SOPHOS

Os desafios da segurança cibernética no setor de manufatura

Analistas de ameaças especializados munidos da inteligência de ameaças líder mundial da Sophos ajudam você a identificar e responder a ameaças avançadas com maior rapidez, 24 horas por dia, 7 dias por semana.

A Indústria 4.0 e as "fábricas inteligentes" estão transformando o setor da manufatura. Sistemas de Controle Industrial (ICS) como SCADA, dispositivos Industrial IoT (IIoT), robótica e análises avançadas estão revolucionando a forma como as fábricas operam nos dias de hoje. Mas a transformação digital extensiva, a convergência da TI/OT e a baixíssima tolerância do setor a períodos de inatividade estão ampliando a superfície de ataque, aumentando os riscos de exploração de vulnerabilidades, vazamento de dados, sabotagem na produção etc. para os fabricantes.

A Sophos protege as organizações de manufatura contra uma avalanche de ataques, inclusive contra ameaças impostas por humanos e que a tecnologia por si só não consegue conter. Da detecção e resposta gerenciadas do MDR à segurança de endpoints e redes, a Sophos capacita os fabricantes a otimizarem suas defesas e liberar suas equipes de TI para que foquem nos negócios.

Documento técnico Sophos. Abril, 2023

Desafios da segurança cibernética na manufatura

Os desafios da segurança cibernética para o setor de manufatura continuam a evoluir devido à rápida digitalização e falta de padrões de segurança cibernética igualmente sofisticados, o que deixou os líderes de TI e OT despreparados para responder às novas ameaças cibernéticas. Além disso, as ameaças cibernéticas ao setor continuam a aumentar em volume e complexidade.

Uma pesquisa da Sophos de 2022 realizada com 419 profissionais de TI que trabalham no setor de manufatura e produção revelou que 55% das organizações foram atingidas por ransomware em 2021 – um aumento de 52% no índice de ataques de ransomware em comparação ao ano anterior.

O custo médio para remediar um ataque de ransomware chegou a US$ 1,23 milhão para os fabricantes. Além disso, um índice significativo de 77% dos entrevistados disseram que o ataque impactou sua capacidade de operar, enquanto 71% disseram que perderam negócios e receita.

Mas não se trata apenas de ransomware. O ambiente de TI da manufatura, de modo geral, se tornou ainda mais desafiador: no decorrer do ano, 61% das organizações relataram um aumento no volume de ataques, 66% relataram um aumento na complexidade dos ataques e 51% relataram um aumento no impacto dos ataques.

55 %
das organizações de manufatura atingidas por ransomware em 2021

$1,23M
custo médio para reparação após um ataque

>1 mês
10% das organizações de manufatura levaram mais de um mês para se recuperar após um ataque

77 %
das organizações de manufatura atingidas por ransomware disseram que o ataque impactou sua capacidade de operação

66 %
dos profissionais de TI no setor de manufatura observaram um aumento na complexidade dos ataques

59 %
dos dados recuperados pelas organizações de manufatura após pagamento do resgate

57 %
dos ataques na manufatura resultaram em dados criptografados

7 %
das organizações de manufatura recuperaram TODOS os dados após pagar o resgate

Fonte: pesquisa global da Sophos em O Estado do Ransomware 2022

Por trás dessas estatísticas, encontram-se várias mudanças no panorama das ameaças:

A profissionalização do crime cibernético
Um dos aspectos mais marcantes no último ano foi o desenvolvimento e a profissionalização do mercado de ameaças cibernéticas. Grupos criminosos se especializaram em componentes específicos de ataque, por exemplo, acesso inicial, ransomware, malware de roubo de informações, entre outras modalidades, oferecendo seus méritos profissionais a outros criminosos como um serviço. O modelo "as-a-service" diminui as competências exigidas para conduzir um ataque, aumentando o volume de adversários e ameaças.

Esses serviços especializados oferecem orientação e recursos de execução aos seus clientes do crime, o que aumenta a eficiência dos ataques. Para ilustrar esse ponto, em março de 2022, um associado do grupo Conti de ransomware-as-a-service publicou um arquivo que incluía uma riqueza de detalhes, diretrizes e informações documentados de modo a instruir um invasor "afiliado" sobre as etapas necessárias para realizar um ataque de ransomware.

Os invasores também adotam muitos dos comportamentos de provedores de serviços de TI legítimos, chegando, inclusive, a pedir às vítimas de ransomware que "avaliem seus serviços" assim que seus arquivos são descriptografados após o pagamento.

A evolução das táticas, técnicas e procedimentos dos invasores

Frequentemente, os adversários exploram as vulnerabilidades na postura de segurança das organizações na tentativa de evitar serem pegos pelas soluções de segurança. Isso inclui:

- **Explorar vulnerabilidades sem patches** – Esse foi o método mais utilizado pelos adversários para se infiltrar nas organizações, de acordo com os chamados a que a equipe de resposta a incidentes da Sophos respondeu no último ano, que foi constatado em 47% dos incidentes.
- **Explorar ferramentas de TI legítimas** – Muitas das ferramentas usadas pelos profissionais de TI também são usadas pelos adversários, incluindo PowerShell e PsExec, para explorar credenciais e dados de acesso roubados. Passando-se por usuários legítimos, os invasores esperam conseguir entrar no ambiente e contaminá-lo.

Os desafios à segurança cibernética para o setor não param por aí. As organizações de manufatura também têm que enfrentar as ameaças internas (tanto maliciosas como acidentais), os requisitos rígidos de conformidade regulatória e os riscos impostos por fornecedores terceirizados, entre outros desafios.

Sophos Security para o setor da manufatura

A Sophos oferece soluções avançadas de segurança cibernética que capacitam as organizações de manufatura a gerenciar e reduzir riscos cibernéticos. Nosso ecossistema de segurança cibernética adaptativa oferece um portfólio completo de produtos e serviços líder de mercado que elevam as defesas dos clientes contra as mais avançadas ameaças, tudo com o suporte inigualável da perícia do Sophos X-Ops em operações de segurança, IA e defesa contra ameaças.



A Sophos proporciona excelentes resultados em segurança cibernética a mais de **530.000 clientes** mundialmente.



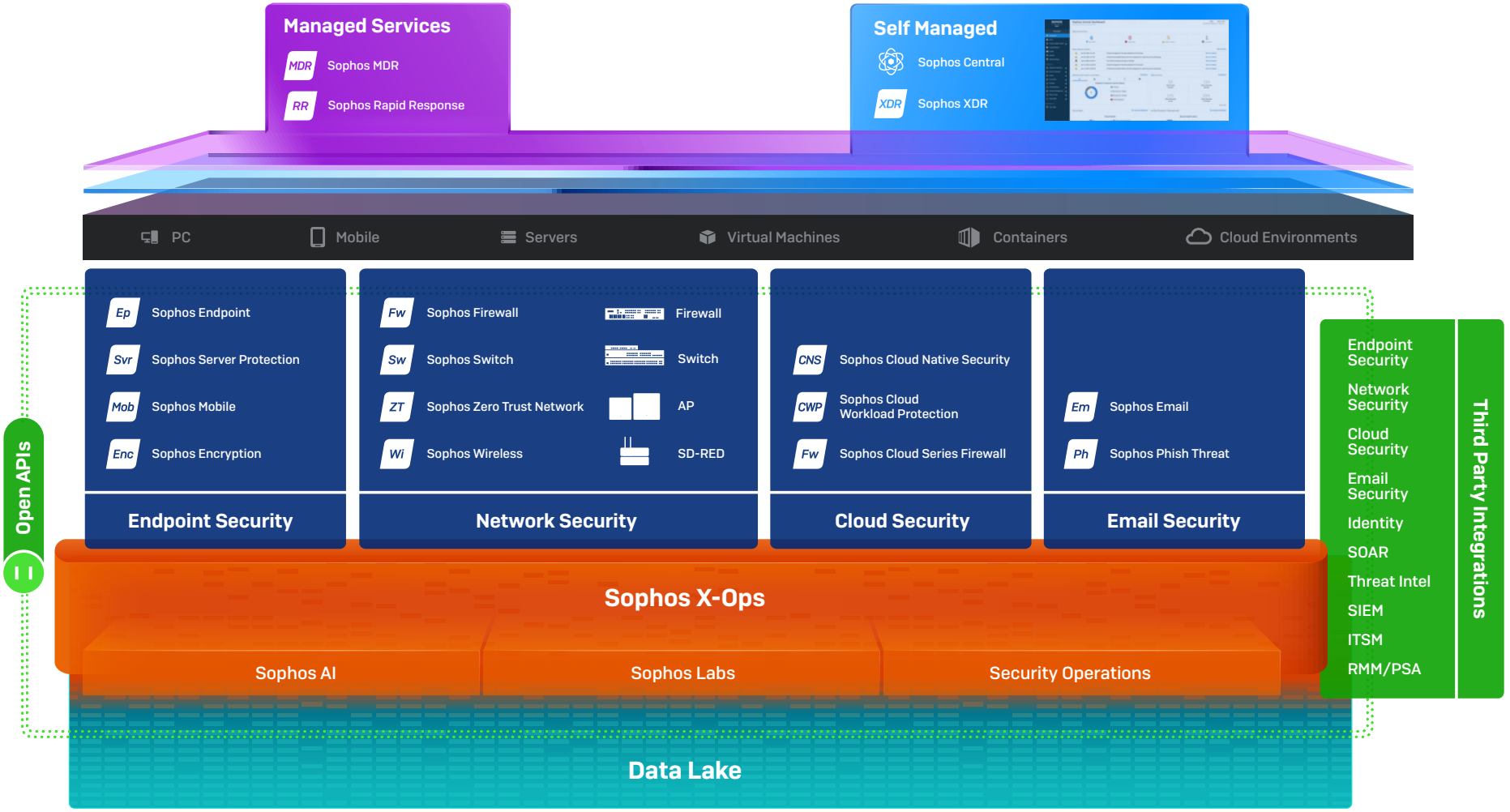
Nenhum fornecedor foi **reconhecido como Gartner Leader** em segurança de endpoint mais vezes do que a Sophos.



O Serviço de MDR, Endpoint e Firewall **mais bem contado** e **mais avaliado** na Gartner Peer Insights.

Em 1º de agosto de 2022

Ecossistema de Segurança Cibernética Adaptativa da Sophos



Casos de uso

A Sophos pode ajudar a lidar com os desafios da segurança cibernética mais comuns enfrentados pelas organizações de manufatura.

Bloqueando ataques avançados liderados por mãos humanas, incluindo ransomware

O Sophos MDR é um serviço totalmente gerenciado – 24 horas por dia, sete dias por semana – entregue por peritos especializados em detectar e responder a ataques cibernéticos que as soluções tecnológicas por si só não conseguem evitar. Nossa equipe de peritos bloqueia ataques avançados liderados por humanos para você, neutralizando as ameaças antes que elas possam causar interrupções em suas operações comerciais ou comprometer seus dados confidenciais.

"Com o Sophos MDR, reduzimos drasticamente o nosso tempo de resposta a ameaças."

Tata BlueScope Steel

"A capacidade do Sophos MDR em remediar e remover ameaças de modo rápido e nos manter informados nos deixa livres para focar em tarefas mais rentáveis."

Tomago Aluminium

"A Sophos libera as equipes de TI para que realizem tarefas mais proativas em vez de serem arrastadas para o gerenciamento dos desafios de segurança."

AG Barr

Com o Sophos MDR, nossos analistas especializados detectam e respondem a ameaças em minutos – trabalhando com a sua tecnologia de preferência – seja na resposta a incidentes de grande escala ou prestando assistência na tomada de decisões mais precisas.

Nós usamos:

- Soluções Sophos premiadas, incluindo nossa proteção de endpoint, firewall, nuvem e e-mail
- Produtos de outros fornecedores, como Microsoft, CrowdStrike, Palo Alto Networks, Fortinet, Check Point, Rapid7, Amazon Web Services (AWS), Google, Okta, Darktrace e muitos outros
- Combinações de nossas tecnologias com as tecnologias de outros fornecedores

O Sophos MDR protege a sua organização contra os ataques avançados que as soluções tecnológicas por si só não conseguem evitar, aumentando o retorno sobre os seus investimentos existentes. Na posição de provedor de MDR mais confiável do mundo, temos uma especialização profunda e abrangente incomparável para combater as ameaças enfrentadas pelo setor de manufatura. Aproveitando dessa telemetria extensiva, podemos gerar "imunidade comunitária", aplicando o aprendizado adquirido da defesa de um cliente do setor de manufatura aos outros clientes do setor e, assim, elevando as defesas de todos.

MAIS CONFIÁVEL	ALTA AVALIAÇÃO	MELHOR PROTEÇÃO
Provedor Nº 1	**4,8/5** Gartner Peer Insights	**38 min** para detectar, investigar e responder
A Sophos tem a confiança de mais organizações para serviços MDR do que qualquer outro provedor	Melhor classificação e mais avaliações em solução MDR, em 1º de agosto de 2022	Nossos analistas são 5 vezes mais velozes do que a mais rápida das equipes internas de SOC

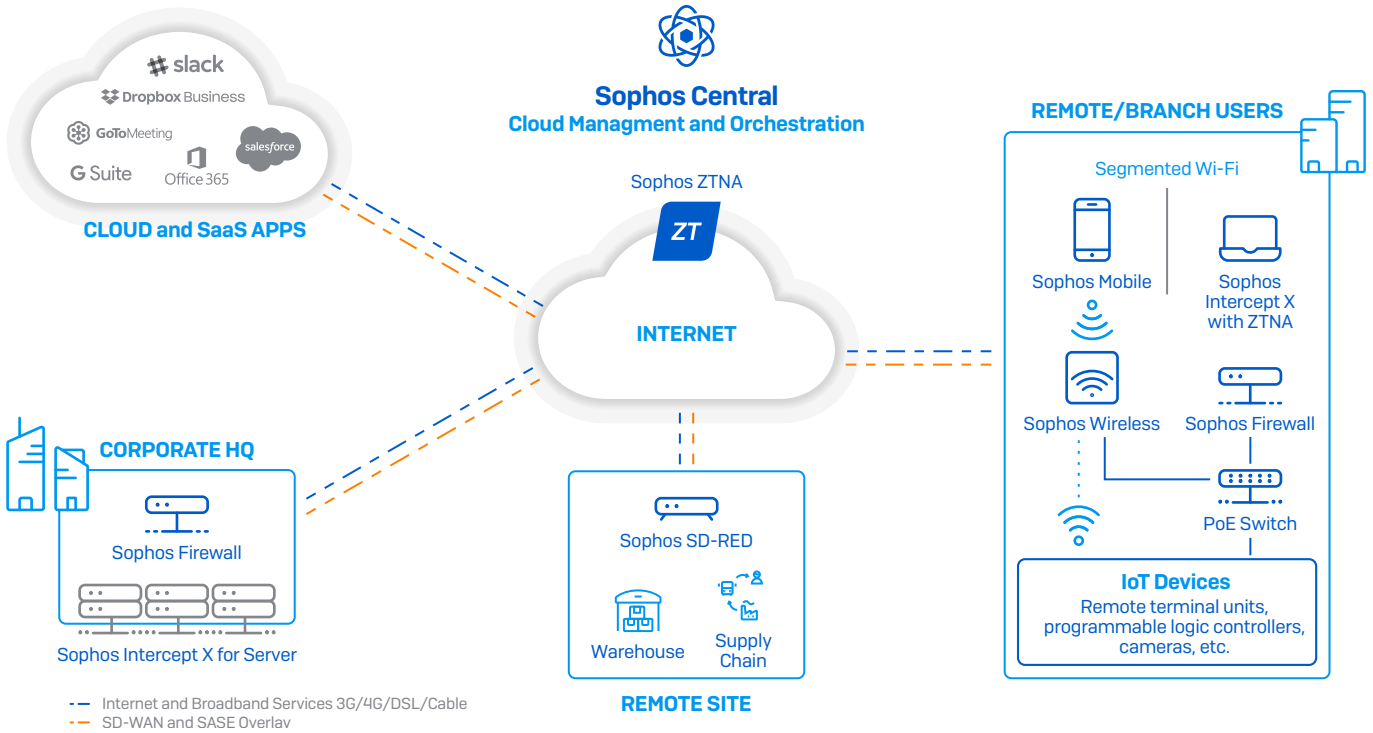
Em setembro de 2022

Protegendo o acesso a dados e sistemas de controle industrial críticos

Os fabricantes precisam adotar uma abordagem Zero Trust nos moldes "confie, mas confira" para garantir o acesso seguro a suas informações proprietárias críticas e também de infraestrutura. A solução Zero Trust Network Access da Sophos continuamente valida a identidade do usuário, a integridade do dispositivo e a conformidade geral antes de conceder acesso a seus dados e aplicativos.

O Sophos ZTNA blinda os seus sistemas RDP (Remote Desktop Protocol) – uma ferramenta comum para administradores e trabalhadores remotos, contudo também um dos vetores mais comuns de ataque pelos malfeitores – contra ataques e oferece acesso seguro apenas a usuários e dispositivos autorizados, incluindo as novas opções sem senha do Microsoft Windows Hello para Empresas que ajudam a proteger ainda mais as credenciais importantes contra possíveis comprometimentos.

Os fabricantes podem conectar dispositivos remotos e filiais em qualquer lugar, entregar aplicativos críticos SaaS e da nuvem, e compartilhar dados com segurança com o portfólio do Sophos Secure Access. Utilize o Sophos ZTNA para o acesso seguro a seus aplicativos, dispositivos Ethernet remotos do Sophos SD-RED para estender a sua rede a filiais e dispositivos remotos, pontos de acesso do Sophos Wireless para conexões de rede sem fio facilitadas e protegidas, e switches de camada de acesso de rede do Sophos Switch para o acesso seguro na LAN. Tudo gerenciado através do Sophos Central, a nossa plataforma de segurança unificada baseada na nuvem.



Protegendo sua rede

O Sophos Firewall oferece proteção poderosa contra as ameaças mais recentes, enquanto acelera o tráfego importante de aplicativos na nuvem, SaaS e SD-WAN. Condecorado com o título de Gartner Customers' Choice de Firewalls de Rede de 2022, o Sophos Firewall integra perfeitamente uma suíte completa de tecnologias de proteção contra ameaças que é fácil de configurar e manter.

A segmentação de rede é uma forma eficiente que as organizações de manufatura podem utilizar para reduzir sua exposição a riscos cibernéticos e voltar aos negócios rapidamente depois de uma violação da segurança. Por exemplo, a rede de TI de uma organização de manufatura pode ser segmentada da rede de OT para prevenir movimentação lateral e infecção lateral. O Sophos Firewall oferece opções de segmentação flexíveis e poderosas por meio de zonas e VLANs. Essas opções oferecem maneiras de separar os níveis de confiança em sua rede, ao mesmo tempo em que oferecem uma proteção adicional contra o acesso mais profundo à rede entre diferentes partes dela.

Você também pode segregar o tráfego no nível do switch, usando o Sophos Switch, que permite a você configurar as VLANs para segmentar o seu tráfego interno e reduzir a superfície de ataque no caso de uma violação de segurança ou infecção.

Protegendo contra ataques de phishing

Golpes de phishing – mais especificamente ataques de spear-phishing – são um dos caminhos mais fáceis dos invasores obterem acesso ao seu sistema e a suas valiosas informações.

Uma das melhores formas de acabar com os ataques de phishing é treinar os seus funcionários para que saibam reconhecer um golpe de phishing. O Sophos Phish Threat oferece um pacote com mais de 30 módulos de treinamento em conscientização em segurança para educar e testar seus usuários finais através de simulações automatizadas de phishing, treinamento e conscientização em qualidade e segurança, e métricas de relatórios acionáveis.

Permita que apenas remetentes de confiança ingressem na caixa de entrada de seus funcionários com o Sophos Email, que faz a varredura de todas as mensagens recebidas em busca de indicadores-chave de phishing, como falsificação de marca e tentativas de clonagem, em tempo real, usando técnicas de autenticação SPF, DKIM e DMARC e análise de anomalia de cabeçalho de e-mail. Isso ajuda a encontrar e bloquear e-mails de phishing antes que cheguem a seus usuários. Você também pode prevenir a perda de dados criando políticas DLP multirregras para grupos de usuários e usuários individuais para assegurar a proteção de dados confidenciais com a descoberta de informações proprietárias e conteúdo confidencial em todos os seus e-mails e anexos.

A maioria dos ataques de phishing infecta a sua rede através de artimanhas que levam os destinatários a clicar em links maliciosos que os levam a baixar malwares em seus dispositivos ou a dar acesso a dados confidenciais aos hackers. Para fortalecer a sua rede contra ataques de phishing, você deve fortalecer a sua segurança de endpoint. Obtenha proteção completa para todos os seus endpoints – Windows, Mac, Linux e máquinas virtuais – com o Sophos Intercept X Endpoint, a nossa solução EDR líder de mercado.

Para otimizar suas defesas, você precisa de proteção em camadas: vários recursos de segurança sofisticados, com cada um assumindo o seu papel na defesa contra ataques avançados. O Sophos Endpoint vem com várias camadas de proteção, incluindo:

- Proteção contra roubo de credenciais, que previne o acesso não autorizado ao sistema.
- Proteção contra explorações para interromper as técnicas usadas pelos adversários.
- Proteção contra ransomwares, que identifica e bloqueia tentativas de criptografia maliciosa.
- Proteção contra adulterações, que impede que os adversários desativem as suas defesas para poderem implantar as cargas nocivas deles.

A combinação de várias camadas de tecnologias de proteção nos permite otimizar as defesas de nossos clientes. Comprovando a qualidade de nossas defesas – e o poder da proteção em camadas –, bloqueamos, de antemão, 99,98% das ameaças (pontuação média da AV-TEST), e, recentemente, recebemos pontuação perfeita em proteção de endpoint nos relatórios da SE Labs.

Protegendo a Propriedade Intelectual (PI) contra roubo

Propriedade intelectual (PI) inclui informações cruciais mantidas pelos fabricantes que os ajudam a se manterem competitivos. Informações confidenciais como design de produtos, fórmulas, patentes em processo e outros know-hows exclusivos de uma organização de manufatura são alvos atraentes para os criminosos cibernéticos, concorrentes e ex-funcionários, pois lhes dão acesso imediato a informações críticas sem que precisem investir tempo e dinheiro em P&D. Para os fabricantes, o roubo de PI pode se converter em grandes perdas comerciais e por vezes até mesmo no término de suas operações.

Defenda seus dados e sua propriedade intelectual treinando seus funcionários a distinguirem possíveis ameaças e crie uma cultura positiva de conscientização sobre segurança na sua organização com simulações automatizadas e treinamento em conscientização sobre segurança com o Sophos Phish Threat.

Mantenha o controle absoluto sobre quem pode acessar dados na sua rede com o Sophos ZTNA. Você pode estabelecer controles granulares para bloquear movimentos laterais internos e assegurar que apenas pessoal autorizado tenha acesso a seus dados confidenciais.

Corrija vulnerabilidades conhecidas e bloqueie ameaças cibernéticas recentes, como ransomwares, ataques sem arquivo, exploits e malwares, em todos os seus dispositivos de endpoint com a proteção de endpoint do Sophos Intercept X. Nossas funcionalidades DLP de prevenção de perda de dados identificam seus dados confidenciais e previnem vazamentos por e-mail, uploads e cópias locais.

Previna violações de dados com o Sophos Email, que lhe permite criar políticas DLP multirregras para usuários para assegurar a proteção de dados confidenciais com a descoberta de conteúdo confidencial em todos os seus e-mails e anexos. Ele também criptografa seus dados confidenciais para interromper as violações.

Protegendo contra ataques internos

O risco de pessoal interno com acesso autorizado a dados proprietários ou controles de operações críticas de manufatura utilizar indevidamente seus privilégios ou violar a confiabilidade do fabricante é uma séria ameaça que o setor de manufatura têm que lidar. O roubo de segredos comerciais, a sabotagem de processos de fabricação ou danos aos equipamentos por meio do acesso remoto são algumas das ameaças impostas por funcionários internos.

Obtenha insights dos usuários e aplicativos que impõem maior risco para assegurar que as suas políticas sejam aplicadas antes que a sua segurança seja comprometida com a inteligência acionável do Quociente de Ameaça de Usuários (QAU) da Sophos. Eleve o seu nível de proteção com o Sophos Firewall, que protege dados sigilosos contra divulgações acidentais e maliciosas usando um controle de políticas completo que administram categorias da web, aplicativos, mídias removíveis e dispositivos móveis usados na sua rede. Ele conscientiza os usuários de todas as áreas do firewall com políticas de acesso baseado no usuário, através da modelagem de tráfego (QoS), e outros recursos de rede, independentemente do endereço IP, localização, rede ou dispositivo.

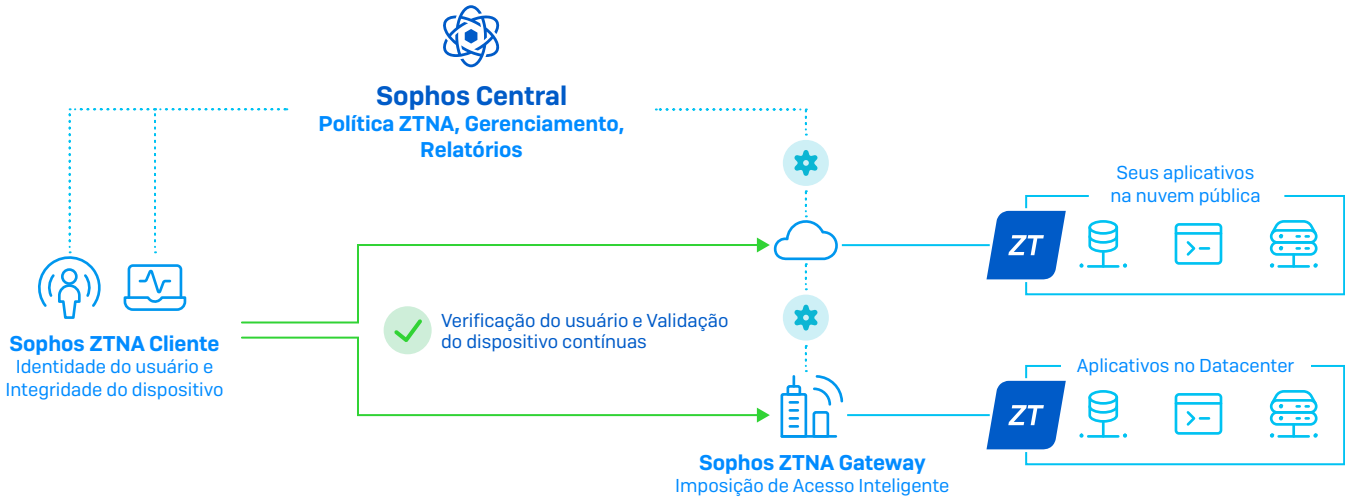
Reduzindo os riscos à cadeia de suprimentos

As cadeias de suprimentos de manufatura são vastas e complexas. Uma vulnerabilidade na rede de um único fornecedor pode se propagar rapidamente e infectar vários outros fornecedores e empresas.

Use IA, prevenção contra exploits, proteção comportamental e outras tecnologias avançadas do Sophos Intercept X para se defender contra ameaças que se infiltram nos fabricantes através de fornecedores terceirizados. Além disso, nossa poderosa funcionalidade XDR permite identificar automaticamente atividades suspeitas, priorizar indicadores de ameaças e fazer uma busca rápida de possíveis ameaças em todos os seus endpoints e servidores.

Obtenha 24 horas de suporte diário, sete dias por semana, com mais de 500 especialistas que trabalham para você sem parar na busca, validação e remediação de possíveis incidentes ou ameaças às cadeias de suprimentos com o Sophos MDR.

Proteja-se contra ataques a cadeias de suprimentos que se fiam no acesso do fornecedor aos seus sistemas utilizando controles de acesso granulares com o ZTNA, que autentica as solicitações de parceiros confiáveis, independentemente do local onde se encontrem. A integração entre o Sophos Endpoint e o Sophos ZTNA previne automaticamente que hosts comprometidos se conectem aos seus recursos de rede, evitando que as ameaças se movam lateralmente pela sua rede e nela se instalem.



Protegendo equipamentos legados

Os fabricantes devem proteger seus processos e sistemas de controle legados e com patches desatualizados das vulnerabilidades conhecidas. Esses dispositivos geralmente têm sistemas operacionais desatualizados ou navegadores que não podem ser atualizados simplesmente porque não recebem mais suporte, mas que, mesmo assim, precisam estar conectados à rede.

O Sophos Firewall e o Sophos SD-RED podem ajudar. Coloque o SD-RED na frente de um dispositivo exposto e ele encapsulará todo o tráfego para o Sophos Firewall para realizar uma varredura de proteção. Se a sua rede for simples, você provavelmente terá que fazer alterações nos esquemas de endereço IP e talvez mudar de topologia – e o nosso pessoal técnico especializado poderá tratar da sua situação e lhe mostrar o caminho que você deve seguir.

Segurança de dados em ambientes de manufatura multinuvem

A nuvem está empoderando as fábricas inteligentes. A adoção da nuvem permite que os fabricantes modernos reúnam os dados das máquinas em tempo real diretamente do chão de fábrica e convertam esse grande volume de dados em inteligência empresarial para ajudar na otimização do processo, apontar ineficiências e ressaltar modos de operar de modo mais sustentáveis. Contudo, a nuvem é um alvo rentável para os criminosos cibernéticos que buscam explorar práticas de segurança cibernética menos estabelecidas do que as práticas aplicadas nos ambientes locais mais tradicionais.

O Sophos Cloud Native Security oferece cobertura de segurança completa a ambientes, cargas de trabalho e identidades multinuvem. Ele protege a infraestrutura da sua rede e os seus dados com a segurança de carga de trabalho de host e contêiner flexível para Windows e Linux. Tecnologias multicamada protegem contra ransomware e outros ataques avançados, incluindo detecções comportamentais nativas na nuvem e em tempo de execução de exploits que identificam ameaças como escapes de contêiner, exploits de kernel e tentativas de escalonamento de privilégios. Além disso, isso facilita controlar os seus gastos com a nuvem. Você pode identificar rapidamente se a sua conta está sendo usada indevidamente e ejetar os adversários antes que os custos cheguem às alturas.

Conclusão:

Ataques cibernéticos como ransomwares, exploits e phishing podem ter sérias consequências para os negócios e a reputação dos fabricantes. Proteger os seus ambientes de TI e dados confidenciais exige uma abordagem de segurança integrada.

A Sophos protege seus sistemas e dados onde quer que residam com os nossos serviços e tecnologias Next-Gen, e permite a você consolidar o gerenciamento da sua segurança reunindo tudo em torno de um único fornecedor. Todas as soluções da Sophos são controladas através de um painel de gerenciamento unificado na nuvem, o Sophos Central, que permite compartilhamento de informações entre produtos em tempo real, gerenciamento centralizado, resposta automatizada a incidentes e insights profundos – tudo isso trabalhando em conjunto aumenta ainda mais a sua proteção ao mesmo tempo em que melhora a eficiência da sua equipe de TI.

Para saber mais sobre como a Sophos protege as organizações de manufatura e tratar dos seus requisitos, entre em contato com o seu representante da Sophos ou solicite a ligação de um de nossos especialistas.

A Gartner não endossa fornecedores, produtos ou serviços representados em suas publicações de pesquisa e não faz sugestões a usuários de tecnologias para selecionarem apenas fornecedores com as mais altas pontuações ou outros reconhecimentos. As publicações de pesquisas da Gartner consistem em opiniões da organização de pesquisa e consultoria da Gartner (Research & Advisory) e não devem ser interpretadas como uma declaração de fato. A Gartner se isenta de toda e qualquer garantia, expressa ou implícita, em respeito a essa pesquisa, incluindo garantias de comercialização ou de um propósito de uso específico.

GARTNER é marca registrada e marca de serviço da Gartner, Inc. e/ou de suas afiliadas nos EUA e internacionalmente, e MAGIC QUADRANT e PEER INSIGHTS são marcas registradas da Gartner, Inc. e/ou de suas afiliadas, que são utilizadas aqui com permissão. Todos os direitos reservados.
O conteúdo do Gartner Peer Insights consiste em opiniões de usuários finais individuais baseadas em suas próprias experiências com fornecedores listados na plataforma e não deve ser interpretado como uma declaração de fato nem como representação da visão da Gartner ou de suas afiliadas. A Gartner não endossa fornecedores, produtos ou serviços representados neste conteúdo nem estabelece qualquer garantia, expressa ou implícita, em respeito a este conteúdo, sua precisão ou completude, incluindo garantias de comercialização ou de um propósito de uso específico.

© Copyright 2023. Sophos Ltd. Todos os direitos reservados.
Empresa registrada na Inglaterra e País de Gales sob o nº. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Reino Unido
A Sophos é marca registrada da Sophos Ltd. Todos os outros nomes de produtos e empresas mencionados são marcas comerciais ou marcas registradas de seus respectivos proprietários.

2023-04-05 EN-WP (NP)

SOPHOS