remoto es una herramienta común para los empleados y administradores remotos, pero también uno de los vectores de ataque más comunes utilizados por los ciberdelincuentes) de los ataques y proporciona un acceso seguro solo a los usuarios y dispositivos autorizados, incluidas las nuevas opciones sin contraseña con Microsoft Windows Hello for Business, que ayudan a proteger aún más las credenciales importantes de un posible ataque.

Con la cartera de Sophos Secure Access, las organizaciones de fabricación pueden conectar de forma segura dispositivos remotos y sucursales desde cualquier lugar, suministrar sus aplicaciones SaaS y en la nube críticas, y compartir datos con seguridad. Use Sophos ZTNA para proteger el acceso a las aplicaciones, dispositivos Ethernet remotos Sophos SD-RED para extender con seguridad la conectividad de red a sus sucursales y dispositivos remotos, puntos de acceso Sophos Wireless para proteger sus redes inalámbricas de forma fácil y segura, y switches de capa de acceso a la red Sophos Switch para un acceso seguro en la LAN. Todo se gestiona a través de Sophos Central, nuestra plataforma de seguridad todo en uno basada en la nube.



Proteger la red

Sophos Firewall ofrece una potente protección contra las amenazas más recientes, al tiempo que acelera su tráfico importante de SaaS, SD-WAN y aplicaciones en la nube. Sophos Firewall, que ha recibido la distinción Gartner Customers' Choice para firewalls de red 2022, se integra perfectamente en un completo paquete de modernas tecnologías de protección que resulta fácil de configurar y mantener.

La segmentación de red es un método eficaz para que las organizaciones de fabricación reduzcan su exposición a los ciberriesgos y vuelvan a la normalidad más rápidamente tras una brecha de seguridad. Por ejemplo, la red de TI de una organización de fabricación puede segmentarse de la red de TO para evitar el movimiento y la infección laterales. Sophos Firewall ofrece opciones de segmentación potentes y flexibles mediante zonas y VLAN. Estas ofrecen formas de separar los niveles de confianza en la red, al tiempo que permiten una protección adicional contra los movimientos laterales entre distintas partes de la red.

También puede segregar el tráfico a nivel de switch con Sophos Switch, que le permite configurar VLAN para segmentar el tráfico interno y reducir la superficie de ataque en caso de infección o filtración de seguridad.

Proteger contra los ataques de phishing

Las estafas de phishing, y más concretamente los ataques de spear phishing, son una de las formas más fáciles que tienen los atacantes de acceder a su sistema y a datos valiosos.

Una de las formas más eficaces de atajar los ataques de phishing es formar a los empleados para que sepan reconocer una estafa de este tipo. Sophos Phish Threat ofrece una colección de más de 30 módulos de formación de concienciación sobre seguridad para formar y poner a prueba a sus usuarios finales mediante simulaciones de ataque automatizadas, formación de calidad de concienciación sobre la seguridad y métricas de informes procesables.

Permita que solo remitentes de confianza lleguen a la bandeja de entrada de sus empleados con Sophos Email, que escanea todos los mensajes entrantes en tiempo real en busca de indicadores clave de phishing, como la falsificación de marcas y los intentos de suplantación de identidad, mediante técnicas de

autenticación SPF, DKIM y DMARC y el análisis de anomalías en encabezados de correo electrónico. Esto ayuda a detectar y bloquear los correos electrónicos de phishing antes de que lleguen a los usuarios. Además, puede evitar la pérdida de datos mediante la creación de políticas DLP de múltiples reglas para grupos y usuarios individuales a fin de garantizar la protección de información sensible, gracias a la detección de información con derecho de propiedad registrado y otro contenido confidencial en todos los correos y archivos adjuntos.

La mayoría de los ataques de phishing infectan los puntos de acceso a la red al incitar a los destinatarios a hacer clic en un enlace malicioso que lleva a descargar malware en el dispositivo o a dar acceso a datos sensibles a los hackers. Para reforzar su red contra los ataques de phishing, debe reforzar la seguridad de sus endpoints. Disfrute de una protección integral para todos sus endpoints (Windows, Mac, Linux y equipos virtuales) con Sophos Intercept X Endpoint, nuestra solución EDR líder del mercado.

Para optimizar sus defensas, necesita una protección multicapa: diversas funciones de seguridad sofisticadas, cada una de las cuales desempeña su papel en la defensa contra ataques avanzados. Sophos Endpoint cuenta con numerosas capas de protección, entre las que se incluyen:

- Protección contra el robo de credenciales que impide el acceso no autorizado al sistema.
- Protección contra exploits para detener las técnicas que utilizan los adversarios.
- Protección antiransomware que identifica y bloquea los intentos de cifrado malicioso.
- Protección contra manipulaciones que impide a los adversarios desactivar las defensas para poder desplegar su carga.

Combinar múltiples capas de tecnologías de protección nos permite optimizar las defensas de nuestros clientes. Prueba de la calidad de nuestras defensas, y del poder de la protección multicapa, es que detenemos el 99,98 % de las amenazas desde un principio (puntuación media de AV-TEST), y recientemente hemos obtenido una puntuación perfecta en el informe de protección para endpoints de SE Labs.

Proteger la propiedad intelectual (PI) contra el robo

La propiedad intelectual (PI) es información crucial que poseen las organizaciones de fabricación y que les ayuda a mantener su competitividad. La información confidencial, como diseños de productos, fórmulas, patentes de procesos y otros conocimientos técnicos exclusivos de una organización de fabricación, son un objetivo atractivo para ciberdelincuentes, competidores y exempleados, ya que les da acceso inmediato a información crítica sin invertir tiempo y dinero en I+D. Para las organizaciones de fabricación, el robo de PI puede suponer enormes pérdidas empresariales y, en ocasiones, el cierre de la empresa.

Para proteger su PI, forme a sus empleados para que estén atentos a posibles amenazas y promueva una cultura positiva de sensibilización sobre la seguridad en su organización con Sophos Phish Threat, que ofrece simulaciones de ataque automatizadas y formación de concienciación sobre la seguridad.

Consiga un control absoluto sobre quién puede acceder a los datos de su red con Sophos ZTNA. Puede establecer controles granulares para bloquear el movimiento lateral y asegurarse de que solo las personas autorizadas puedan acceder a los datos confidenciales.

Reduzca las vulnerabilidades conocidas y detenga las amenazas de ciberseguridad más recientes, como el ransomware, los ataques sin archivos, los exploits y el malware, en todos sus dispositivos endpoint con la protección de Sophos Intercept X Endpoint. Nuestras funciones de prevención de pérdida de datos (DLP) identifican sus datos confidenciales y previenen filtraciones a través del correo electrónico, cargas y copias locales.

Evite las filtraciones de datos con Sophos Email, que le permite crear políticas DLP de múltiples reglas para usuarios a fin de garantizar la protección de información sensible, gracias a la detección de contenido confidencial en todos los correos y archivos adjuntos. También cifra fácilmente sus datos confidenciales para detener las filtraciones.

Proteger contra las amenazas internas

El riesgo de que usuarios internos con acceso autorizado a información con derecho de propiedad registrado o a controles de operaciones de fabricación vitales hagan un uso indebido de sus privilegios o quebranten la confianza del fabricante es una amenaza crítica ante la que el sector de la fabricación debe responder. Robar secretos comerciales, sabotear procesos de fabricación o dañar equipos mediante el acceso remoto son algunas de las amenazas que representan los usuarios internos.

Obtenga información procesable sobre sus usuarios y las aplicaciones con un mayor índice de riesgo con el cociente de amenazas por usuario (UTQ) de Sophos para garantizar la aplicación de las políticas antes de que la seguridad se vea comprometida. Lleve su protección más allá con Sophos Firewall, que protege sus datos confidenciales de divulgaciones accidentales o malintencionadas con un control de políticas completo sobre categorías web, aplicaciones, medios extraíbles y dispositivos móviles utilizados en su red. Permite la concienciación de los usuarios en todas las áreas del firewall con políticas de acceso basadas en el usuario para el conformado de tráfico (QoS) y otros recursos de red, independientemente de la dirección IP, la ubicación, la red o el dispositivo.

Reducir los riesgos en la cadena de suministro

Las cadenas de suministro del sector de la fabricación son extensas y complejas. Una vulnerabilidad en cualquiera de las redes de un proveedor puede propagarse rápidamente para infectar a múltiples proveedores y empresas.

Protéjase de las amenazas que penetran en las organizaciones de fabricación a través de proveedores externos mediante el uso de la IA, la prevención de exploits, la protección comportamental y otras tecnologías avanzadas de Sophos Intercept X. Además, la potente funcionalidad XDR le permite identificar automáticamente la actividad sospechosa, priorizar los indicadores de amenazas y buscar rápidamente las posibles amenazas en endpoints y servidores.

Con Sophos MDR, obtiene asistencia experta 24/7 con más de 500 especialistas que buscan, validan y remedian de forma ininterrumpida y proactiva posibles amenazas e incidentes en la cadena de suministro en su nombre.

Protéjase de los ataques a la cadena de suministro que dependen del acceso de los proveedores a sus sistemas mediante controles de acceso muy granulares con Sophos ZTNA, que autentica las solicitudes de asociados de confianza, independientemente de su ubicación. La integración única de Sophos Endpoint y Sophos ZTNA evita automáticamente que los hosts comprometidos se conecten a los recursos de la red, lo cual impide que las amenazas se propaguen lateralmente y se afiancen en su red.



Proteger los sistemas heredados

Las organizaciones de fabricación deben proteger sus sistemas y procesos de control de producción heredados o desactualizados frente a las vulnerabilidades conocidas. Estos dispositivos suelen ejecutar sistemas operativos desfasados o navegadores que no pueden actualizarse porque ya no son compatibles, pero que necesitan estar conectados a la red.

Sophos Firewall y Sophos SD-RED pueden ayudarle en este sentido. Utilice Sophos SD-RED delante de un dispositivo expuesto; canalizará todo el tráfico a un dispositivo Sophos Firewall de protección para escanearlo. Si su red es plana, es probable que tenga que hacer cambios en los esquemas de direcciones IP y en la posible topología de los switches; nuestros especialistas técnicos pueden analizar su situación y mostrarle cómo hacerlo.

Proteger los datos en entornos multinube de fabricación

La nube impulsa las fábricas inteligentes. La adopción de la nube está permitiendo a las organizaciones de fabricación modernas recopilar datos de las máquinas de los talleres en tiempo real y convertir grandes volúmenes de datos en inteligencia empresarial que les ayude a optimizar los procesos, detectar ineficiencias e identificar formas de operar más sostenibles. Sin embargo, la nube también es un objetivo importante para los ciberdelincuentes que buscan explotar prácticas de ciberseguridad menos establecidas que en los entornos locales tradicionales.

Sophos Cloud Native Security proporciona una completa cobertura de seguridad multinube en todos los entornos, cargas de trabajo e identidades. Protege su infraestructura y sus datos en la nube con una seguridad flexible para las cargas de trabajo de hosts y contenedores en Windows y Linux. Las tecnologías multicapa protegen contra el ransomware y otros ataques avanzados, incluidas las detecciones nativas en la nube en tiempo de ejecución de comportamientos y exploits que permiten identificar amenazas como escapes de contenedor, exploits del kernel e intentos de aumento de privilegios. Además, también facilita el control del gasto en la nube. Puede detectar rápidamente si se está abusando de su cuenta y expulsar a los adversarios antes de que la factura se dispare.

Conclusión:

Ciberataques como el ransomware, los exploits y el phishing pueden tener graves consecuencias para el negocio y la reputación de las organizaciones de fabricación. Proteger los entornos de TI y los datos confidenciales requiere un enfoque integrado a la seguridad.

Sophos protege sus sistemas y datos dondequiera que estén con nuestros servicios y tecnologías next-gen, a la vez que le permite consolidar la gestión de su seguridad con un único proveedor. Todas las soluciones de Sophos se gestionan a través de una consola de administración unificada basada en la nube, Sophos Central, que permite compartir información en tiempo real entre productos, gestionarlos de forma centralizada, responder a incidentes de forma automatizada y obtener análisis detallados. Todo ello funciona de forma conjunta y aumenta aún más su protección, a la vez que mejora la eficiencia de su equipo de TI.

Para obtener más información sobre cómo Sophos protege a las organizaciones de fabricación y analizar sus necesidades, póngase en contacto con su representante de Sophos o solicite una llamada de nuestros especialistas en seguridad.

Gartner no apoya a ninguna compañía, producto o servicio mencionado en los estudios publicados y no aconseja a los usuarios de tecnologías que elijan solamente a los proveedores con las clasificaciones más altas. Los estudios publicados por Gartner están compuestos por las opiniones de su equipo de investigación y asesoramiento y no deben considerarse declaraciones de hecho. Gartner renuncia a todas las responsabilidades, explícitas o implícitas, con respecto a este estudio, incluida cualquier garantía de comercialización o conveniencia para fines particulares.

GARTNER es una marca de servicio y marca registrada de Gartner, Inc. y/o asociados en EE. UU. y en otros países, y MAGIC QUADRANT y PEER INSIGHTS son marcas registradas de Gartner, Inc. y/o asociados y se utilizan aquí con permiso. Reservados todos los derechos.

El contenido de Gartner Peer Insights consiste en las opiniones de usuarios finales individuales basadas en sus propias experiencias con los proveedores que aparecen en la plataforma; no deben considerarse declaraciones de hecho, ni representan las opiniones de Gartner ni de sus afiliados. Gartner no apoya a ningún proveedor, producto o servicio mencionado en este contenido ni ofrece ninguna garantía, expresa o implícita, con respecto a este contenido, sobre su exactitud o integridad, incluida cualquier garantía de comercialización o conveniencia para fines particulares.