

Perspectivas de ciberseguridad industrial 2023-2030

Fortinet



Las tendencias macro que sustentan una mayor inversión en ciberseguridad de OT siguen siendo fuertes

A pesar de las desafiantes condiciones económicas globales, el gasto en ciberseguridad de OT ha seguido aumentando. Hay 3 impulsores para la inversión: transformación digital, regulación y gestión de riesgos.

La creciente interconectividad entre dispositivos, sistemas y procesos de OT ha facilitado la transformación digital de las operaciones industriales, aumentando la demanda de servicios de computación en la nube, análisis de datos, gemelos digitales y aprendizaje automático. La convergencia entre TI y OT ha acelerado aún más esta tendencia, facilitando una perfecta integración e intercambio de datos entre dos entornos previamente aislados. El nuevo propietario de activos digitales se caracteriza por mayores niveles de interoperabilidad y colaboración, lo que permite la optimización de procesos y ganancias de productividad. Los beneficios de la transformación digital deben gestionarse junto con la mayor exposición a las vulnerabilidades de TI y OT, lo que requiere nuevas políticas, procesos y procedimientos de ciberseguridad para garantizar la resiliencia de los futuros modelos operativos.

La regulación sigue influyendo en las decisiones de adquisición. Se están fortaleciendo los esfuerzos para hacer cumplir la ley, la regulación se está expandiendo para cubrir más sectores industriales y cadenas de suministro y existe una necesidad creciente de mayores niveles de resiliencia. Ejemplos en los Estados Unidos incluyen la Directiva Operativa Vinculante 23-01 de CISA y la Directiva SD 1580/82-2022-01 de la TSA, que entró en vigor en 2023 y la OMB M-22-09 se centra en establecer confianza cero (Zero Trust) en la infraestructura operada por el gobierno federal. La directiva NIA 2 será aplicable en todos los países de EE. UU. a partir de 2024 y ahora incluye sectores manufactureros clave, aumentando la cobertura del 21% al 36% de la base económica de la UE, mientras que la Ley de Resiliencia de Entidades Críticas (CER) cubre infraestructuras críticas. Australia, India, Japón y Canadá han lanzado recientemente nuevas regulaciones o están en proceso de revisar el estado actual.

El último factor que contribuye al aumento de la inversión es una mayor conciencia ejecutiva sobre el riesgo de OT debido a los incidentes de ransomware ampliamente reportados que afectan a sus colegas de la industria. Esto ha dado como resultado una mejor gobernanza y un enfoque en la resiliencia de la ciberseguridad. La investigación de Orange Cyberdefense destaca que el sector manufacturero fue el sector industrial más atacado en 2022, debido en parte a su gran tamaño y, desde la perspectiva de los atacantes, a su relativo atractivo (las puntuaciones CVSS de manufactura son un 33% más altas que el promedio mundial).

También destaca que el 58% de los incidentes se deben a errores internos y errores de configuración. Los propietarios de activos deben protegerse nuevamente de las amenazas externas, pero también monitorear de cerca los procesos internos.

Requerimientos de ciberseguridad en evolución

La responsabilidad de la ciberseguridad de OT difiere según la organización. Puede ser el equipo de operaciones, el director de ingeniería o el CISO. Para simplificar, nos referimos al equipo responsable de la ciberseguridad de OT como líderes de seguridad de OT.

El objetivo principal de los líderes de seguridad de OT es garantizar que se minimice el riesgo de que un incidente cibernético afecte la confiabilidad, disponibilidad y seguridad de las operaciones. Esto requiere identificación y gestión de vulnerabilidades, así como una capa de controles para evitar que los actores de amenazas accedan a las redes. El punto de partida lógico es identificar y clasificar todos los activos, aunque rara vez es una tarea sencilla. Las plantas pueden tener 30 años, no tener un registro oficial de activos y depender de un mosaico de diferentes sistemas y sensores OEM. Los líderes de seguridad deben tener visibilidad de los activos que administran, el estado del firmware y de los parches de esos activos, y a qué se están conectando.



Una vez que se identifican y registran los activos, los líderes de seguridad de OT deben abordar las vulnerabilidades que conocen y entienden e implementar procesos para monitorearlos y administrarlos continuamente. Esto puede incluir cambiar contraseñas predeterminadas, implementar administración de parches y monitorear los controles de acceso.

La defensa en profundidad (DiD) es el modelo tradicional de seguridad por capas aplicado a entornos OT y comprende una serie de controles técnicos y administrativos para proteger datos, aplicaciones, endpoints y la red. Esto dificulta a los adversarios moverse lateralmente, impidiéndoles explotar las vulnerabilidades. Los controles técnicos incluyen firewalls en el límite de la red de TI/OT y entre zonas para garantizar una segmentación, protección de endpoints y control de acceso adecuados. El monitoreo de la red OT brinda una capa adicional, detectando anomalías y automatizando la respuesta.

Sin embargo, a medida que las redes convergen y el intercambio de datos entre la fábrica y la nube se expande, también aumenta el alcance de la amenaza. DiD por sí solo no es suficiente para proteger las operaciones OT. Las organizaciones modernas requieren un enfoque de seguridad que aplique políticas, monitoree y organice a través de una red compleja de infraestructura digital, entidades y activos físicos.

El principio de gestión de la superficie de ataque (Attack Surface Management; ASM) ayuda a abordar el desafío de identificar, evaluar y mitigar las vulnerabilidades que existen dentro de la infraestructura física y digital de una organización y de las entidades externas, incluida la cadena de suministro y los socios OEM.



ASM se centra en identificar y gestionar riesgos a través de un enfoque proactivo para la gestión de la seguridad, mientras que DiD se centra en la superposición de controles para proteger contra amenazas.

Los enfoques son totalmente complementarios como se indica en NIST 800-53, que describe la reducción de la superficie de ataque como *“alineado con los análisis de amenazas y vulnerabilidades y arquitectura y diseño de sistemas. La reducción de la superficie de ataque es una forma de reducir el riesgo para las organizaciones al darles a los atacantes menos oportunidades de explotar debilidades o deficiencias, es decir (vulnerabilidades potenciales) dentro de los sistemas, componentes del sistema y servicios del sistema”*. Se recomienda una defensa en capas como parte de la arquitectura de seguridad general junto con un enfoque de ‘privilegios mínimos’ para gestionar el acceso a la red.

Los líderes de seguridad de OT están implementando cada vez más ASM. Esto incluye el descubrimiento de activos, la evaluación de riesgos y la remediación. También debe incluir planes de respuesta específicos de OT basados en la comprensión de las tácticas, técnicas y procedimientos (TTP) que pueden ser exclusivos del sector industrial.

Una postura sólida de seguridad de OT requiere que los controles técnicos sean interoperables. Los firewalls, IDS, antivirus y soluciones de control de acceso implementadas en el marco DiD deben integrar e intercambiar datos, permitiendo la orquestación de procesos y flujos de trabajo de seguridad para mejorar la detección de amenazas y la respuesta a incidentes. Esto también incluye los componentes de ASM, que brindan a los líderes de seguridad de OT una operación de seguridad unificada y automatizada.

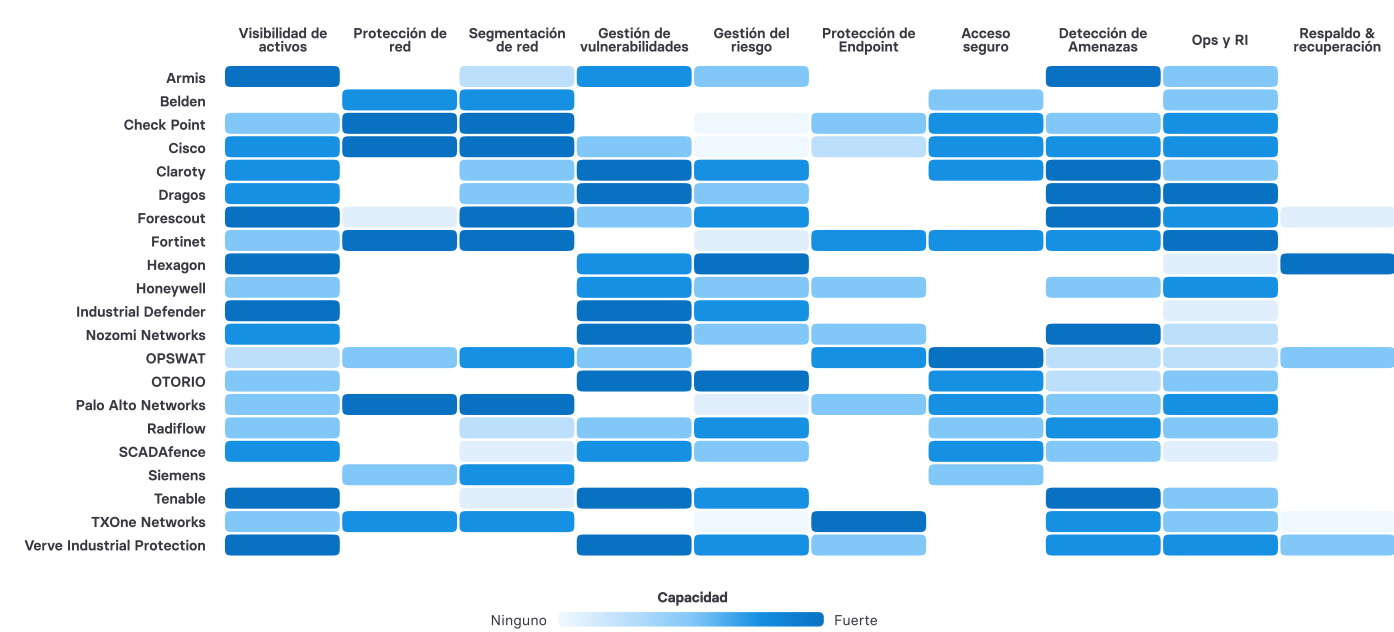
Selección de proveedores de seguridad

No existe un único proveedor que proporcione funciones nativas que cubran todos los controles técnicos de seguridad. Los líderes de seguridad de OT que planean implementar un nuevo programa de seguridad, consolidar proveedores o actualizar su programa de seguridad deben buscar un enfoque de plataforma que garantice que las soluciones de los proveedores puedan integrarse. Una ventaja de utilizar una única plataforma es que traslada la carga de la integración al proveedor de la plataforma. El proveedor de la plataforma se hace responsable de garantizar que sus productos interoperan, reduciendo así la carga de la deuda tecnológica que asume el propietario del activo.

El ecosistema consta de dos categorías principales de proveedores. Los proveedores de protección de redes OT suelen ofrecer firewalls, incluida la cobertura de protocolos industriales y una gama de funciones adicionales, desde protección de endpoints hasta SOCaaS. Los principales casos de uso incluyen protección de red, segmentación y gestión de acceso, pero muchos también ofrecen soluciones de visibilidad. La mayoría de los proveedores también tienen una sólida plataforma de seguridad de TI, lo que permite a las empresas industriales gestionar las operaciones de seguridad de TI y OT por separado o fusionarlas en una sola operación.

Los proveedores de visibilidad de activos y gestión de amenazas brindan visibilidad, gestión de vulnerabilidades y detección de amenazas respaldadas por inteligencia de amenazas específica de OT. Estos proveedores generalmente ofrecen productos para OT ASM, aunque cada proveedor tiene sus propias fortalezas únicas, que van desde el tipo de implementación, los servicios administrados o la capacidad (administración de acceso remoto, respuesta a incidentes, etc.)

Los siguientes proveedores, revisados en el último análisis de WA sobre la industria de ciberseguridad OT, brindan soluciones e integraciones de plataforma y deben ser considerados por los líderes de seguridad.



Al seleccionar proveedores, los líderes de seguridad OT también deben considerar la dirección estratégica de los proveedores. Los analistas de WA notaron innovaciones significativas en toda la industria durante los últimos 18 meses, y las hojas de ruta técnicas de algunos proveedores son particularmente sólidas, incluidas mejoras en la usabilidad de la plataforma, nuevas integraciones, mejoras en el análisis de riesgos y nuevos casos de uso de OT.

Perfil: Fortinet



Fortinet es una empresa que cotiza en bolsa con sede en Sunnyvale, California, Estados Unidos. La empresa es uno de los principales proveedores de redes y ciberseguridad con una cartera amplia e integrada de más de 50 productos de nivel empresarial que abordan múltiples casos de uso de redes y seguridad. La empresa continúa creciendo con fuerza y presta servicios a más de 660,000 clientes con una facturación de 5,600 millones de dólares en el año fiscal 2022.

Resumen

La inversión en investigación e innovación ha permanecido consistentemente alta, lo que ha resultado en un extenso portafolio de patentes (1,285). Esto está respaldado por una red global de centros de desarrollo y centros de excelencia, incluyendo una reciente inversión en Japón. Fortinet es un proveedor líder de soluciones de ciberseguridad de TI y OT para los sectores industrial y de infraestructura crítica, con una alta base de clientes y una sólida cobertura de todas las verticales industriales.

Las prioridades declaradas de la empresa en 2023 son ser el número 1 en firewalls de red, SD-WAN y seguridad OT. El negocio de OT ha crecido con fuerza, superando el crecimiento promedio del mercado, debido a una mayor inversión en productos, personal y operaciones de ventas y marketing específicos de OT.

El OT Aware Security Fabric (Security Fabric consciente de OT) de Fortinet está compuesto por una amplia gama de productos de seguridad que permiten redes seguras, acceso de confianza cero y operaciones de seguridad, todo respaldado por servicios de seguridad que incluyen servicios FortiGuard especializados en OT, más de 3,000 firmas de aplicaciones OT y más de 600 firmas de amenazas OT.

Los productos nativos de Fortinet abordan con solidez la mayoría de los casos de uso de ciberseguridad de OT y los socios del ecosistema de la alianza tecnológica brindan soluciones complementarias. Esto brinda a los clientes una plataforma de ciberseguridad de extremo a extremo que aborda IEC-62443, NIST CSF, MITRE ATT&CK para ICS y otros estándares relevantes.

Posicionamiento

La estrategia de OT está alineada para abordar los desafíos emergentes de los clientes relacionados con asegurar una mayor conectividad en la nube, garantizar un acceso remoto seguro, permitir operaciones de TI/OT seguras y convergentes y la gestión efectiva de amenazas y vulnerabilidades. Esto se logra a través del OT Aware Security Fabric, que incluye proveedores de gestión de amenazas y vulnerabilidades, socios OEM Fabric-Ready e integradores de sistemas.

La fortaleza de Fortinet es su capacidad para brindar soluciones de seguridad en todo el modelo Purdue, desde el sensor hasta la nube. Los socios y clientes de la industria a menudo citan las soluciones de Fortinet como fáciles de implementar, usar y escalar.

El compromiso de Fortinet con la ciberseguridad de OT es evidente en sus continuas inversiones en productos. La cartera ha crecido significativamente en los últimos 3 años y las incorporaciones recientes incluyen nuevos casos de uso como la gestión del acceso remoto seguro (FortiPAM) y visibilidad de activos y redes en la vista de FortiOS OT.

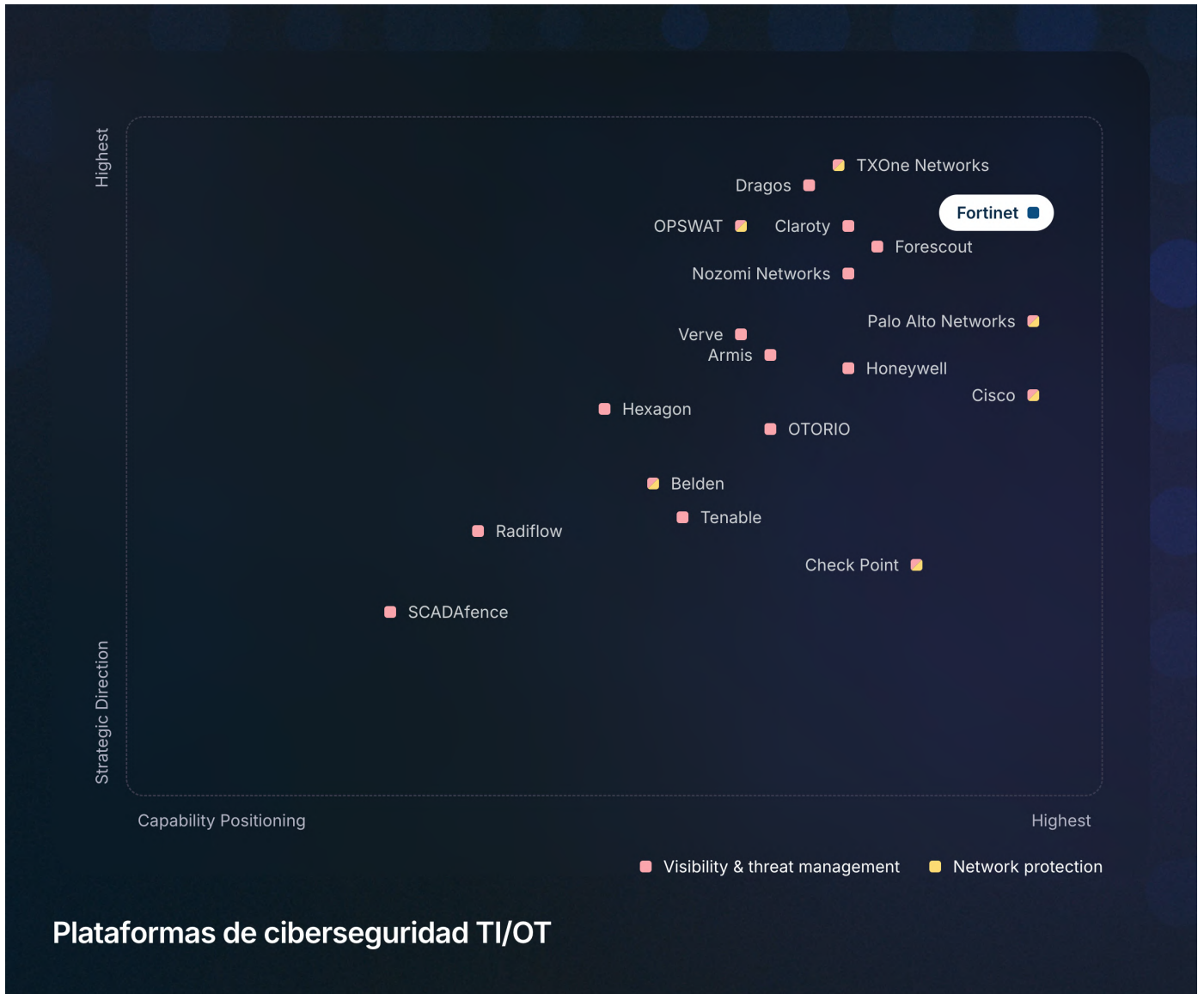
Los desarrollos también incluyen visualización e informes mejorados y también ha habido lanzamientos importantes relacionados con MITRE ATT&CK para ICS.

Es probable que los desarrollos futuros incluyan la incorporación de FortiNDR al OT Aware Security Fabric, mejoras en la gestión de cumplimiento y la inclusión de nuevas funciones de las recientes adquisiciones FortiPolicy y Volon FortiRecon. Más allá de los productos y soluciones, el enfoque de Fortinet de ser el número 1 en seguridad de OT ha ido acompañado de un extenso equipo de expertos, centros de experiencia y cursos de formación y concientización para mejorar el valor y la experiencia del cliente.

Conocido por

- Empresa líder mundial en ciberseguridad
- Conjunto amplio e integrado de soluciones de seguridad.
- Innovación en ciberseguridad y redes
- Gran ecosistema de socios
- Creciente presencia en el mercado de ciberseguridad de OT

Plataformas de ciberseguridad TI/OT



Las plataformas de ciberseguridad de TI/OT incluyen varios productos nativos y se integran con otros productos o plataformas para brindar al cliente una visión única y unificada de las operaciones.

Definición

El mercado se compone de dos tipos de proveedores, los que brindan visibilidad y gestión de amenazas y los que tienen una sólida cartera de productos de protección de redes. Los líderes de seguridad normalmente dependerán de al menos un proveedor de cada categoría. Sin embargo, los competidores están ampliando su funcionalidad y es cada vez más común que

los proveedores ofrezcan soluciones tanto de visibilidad y gestión de amenazas como de protección de redes.

Puede encontrar más información sobre el mercado y las tendencias de la industria en el informe relacionado de WA Insight, “Industrial Cybersecurity Industry Analysis”.

Evaluación

Las siguientes tecnologías están incluidas en la evaluación:

- Visibilidad de activos
- Protección de red
- Segmentación de red
- Administración de vulnerabilidades
- Gestión de riesgo
- Protección del endpoint
- Acceso seguro
- Detección de amenazas
- Operaciones seguras y respuesta a incidentes
- Respaldo y recuperación

Calificación

Los competidores deben cumplir con los siguientes criterios para calificar y ser considerados en el ‘IT/OT Cybersecurity Platform Navigator’

- La empresa cuenta con soluciones nativas en al menos 4 categorías tecnológicas.
- Los productos relevantes se integran en una plataforma centralizada.
- La plataforma ingiere información de otras plataformas o fuentes para enriquecer los datos.
- La plataforma tiene una sofisticada función de administración central que proporciona análisis e informes para que los analistas monitoreen y administren las operaciones de seguridad.
- La plataforma tiene capacidades SIEM o se integra con plataformas SOAR.
- La empresa tiene una sólida cobertura en más de una región geográfica.

Metodología

Puede encontrar más información sobre la metodología de WA en el sitio web: <https://navigator.westlandsadvisory.com>

Visibilidad de OT y gestión de amenazas



Las plataformas de visibilidad y gestión de amenazas incluyen descubrimiento de activos y redes, contextualización, gestión de vulnerabilidades y detección de amenazas. La plataforma normalmente se integrará con otras plataformas de seguridad o con SIEM.

Definición

El mercado se compone de varios proveedores que utilizan diferentes enfoques. Esto incluye competidores exclusivos de visibilidad y gestión de activos que utilizan descubrimiento basado en agentes, empresas de detección de amenazas que utilizan escaneo pasivo, entre otras técnicas, y proveedores de redes que ofrecen visibilidad y detección de amenazas a

través de firewalls o integrados en switches. Puede encontrar más información sobre el mercado y las tendencias de la industria en el informe relacionado de WA Insight, “Industrial Cybersecurity Industry Analysis”.

Evaluación

Se incluyen las siguientes tecnologías:

- Visibilidad de activos que incluye escaneo activo y descubrimiento basado en agentes.
- Administración de vulnerabilidades.
- Gestión de riesgos que incluye cuantificación, gestión de configuración y gestión de cumplimiento.
- Detección de amenazas, incluido aprendizaje automático, análisis del comportamiento de usuarios y entidades (UEBA) y firmas.

Calificación

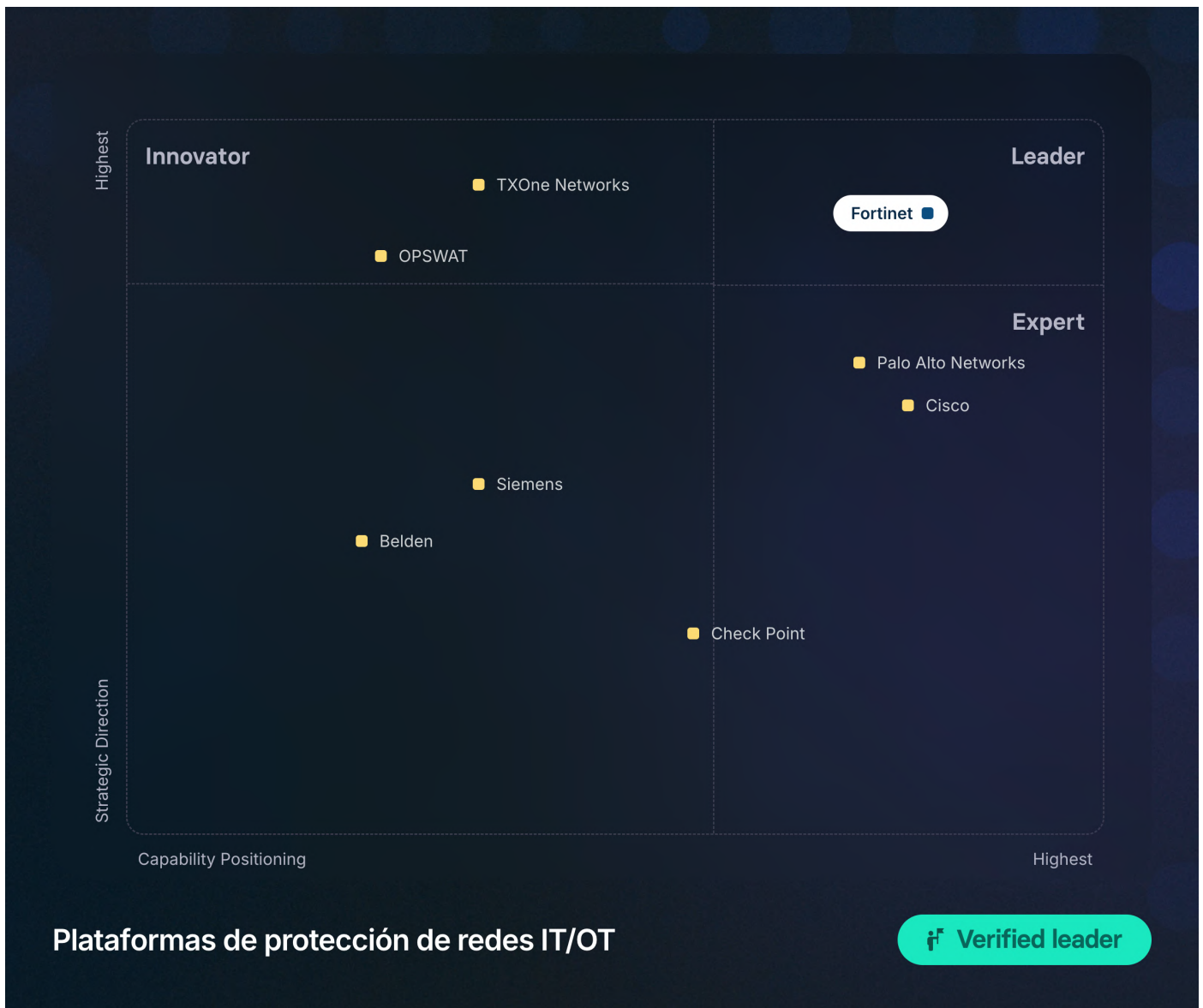
Los competidores deben cumplir con los siguientes criterios para calificar y ser considerados en el ‘IT/OT Administración Navigator’:

- La compañía debe ofrecer soluciones nativas para la visibilidad de activos y la detección de amenazas.
- Los productos relevantes se integran en una plataforma centralizada.
- La plataforma ingiere información de otras plataformas o fuentes para enriquecer los datos y brindar contexto.
- La plataforma tiene una sofisticada función de administración central que proporciona análisis e informes para que los analistas monitoreen y administren las operaciones de seguridad.
- La plataforma tiene capacidades SIEM o se integra con plataformas SOAR.
- La empresa tiene una sólida cobertura en más de una región geográfica.

Metodología

Puede encontrar más información sobre la metodología de WA en el sitio web: <https://navigator.westlandsadvisory.com>

Plataformas de protección de redes IT/OT



La protección de redes OT es parte integral de un enfoque de defensa en profundidad, brindando protección en el límite de la red a través del monitoreo de la red y la aplicación de políticas.

Definición

Las plataformas de protección de redes tienen varias funciones nativas, incluidas firewalls y control de acceso. Los casos de uso pueden incluir visibilidad de la red, segmentación, aplicación de políticas de confianza cero y respuesta a incidentes. La mayoría de las plataformas de protección de redes también incluye otros controles técnicos nativos (por

ejemplo, protección de endpoints) o se integran con herramientas de terceros. La plataforma organiza y proporciona visibilidad y control centralizados de las operaciones de ciberseguridad de OT.

Puede encontrar más información sobre el mercado y las tendencias de la industria en el informe relacionado de WA Insight, “Industrial Cybersecurity Industry Analysis”.

Evaluación

Las siguientes funciones están incluidas en la evaluación:

- Protección de red que incluye firewalls, IPA, gateways unidireccionales y diodos de datos.
- Segmentación de red incluyendo firewalls, VLAN, listas de control de acceso (ACL), ADN y micro segmentación sin agentes a través de identificación y agrupación lógica de activos y dispositivos.
- Protección del endpoint que incluye escaneo de malware, listas blancas de aplicaciones y administración de parches y protección de USB.
- Acceso seguro que incluye PAM, VPN y ZTNA.
- Operaciones de seguridad y respuesta a incidentes, incluidos SIEM, SOAR, XDR y EDR, además de guías.

Calificación

Los competidores deben cumplir con los siguientes criterios para calificar y ser considerados en el ‘Network Protection Platform Navigator’:

- La compañía debe ofrecer soluciones nativas para la protección de la red OT, incluidos todos o uno de NGFW, IPA y diodo de datos.
- Los productos relevantes se integran en una plataforma centralizada con otros productos de protección de red, incluida la gestión de acceso.
- La plataforma ingiere información de otras plataformas o fuentes para enriquecer los datos y brindar contexto.
- La plataforma tiene una sofisticada función de administración central que proporciona análisis e informes para que los analistas monitoreen y administren las operaciones de seguridad, brindando visibilidad y administración de redes y dispositivos.
- La plataforma tiene capacidades SIEM o se integra con plataformas SOAR.
- La empresa tiene una sólida cobertura en más de una región geográfica.

Metodología

Puede encontrar más información sobre la metodología de WA en el sitio web: <https://navigator.westlandsadvisory.com>

Conclusiones

Las redes OT son a menudo ricas en datos y pobres en información y aún no se pueden derivar enormes beneficios de una mayor explotación de datos. Para acelerar la transformación digital, los propietarios de activos necesitan visibilidad de los activos y de la red, pero también necesitan gestionar los datos y las alertas de manera eficiente. Esto ha resultado en innovación no solo para identificar activos, sino también para categorizar, perfilar y automatizar la gestión de riesgos y vulnerabilidades. El descubrimiento de activos y la gestión de vulnerabilidades son segmentos de productos de alto crecimiento y abordan los riesgos "conocidos" para las operaciones. Además de los firewalls y la segmentación de redes, la gestión de acceso y la protección de endpoints, estos controles ofrecen sólidas medidas de protección.

Existe un requisito creciente en las regulaciones y estándares para garantizar que se cubran las "incógnitas" que requieren un monitoreo continuo mediante escaneo pasivo o activo para detectar y alertar si hay desviaciones de la línea de base. Para protegerse contra escenarios desconocidos, los propietarios de activos deben avanzar hacia la implementación de un modelo de seguridad basado en operaciones resilientes y un enfoque en las personas, la tecnología y los procesos para garantizar que las organizaciones puedan resistir y recuperarse de un incidente cibernético con una interrupción mínima en las operaciones. ASF es clave para adelantarse a las amenazas mientras está bien documentado. Los procedimientos de respuesta a incidentes facilitan una respuesta coordinada, oportuna y eficaz.

Para 2030, esperamos que la madurez de la ciberseguridad de OT haya avanzado significativamente en las empresas de servicios públicos y en las grandes organizaciones manufactureras transnacionales. Muchas organizaciones tendrán operaciones de seguridad convergentes que brindarán visibilidad a toda la empresa, con equipos de OT dedicados y capacitados en procesos y procedimientos. La seguridad será gestionada cada vez más por plataformas en la nube, ya sea por los propietarios de activos o por un proveedor de servicios administrados y habrá un enfoque cada vez mayor en la gestión y protección de las redes inalámbricas 5G. WA también espera mayor madurez de la ciberseguridad en la cadena de suministro y una mayor base instalada de operaciones industriales construidas sobre principios de seguridad por diseño. Los líderes de seguridad deben asegurarse de trabajar con socios que tengan soluciones para abordar los requerimientos actuales y futuros de la industria.