

Panorama de Cibersegurança Industrial 2023-2030

Fortinet



Macrotendências que sustentam um maior investimento em cibersegurança para OT continuam em alta

Apesar das condições econômicas globais desafiadoras, os investimentos em cibersegurança para OT têm continuado a aumentar. Existem 3 impulsionadores: transformação digital, regulamentação e gestão de riscos.

A crescente interconectividade entre dispositivos, sistemas e processos para OT tem facilitado a transformação digital das operações industriais, aumentando a demanda por serviços de computação em nuvem, análise de dados, gêmeos digitais e machine learning. A convergência entre IT e OT acelerou ainda mais essa tendência, promovendo a integração e a troca de dados contínuas entre dois ambientes anteriormente distantes. O novo proprietário de ativos digitais é caracterizado por níveis mais elevados de interoperabilidade e colaboração, permitindo a otimização de processos e ganhos de produtividade. Os benefícios da transformação digital precisam ser gerenciados juntamente com o aumento da exposição a vulnerabilidades em IT e OT, exigindo novas políticas, processos e procedimentos de cibersegurança para garantir a eficiência dos futuros modelos operacionais.

A regulamentação continua a influenciar as decisões de aquisição. Os esforços de fiscalização estão se fortalecendo, a regulamentação está se ampliando para abranger mais setores da indústria e cadeias de suprimentos, além de haver uma crescente demanda por níveis mais elevados de resiliência. Os exemplos nos Estados Unidos incluem, a Diretiva Operacional Vinculante 23-01 da CISA e a Diretiva SD 1580/82-2022-01 da TSA, que se tornaram aplicáveis em 2023. Além disso, há o foco da M-22-09, da OMB, em estabelecer a Confiança Zero na infraestrutura operada pelo governo federal. A Diretiva NIS 2 será exigível em todos os países da UE a partir de 2024, e passa a incluir os principais setores industriais, aumentando a cobertura de 21% para 36% da base econômica da UE. Ao mesmo tempo, o ato de Resiliência de Entidades Críticas (CER) abrange a infraestrutura crítica. Austrália, Índia, Japão e Canadá lançaram recentemente novas regulamentações ou estão em processo de revisão do status atual.

O último fator que contribui para o aumento dos investimentos é a crescente conscientização dos executivos em relação ao risco de OT, devido aos incidentes de ransomware amplamente divulgados que afetaram colegas do setor. Isso resultou em uma melhoria na governança e um foco na resiliência da cibersegurança. A pesquisa da Orange Cyberdefense destaca que o setor manufatureiro foi o mais atacado em 2022, em parte devido ao seu tamanho considerável e, do ponto de vista do invasor, à sua relativa atratividade (as pontuações de CVAA do setor manufatureiro são 33% mais elevadas do que a média global). Além disso, ele

ressalta que 58% dos incidentes resultam de erros internos e configurações incorretas. Portanto, os detentores de ativos precisam se proteger contra ameaças externas, enquanto monitoram de perto os processos internos.

Evolução dos Requisitos de Cibersegurança

A responsabilidade pela cibersegurança para OT varia de acordo com a organização. Pode ser da equipe de Operações, do Diretor de Engenharia ou do CISO. Para simplificar, nos referimos à equipe responsável pela cibersegurança para OT, como Líderes de Segurança em OT.

O principal objetivo dos Líderes de Segurança em OT é garantir que o risco de um incidente cibernético afetar a Confiabilidade, a Disponibilidade e a Segurança das operações seja minimizado. Isso requer a identificação e gestão de vulnerabilidades, bem como uma camada de controles para evitar que atores maliciosos acessem as redes. O ponto de partida lógico é identificar e classificar todos os ativos, embora isso raramente seja uma tarefa simples. As instalações podem ter 30 anos de idade, sem um registro oficial de ativos e dependentes de um emaranhado de sistemas e sensores OEM diferentes. Os Líderes de Segurança precisam ter visibilidade dos ativos que estão gerenciando, do status do firmware e atualizações desses ativos, e do que eles estão conectados.



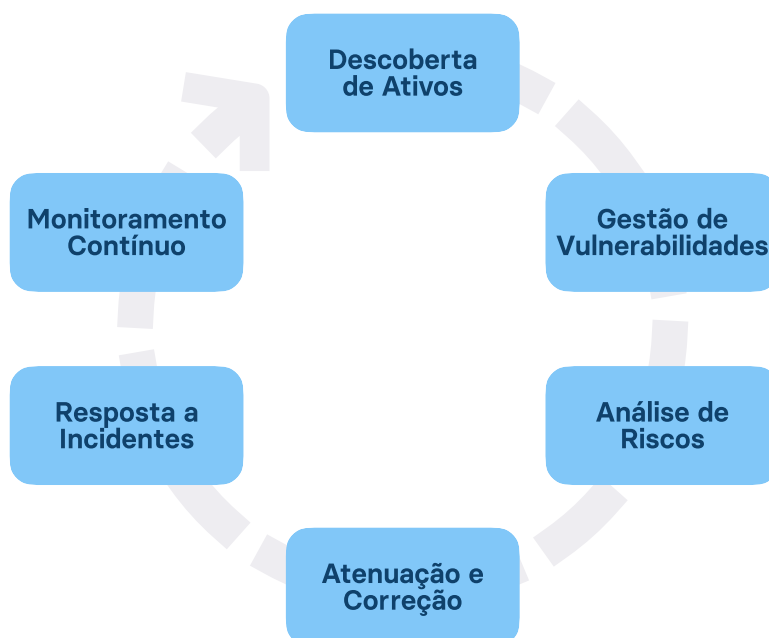
Assim que os ativos forem identificados e registrados, os Líderes de Segurança em OT devem lidar com vulnerabilidades conhecidas e compreendidas, e implementar processos para monitorá-las e gerenciá-las continuamente. Isso pode incluir a alteração de senhas

padrão, a implementação do gerenciamento de patches e o monitoramento dos controles de acesso.

A Defesa em Profundidade (DiD) é o modelo tradicional de segurança em camadas aplicado a ambientes de OT e compreende uma série de controles técnicos e administrativos para proteger dados, aplicativos, endpoints e a rede. Isso torna mais difícil para invasores se moverem lateralmente, impedindo que explorem vulnerabilidades. Os controles técnicos incluem firewalls nos limites da rede de IT/OT e entre as zonas, para garantir uma segmentação adequada, proteção de endpoints e controle de acesso. O monitoramento da rede OT fornece uma camada adicional, detectando anomalias e automatizando respostas.

No entanto, à medida que as redes convergem e a troca de dados entre a área de produção e a nuvem se expande, o escopo da ameaça também aumenta. A DiD por si só não é suficiente para proteger as operações de OT. Organizações modernas exigem uma abordagem de segurança que aplique políticas, monitore e orquestre em uma complexa rede de infraestrutura digital, entidades e ativos físicos.

O princípio do Gerenciamento da Superfície de Ataque (ASM) ajuda a enfrentar o desafio de identificar, avaliar e atenuar as vulnerabilidades existentes na infraestrutura digital e física de uma organização, bem como em entidades externas, incluindo a cadeia de suprimentos e parceiros OEM.



O ASM concentra-se na identificação e gestão de riscos por meio de uma abordagem proativa à gestão da segurança, enquanto a DiD está focada na estratificação de controles para se proteger contra ameaças.

As abordagens são totalmente complementares, conforme observado no NIST 800-53, que descreve a redução da Superfície de Ataque como estando *"alinhada com análises de ameaças e vulnerabilidades, bom como arquitetura e design de sistemas. A redução da Superfície de Ataque é um meio de diminuir o risco para as organizações, dando aos invasores menos oportunidades de explorar fraquezas ou deficiências (ou seja, possíveis vulnerabilidades) dentro dos sistemas, componentes e serviços do sistema."* Recomenda-se uma defesa em camadas como parte da arquitetura geral de segurança, juntamente com uma abordagem de privilégio mínimo para gerenciar o acesso à rede.

ASM vem sendo cada vez mais implementado pelos Líderes de Segurança em OT. Isso inclui a descoberta de ativos, a avaliação de riscos e a correção. Também deve compreender planos de resposta específicos para OT, baseados em uma compreensão das Táticas, Técnicas e Procedimentos (TTPs) que podem ser únicos para o setor industrial.

Uma postura de segurança robusta para OT requer que os controles técnicos sejam interoperáveis. As soluções de firewalls, IDS, antivírus e controle de acesso implementadas na estrutura DiD devem se integrar e compartilhar dados, permitindo a organização de processos de segurança e fluxos de trabalho a fim de melhorar a detecção de ameaças e a resposta a incidentes. Isso também inclui os componentes do ASM, fornecendo aos Líderes de Segurança em OT uma operação de segurança unificada e automatizada.

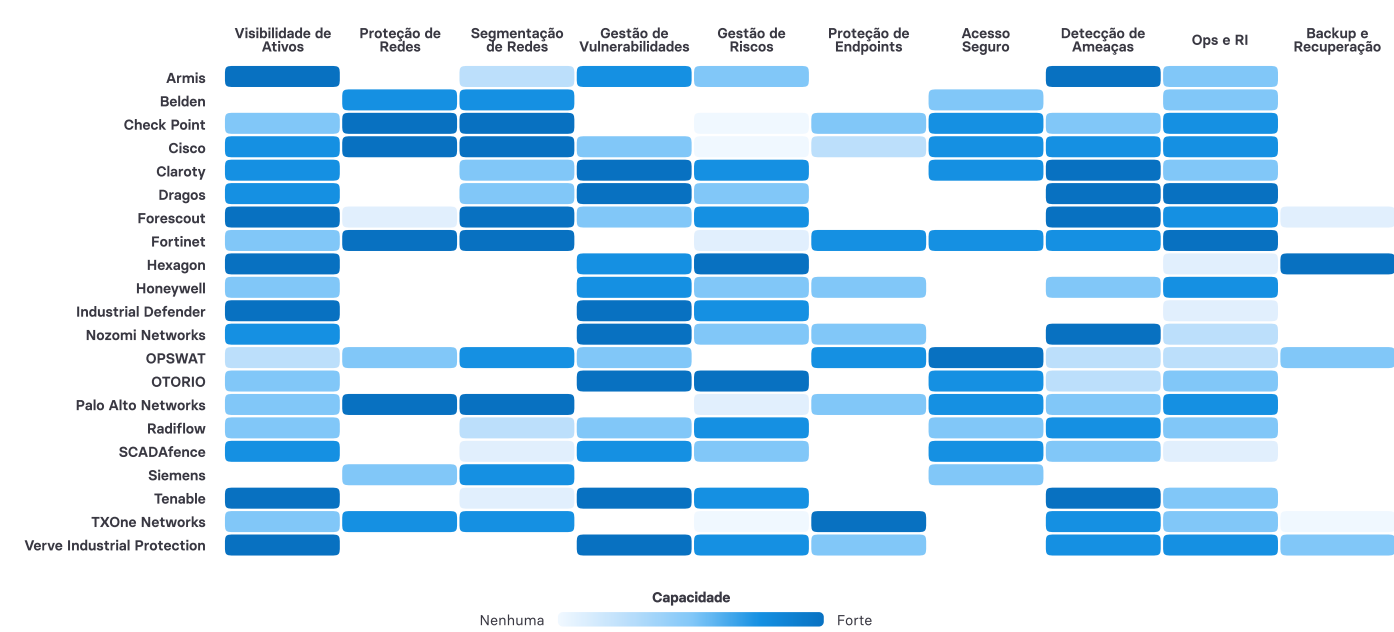
Seleção do Fornecedor de Segurança

Não existe um único fornecedor que ofereça recursos nativos abrangendo todos os controles de segurança técnica. Os Líderes de Segurança em OT que planejam implementar um novo programa de segurança, consolidar fornecedores ou atualizar seu programa devem adotar uma abordagem de plataforma, garantindo que as soluções dos fornecedores possam ser integradas. Uma vantagem de usar uma única plataforma é que ela transfere a carga da integração para o fornecedor. Este, se torna responsável por garantir a interoperabilidade de seus produtos, reduzindo assim o peso do débito tecnológico que o Proprietário do Ativo assume.

O ecossistema consiste em duas principais categorias de fornecedores. Os fabricantes de Proteção de Redes para OT geralmente oferecem firewalls, incluindo cobertura de protocolos industriais, e uma variedade de recursos adicionais, desde proteção de endpoint até SOCaaS. Os principais casos de uso incluem proteção de redes, segmentação e gerenciamento de acesso, mas muitos também oferecem soluções de visibilidade. A maioria, ainda possuem uma plataforma de segurança de IT robusta, permitindo que empresas industriais gerenciem as operações de segurança de IT e OT separadamente ou as integrem em uma única operação.

Fornecedores de Visibilidade de Ativos e Gestão de Ameaças oferecem visibilidade, gestão de vulnerabilidades e detecção de ameaças, apoiados por inteligência de ameaças específicas para OT. Esses fornecedores geralmente fornecem produtos para ASM em OT, embora cada um tenha seu próprio diferencial, que varia desde o tipo de implantação até serviços gerenciados ou recursos (gerenciamento de acesso remoto, resposta a incidentes, etc.).

Os seguintes fornecedores, revisados na análise mais recente da WA sobre o Setor de Cibersegurança para OT, oferecem soluções e integrações de plataforma e devem ser considerados pelos Líderes de Segurança.



Ao selecionar, os Líderes de Segurança em OT também devem considerar a direção estratégica dos fornecedores. Os analistas da WA observaram inovações significativas em todo o setor nos últimos 18 meses, e os roteiros técnicos de alguns fornecedores são particularmente robustos, incluindo melhorias na usabilidade da plataforma, novas integrações, refinamentos na análise de riscos e novos casos de uso para OT.

Perfil: Fortinet



A Fortinet é uma empresa de capital aberto sediada em Sunnyvale, Califórnia, Estados Unidos. É um dos principais fornecedores de cibersegurança e redes, com um portfólio amplo e integrado de mais de 50 produtos de nível empresarial voltados para vários casos de uso em segurança e redes. A empresa continua a crescer fortemente, atendendo a mais de 660 mil clientes e com um faturamento de US\$ 5,6 bilhões no ano fiscal de 2022.

Resumo

O investimento em pesquisa e inovação tem se mostrado consistentemente alto, resultando em um extenso portfólio de patentes (1.285). Isso é respaldado por uma rede global de Centros de Desenvolvimento e Centros de Excelência, incluindo investimentos recentes no Japão. A Fortinet é fornecedora líder em soluções de cibersegurança em IT e OT para os setores industrial e de infraestrutura crítica, com uma extensa base de clientes e ampla cobertura de todos os segmentos industriais.

As prioridades estabelecidas pela empresa em 2023 são se tornar a número 1 em Firewalls de Rede, SD-WAN e Segurança para OT. O setor de OT tem crescido significativamente, superando o aumento médio do mercado, devido ao maior investimento em produtos específicos para OT, na equipe, e nas operações de vendas e marketing.

O OT Aware Security Fabric da Fortinet é composto por uma ampla gama de produtos de segurança, que permitem Redes Seguras, Acesso Confiança Zero e Operações de Segurança. Tudo isso é apoiado por serviços de segurança que incluem os Serviços FortiGuard, especializados em OT, com mais de 3.000 assinaturas de aplicativos para OT e mais de 600 assinaturas de ameaças para OT.

Os produtos nativos da Fortinet abordam de forma eficaz a maioria dos casos de uso de cibersegurança para OT, com parceiros do ecossistema Tech Alliance fornecendo soluções complementares. Isso proporciona aos clientes uma plataforma abrangente de cibersegurança que atende aos padrões IEC-62443, NIST CSF, MITRE ATT&CK para ICS e outras normas importantes.

Posicionamento

A estratégia para OT está voltada para enfrentar os desafios emergentes dos clientes no que diz respeito à segurança decorrente do aumento da conectividade em nuvem, visando garantir acesso remoto seguro, permitindo operações seguras e convergentes de IT/OT, e o eficaz gerenciamento de ameaças e vulnerabilidades. Isso é alcançado por meio do OT Aware Security Fabric, que inclui fornecedores de Gestão de Ameaças e Vulnerabilidades, Fabric-Ready OEM e Integradores de Sistemas.

A força da Fortinet reside em sua capacidade de fornecer soluções de segurança que abrangem todo o Modelo Purdue, do sensor à nuvem. Parceiros da indústria e clientes costumam citar as soluções da Fortinet como fáceis de implantar, usar e dimensionar.

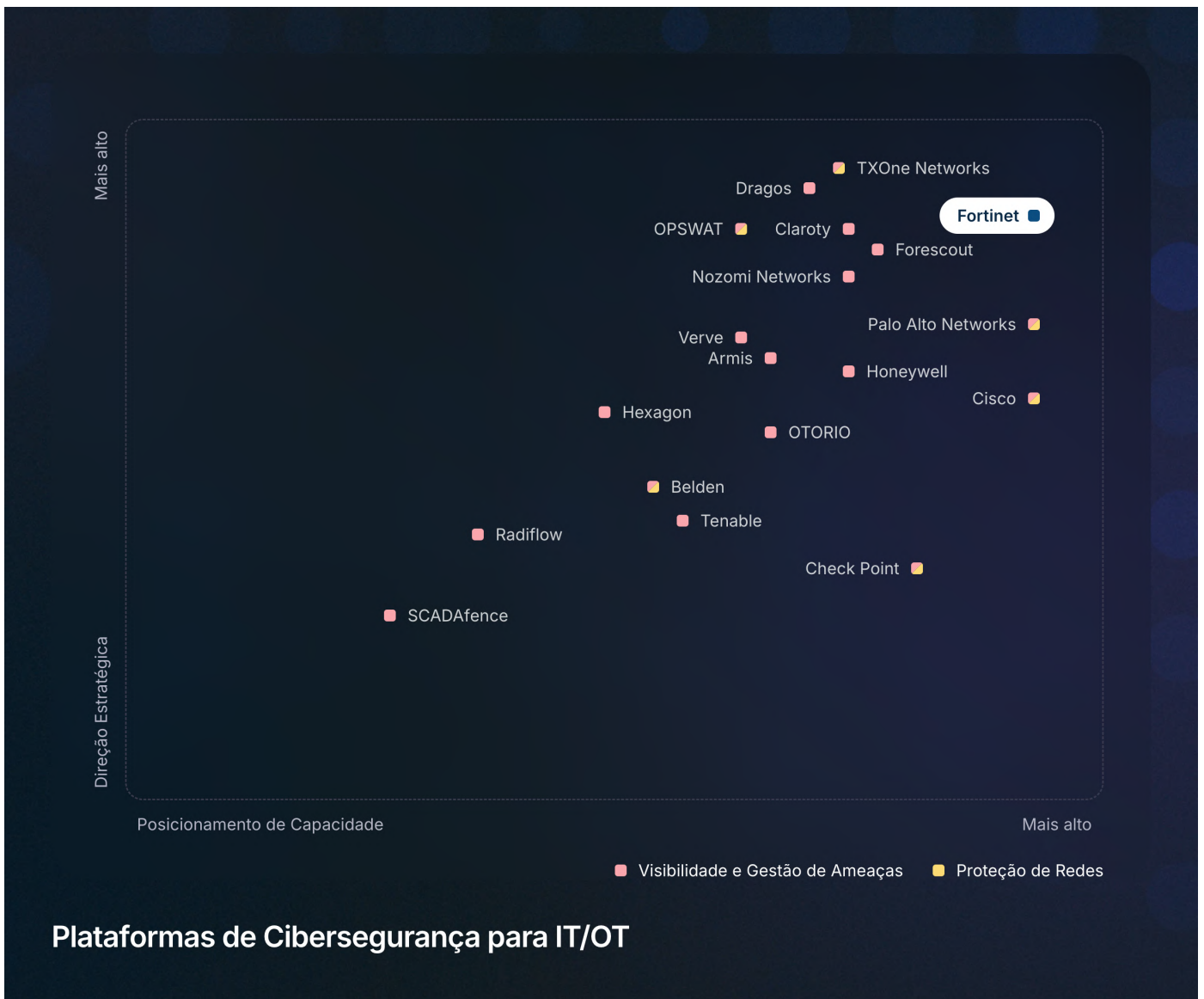
O compromisso da Fortinet com a cibersegurança para OT é evidente em seus contínuos investimentos em produtos. Seu portfólio cresceu significativamente nos últimos 3 anos, e as adições recentes incluem novos casos de uso, como Gerenciamento de Acesso Remoto Seguro (FortiPAM) e a visibilidade de ativos e redes no FortiOS OT View. Os avanços também incluem melhorias na visualização e nos relatórios, além de lançamentos importantes relacionados ao MITRE ATT&CK para ICS.

Os futuros progressos provavelmente irão incluir a integração do FortiNDR ao OT Aware Security Fabric, melhorias no gerenciamento de conformidade e a inclusão de novos recursos das recentes aquisições, FortiPolicy e Volon FortiRecon. Além de produtos e soluções, o foco da Fortinet em ser a número 1 em Segurança para OT vem acompanhado de uma equipe de especialistas ampliada, centros de experiência e cursos de treinamento e conscientização para melhorar o valor e a experiência do cliente.

Conhecida por

- Empresa Líder Global em Cibersegurança
- Conjunto Amplo e Integrado de Soluções de Segurança
- Inovação em Cibersegurança e Redes
- Grande Ecossistema de Parceiros
- Crescente Presença no Mercado de Cibersegurança para OT

Plataformas de Cibersegurança para IT/OT



As Plataformas de Cibersegurança para IT/OT incluem vários produtos nativos e integram-se com outros produtos ou plataformas para fornecer ao cliente uma visão única e unificada das operações.

Definição

O mercado é composto por dois tipos de fornecedores: aqueles que oferecem Visibilidade e Gestão de Ameaças e aqueles que possuem um portfólio de produtos de Proteção de Redes robusto. Líderes de Segurança geralmente contam com pelo menos um fornecedor de cada categoria. No entanto, os competidores estão expandindo suas capacidades e é cada vez

mais comum os fornecedores oferecerem tanto soluções de Visibilidade e Gestão de Ameaças quanto de Proteção de Redes.

Mais informações sobre o mercado e as tendências do setor estão disponíveis no relatório "Industrial Cybersecurity Industry Analysis", da WA Insight.

Avaliação

As seguintes tecnologias estão incluídas na avaliação:

- Visibilidade de Ativos
- Proteção de Redes
- Segmentação de Redes
- Gestão de Vulnerabilidades
- Gestão de Riscos
- Proteção de Endpoints
- Acesso Seguro
- Detecção de Ameaças
- Ops de Segurança & RI
- Backup & Recuperação

Qualificação

Os concorrentes devem atender aos seguintes critérios para se qualificarem para consideração no Navegador de Plataformas de Cibersegurança para IT/OT:

- A empresa possui soluções nativas em pelo menos 4 categorias de tecnologia.
- Os produtos importantes se integram em uma plataforma centralizada.
- A plataforma recebe informações de outras plataformas ou fontes para enriquecer os dados.
- A plataforma possui uma sofisticada função de gerenciamento central que fornece análises e relatórios para os analistas monitorarem e gerenciarem as operações de segurança.
- A plataforma possui recursos de SIEM ou se integra a plataformas SOAR.
- A empresa tem forte cobertura em mais de uma região geográfica.

Metodologia

Mais informações sobre a metodologia da WA podem ser encontradas no site: <https://navigator.westlandsadvisory.com>

Visibilidade e Gestão de Ameaças em OT



As plataformas de Visibilidade e Gestão de Ameaças incluem descoberta de ativos e redes, contextualização, gerenciamento de vulnerabilidades e detecção de ameaças. Normalmente, a plataforma irá se integrar a outras plataformas de segurança ou ao SIEM.

Definição

O mercado é composto por uma série de fornecedores que utilizam abordagens distintas. Isso inclui concorrentes especializados em visibilidade e gerenciamento de ativos, que usam descoberta baseada em agentes. Também tem aquelas empresas de detecção de ameaças que empregam varredura passiva, entre outras técnicas, além de fornecedores de redes que

oferecem visibilidade e detecção de ameaças por meio de firewalls ou incorporados em switches. Mais informações sobre o mercado e as tendências do setor estão disponíveis no relatório "Industrial Cybersecurity Industry Analysis", da WA Insight.

Avaliação

As seguintes tecnologias estão incluídas:

- Visibilidade de Ativos, incluindo varredura ativa e descoberta baseada em agentes.
- Gestão de Vulnerabilidades.
- Gestão de Riscos, incluindo quantificação, gerenciamento de configuração e gerenciamento de conformidade.
- Detecção de Ameaças, incluindo Machine Learning, Análise Comportamental de Usuários e Entidades (UEBA) e Assinaturas.

Qualificação

Os concorrentes devem atender aos seguintes critérios para se qualificarem para consideração no Navegador de Visibilidade e Gestão de Ameaças para IT/OT:

- A empresa deve fornecer soluções nativas para visibilidade de ativos e detecção de ameaças.
- Os produtos importantes se integram em uma plataforma centralizada.
- A plataforma recebe informações de outras plataformas ou fontes para enriquecer os dados e fornecer contexto.
- A plataforma possui uma sofisticada função de gerenciamento central que fornece análises e relatórios para os analistas monitorarem e gerenciarem as operações de segurança.
- A plataforma tem recursos de SIEM ou se integra a plataformas SOAR.
- A empresa tem forte cobertura em mais de uma região geográfica.

Metodologia

Mais informações sobre a metodologia da WA podem ser encontradas no site: <https://navigator.westlandsadvisory.com>

Plataformas de Proteção de Redes para IT/OT



A Proteção de Redes para OT é parte integrante de uma abordagem de Defesa em Profundidade, fornecendo proteção nos limites da rede por meio do monitoramento da rede e da aplicação de políticas.

Definição

As plataformas de Proteção de Redes possuem vários recursos nativos, incluindo firewalls e controle de acesso. Os casos de uso podem incluir visibilidade de rede, segmentação, aplicação de políticas de Confiança Zero, além de resposta a incidentes. A maioria das plataformas de proteção de redes também inclui outros controles técnicos nativos (por

exemplo, proteção de endpoints) ou se integra a ferramentas de terceiros. A plataforma orquestra e fornece visibilidade e controle centralizados das operações de cibersegurança para OT.

Mais informações sobre o mercado e as tendências do setor estão disponíveis no relatório "Industrial Cybersecurity Industry Analysis", da WA Insight.

Avaliação

Os seguintes recursos estão incluídos na avaliação:

- Proteção de Redes, incluindo Firewalls, IPS, gateways unidirecionais e diodos de dados.
- Segmentação de Redes, incluindo Firewalls, VLANs, Listas de Controle de Acesso (ACL), SDN e Segmentação Micro sem agente por meio da identificação e agrupamento lógico de ativos e dispositivos.
- Proteção de Endpoints, incluindo varredura de malware, listas brancas de aplicativos e gerenciamento de patches, além de proteção USB.
- Acesso Seguro, incluindo PAM, VPN e ZTNA.
- Operações de Segurança e Resposta a Incidentes, incluindo SIEM, SOAR, XDR e EDR, além de manuais.

Qualificação

Os concorrentes devem atender aos seguintes critérios para se qualificarem para consideração no Navegador de Plataformas de Proteção de Redes para IT/OT:

- A empresa deve fornecer soluções nativas para proteção de redes para OT, incluindo todos ou um dos produtos NGFW, IPS e Data Diode.
- Os produtos importantes se integram em uma plataforma centralizada com outros produtos de proteção de redes, incluindo gerenciamento de acesso.
- A plataforma recebe informações de outras plataformas ou fontes para enriquecer os dados e fornecer contexto.
- A plataforma possui uma sofisticada função de gerenciamento central que fornece análises e relatórios para os analistas monitorarem e gerenciarem as operações de segurança, proporcionando visibilidade e gerenciamento de redes e dispositivos.
- A plataforma tem recursos de SIEM ou se integra a plataformas SOAR.
- A empresa tem forte cobertura em mais de uma região geográfica.

Metodologia

Mais informações sobre a metodologia da WA podem ser encontradas no site: <https://navigator.westlandsadvisory.com>

Conclusão

As redes para OT são muitas vezes Ricas em Dados, mas Pobres em Informações, com enormes benefícios ainda a serem obtidos de uma exploração de dados mais abrangente. Para acelerar a transformação digital, os Proprietários de Ativos precisam de visibilidade de ativos e redes, mas também necessitam gerenciar os dados e alertas de forma eficiente. Isso tem resultado em inovações não apenas para identificar ativos, mas também para categorizá-los, perfilá-los e automatizar o gerenciamento de riscos e vulnerabilidades. A descoberta de ativos e o gerenciamento de vulnerabilidades são segmentos de produtos de alto crescimento e abordam os riscos "conhecidos" para as operações. Juntamente com firewalls e segmentação de rede, gerenciamento de acesso e proteção de endpoints, esses controles fornecem fortes medidas de proteção.

Há uma exigência cada vez maior em regulamentações e padrões, para garantir que os "desconhecidos" sejam abordados. Essa exigência implica num monitoramento contínuo por meio de varreduras passivas ou ativas. O objetivo é detectar e alertar sobre desvios em relação à linha de base. Para se proteger contra cenários desconhecidos, os proprietários de ativos devem adotar a implementação de um modelo de segurança baseado em operações resilientes e com foco em pessoas, tecnologia e processos. Tudo isso, para garantir que as organizações sejam capazes de resistir e se recuperar de um incidente cibernético com o mínimo de interrupção das operações. O ASF é fundamental para antecipar ameaças, enquanto procedimentos de Resposta a Incidentes bem documentados facilitam uma resposta coordenada, rápida e eficaz.

Até 2030, esperamos que a maturidade em cibersegurança para OT tenha progredido significativamente nas empresas de serviços públicos e nas grandes organizações de manufatura transnacionais. Muitas organizações terão operações de segurança convergentes, que fornecem visibilidade em toda a empresa, com equipes dedicadas à OT, treinadas em processos e procedimentos. A segurança será cada vez mais gerenciada por plataformas em nuvem, seja pelos proprietários dos ativos ou por um provedor de serviços gerenciados, e haverá um foco crescente na gestão e proteção de redes 5G sem fio. Além disso, a WA também espera uma maior maturidade em cibersegurança da cadeia de suprimentos e uma base instalada maior de operações industriais construídas com base em princípios de segurança por design. Nesse contexto, é fundamental que os líderes de Segurança garantam que trabalhem com parceiros que tenham soluções para atender aos requisitos atuais e futuros da indústria.