SOPHOS
Cybersecurity evolved.

Protegendo a Organização Global

Qualquer lugar. Qualquer dispositivo. Qualquer recurso.

Documento técnico Sophos Fevereiro de 2021

O trabalho remoto chegou para ficar: de acordo com a Gartner, 74% das organizações esperam que alguns de seus funcionários trabalhem remotamente quando a pandemia acabar[1]. Consequentemente, os recursos que as pessoas precisam para desempenhar suas tarefas também estarão em vários lugares: servidores no escritório, aplicativos na nuvem, como o Office 365 ou o Salesforce, e ambientes de rede privada ou pública no Amazon Web Services (AWS) e Microsoft Azure.

As equipes de TI têm a tarefa de proteger cada usuário e cada recurso onde quer que estejam. Enquanto isso, os agentes de ataque continuam a encontrar novos meios, melhores e mais subversivos, de penetrar nas organizações virtuais a cada interseção.

Proteger as organizações onde pessoas e recursos podem estar em qualquer lugar requer:

- Conectividade segura, de modo que os usuários possam acessar recursos em qualquer lugar: de casa, do cliente ou do escritório
- Proteção dos dispositivos usados para fazer essas conexões: computadores desktop, notebooks, telefones móveis e tablets
- Proteção de dados e cargas de trabalho que os usuários precisam acessar, estejam eles na nuvem ou na sua rede local
- Gerenciamento simplificado, de modo que as equipes de TI possam gerenciar organizações distribuídas de qualquer lugar, sem aumentar suas cargas de trabalho

Felizmente, a Sophos atende a todas essas áreas. Oferecemos um portfólio completo de produtos de segurança Next Gen com capacidade de proteção avançada. Tudo é controlado através de uma única plataforma de segurança na web que reduz o encargo da administração diária e capacita as equipes de TI para gerenciar a segurança de suas organizações de qualquer lugar.

Essa descrição da solução demonstra como a Sophos trata cada um desses requisitos. Também explora seus benefícios de produtividade e proteção ao empregar o sistema de segurança cibernética da Sophos para proteger a sua organização.

Conexão segura

Não há dúvida de que a pandemia da COVID levou a um aumento gigantesco no trabalho remoto. Durante maio de 2020, 62% dos funcionários nos EUA trabalharam de casa. Contudo, o trabalho remoto já era uma tendência mesmo antes do surto da COVID, e muitos funcionários de escritório já estavam fazendo a transição para o trabalho de casa alguns dias por semana. No Reino Unido, o trabalho remoto subiu para uma taxa de 74% na última década, enquanto na Austrália cerca de um terço da força de trabalho já trabalhava de casa.

O trabalho remoto é incrivelmente benéfico para empresas e funcionários: os funcionários economizam tempo e dinheiro de locomoção a seus ambientes de trabalho enquanto podem desfrutar de flexibilidade e maior produtividade, e as organizações reduzem custos e taxas de rotatividade de funcionários. Mas para as equipes de TI, o trabalho remoto em longo prazo cria desafios adicionais de segurança. Estejam eles conectados da sala de estar, em visita a um cliente ou tomando um café em um dos milhares de hotspots Wi-Fi a milhares de quilômetros de distância, seus funcionários precisam que a sua rede e os seus dados permaneçam protegidos o tempo todo.

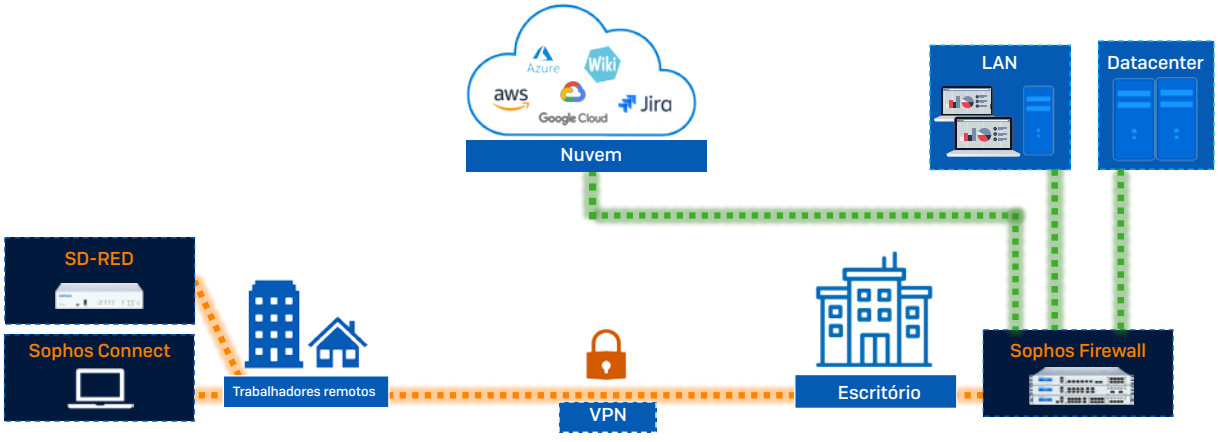
Com a Sophos, seus funcionários podem se conectar com rapidez, eficiência e segurança e trabalhar de qualquer lugar no globo – e oferecemos opções de acesso por VPN tradicional e também por Zero Trust Network Access (ZTNA).

VPN

Use o nosso **cliente Sophos Connect VPN** de implantação fácil e gratuita em conjunto com o **Sophos Firewall** para conectar trabalhadores remotos ao escritório central e a seus recursos na nuvem. Com mais de 1,4 milhão de usuários mundialmente, o Sophos Connect oferece aos usuários remotos o acesso seguro a recursos na rede corporativa ou na rede pública a partir de dispositivos Windows e macOS.

Para proporcionar o melhor em conectividade remota, o **Sophos SD-RED** (Remote Ethernet Device) oferece um dispositivo com a simplicidade plug-and-play que funciona com o **Sophos Firewall** para conectar filiais, localidades remotas e indivíduos à sua rede principal (seja física ou na nuvem).

Isso proporciona uma VPN dedicada AlwaysOn ou com encapsulamento dividido que é fácil de implantar e gerenciar com opções flexíveis. Ela é também bastante pequena e portátil, tornando-a ideal para gerentes de alto escalão e outras pessoas que precisam de acesso a uma conexão segura a qualquer hora, de qualquer lugar.



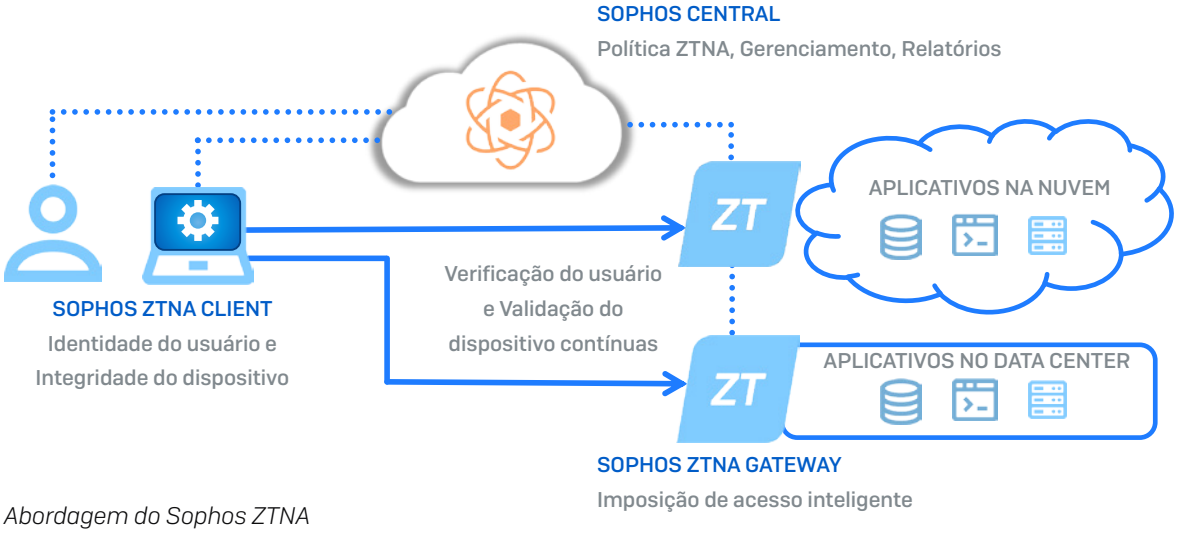
Conectividade remota segura com o Sophos Firewall e o Sophos Connect VPN e SD-RED

ZTNA

Por anos, a tecnologia VPN tem capacitado os trabalhadores para se conectarem remotamente com grande sucesso. Ela foi a grande salvadora no início da pandemia, permitindo que as organizações se voltassem rapidamente para o trabalho remoto seguro em apenas alguns dias. Contudo, muitas organizações estão começando a exigir mais do que a VPN foi desenvolvida para oferecer.

O **Sophos Zero Trust Network Access (ZTNA)** é uma excelente alternativa para a VPN de acesso remoto, possibilitando que os usuários se conectem a recursos corporativos de qualquer lugar de um modo simples e transparente. Ao mesmo tempo, ele também aumenta a sua segurança por meio da constante verificação do usuário — geralmente com autenticação multifator e um provedor de identidade — e validação da integridade e conformidade do dispositivo.

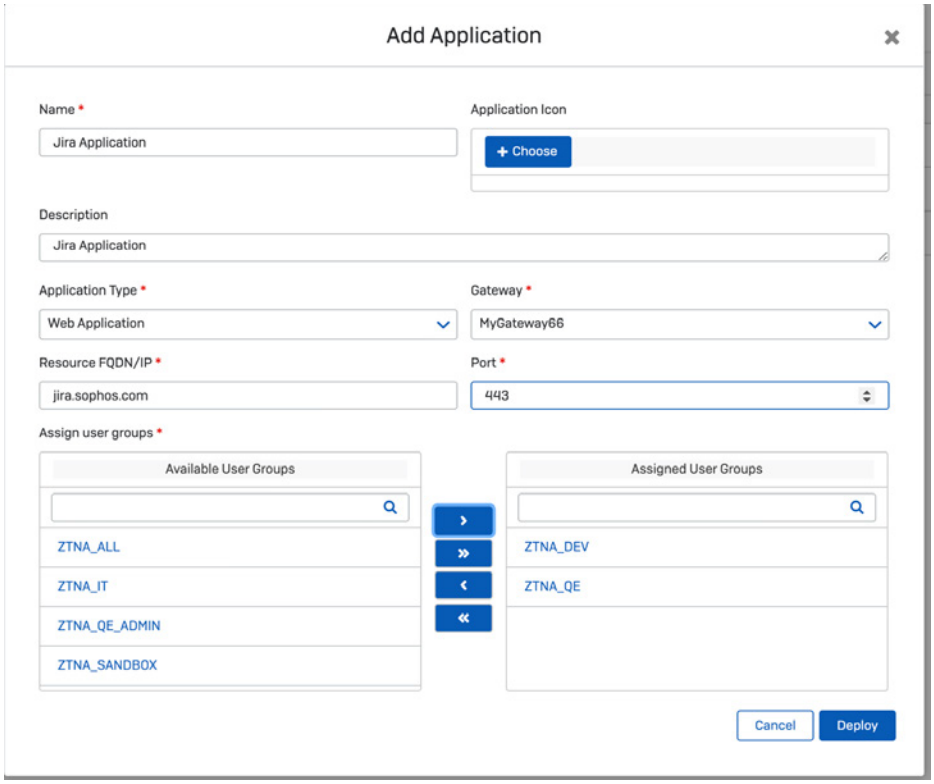
O Sophos ZTNA garante que o seu dispositivo esteja registrado, atualizado, adequadamente protegido e com criptografia habilitada. Ele usa essas informações para tomar decisões baseadas em políticas personalizadas e determinar o acesso e o privilégio dos usuários a seus aplicativos críticos na rede.



Abordagem do Sophos ZTNA

Com o Sophos ZTNA você pode:

- Melhorar as suas defesas cibernéticas. O Sophos ZTNA oferece controles granulares: qualquer usuário, qualquer dispositivo ou qualquer aplicativo pode ser controlado individualmente baseado na política da corporação e no nível de risco em que você esteja confortável. Isso também elimina o conceito da confiança implícita em um indivíduo com base em sua presença na rede, elevando a proteção e minimizando o risco de movimentos laterais internos dentro da rede ao avaliar continuamente a identidade e a integridade do dispositivo antes de permitir o acesso.
- Aumentar a eficiência. Como o Sophos ZTNA é gerenciado por meio da plataforma Sophos Central, fica mais fácil registrar novos usuários ou apoiar um ambiente de trabalho dinâmico. Além disso, fica mais transparente para os usuários finais, proporcionado uma experiência de conexão do tipo que "simplesmente funciona" quando comparada com a VPN.



Adicione aplicativos com facilidade com o Sophos ZTNA

Seja qual for o seu método escolhido, os produtos de segurança premiados da Sophos ajudarão a proteger seus funcionários em qualquer lugar e em qualquer dispositivo.

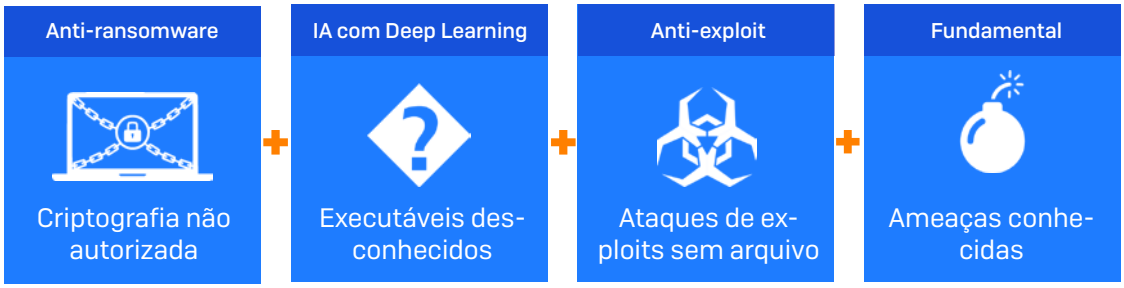
Proteger dispositivos

Entre os respondentes, 51% deles foram atingidos por ransomware no último ano, e os invasores criptografaram dados com êxito em 73% dos ataques[2].

Some essas estatísticas alarmantes com a necessidade de proteger todo e qualquer tipo de equipamento – computadores desktops, notebooks, dispositivos corporativos e pessoais – e uma grande variedade de sistemas operacionais – do Windows, macOS, Linux, Android, Chromebook e iOS – e você terá uma fórmula explosiva para dores de cabeça cibernéticas.

O **Sophos Intercept X** oferece a melhor proteção do mundo a todos esses dispositivos e plataformas. Você se beneficia das múltiplas camadas de tecnologia que barram os invasores em pontos variados na estrutura kill chain, incluindo:

- Proteção contra ransomwares, que impede a criptografia não autorizada de arquivos, discos rígidos e registros de boot, retornando-os a um estado seguro
- IA com Deep Learning, que utiliza milhões de atributos de arquivo para analisar ameaças e prevenir malwares conhecidos e ainda inéditos, barrando-os antes que possam ser executados
- Tecnologia Anti-Exploit, para bloquear explorações de vulnerabilidades, técnicas de adversários ativos, e ataques sem arquivo e baseados em script
- Proteção básica baseada em assinatura, que interrompe as ameaças conhecidas



Além disso, o Sophos Intercept X protege qualquer dispositivo em qualquer plataforma – desse modo, seus funcionários podem trabalhar com segurança nos dispositivos de sua escolha:

- Computadores desktops e notebooks com Windows e macOS
- Servidores Windows ou Linux
- Ambientes desktop virtuais hospedados em provedores de nuvem
- Dispositivos móveis com Android, iOS ou Chromebook

Endpoint Detection and Response (EDR)

Os ataques virtuais mais devastadores envolvem ataques conduzidos por pessoas que frequentemente exploram ferramentas e processos legítimos como o PowerShell. Os hackers dinâmicos conseguem burlar protocolos e produtos de segurança ao modificar suas táticas, técnicas e procedimentos (TTPs). Uma vez que estejam dentro da sua rede, os invasores podem se mover internamente para exfiltrar dados, implantar ransomwares e instalar malwares e backdoors para futuros ataques.

Para parar esses ataques conduzidos por humanos é preciso caça a ameaças conduzida por humanos. **Intercept X with EDR** (Endpoint Detection and Response) oferece as ferramentas que você precisa para desempenhar a caça a ameaças no mesmo painel de controle usado para gerenciar a sua proteção de endpoint Intercept X.

O primeiro ERD desenhado para analistas de segurança e administradores de TI. Enquanto outras ferramentas de EDR exigem pessoal dedicado ou um centro de operações de segurança (SOC), o Sophos EDR é simples de usar sem sacrificar sua capacidade de desempenhar análises robustas.

Com o Intercept X with EDR, você pode investigar indícios suspeitos e ameaças – e melhorar a sanitização da sua TI – com as poderosas consultas SQL personalizáveis. Casos de uso comuns incluem:

- Lentidão de execução do Chrome. Identificar quais extensões do Chrome não autorizadas foram instaladas
- Verificação de atividade da rede. Procurar tentativas malsucedidas de login e comunicação ativa do PowerShell
- Consultas de software. Verificar se arquivos confidenciais foram removidos de dispositivos e/ou se você não excedeu o uso da licença de software
- Investigação de phishing. Identificar usuários que clicaram em um link suspeito e se baixaram arquivos

Além disso, você pode acessar dispositivos remotamente usando uma ferramenta de linha de comando para resolver problemas, como reinicializar dispositivos, encerrar processos ativos, executar scripts ou programas, editar arquivos de configuração, executar ferramentas forenses e instalar/desinstalar softwares.

Managed Detection and Response (MDR)

Se você não tem tempo, capacidade ou expertise para sair no encalço de ameaças e fazer a sua própria investigação, o **Sophos Managed Threat Response** (MTR) está aqui para ajudar.

O Sophos MTR é uma equipe de caçadores de ameaças e especialistas em resposta que oferece 24 horas de monitoramento, detecção e resposta a ameaças, sete dias por semana, nos moldes de um serviço totalmente gerenciado. Eles caçam ameaças de forma proativa, validando ameaças e incidentes potenciais – e bloqueando-os antes que causem danos.

Também correlacionam feeds de dados de suas soluções de proteção Sophos para identificar indicadores de comprometimento. Diferentemente de outros serviços de detecção e resposta gerenciados, a Sophos não apenas notifica você sobre os problemas – nós também determinamos e aplicamos as ações mais apropriadas para neutralizar a ameaça.

Dispositivos móveis

Quando os funcionários utilizam dispositivos pessoais para trabalhar, as equipes de TI se deparam com o desafio de proteger os dados da empresa sem comprometer a privacidade do usuário. A nossa solução unificada de gerenciamento de endpoint, o **Sophos Mobile**, protege dispositivos com iOS, Android, Chrome OS, Windows 10 e macOS. Com ela, você protege qualquer combinação de dispositivo pessoal e propriedade corporativa com o mínimo de esforço – ideal para ambientes BYOD, em que os usuários usam seus próprios equipamentos para trabalhar.

Com o Sophos Mobile, você está capacitado para:

- Interromper ameaças a dispositivos móveis. Obtenha defesa líder do setor contra ataques de malware, phishing, man-in-the-middle e outros tipos a dispositivos móveis, tudo com o poder do Intercept X
- Proteger dados corporativos. Opte pelo gerenciamento completo ou apenas de contêiner de acordo com as suas necessidades
- Reduzir o encargo de administração. A flexibilidade do portal de autoatendimento permite que os usuários registrem seus dispositivos móveis pessoais com macOS ou Windows 10, redefinam senhas e obtenham ajuda, tudo sem o envolvimento do departamento de TI

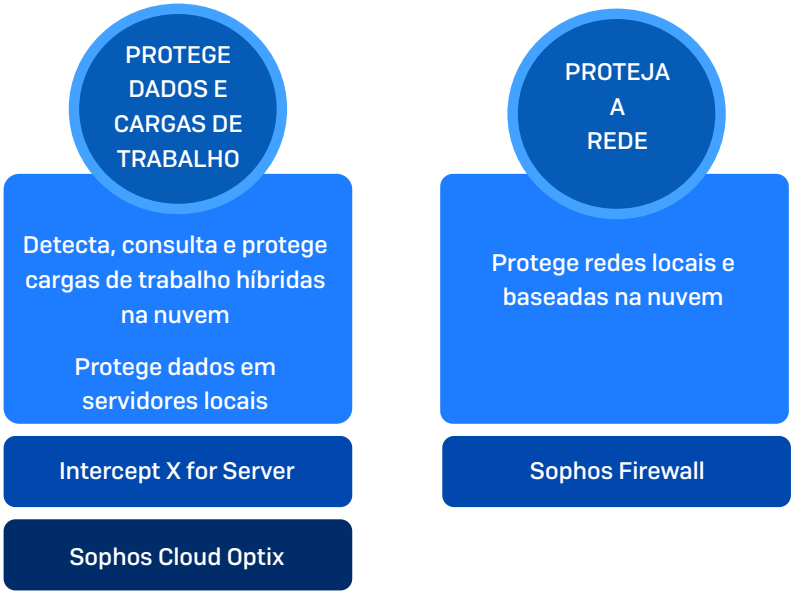
Recursos de segurança

Conforme as necessidades da sua organização, você talvez tenha servidores instalados localmente, consumindo aplicativos baseados na nuvem; ou talvez esteja hospedando recursos em ambientes de nuvem pública ou privada no AWS, Azure ou GCP. Muito provavelmente você está fazendo tudo isso.

A nuvem está rapidamente se tornando cada vez mais essencial para as operações diárias das organizações. Com isso, os criminosos virtuais estão sempre alertas na busca das oportunidades que a nuvem oferece – tanto que 70% das empresas que usam nuvem pública passaram por um incidente de segurança nos últimos 12 meses[3].

Quando se trata de proteger os seus recursos, onde quer que estejam localizados, você precisa de duas coisas:

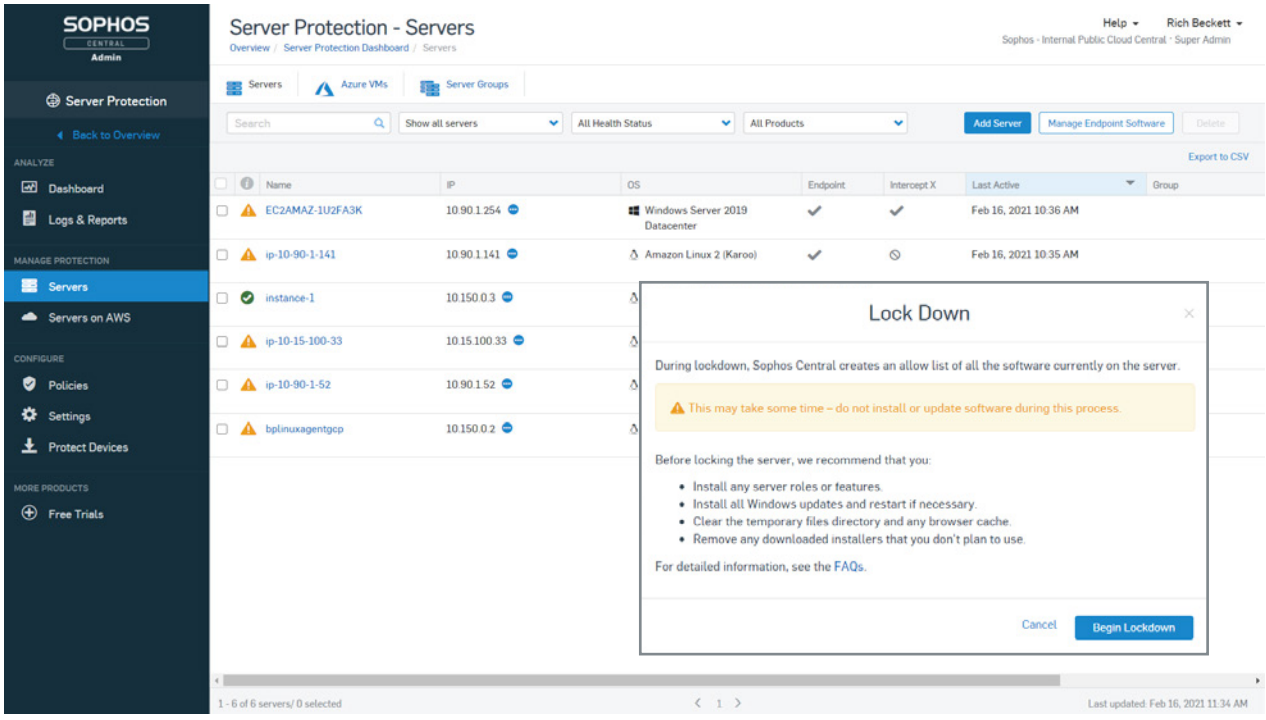
1. Proteger os dados e as cargas de trabalho
2. Proteger a rede onde se encontram, para manter os invasores afastados



Protegendo seus dados e cargas de trabalho

Seus dados e cargas de trabalho são os seus ativos mais importantes. O **Sophos Intercept X for Server** protege ambientes de carga de trabalho na nuvem, no local ou híbridos. Ele protege computadores virtuais e máquinas virtuais Windows e Linux contra as ameaças mais recentes.

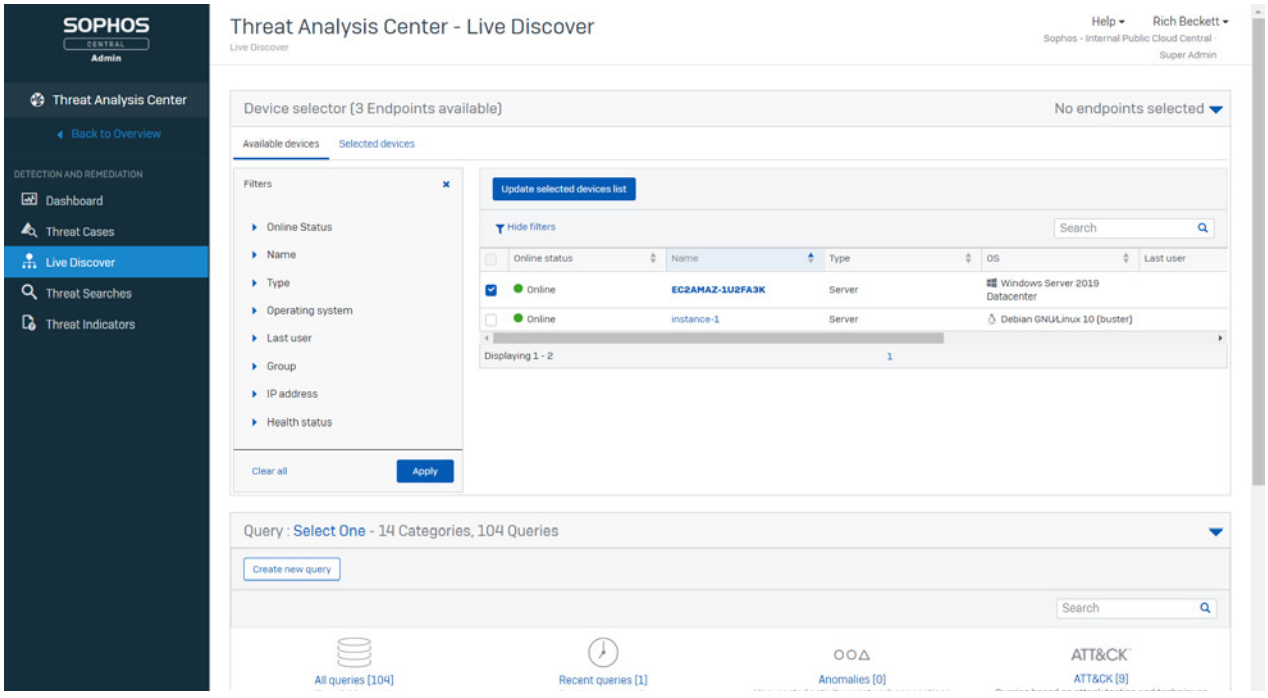
- Detenha ataques avançados. Incluindo ransomwares, ataques baseados em exploit e malwares nunca antes vistos
- Bloqueie suas cargas de trabalho no servidor. Controle o que pode e não pode ser executado e receba notificações sobre tentativas de alteração não autorizadas
- Gerencie tudo de modo centralizado. Implante e mantenha tudo a partir de um único painel de controle, com cenários mistos que incluem cargas de trabalho na nuvem e em servidores locais



Intercept X for Server

Você também pode estender suas investigações EDR a seus servidores, estejam eles no local ou na nuvem, com o **Intercept X for Server with EDR**. Isso o capacita a:

- Desempenhar operações de TI críticas e tarefas de caça a ameaças. Identifique problemas de desempenho, veja o que está instalado onde e saia no encalço de atividades suspeitas
- Detectar automaticamente cargas de trabalho na nuvem. Fique de olho em serviços críticos na nuvem, incluindo buckets S3, bancos de dados e funções sem servidor
- Detectar implantações inseguras. Conte com o monitoramento de IA constante dos seus ambientes de nuvem e notificação de irregularidades



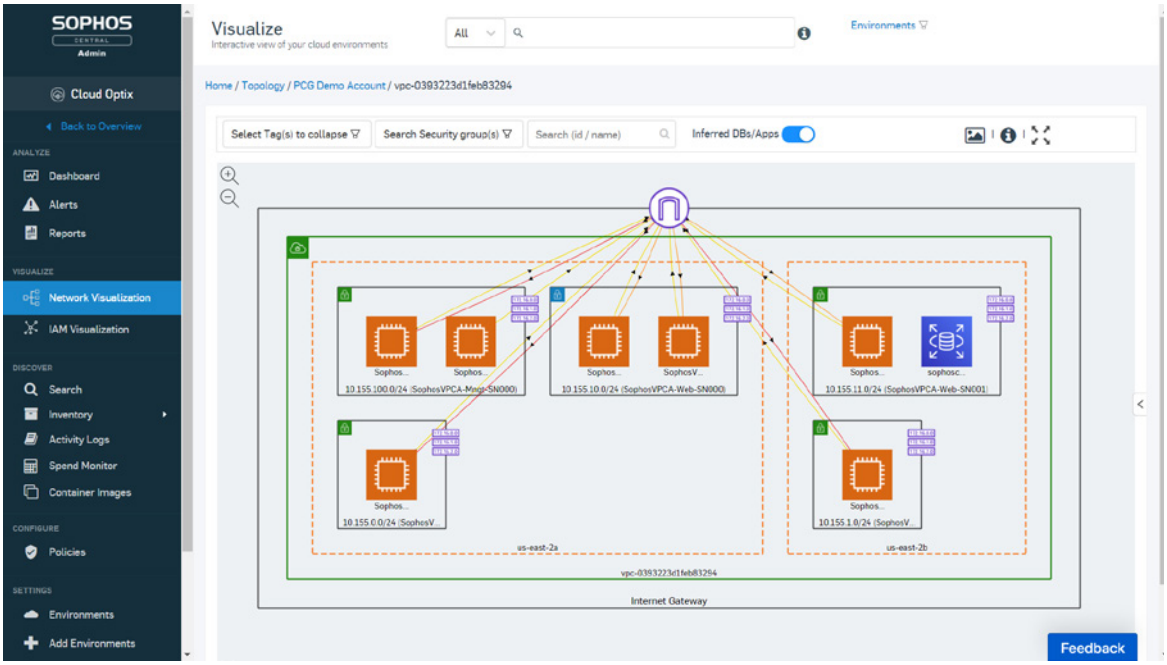
Estenda suas investigações EDR para o seu servidor

Proteção é um lado da moeda quando se trata de proteger dados e cargas de trabalho. Visibilidade é o outro.

Você precisa de uma linha de visão clara e contínua sobre o que está sendo executado e a sua capacidade de configurar serviços de provedores de nuvem para evitar brechas na segurança.

O **Sophos Cloud Optix**, nossa solução de Gerenciamento de Postura de Segurança na Nuvem, oferece a visibilidade que você precisa para proteger a sua organização, incluindo:

- Visibilidade multinuvem. Inventários detalhados de recursos na nuvem, incluindo servidores, contêineres, armazenamento, rede e IAM para AWS, Azure e GCP
- Priorização baseada em risco. Análise contínua de configurações em busca de riscos de segurança e acesso IAM superprivilegiado
- Gerenciamento de conformidade. Monitoramento de conformidade ininterrupto, com modelos prontos para usar, políticas personalizadas e ferramentas de colaboração
- Segurança integrada. Identificação do Sophos Firewalls e proteção de cargas de trabalho no AWS
- Otimização de custos da nuvem. Gerenciamento de gastos do AWS e Azure em uma única tela



Sophos Cloud Optix

Enquanto os alertas de segurança são úteis para os seus ambientes de nuvem com serviços como o Amazon GuardDuty, que oferece excelente valor, também fica mais fácil você se perder em meio ao alto volume de notificações. Isso pode tornar quase impossível reconhecer quais notificações realmente precisam ser atendidas.

Na Sophos, nós usamos o Sophos Cloud Optix para proteger os ambientes do Amazon Web Services usados para hospedar o Sophos Central, a nossa plataforma de segurança cibernética. Um dos maiores benefícios que a nossa própria equipe de segurança obteve com o Cloud Optix foi a habilidade de se concentrar no que é realmente importante.

"Com o Sophos Cloud Optix, nós minimizamos muito a exaustão dos alertas. A poderosa inteligência artificial incorporada no Sophos Cloud Optix correlaciona os dados e nos mostra o que é verdadeiramente significativo e praticável."

Ross McKerchar, VP e CISO, Sophos

Proteja a rede

Para resguardar os seus recursos você também precisa proteger as redes onde eles são executados. O **Sophos Firewall** oferece proteção e visibilidade sem igual para ambientes locais, AWS e Azure.

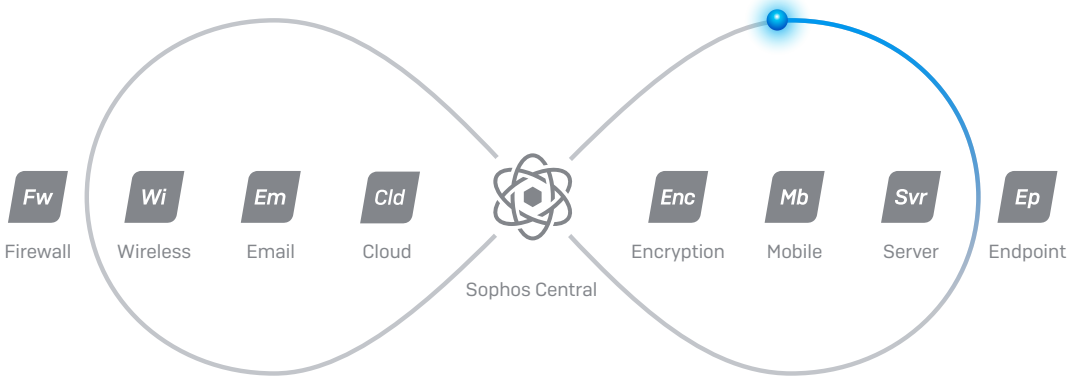
- Proteção multicamada e integrada para bloquear até mesmo as ameaças mais avançadas
- Um poderosa unidade de solução para WAF, IPS, ATP, filtragem de URL, roteamento baseado em caminho e bloqueio em nível de país, com relatórios extensivos, incluindo um insight completo do usuário e da atividade da rede
- Visibilidade de aplicativos na nuvem, descoberta de TI sombreada e resposta a ameaças automatizada
- Capacidade de fortalecer suas cargas de trabalho na nuvem contra tentativas de invasão de hackers, como injeção SQL e scripts entre sites, enquanto proporciona acesso seguro a usuários com a autenticação de proxy reversa
- Flexibilidade de execução como uma solução autônoma e de alta visibilidade

Para facilitar a implantação baseada na nuvem, tudo fica disponível em uma imagem de máquina virtual única e pré-configurada.

Gerenciamento simplificado

Com a Sophos, você pode gerenciar toda a sua segurança através de uma única plataforma na web: o Sophos Central. Ele acaba com o acesso individualizado a painéis para proteger a sua organização: tudo concentrado em um só lugar. Também permite que você faça investigações cruzadas entre produtos com facilidade, correlacionando dados de vários serviços com rapidez.

Como o Sophos Central é hospedado na nuvem, ele é ideal para equipes de TI dispersas. Com mais de 400.000 usuários mundialmente, você pode ficar tranquilo, sabendo que está usando a plataforma de segurança cibernética mais confiável do mundo.



O Sophos Central também permite que os produtos Sophos compartilhem informações de segurança e integridade sobre ameaças em tempo real e trabalhem em sintonia para responder automaticamente a ameaças – a isso chamamos Segurança Sincronizada. Alguns benefícios:

- Resposta automatizada a incidentes. Se um produto Sophos detecta algo suspeito, como uma infecção por malware ou um dispositivo fora de conformidade, ele compartilha a informação com o restante do sistema de segurança cibernética. Em seguida, os outros produtos respondem automaticamente ao incidente, em segundos. Por exemplo:
  - O Sophos Firewall isola os dispositivos infectados instantaneamente, impedindo que a ameaça se alastre e bloqueando o movimento interno lateral.
  - O Intercept X faz a varredura automática do endpoint quando são detectadas caixas de correio comprometidas, limitando o impacto das ameaças transmitidas por e-mail.
  - O Sophos Wi-Fi restringe o acesso à rede por dispositivos incompatíveis, mantendo os dispositivos ilegítimos e inseguros fora da sua rede sem fio.
- Insights únicos. As equipes de TI desfrutam de maior visibilidade e controle de suas redes, com a capacidade de:
  - Identificar dispositivos infectados pelo nome em lugar do endereço IP, acelerando as investigações de segurança.
  - Identificar todos os aplicativos na rede. Em média, 43% do tráfego de rede passam como "não classificado", de modo que o pessoal de TI fica sem saber se ele é bom, mau ou mal-intencionado. Com o Synchronized Security, o Sophos Firewall e o Intercept X trabalham juntos para identificar e classificar automaticamente TODOS os aplicativos na rede.

Proteção ímpar. Eficiência ímpar.

Com um sistema de segurança cibernética da Sophos você tem proteção Next Gen: uma única plataforma de gerenciamento, o compartilhamento de inteligência de ameaças entre produtos e a resposta automatizada a incidentes. Juntos, esses recursos proporcionam ganhos extraordinários em eficiência e produtividade para as equipes de TI.

De fato, os clientes que têm o Sophos Intercept X e o Sophos Firewall, gerenciados através do Sophos Central, disseram consistentemente que são capazes de **duplicar a eficiência da equipe de TI** e ainda assim registrar **uma queda de 85% nos incidentes de segurança**.

"Ter ferramentas que detectam e corrigem automaticamente a maioria dos eventos de segurança permite que a nossa pequena equipe de TI gerencie a segurança da empresa e impeça que fique comprometida."

Diretor de tecnologia, provedor de serviços de software

Protegendo qualquer lugar. Qualquer dispositivo. Qualquer recurso.

Não há como retroceder a mudança à flexibilidade do trabalho remoto e ao crescente uso da nuvem. Eles facilitam nossas vidas, mas também apresentam novos desafios para as equipes de TI e novas oportunidades para os impostores. Assegurar esse novo ambiente requer conexões protegidas, recursos protegidos e dispositivos protegidos, onde quer que estejam, sem onerar as equipes de TI.

A Sophos pode ajudá-lo a encarar esses desafios modernos com soluções poderosas e confiáveis. Entre em contato com um representante da Sophos para tratar dos seus requisitos, ou ative um teste de avaliação sem compromisso para experimentar qualquer um dos nossos produtos.

1 https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2

2.Rodapé O Estado do Ransomware 2020, Sophos

3.Rodapé O Estado da Segurança da Nuvem 2020, Sophos

Vendas na América Latina
E-mail: latamsales@sophos.com

Vendas no Brasil
E-mail: Brasil@sophos.com

210215 WPPTBR (MP)

SOPHOS