Seguridad para infraestructura crítica de Forcepoint

Protección de la frontera de TO/TI y más allá

Forcepoint

Folleto

Las organizaciones que prestan los servicios de infraestructura crítica de los que todos dependemos buscan constantemente cómo aumentar la productividad, volverse más ágiles, acelerar la innovación y, en última instancia, disminuir los costos e incrementar las ganancias. Sin embargo, uno de los principales desafíos que enfrentan al perseguir estos objetivos es cómo defenderse mejor contra los ataques cibernéticos y, a la vez, mantener la integridad y disponibilidad del sistema de las que dependen las empresas.

Los ataques cibernéticos sobre infraestructura crítica están creciendo en frecuencia y posible gravedad. Ya sea que se trate de Stuxnet que utiliza una combinación de ataques de día cero contra los sistemas, o apunta a tecnología de seguridad industrial de proveedores de automatización y climatización, o Shamoon 3 que dirige su ofensiva a los sectores del petróleo, el gas, la energía y las telecomunicaciones en Oriente Medio y más allá. Defenderse contra los ataques cibernéticos es un desafío constante. La protección eficaz contra estos ataques requiere de soluciones flexibles que puedan adaptarse a los contextos y dificultades únicos de cada industria y, a la vez, sean lo suficientemente resistentes para impedir el acceso al adversario más avanzado o persistente.

Los desafíos de la transferencia de datos segura

Los proveedores de infraestructura crítica que buscan garantizar la integridad de los datos entre sitios distribuidos y aislados, cumplir con requisitos regulatorios/gubernamentales, y brindar escalabilidad mediante la contracción y simplificación de la infraestructura de seguridad deben encontrar soluciones a los siguientes desafíos de transferencia de datos segura:

Extracción de datos

Uno de los requisitos más comunes en la frontera de TO/TI es la necesidad de extraer datos históricos o información de registros de la red de TO (tecnología operativa) para su análisis en la red de TI (tecnología de la información). Se puede suponer que los datos que se desplazan en esta dirección son "seguros" y, por lo tanto, la preocupación principal es garantizar que los atancantes no puedan usar el canal de comunicación en sí para saltar la valla electrónica y pasar de la red de TI a la de TO.

Importación de actualizaciones de software

Otro requisito común en la frontera de TI/TO es la necesidad de importar actualizaciones de software, como las actualizaciones de Windows/Linux y de firmas de antivirus. Un gateway unidireccional puede ser una solución eficaz, garantizando que el tráfico solo pueda fluir en una dirección entre servidores de actualizaciones preconfigurados que residen a uno y otro lado de la frontera.

Importación de archivos de TI

El desafío de mantener la seguridad en la frontera de TI/TO se vuelve mucho más complejo y lleno de matices en lo que respecta a la importación de archivos de TI (contenido rico del tipo que se usa a diario en la red empresarial) de la red de TI a la de TO. Los manuales, documentos de mantenimiento y de cumplimiento en archivos de Office, PDF y diagramas son esenciales para la operación fluida de plantas y maquinaria. Sin embargo, este tipo de datos complejos son el soporte preferido de los atacantes cibernéticos que buscan implantar malware y establecer canales de comando y control remotos.

Monitoreo seguro en la nube

La administración de activos y redes de TO en la nube, ya sea para visualizar datos históricos, monitorear esos activos en tiempo real o incluso controlarlos de forma remota, brinda enormes beneficios comerciales. Sin embargo, para disfrutar de estos beneficios, los proveedores de infraestructura crítica necesitan estar seguros de que los enlaces entre la red de TO y la plataforma de monitoreo en la nube no puedan ser utilizados por un atacante para comprometer los activos y la red de TO.

Delimitación de la empresa

Con la convergencia de TI y TO, las infraestructuras críticas son ahora el blanco principal de los atacantes cibernéticos. El uso de máquinas en red, automatización y dispositivos de la Internet de las cosas (IoT) sigue creciendo, pero muchos de estos dispositivos no fueron diseñados con la seguridad como una característica clave. Los delincuentes cibernéticos lo saben bien. El malware que se entrega a la red de TI mediante documentos de Office, PDF e imágenes en correos electrónicos o descargas de la web está diseñado para comprometer no solo a las estaciones de trabajo de la empresa, sino también para desplazarse lateralmente y "saltar" la frontera de TI/TO.

Cartera de productos de infraestructura crítica de Forcepoint

Forcepoint ofrece una cartera completa de productos diseñados para ayudar a los proveedores de infraestructura crítica a afrontar los siguientes desafíos:

Next-Generation Firewall

Forcepoint Next-Generation Firewall (NGFW) es un firewall de última generación que combina redes rápidas y flexibles (SD-WAN y LAN) con seguridad líder en la industria para conectar y proteger a las personas y los datos que utilizan mediante redes empresariales diversas y en evolución. Forcepoint NGFW brinda seguridad, desempeño y operaciones coherentes en sistemas físicos, virtuales y en la nube. Está diseñado desde cero para ofrecer una alta disponibilidad y escalabilidad, así como administración centralizada con visibilidad completa de 360°.

Gateway unidireccional (Data Diodes)

Forcepoint Data Diodes es un diodo de datos que garantiza la transferencia unidireccional segura con aislamiento óptico,y permite a las organizaciones delimitar fronteras entre las redes confiables y no confiables mediante la creación de un canal de comunicación unidireccional físicamente seguro. Ideal para protocolos unidireccionales, Data Diodes (antecedente poco claro) permite enviar datos desde una red segura a otra; los datos se transfieren a través de la luz en lugar de señales eléctricas, lo que garantiza que los datos puedan ingresar, pero nunca salir.

Data Guard

Forcepoint Data Guard posibilita la transferencia automatizada y bidireccional de datos sumamente complejos, incluso la transmisión de video en tiempo real a través de redes segregadas. Con la inspección profunda del contenido y el control altamente granular basado en políticas sobre origen, destino y contenido, Data Guard es ideal para la transferencia de datos de dominio cruzado y apunta a los requisitos de seguridad de alto control específicos de los entornos gubernamentales.

High Speed Verifier

Forcepoint High Speed Verifier (HSV), un comprobador de alta velocidad, es una solución de hardware basada en diodos diseñada para entornos en los que las aplicaciones bidireccionales necesiten transferir datos de manera segura, como el monitoreo de TO en la nube. El HSV combina múltiples diodos unidireccionales, interrupciones de protocolo (protocol breaks) y verificaciones de integridad en una única unidad. La verificación de datos se aplica mediante el uso de matrices de puertas programables (FPGA) lo que significa que un atacante no puede comprometer remotamente el HSV y se puede habilitar el desarme y la reconstrucción de contenido (CDR) como opción. El HSV puede desplegarse para proteger la transferencia de datos entre TO y TI, TI y TO, y TO y la nube.

Zero Trust Content Disarm and Reconstruction (CDR)

Forcepoint Zero Trust CDR, el producto de desarme y reconstrucción de contenido (CDR) de Zero Trust, funciona con el comprobador de alta velocidad (HSV) para entregar datos 100 % libres de malware sin utilizar detección. Funciona mediante la extracción de la información comercial válida de los archivos, la verificación de que la información extraída está bien estructurada y, luego, la creación de nuevos archivos para transportar la información a su destino. Este enfoque único de Zero Trust se aplica a todos los datos, sin importar si contienen una amenaza o no. Hace que los archivos de TI como las imágenes y los documentos de Office y los PDF queden libres de amenazas. También puede aplicarse al tráfico de aplicaciones web típicamente utilizado para monitorear redes de TO en la nube.

Resumen de la solución

CASO	REQUISITOS	CONSIDERE ESTAS SOLUCIONES
Extracción de datos de TO a TI	Transferencia de datos segura y confiable sin pérdida de datos. Canal de comunicación que un atacante no puede utilizar como vínculo de retorno para acceder a la red de TO.	• Data Diodes o High Speed Verifier con Zero Trust CDR • NGFW
Importación de actualizaciones de software de TI a TO	Transferencia de datos segura y confiable sin pérdida de datos. Canal de comunicación que un atacante no puede utilizar para introducir malware a la red de TO o exfiltrar datos fuera de esta.	• Data Diodes o High Speed Verifier con Zero Trust CDR • NGFW
Importación de archivos de TI a la red de TO	Alta garantía de que los archivos que ingresan al entorno de TO están libres de malware y no pueden utilizarse como un vector para atacar la red de TO, plantas o activos.	• High Speed Verifier con Zero Trust CDR o Data Guard • NGFW
Monitoreo de redes de TO desde la nube	Transferencia de datos segura y confiable sin pérdida de datos. Soporte para protocolos de aplicaciones web bidireccionales con los mismos niveles de control que si el canal de comunicación fuera unidireccional y aplicado en hardware. Limitación de los datos de la aplicación a esquemas predefinidos para garantizar que no puedan utilizarse con el objeto de atacar la red de TO, plantas y activos.	• High Speed Verifier con Zero Trust CDR • NGFW
Delimitación de la empresa	Una postura de seguridad de Zero Trust para todo el contenido entrante que llega a la red empresarial.	• High Speed Verifier con Zero Trust CDR • NGFW

Forcepoint

forcepoint.com/contact

Acerca de Forcepoint

Forcepoint simplifica la seguridad para las empresas y los gobiernos de todo el mundo. La plataforma todo en uno y realmente nativa en la nube de Forcepoint facilita la adopción de un enfoque de Zero Trust y evita el robo o la pérdida de datos confidenciales y propiedad intelectual sin importar desde donde trabajen las personas. Con sede en Austin, Texas, Forcepoint crea entornos seguros y confiables para los clientes y sus empleados en más de 150 países. Conéctese con Forcepoint a través de www.forcepoint.com, Twitter y LinkedIn.

[Forcepoint-Critical Infrastructure Security-Brochure-ES] 07Apr2022