SOPHOS
Cybersecurity evolved.

Guia de Segurança Cibernética para a Área de Saúde

Segurança cibernética na área de saúde – interrompe ataques na mira dos invasores sem atravancar os cuidados aos pacientes

Resumo da Solução Sophos. Abril, 2021

Segurança cibernética e cuidados ao paciente

Quando pensamos na saúde dos pacientes, o que nos vem à mente são médicos, enfermeiros e outros profissionais da área de saúde que oferecem serviços médico-hospitalares. Mas com a crescente dependência de tecnologias do setor de saúde – desde inteligência artificial e computação na nuvem até dispositivos conectados – e a contínua evolução das técnicas de ataque pelos invasores, a segurança cibernética desempenha um papel direto e significativo na capacitação de entrega dos cuidados de saúde.

"A segurança cibernética ineficiente é um perigo claro e constante à segurança do paciente... incidentes cibernéticos podem causar sérias interrupções aos sistemas de saúde e contribuir diretamente a danos aos pacientes."

Institute of Global Health Innovation, Imperial College, Londres

A pandemia da COVID-19 acelerou a adoção de tecnologias digitais na área médica, como soluções de monitoramento remoto de pacientes, consultas online e dispositivos de uso doméstico, levando ao aumento do pessoal envolvido na mobilidade de dados. Enquanto essas mudanças geraram melhorias significativas na eficiência do setor de saúde que irão perdurar e evoluir em longo prazo, elas também geraram aumento nos desafios à segurança cibernética que as equipe de TI enfrentam.

"[Os invasores cibernéticos] estão explorando o fato de que a digitalização no futuro do setor de saúde se tornará mais e mais importante."

John Noble, Presidente, Information Assurance and Cyber Security Committee, NHS Digital

Desafios de segurança cibernética à área de saúde

Uma pesquisa da Sophos realizada em 2021 com 328 profissionais de TI da área de saúde em 30 países revelou que a cibersegurança está ficando mais difícil. Dos respondentes, 63% disseram que o número de ataques cibernéticos que enfrentaram aumentou no decorrer de 2020 – provavelmente impulsionados, ao menos em parte, por adversários se aproveitando da pandemia em seus ataques. Portanto, não é de surpreender que 70% disseram que a carga de trabalho voltada à segurança cibernética aumentou no decorrer de 2020.

Não é apenas o volume de ataques que está aumentado – eles também estão ficando mais complexos. O resultado: 60% disseram que os ataques cibernéticos estão muito avançados para as suas equipes de TI lidarem com eles por conta própria.

63 %
Número de ataques cibernéticos aumentou no decorrer de 2020

60 %
Ataques cibernéticos estão muito avançados para as equipes de TI lidarem por conta própria

70 %
Carga de trabalho da segurança cibernética aumentou no decorrer de 2020

A complexidade é inimiga da segurança

Em geral, as organizações da área de saúde apresentam o maior índice médio de uso de pessoal de TI por usuário individual. Quanto maior a complexidade da infraestrutura de segurança mais difícil fica para as equipes de TI sobrecarregadas se manter em dia, bem como aproveitar as vantagens oferecidas pela capacidade de proteção.

Sophos: protegendo a saúde

A Sophos trabalha com organizações da área de saúde em âmbito global para tratar de seus desafios com a segurança cibernética e possibilitar cuidados ininterruptos aos pacientes. Frente à crescente frequência e sofisticação dos ataques, podemos ajudá-lo a manter os seus dados e a sua organização protegidos e capacitar suas equipes de TI para reduzir a carga de trabalho dedicada à segurança cibernética. Leia os detalhes sobre como podemos ajudar a lidar com os desafios da segurança cibernética mais comuns que as organizações de saúde enfrentam.

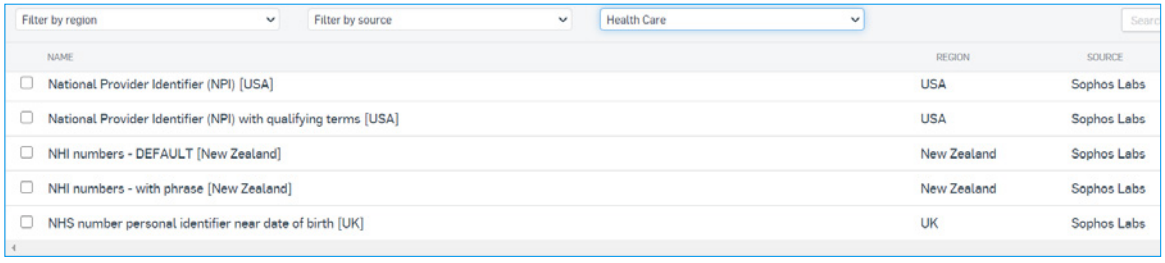
Proteja dados confidenciais onde quer que se hospedem

As organizações da área de saúde controlam diversas formas de dados confidenciais, que vão prontuários médicos até dados de registro de trabalho e informações identificáveis pessoais (PII). Com tantos tipos diferentes de dados confidenciais nas organizações de saúde – e tantos lugares diferentes onde são armazenados e utilizados – protegê-los pode ser algo difícil.

As ferramentas da Sophos para proteção preventiva e ativa oferecem segurança para toda a sua rede de serviços médico-hospitalares diretamente nos dispositivos, individualmente.

Proteja dispositivos ou cargas de trabalho que armazenam os dados

O **Sophos Intercept X** para endpoints e servidores emprega múltiplas camadas de proteção para a segurança de dados em Windows, Mac, Linux e máquinas virtuais. As regras de proteção contra a perda de dados especificamente voltadas à área de saúde se utilizam de termos e dados do setor para elevar o seu nível de proteção.



O **Sophos Device Encryption** oferece um modo rápido e fácil de assegurar que dispositivos Windows e macOS sejam encriptados com segurança, de modo a proteger os seus dados – e garantir a conformidade – caso sejam perdidos ou roubados.

Proteja a rede por onde os dados passam

O **Sophos Firewall** usa a tecnologia de detecção de ameaça baseada em inteligência artificial para impedir que os ataques atinjam seus dados confidenciais de saúde, sistemas hospitalares essenciais e outras partes do ecossistema.

Previna a perda por e-mail – deliberada ou acidental

O **Sophos Email** criptografa informações identificáveis pessoais, prontuários médicos, exames, imagens e outros dados confidenciais de modo a evitar violações maliciosas e acidentais de dados.

Controle o acesso aos dados

O **Sophos Zero Trust Network Access (ZTNA)** lhe dá controle absoluto sobre quem pode acessar dados na sua rede. Controles detalhados bloqueiam os movimentos laterais internos e asseguram que apenas pessoas autorizadas tenham acesso a dados confidenciais.

Confronte a ameaça do ransomware à área de saúde

O ransomwares está ficando mais inteligente e extenuante, e a área de saúde é um alvo lucrativo. No caso da área de saúde, o custo do ransomware não se limita apenas a pagar o resgate. O custo de perder dados de pacientes e atrasar ou cancelar tratamentos médicos pode chegar a proporções devastadoras. As ferramentas da Sophos de prevenção e caça a ameaças evoluem constantemente para se manter na dianteira do ransomware, defendendo os seus dados e a sua rede contra esses ataques de forma proativa.

Não deixe que o ransomware o mantenha refém

A Sophos se orgulha de ser líder mundial na proteção de empresas contra ransomwares.

O **Sophos Intercept X** é a melhor proteção do mundo contra ransomware para endpoints e servidores. Ele introduz várias camadas de segurança para reconhecer e parar ransomwares logo em seu estágio inicial, incluindo:

- CryptoGuard, que reverte arquivos automaticamente para um estado seguro na eventualidade de serem criptografados por um agente não autorizado
- Deep Learning com tecnologia IA, que bloqueia ransomwares conhecidos e desconhecidos
- Proteção contra explorações que param as técnicas que os invasores usam para baixar e instalar ransomwares
- Proteção básica baseada em assinatura pelo SophosLabs

O **Sophos Managed Threat Response (MTR)** proporciona o mais alto nível de proteção contra ransomware, oferecendo recursos proativos de caça, detecção e resposta a ameaças, tudo entregue através de um serviço gerenciado por uma equipe de especialistas 24 horas por dia. Estamos em constante vigília, inclusive enquanto você dorme.

O **Sophos Rapid Response** oferece suporte emergencial durante ataques ativos de ransomware, mesmo que você não seja um cliente da Sophos. Nossa equipe o ajudará a controlar um ataque com rapidez para proteger suas redes, aplicativos e dados, bem como mitigar danos e períodos de inatividade.

A realidade do ransomware no sistema de saúde

34% atingidos por ransomware no último ano

65% dos ataques criptografaram dados

34% pagaram o resgate

US$1,27 milhão é o custo médio de recuperação

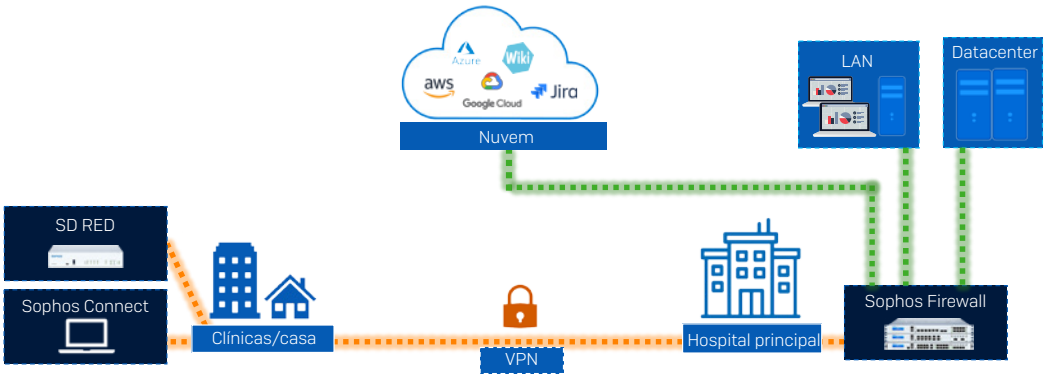
O Estado do Ransomware 2021, Sophos

Dê a seus usuários acesso seguro de qualquer lugar

Os funcionários da área de saúde, atuando na linha de frente em hospitais ou trabalhando de casa, precisam ter acesso ininterrupto a dados confidenciais de pacientes e ao sistema de saúde. As ferramentas da Sophos permitem a seus usuários conexão com segurança em qualquer localidade, sem afetar o trabalho vital que o sistema de saúde oferece.

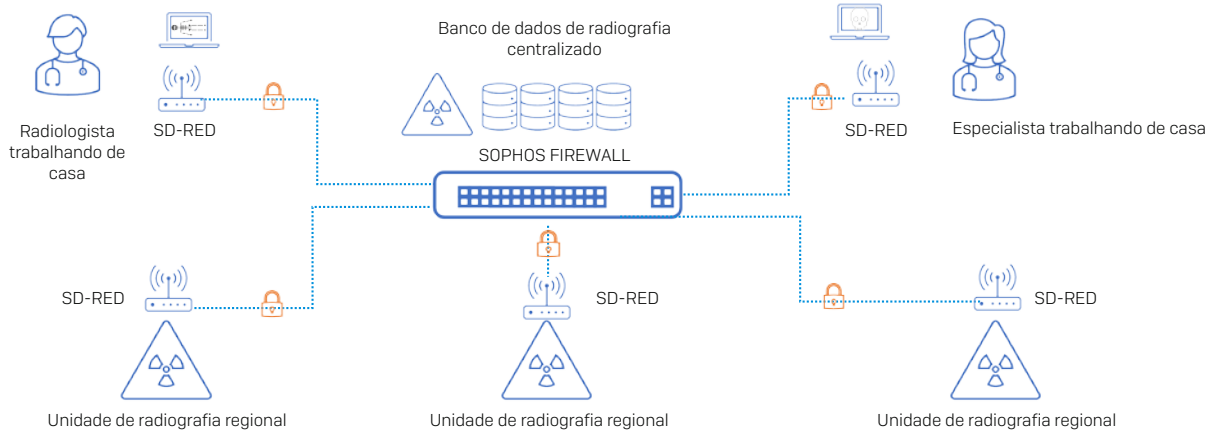
Capacite os usuários a se conectar de qualquer localidade

O **Sophos Firewall** oferece conexões seguras a Windows e macOS através do serviço Sophos Connect VPN gratuito. Ele é fácil de implantar e configurar, dando a seus usuários remotos o acesso seguro a recursos na rede ou na nuvem pública a partir de dispositivos Windows e macOS. Com mais de 1,4 milhão de clientes ativos, você pode estar certo de que estará em boa companhia.



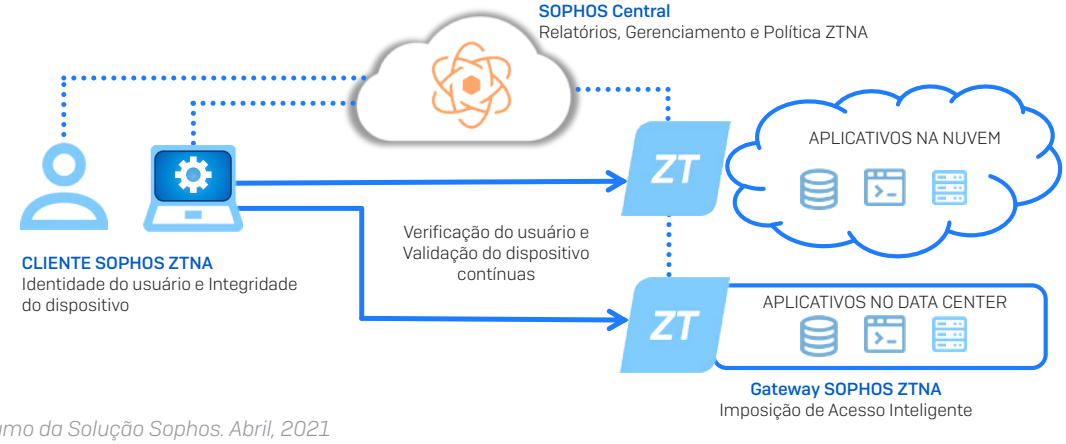
O Sophos Firewall oferece acesso remoto seguro através do cliente Sophos Connect e dispositivos SD-RED

Para proporcionar o melhor em conectividade remota segura, o **SD-RED** (dispositivo ethernet remoto) oferece um pequeno dispositivo plug-and-play que funciona com o **Sophos Firewall** para conectar localidades remotas e indivíduos à sua rede principal. Ideal para clínicas e unidades médicas, bem como pessoas com dados altamente confidenciais.



Exemplo de uso de radiografia do Sophos Firewall e SD-RED

Para promover o acesso à segurança next-gen, o **Sophos Zero Trust Network Access** coloca a identidade no centro do seu sistema de defesa, constantemente validando o usuário, o dispositivo e a conformidade com as políticas. Ele oferece uma experiência transparente aos usuários que "simplesmente funciona", capacitando as equipes de TI a colocar os novos usuários em ação o mais rápido possível.



Reforce a sua equipe de TI

Nossa pesquisa de 2020 com 5.000 gerentes abrangendo diferentes setores, inclusive a área de saúde, revelou que 81% dos respondentes disseram que a capacidade de encontrar e reter profissionais de segurança de TI qualificados é um grande desafio à capacidade de suas organizações de fornecer segurança de TI.

Se você precisa adicionar especialidade ou complementar os seus recursos humanos, os profissionais em segurança da Sophos podem ser uma extensão da sua equipe, mantendo sistemas de saúde e dados de pacientes seguros, 24 horas por dia.

Especialistas em segurança dedicados para reforçar sua equipe de TI

O **Sophos Managed Threat Response (MTR)** é formado por uma equipe de peritos em caça e resposta a ameaças que atua como uma extensão do seu próprio pessoal. Eles oferecem ao departamento de TI em áreas médico-hospitalares a capacidade adicional e a perícia complementar necessárias para lidar com toda a carga de ameaças.

A equipe Sophos MTR monitora o seu ambiente 24/7, saindo no encalço de possíveis ameaças e incidentes para validar seu potencial destrutivo. Se virem algo suspeito, eles podem entrar em contato com os especialistas em malware no SophosLabs para investigar e destrinchar indicadores suspeitos.

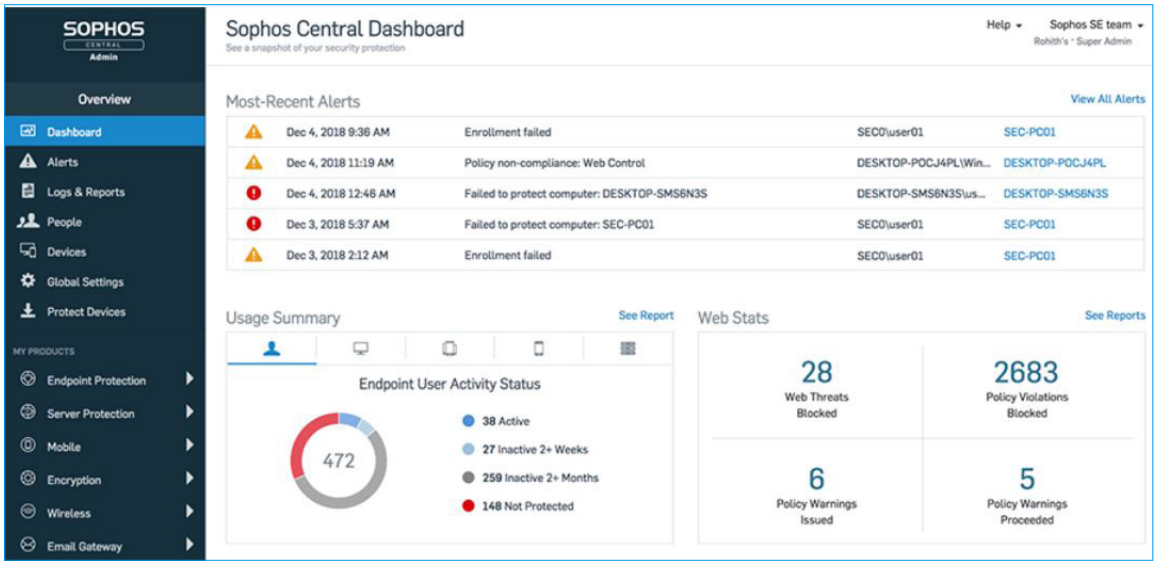
Além disso, se você assim desejar, as equipes Sophos MTR também poderão tomar todas as providências por você. Diferentemente de outros serviços de detecção e resposta gerenciados, nossa equipe não apenas o notifica sobre os problemas, mas também neutralizar a ameaça para você. Definitivamente é você quem decide o nível de ação que deseja que adotemos e como trabalhar com a sua equipe.

Gaste menos tempo administrando a segurança cibernética

Quando seus recursos de TI são limitados, fica difícil peneirar a avalanche de alertas de segurança para decidir quais deles examinar primeiro. A Sophos ajuda você a remover empecilhos e examinar a segurança em um único painel. Usando a automação, você soluciona os problemas antes de ter que se preocupar com eles, e assim pode focar seu tempo na construção de estratégias novas e diferentes.

Simplifique o gerenciamento da segurança cibernética

O Sophos Central é a nossa plataforma unificada baseada na web onde você pode gerenciar todos os produtos de segurança da Sophos. Nada de ficar mudando de painel para painel para proteger a sua organização: com o Sophos Central, você pode facilmente implantar e gerenciar a sua proteção e conduzir investigações entre produtos que correlacionam dados de múltiplos serviços, tudo em um único lugar.



Gerencie toda a sua segurança cibernética através da plataforma Sophos Central

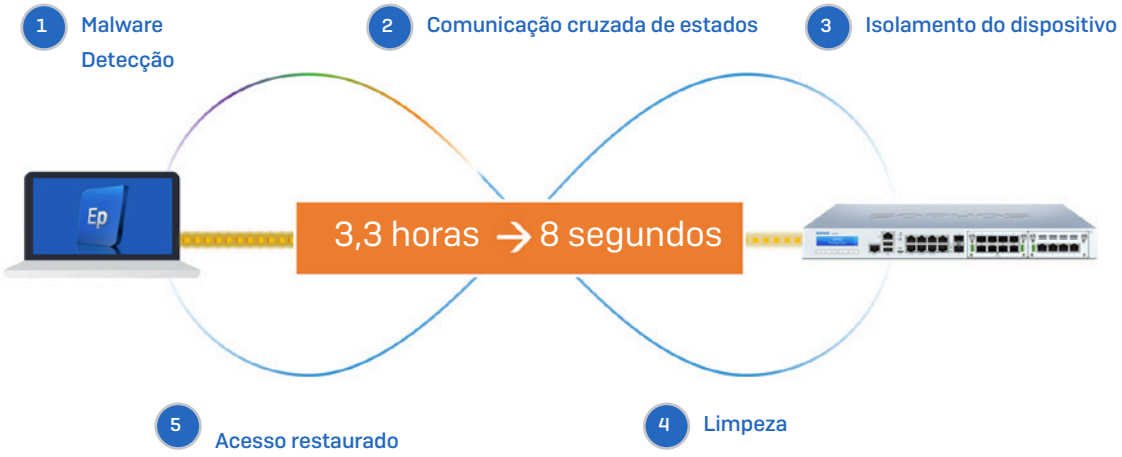
Automatize a sua proteção

O Sophos Central permite que os produtos Sophos compartilhem informações ativamente e trabalhem em tempo real para responder automaticamente a incidentes. Essa integração e automação eleva o seu nível de proteção ao mesmo tempo que reduz o peso da carga de trabalho para as equipes de TI.

Exemplo 1: Resposta automatizada a incidentes

- Se o Sophos Intercept X identifica uma ameaça no endpoint, ele notifica o Sophos Firewall instantaneamente.
- O Sophos Firewall isola automaticamente o endpoint infectado da rede e também de outros dispositivos na mesma LAN.
- O Intercept X elimina a ameaça e notifica o Sophos Firewall assim que estiver pronto.
- O Sophos Firewall restaura o acesso à rede imediatamente.

O processo todo, que leva algo em torno de três horas e meia quando realizado manualmente, ocorre em menos de oito segundos.

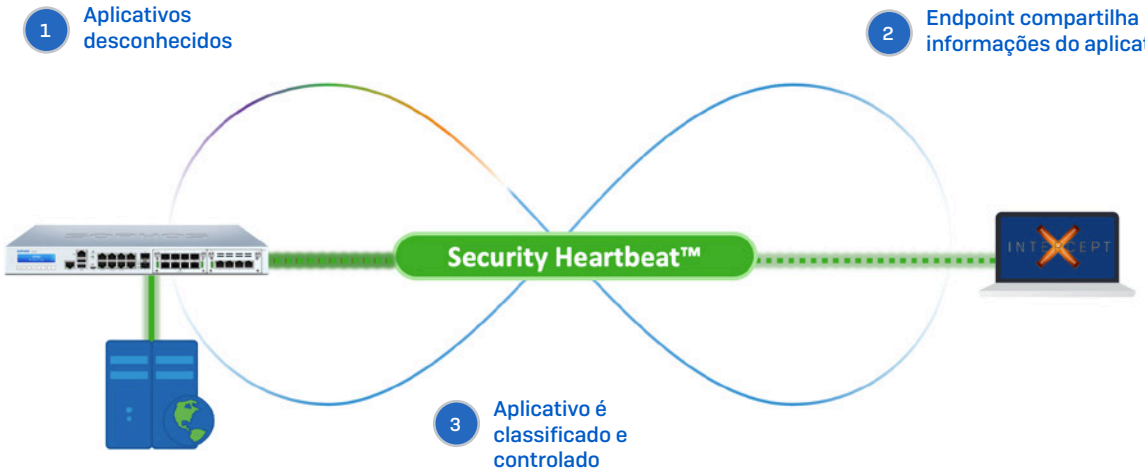


Automação de resposta a incidentes

Exemplo 2: Identificação de todos os aplicativos indesejados na rede

Em média, 43% do tráfego da rede passa despercebido. Alguns aplicativos são personalizados e não têm uma assinatura padrão. Outros desejam esconder sua identidade do firewall, certamente porque as intenções não são das melhores.

- Se o Sophos Firewall observar um aplicativo que não corresponde a uma assinatura conhecida, ao invés de atribuí-lo a um bucket de tráfego genérico, como "HTTPS", o Sophos Firewall contata o Sophos Intercept X.
- O Intercept X passa o nome, patch e categoria do aplicativo para o Sophos Firewall para classificação. O aplicativo é automaticamente atribuído ao grupo apropriado.
- Se o grupo tiver medidas de controle aplicadas (ou seja, bloqueio), as mesmas regras serão aplicadas. Se necessário, por exemplo, com aplicativos personalizados, o administrador pode definir manualmente uma categoria e política para aplicar.



Identificação de todos os aplicativos e processos na rede

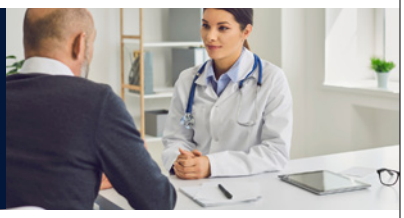
Reduza o TCO em ambientes do mundo real

Os benefícios de um sistema de segurança cibernética da Sophos só aumentam. A combinação de tecnologias next-gen, resposta automatizada, compartilhamento de informações em tempo real e uma plataforma de gerenciamento unificado causa um grande impacto tanto na proteção como no custo total de propriedade (TCO) geral.

*Clientes com o Sophos Intercept X Endpoint e o Sophos Firewall disseram que teriam que **dobrar o quadro de funcionários de segurança para manter o mesmo nível de proteção** se não tivessem um sistema Sophos, apontando uma redução de 85% em incidentes de segurança.*

CUSTOMER CASE STUDY **HEALTHCARE PROVIDER, U.S.**

A regional healthcare provider whose services include inpatient and outpatient care, medical practices, nursing homes, and a range of specialist services.



Business impact of a Sophos cybersecurity ecosystem

50% reduction in IT security resource requirements
The customer has three employees dedicated to cybersecurity. They calculate they would, if they didn't use Sophos, need to employ three additional full-time security analysts solely to cover incident response.

90%-plus reduction in day-to-day cybersecurity workload
Prior to Sophos, reviewing logs and investigating areas of concern would take an entire day. Now they achieve the same level of confidence in just 30 minutes.

85% reduction in security incidents
Previously, they experienced three incidents each day on average. This has now dropped to an average of one every three days.

90%-plus reduction in time to investigate an incident
Before using Sophos, it took the team roughly three hours to thoroughly investigate an incident. This has now dropped to less than 15 minutes, with everything done remotely via the Sophos Central platform and without disrupting other users and impacting system availability.

CUSTOMER-AT-A-GLANCE

Number of users
4,500 employees

Sophos solutions
- Sophos XG Firewall
- Sophos Intercept X Advanced with EDR
- Sophos Intercept X for Server Protection (Windows, Linux, and virtual machines)

CUSTOMER CASE STUDY **CLINICAL TRIALS PROVIDER, U.S.**

A private sector organization that provides the clinical trial data needed to secure regulatory approval for new medications.

Business impact of a Sophos cybersecurity ecosystem

50% reduction in IT resource requirements
Currently, the customer spends one hour a day reviewing logs and investigating issues. They advise that they would need to hire one or two more security engineers just to manage the logs if they moved away from Sophos.

33% reduction in time to deal with a potential issue
Previously, to address a security issue with a device, they would reimage the machine, which took between 90 minutes and two hours. With Sophos, they can conduct a full investigation and remediate in approximately one hour – with no reimaging.

88% reduction in threat risk due to faster issue identification
Prior to using Sophos, it took a full day just to investigate the logs to find the issues. With Sophos, the IT team can identify new issues for investigation within minutes of a suspicious event arriving.

Improved user behavior
As users are aware that the IT team can now address issues quickly and without impacting work, they are far more willing to report issues or concerns.

CUSTOMER-AT-A-GLANCE

Number of users
150 employees across four locations

IT team
Two IT staff, covering all areas including cybersecurity

Sophos solutions
- Sophos XG Firewall
- Sophos Intercept X Advanced with EDR
- Sophos Device Encryption

Dê aos profissionais de saúde proteção segura

No intenso ambiente de trabalho da área de saúde, os riscos causados por erro humano sempre serão difíceis de eliminar e controlar. A Sophos oferece uma rede de segurança vital para que as pessoas possam trabalhar com rapidez, sem preocupação.

Impeça que as ameaças atinjam seus usuários

Podemos ajudar a aliviar a pressão nos seus usuários – e por extensão, na sua equipe de TI – ao impedir que as ameaças atinjam os seus usuários:

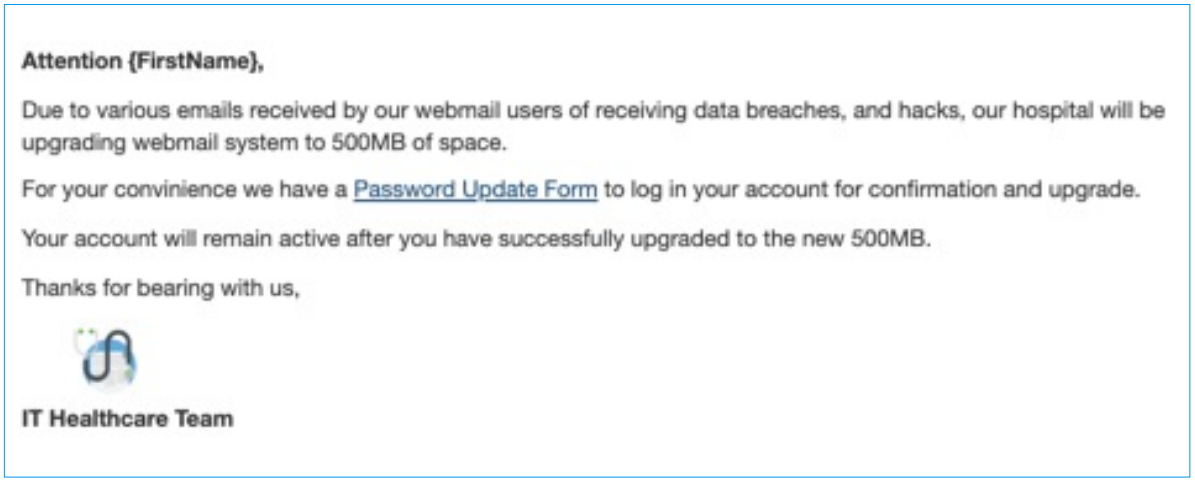
O **Intercept X with EDR** combina anti-ransomware, prevenção contra exploit e detecção com tecnologia de IA para barrar as ameaças em múltiplos e diferentes pontos na cadeia de ataque. Os usuários podem ficar descansados, sabendo que a melhor proteção de endpoint do mundo está sempre alerta para defendê-los.

O **Sophos Email** coloca a segurança com tecnologia de IA diretamente na caixa de entrada dos seus usuários. Ele identifica e-mails maliciosos e os remove automaticamente, antes que os usuários tenham a chance de clicar no link suspeito.

O **ecossistema de segurança cibernética da Sophos** permite que os produtos Sophos trabalhem em conjunto para responder automaticamente a ameaças, interrompendo e eliminando ameaças em apenas alguns segundos.

Treine os seus usuários para identificar ameaças

O **Sophos Phish Threat** ajuda os usuários a identificar e-mails maliciosos por meio de treinamento online e simulações de e-mails de phishing. Você pode direcionar o treinamento àqueles que mais precisam, seja pela natureza de seus cargos ou pelo rendimento que demonstraram nos testes simulados.



Attention {FirstName},

Due to various emails received by our webmail users of receiving data breaches, and hacks, our hospital will be upgrading webmail system to 500MB of space.

For your convinience we have a Password Update Form to log in your account for confirmation and upgrade.

Your account will remain active after you have successfully upgraded to the new 500MB.

Thanks for bearing with us,

IT Healthcare Team

Amostra de e-mail de simulação de phishing no Sophos Phish Threat

Implemente a segurança que não desestabiliza o sistema de saúde

Manter tudo funcionando e em constante operação é muito mais importante no setor de saúde do que na maioria dos outros setores. Por isso que muitos usuários do sistema de saúde implementam aplicativos sem aprovação para facilitar o trabalho, o que deixa a sua rede e os seus dados expostos a altos riscos. A Sophos ajuda a combater a TI sombra sem interferir nas suas operações diárias.

Proteção avançada que mantém a harmonia do movimento

O **Intercept X with EDR** protege os seus endpoints e servidores, barrando as ameaças sem atrapalhar os seus usuários. As funcionalidades do EDR permitem que você consulte o dispositivo de seus usuários remotamente e, se necessário, aplique correções máquinas e computadores.

O **Sophos Firewall** mantém a sua rede protegida contra ameaças e facilita a priorização do tráfego de rede confiável, garantindo que os processos críticos possam continuar sem interrupções. Além disso, ele lhe dá a visibilidade e controle da TI sombra, permitindo identificar e interromper atividades que possam colocar a sua organização em risco.

Os produtos Sophos são excelentes por si só e ainda melhores em conjunto. Como vimos até então, o Sophos Intercept X e o Sophos Firewall trabalham juntos para responder automaticamente a ameaças e melhorar a visibilidade.

Proteja tecnologias legadas

Um desafio frequente entre muitas das organizações da área de saúde é a necessidade de proteger equipamentos legados. Esses dispositivos geralmente têm sistemas operacionais desatualizados que não podem ser atualizados devido a questões reguladoras, mas que precisam estar conectados à rede. Se o dispositivo não puder receber patches ou atualizações e não tiver uma solução de antivírus ou antimalware compatível, você precisa buscar uma solução física.

O **Sophos Firewall** e o **SD-RED** (dispositivo ethernet remoto) podem ajudar nesse caso. Ao colocar um SD-RED na frente de um dispositivo exposto, ele pode encapsular todo o tráfego para o Sophos Firewall para realizar uma varredura de proteção. Se a sua rede for bastante simples, você provavelmente terá que fazer algumas pequenas alterações nos esquemas de endereço IP e talvez mudar de topologia – e o nosso pessoal técnico especializado poderá tratar da sua situação em particular e recomendar o melhor caminho para você seguir.

Proteja equipamentos legados

Conclusão

Proteger ambientes de TI na área de saúde e os dados confidenciais que movimentam requer uma segurança em camadas. Ao implementar uma segurança inteligente em cada ponto vulnerável, de redes a dados, você pode proteger seus sistemas, funcionários e pacientes contra riscos internos e externos.

Todas as soluções Sophos são parte do nosso ecossistema de segurança cibernética adaptativa. Elas são excelentes por si só – muitas organizações começam com um único produto – e trabalham ainda melhor em conjunto. Conforme a sua proteção Sophos aumenta, aumentam também os benefícios intrínsecos de um ecossistema integrado: o compartilhamento da informação, o gerenciamento centralizado em um único painel, a resposta automatizada, os 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.

Protegendo a saúde: ecossistema de segurança cibernética da Sophos

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

Solicite o contato de nossos especialistas em segurança ainda hoje!

A Sophos oferece soluções de segurança cibernética líder do setor para empresas de todos os tamanhos, protegendo-as em tempo real de ameaças avançadas como malware, ransomware e phishing. Com recursos comprovados de última geração, seus dados comerciais ficam protegidos de modo eficiente por produtos que incorporam inteligência artificial e machine learning.

2021-05-05 (SB-NP)

SOPHOS