RESUMEN DE LA SOLUCIÓN

Lograr la plena transparencia y el control centralizado en entornos de OT con Fortinet

Resumen ejecutivo

La convergencia de la tecnología de la información (IT) y la tecnología operacional (OT) amplía la superficie de ataque de OT, lo que sitúa a los analistas de operaciones de red bajo una presión enorme para mantener la seguridad, el tiempo de actividad y la protección. La OT requiere ahora una infraestructura de seguridad integrada para proporcionar visibilidad, control y reconocimiento contextual de dispositivos, además de las vías que pueden ofrecer a un conjunto cada vez más amplio de amenazas basadas en Internet. Fortinet Security Fabric ofrece una arquitectura de seguridad integral para entornos de OT. Ofrece una protección integrada y automatizada a través de la segmentación, el control de acceso a la red (NAC) y la gestión de eventos e información de seguridad (SIEM).

Casi tres cuartas partes de las organizaciones de OT han experimentado una intrusión de malware en los últimos 12 meses, causando daños a la productividad, los ingresos, la confianza en la marca, la propiedad intelectual y la seguridad física.[1]

Un 78% de las organizaciones de OT solo tienen visibilidad centralizada parcial de soluciones de ciberseguridad implementadas en sus entornos.[4]

Necesidad de un aumento de la visibilidad, el control y el reconocimiento contextual

La superficie de ataque de OT se está ampliando rápidamente. Los sistemas sensibles en entornos críticos industriales y de infraestructura se enfrentan a nuevos riesgos debido a cambios en la infraestructura, como la sustitución de las conexiones de OT en serie por conexiones digitales y el rápido crecimiento del número de dispositivos y sistemas conectados a Internet.

A pesar de todos estos desafíos, los analistas de operaciones de red deben mantener el tiempo de actividad y la seguridad en todo momento. Y en lo relativo a la ciberseguridad, los entornos de OT han sido descuidados históricamente. Esto se debe a que, hasta hace poco, una «air gap» (separación completa de la red informática) mantenía estos sistemas alejados de las amenazas. Sin embargo, hoy en día, el malware puede atacar los sistemas de OT a través de conexiones de IT, como las campañas de suplantación de identidad por correo electrónico.[2,3]

La priorización de la seguridad de OT ha recibido mucha atención recientemente. Pero la transposición de las estrategias tradicionales de seguridad informática a OT no es la adecuada para los sistemas confidenciales, a menudo heredados, de estos entornos. Para mantener operaciones seguras y funcionales, las organizaciones necesitan tres capacidades críticas de ciberseguridad:

Visibilidad

La protección de los entornos modernos de OT comienza con el establecimiento de una visibilidad continua de cada activo conectado a la red, tanto por cable como de manera inalámbrica. La seguridad debe realizar un seguimiento de todos los dispositivos conectados en la organización a medida que se unen, salen o se mueven de un lugar a otro.

Control

Las organizaciones deben ser capaces de aplicar y hacer cumplir las políticas de acceso basadas en quién y qué está conectado para proteger las operaciones de OT de posibles amenazas basadas en IT. Los controles dinámicos basados en roles pueden agrupar aplicaciones, vincular datos y limitar el acceso a grupos específicos a fin de fortalecer las defensas de OT. Este tipo de segmentación basada en la intención proporciona un control detallado que ajusta el acceso basándose en la evaluación continua de la confianza de los dispositivos y los usuarios.

Conocimiento de la situación

Cuando se ataca un dispositivo individual en un entorno de OT, las organizaciones necesitan alertas instantáneas e información contextual sobre la amenaza para comprender rápidamente qué medidas tomar y dónde buscar. La seguridad de OT requiere una gestión de riesgos y una correlación de eventos unificadas para contribuir a agilizar el análisis, automatizar las respuestas y acelerar la reparación, especialmente teniendo en cuenta los graves límites de los recursos de personal de la mayoría de las organizaciones.

Más de la mitad (53 %) de las organizaciones carecen de la segmentación de red interna para limitar la propagación de las amenazas dentro de las redes de OT.[5]

La escasez de profesionales de ciberseguridad en todo el mundo ha aumentado a casi 3 millones de puestos vacantes.[6]

Arquitectura de seguridad integrada para OT

Fortinet Security Fabric conecta diferentes soluciones de seguridad implementadas a través de un entorno de OT en un ecosistema de seguridad coordinado. Este tipo de arquitectura de seguridad integrada coordina las defensas cibernéticas en una organización para permitir la visibilidad, el control y la conciencia de la situación con el fin de proteger los entornos de OT actuales. Si un dispositivo conectado muestra un comportamiento sospechoso, Security Fabric cuenta tanto con la cobertura como con las capacidades para detectar y resolver el problema con rapidez.

Dentro de los entornos de OT, Security Fabric incluye soluciones Fortinet como los robustos firewalls de última generación **FortiGate** (NGFW), la conmutación segura en **FortiSwitch** (con cable) y **FortiAP** (inalámbrico), la protección de dispositivos de extremos **FortiClient** y **FortiManager** para una visibilidad transparente y una gestión centralizada de todos los dispositivos implementados en toda la organización.

Fortinet Security Fabric también contribuye a controlar el acceso a los sistemas críticos sin interrumpir su funcionamiento. Tradicionalmente, los controles de acceso asumían valores de confianza inalterables para los usuarios, dispositivos y aplicaciones. Pero en realidad, la confiabilidad de los usuarios y dispositivos puede fluctuar debido a los cambios normales en las operaciones empresariales o como resultado de las amenazas emergentes. La **segmentación basada en la intención** vincula el control de acceso a niveles de confianza continuamente actualizados en función de la información adquirida tanto de fuentes internas como externas.

En concreto, la segmentación basada en la intención de Fortinet admite un control de acceso dinámico y granular que supervisa continuamente el nivel de confianza del usuario y adapta las políticas de seguridad conforme a ello. Los activos de IT críticos se aíslan para garantizar una detección y prevención rápidas de amenazas mediante el análisis y la automatización. Impulsada por los **NGFW de FortiGate** físicos y virtuales, la segmentación basada en la intención proporciona un control integral de la red de OT para el tráfico de este a oeste y de norte a sur.

Pero la seguridad no significa nada en OT si interrumpe el funcionamiento de los sistemas críticos de alguna manera. A lo largo de su historia, Fortinet ha demostrado su experiencia en OT a través de la inversión en una arquitectura de seguridad de OT dedicada. Las soluciones de Fortinet se desarrolladas por expertos en la materia que comprenden las necesidades particulares de seguridad y operativas de estos entornos únicos. Security Fabric proporciona una solución arquitectónica completa para la protección integral, frente al enfoque “a la carta” de otros proveedores con productos y servicios individuales que solo pueden abordar los vectores de ataque de uno en uno.

Soluciones para una transparencia de OT profunda

Las soluciones de protección de extremos mejoran la visibilidad y el control de los dispositivos dentro de los entornos de OT. Tres de estos elementos de Fortinet Security Fabric que desempeñan roles críticos en la protección de extremos son:

FortiSIEM

La seguridad efectiva de OT requiere tanto transparencia como contexto para ayudar a los analistas de operaciones de red en el triaje rápido de alertas, el seguimiento de dispositivos y la corrección de problemas. FortiSIEM ofrece SIEM de varios proveedores para una visibilidad completa, correlación, respuestas automatizadas y reparación en una solución única para ayudar a liberar los recursos de personal y mejorar la detección de fugas.

FortiClient

FortiClient proporciona seguridad en los entornos de OT para las estaciones de trabajo y los dispositivos conectados de BYOD. Ofrece protección de extremos crítica como antivirus, antimalware, antiexplotación, firewall de aplicaciones web (WAF) y filtrado web. También incluye un Fabric Agent para telemetría de extremos, que conecta FortiClient con la seguridad de FortiGate NGFW.

FortiNAC

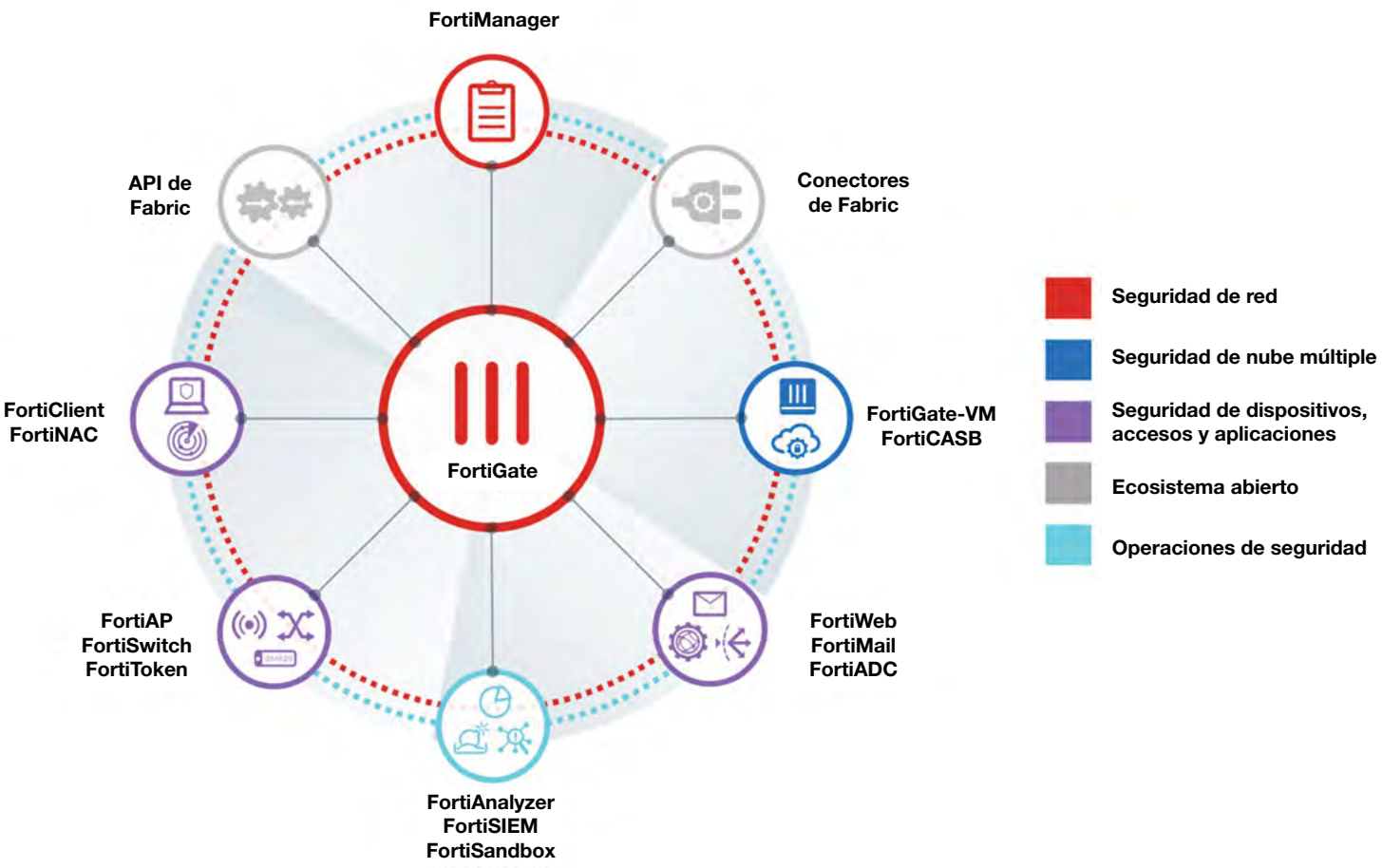
FortiNAC ayuda a proteger los dispositivos y sistemas en OT que pueden carecer de la seguridad incorporada propia suficiente, incluidos los dispositivos del Internet de las cosas (IoT)/Internet industrial de las cosas (IIoT), los controladores lógicos programables (PLC), así como los sistemas de control industrial (ICS) y sus sistemas de subconjuntos de control de supervisión y adquisición de datos (SCADA). En coordinación con otras soluciones de Security Fabric, FortiNAC ayuda a proteger las redes de OT altamente distribuidas frente a las amenazas mediante la detección de extremos con vulnerabilidades sin parches.

Para extremos no críticos, puede eliminarlos de la red al instante y de manera automática hasta que tengan los parches suficientes. También puede devolver automáticamente ese extremo a la red desde un panel central. En el caso de un ataque multivectorial a gran escala (por ejemplo, botnets) u otra situación de emergencia en la que el acceso deba limitarse estrictamente por motivos de seguridad, FortiNAC tiene la capacidad de bloquear la red y no permitir que se incorporen nuevos dispositivos sin la aprobación manual.

Elegir la seguridad diseñada para OT

Debido a la convergencia de OT e IT, los analistas de operaciones de red deben proteger ahora sus delicados sistemas de OT de una creciente oleada de amenazas basadas en Internet. Para apoyar esta evolución, Fortinet Security Fabric proporciona una base de visibilidad transparente, controles basados en políticas y un conocimiento inmediato de la situación que está específicamente diseñado para entornos de OT.

Security Fabric integra tecnologías específicas (segmentación, SIEM, NAC, protección de extremos, conmutación e inalámbrica) para proteger la OT frente a las amenazas generalizadas basadas en IT. Los analistas de operaciones de red deben evaluar su seguridad actual de OT planteando algunas preguntas básicas:



Fortinet Security Fabric ofrece una arquitectura de seguridad unificada e integrada que desbloquea la automatización.

Mi seguridad de OT...

- ¿aprovecha una arquitectura de seguridad integrada que conecta todas las partes de la infraestructura de seguridad en un ecosistema cohesivo y colectivo?
- ¿proporciona una mayor visibilidad para que la detección de la red de OT para comprenda la postura de seguridad actual?
- ¿descubre y clasifica los dispositivos de IoT e IIoT según los factores de riesgo asociados como vulnerabilidades, calificaciones de seguridad e incluso la utilización?
- ¿aplicar segmentación basada en la intención para aumentar la resiliencia de las redes de OT?
- ¿incorpora soluciones como SIEM y NAC para detectar usuarios y dispositivos sospechosos?
- ¿pone en práctica la inteligencia para conocimiento de la situación en tiempo real sin interrumpir las operaciones principales?
- ¿permite la gestión de seguridad simplificada desde un panel único?

[1] "State of Operational Technology and Cybersecurity Report", Fortinet, marzo de 2019.
[2] "DHS Alert ICS-ALERT-14-176-02A", Cybersecurity and Infrastructure Security Agency, 22 de agosto de 2018.
[3] Catalin Cimpanu, "The Clever Phishing Trick Used by Hackers Targeting the US Energy Sector", BleepingComputer, 10 de julio de 2017.
[4] "State of Operational Technology and Cybersecurity Report", Fortinet, marzo de 2019.
[5] Ibid.
[6] "Cybersecurity Skills Shortage Soars, Nearing 3 Million", (ISC)², 18 de octubre de 2018.

www.fortinet.com

22 abril, 2020 3:59 p. m.
360483-0-0-ES
sb-network-operations-analyst_A4_ES