

**SOPHOS**

# ***SEGURANÇA VIRTUAL EVOLUTIVA: O IMPACTO DA SOPHOS NOS NEGÓCIOS***

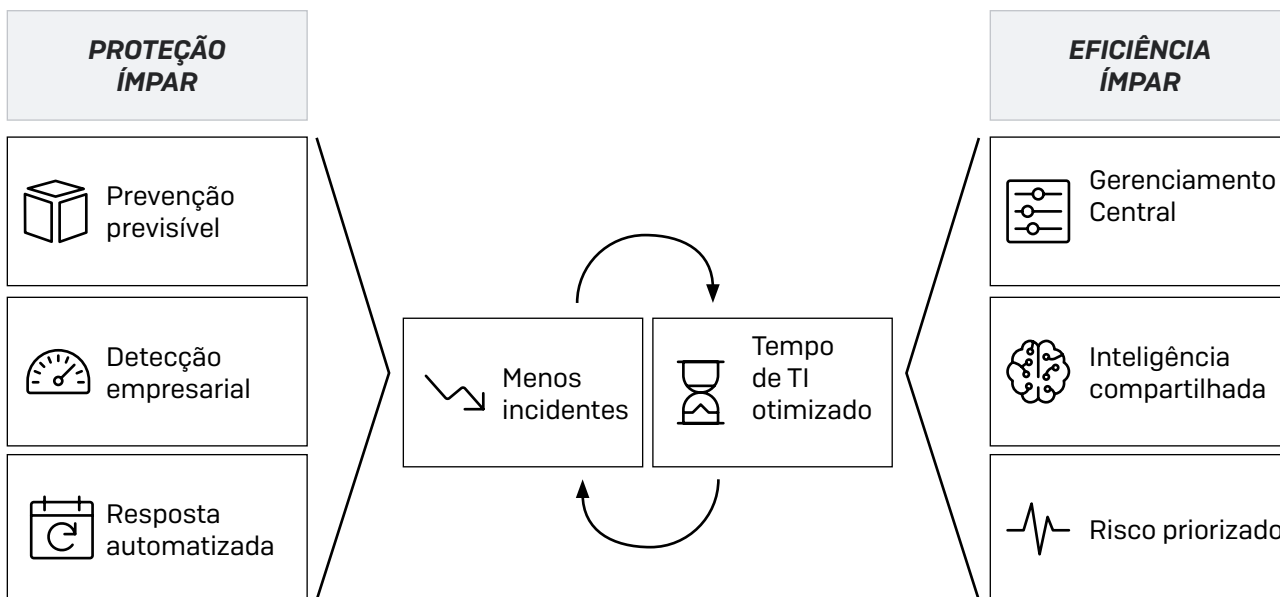
Quantificando os benefícios na vida real da proteção e eficiência do sistema de segurança virtual da Sophos em cinco estudos de casos de clientes

## Introdução

Quando escolhe a Sophos para se proteger contra ameaças, você se beneficia do primeiro – e melhor – sistema de segurança virtual do mundo:

- ▶ **Portfólio completo de produtos e serviços next gen.** Podemos ajudá-lo com todas as suas necessidades em segurança virtual: proteção de endpoints, dispositivos móveis e servidores, EDR, Firewall Next Gen, E-mail, UEM e mais. Seja uma implantação de rede completa, híbrida ou local, estamos aqui para protegê-la.
- ▶ **Proteção ímpar.** Beneficie-se das mais novas tecnologias e da grande expertise das nossas equipes do SophosLabs renomadas mundialmente em ciência de dados e caça a ameaças. A detecção de nível empresarial bloqueia os avançados ataques de hoje, enquanto redes neurais de Deep Learning alimentadas por inteligência artificial impedem de modo previsível as ameaças ainda desconhecidas. Os produtos Sophos também trabalham em conjunto e em tempo real, aumentando ainda mais a sua proteção. Eles compartilham informações de segurança e integridade sobre ameaças e respondem automaticamente aos incidentes.
- ▶ **Uma única plataforma de gerenciamento.** Gerencie toda a sua proteção Sophos através do Sophos Central, nossa plataforma de gerenciamento na nuvem. Utilizando inteligência compartilhada, ele proporciona informações de prioridade do risco, enquanto investigações guiadas indicam as ações recomendadas para cada cenário.

O sistema de segurança virtual da Sophos  **aumenta a proteção**  enquanto  **reduz o custo total de propriedade (TCO)** . Para isso, ele cria um círculo virtuoso onde proteção ímpar e eficiência ímpar reforçam sua eficácia continuamente.



Esse círculo virtuoso o capacita a aumentar significativamente a eficiência da sua equipe de TI e reduzir sua exposição a ameaças – sem aumentar seu quadro de funcionários.

## Impacto no cliente

Para medir o impacto do sistema de segurança virtual da Sophos em ambientes reais de clientes reais, entrevistamos cinco clientes Sophos na América do Norte, Europa e Ásia. Cada cliente ofereceu um diferente cenário, com variadas estruturas organizacionais, desafios e exigências comerciais. Contudo, uma grande revelação foi comum a todos:

*Os clientes disseram que precisariam **dobrar** o quadro de funcionários de segurança para manter o mesmo nível de proteção se não tivessem um sistema de segurança virtual Next Gen da Sophos.*

Também disseram passar por menos incidentes de segurança e que podem identificar e responder mais rapidamente aos problemas que ocorrem. Os resultados de usar o Sophos são:

- Redução de 50% nos custos com o quadro de funcionários de segurança de TI
- Redução de mais de 90% no tempo gasto na administração diária da segurança virtual
- Redução de mais de 90% no tempo necessário para identificar os problemas de TI
- Redução de 85% no número de incidentes de segurança
- Redução significativa no tempo de inatividade na organização como um todo

## Cliente A: provedor na área de saúde, EUA

- 4.500 funcionários
- 80 funcionários de TI, dos quais, três dedicados à segurança virtual
- Produtos Sophos: Intercept X Advanced with EDR, XG Firewall, Intercept X for Server Protection (Windows, Linux e máquinas virtuais)

O Cliente A é um provedor regional na área de saúde que oferece serviços como: atendimento médico ambulatorial e internações, procedimentos médicos, casa de repouso e uma variedade de serviços especializados.

## Impacto nos negócios

### ▸ **Redução de 50% na necessidade de recursos de segurança de TI**

O cliente emprega, atualmente, três funcionários dedicados à segurança virtual. Eles calcularam que, se não usassem a Sophos, precisariam empregar três analistas de segurança extras em período integral exclusivamente para responder a incidentes.

Antes da Sophos, a equipe fazia bastante trabalho manual para identificar o que acontecia na rede, e passavam grande parte do tempo identificando incidentes. Agora, a Sophos identifica os problemas proativamente para eles e resolve a situação automaticamente em 95% dos casos. O resultado é uma equipe focada na solução dos 5% de problemas que exigem o envolvimento humano.

### ▸ Redução de mais de 90% na administração diária da segurança

O gerente de segurança de TI gasta 30 minutos diários examinando logs e investigando tudo o que seja preocupante. Antes da Sophos, costuma levar o dia todo para obter o mesmo nível de informações e confiabilidade. Com a Sophos, todos os dados são consolidados em uma única plataforma de gerenciamento e apresentados em um formato consistente, facilitando a identificação e a resposta aos problemas. Isso retira a carga diária da onerosa tarefa de mapear dados provenientes de várias fontes para tentar identificar e separar os suspeitos dos malignos e dos benignos.

### ▸ Redução de 85% em incidentes de segurança

Por ser um hospital, o estabelecimento mantém uma grande quantidade de dados confidenciais de identificação pessoal, bem como informações de pagamento, o que faz dele um alvo para os criminosos cibernéticos. Antes da Sophos, eles passavam por uma média de três incidentes por dia que exigiam investigação mais aprofundada. Com a Sophos, houve uma queda para uma média de uma investigação a cada três dias.

### ▸ Mais de 90% de redução no tempo para investigar um incidente

Antes da Sophos, realizar uma investigação completa de um incidente levava cerca de três horas, incluindo obter acesso local ao computador afetado. Agora leva no máximo 15 minutos, fazendo tudo remotamente através da plataforma Sophos Central.

Anteriormente, a equipe precisava desabilitar o adaptador de rede e ter o equipamento físico em mãos para investigar e resolver o problema antes de reconectá-lo manualmente. Precisava também acomodar o fluxo de trabalho dos usuários: por exemplo, aguardar até que os médicos atendessem seus pacientes para então ter acesso ao sistema para reparos. A capacidade de isolar o dispositivo através do painel do Sophos Central permite à equipe investigar o problema remotamente sem causar impacto ao usuário e à disponibilidade do sistema.

A redução no tempo de investigação e a capacidade de gerenciar tudo remotamente também diminuiu significativamente a interferência no trabalho de outros funcionários do hospital.

### ▸ Proteção continuada durante as investigações

Anteriormente, os dispositivos eram removidos da rede para investigação manual e não recebiam atualizações de proteção enquanto estavam offline. Com a Sophos, quando a equipe de TI isola um dispositivo para investigar um problema, ele permanece online e continua a receber atualizações de proteção.

The screenshot displays the Sophos Central Admin interface for a device named 'Victim5-Win10'. The interface is divided into a sidebar on the left and a main content area on the right. The sidebar contains navigation options such as Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, Global Settings, and Protect Devices. The main content area shows the configuration for the device, including a 'SUMMARY' tab and an 'EVENTS' tab. The 'SUMMARY' tab displays a 'Recent Events' table with the following data:

Event Type	Time	Description
Update succeeded	May 15, 2020 9:14 AM	Update succeeded
Real time protection re-enabled	May 15, 2020 9:10 AM	Real time protection re-enabled
Real time protection disabled	May 15, 2020 9:08 AM	Real time protection disabled
Update succeeded	May 15, 2020 8:57 AM	Update succeeded
Update succeeded	May 15, 2020 8:37 AM	Update succeeded

The 'Agent Summary' section shows the following information:

- Last Activity: 34 minutes ago
- Last Agent Update: 17 minutes ago (Update Successful)
- Agent Version: 10.8.7 VE3.78.7 (Release Notes)
- Assigned Products: Licensed (Core Agent) and Assigned (Core Agent)

An orange arrow points to the 'Isolate' button in the device configuration panel, which is highlighted in orange.

## Cliente B: provedor na área de educação, Índia

- 700 funcionários
- Sede em Bangalore, além de gerentes locais em instalações pela Índia e por toda a região sudeste da Ásia
- Produtos Sophos: Intercept X Advanced with EDR, Intercept X Advanced for Server, XG Firewall

O Cliente B oferece serviços de ensino a escolas e universidades pela Índia e por toda a região sudeste da Ásia. Controlam dezenas de milhares de estudantes através de uma equipe de TI centralizada baseada na sede da empresa em Bangalore, juntamente com uma equipe de gerentes locais nas instalações.

### Impacto nos negócios

- **Redução de 50% nos recursos necessários para o gerenciamento diário da segurança**

Anteriormente, empregavam quatro engenheiros para gerenciar a segurança diária. Desde que mudaram para a Sophos, precisam apenas de dois engenheiros para cobrir a segurança em toda a empresa.

- **Redução de 94% no tempo dedicado a identificar áreas de alto risco que exigem investigação**

Antes da Sophos, o cliente precisava de três a quatro horas para identificar os problemas críticos que exigiam maior foco e investigações aprofundadas. Agora leva apenas de 10 a 15 minutos para identificar prioridades de segurança em toda a organização no Sophos Central.

- **Redução de 98% no tempo necessário para identificar a fonte do mau tráfego na rede**

A implantação anterior de segurança da rede levava dois dias (e às vezes mais) para identificar qual dispositivo na rede estava causando problemas de desempenho ou segurança. Agora leva apenas 15 minutos para encontrar o problema e tratar dele.

- **Redução de 95% no tempo gasto no gerenciamento de atualizações de firmware**

A implantação anterior de segurança da rede também criava problemas de disponibilidade e risco porque cada atualização de software levava de três a quatro horas. Agora, com a Sophos, demora apenas 10 minutos por atualização. Com 20 a 25 atualizações por ano, isso equivale a uma economia de 75 horas por ano em atualizações [o equivalente a duas semanas de trabalho em período integral].

## Cliente C: provedor de ensaios clínicos, EUA

- 150 funcionários distribuídos em quatro localidades
- Dois funcionários de TI cobrindo todas as áreas, inclusive segurança virtual
- Produtos Sophos: Intercept X Advanced with EDR, XG Firewall, Central Device Encryption

O Cliente C é uma organização do setor privado que fornece os dados de ensaios clínicos necessários para assegurar a aprovação reguladora de novos medicamentos. Devido à natureza do trabalho, eles mantêm grandes quantidades de informações pessoais confidenciais.

### Impacto nos negócios

- **Redução de 50% nas necessidades de recursos de TI**

Esse cliente tem uma pequena equipe de apenas duas pessoas para gerenciar todos os aspectos do departamento de TI. Atualmente gastam uma hora por dia examinando logs e investigando tudo o que seja preocupante. Se deixassem de lado a Sophos, disseram que precisariam contratar mais um ou dois engenheiros de segurança apenas para monitorar os logs.

› **Redução de 33% no tempo necessário para tratar de um possível problema**

Anteriormente, quando tinham um problema de segurança com um dispositivo, a solução deles era refazer a imagem da máquina, o que levava entre 90 minutos e duas horas. Agora eles podem realizar uma investigação aprofundada: do isolamento do sistema e caça completa a ameaças até a total varredura de segurança e remediação final em aproximadamente uma hora, sem refazer a imagem da máquina. Um benefício adicional que obtiveram com a abordagem da Sophos é que o usuário pode começar a produzir tão logo a investigação seja concluída, ao passo que, quando refaziam a imagem também perdiam tempo redefinindo a configuração e as personalizações na máquina.

› **Redução de 88% no risco de ameaças, já que identificam problemas muito mais rápido**

Com o sistema de segurança virtual da Sophos, a equipe de TI pode identificar novos problemas que precisam ser investigados em minutos da chegada de um evento suspeito. Antes da Sophos, levava o dia todo para percorrer todos os logs para encontrar os problemas que precisavam de investigação. Essa redução no tempo de resposta diminuiu significativamente a exposição a ameaças.

› **Comportamento do usuário melhorado**

Com a Sophos, os usuários sabem que a equipe de TI pode tratar de problemas e incidentes rapidamente sem incorrer em tempo de inatividade ou trabalho extra. O resultado é que, agora, os usuários estão muito mais propensos a relatar problemas ou preocupações à equipe de TI (por exemplo, quando clicam em um link potencialmente malicioso em um e-mail).

## Cliente D: provedor de serviços públicos, Sérvia

- › 300 funcionários
- › 10 funcionários de TI, dos quais, quatro focados em segurança virtual
- › Produtos Sophos: Intercept X Advanced, Intercept X Advanced for Server, XG Firewall, Sophos Email, Sophos Mobile

O Cliente D é uma organização do setor público que atende a capital sérvia, Belgrado. Esse cliente da Sophos de longa data migrou para os nossos produtos Next Gen que são gerenciados através do Sophos Central.

### Impacto nos negócios

› **Redução de 50% no tempo gasto no gerenciamento diário da segurança**

Agora gastam 30 minutos por dia na administração de segurança, análise de alertas, logs, usuários, dispositivos e aplicativos no painel de gerenciamento do Sophos Central, para assegurar que tudo esteja nos conformes. Anteriormente, esse gerenciamento diário de segurança levava o dobro do tempo para determinar os problemas de alta prioridade para abordar e as ações a tomar.

› **Redução de mais de 90% no tempo gasto no gerenciamento diário da segurança em comparação a outros fornecedores**

O cliente estima que, baseado em experiências anteriores, o gerenciamento diário da segurança levaria o dia todo se realizado com outros fornecedores, em comparação a apenas 30 minutos com a Sophos.

› **Nenhum grande incidente de segurança**

O cliente vem usando a Sophos há anos e não teve nenhum grande problema de segurança nos últimos 8 a 10 anos. Isso sem falar que as ameaças não chegam até eles: do contrário, seus produtos Sophos resolvem as ameaças de modo rápido e silencioso em segundo plano, sem que o usuário nem mesmo saiba o que está acontecendo.

## Cliente E: agência reguladora, Eslovênia

- 150 funcionários, dos quais, um terço trabalha remotamente e dois terços trabalham na matriz
- Dois funcionários de TI cobrindo todas as áreas, inclusive segurança virtual, mais o suporte de um provedor externo para grandes projetos
- Produtos Sophos: Sophos Endpoint Protection, Intercept X Advanced for Server, XG Firewall, Sophos Mobile, Sophos Device Encryption

O Cliente E é uma organização do setor público responsável por assegurar que os produtos atendam as normas necessárias. Esse cliente da Sophos de longa data migrou para os nossos produtos Next Gen que são gerenciados através do Sophos Central.

### Impacto nos negócios

- **Redução de 50% no tempo gasto no gerenciamento diário da segurança**  
Eles gastam de 15 a 30 minutos por dia na administração de segurança: verificação de firewall, análise de alertas, limpeza de e-mails em quarentena, etc. Anteriormente, gastavam, pelo menos, duas vezes mais. Esse aumento em eficiência é resultado da capacidade de gerenciar todos os seus produtos de segurança em um único lugar, sem precisar trocar entre aplicativos e servidores.
- **Nenhum grande incidente de segurança**  
O cliente não consegue se lembrar de um único grande incidente de segurança desde que começou a usar a Sophos.

## Conclusão

Como os depoimentos dos clientes demonstram, a abordagem da Sophos em segurança virtual proporciona real proteção e economia. Isso ajuda a aumentar significativamente a eficiência da sua equipe de TI e a reduzir a sua exposição a ameaças – tudo isso sem aumentar o seu quadro de funcionários.

Ainda que o ambiente comercial, recursos e desafios dos nossos clientes variem de organização para organização, eles relatam consistentemente uma redução de 50% na carga de trabalho em segurança de TI utilizando o sistema de segurança virtual da Sophos. Os clientes podem ver uma redução de 90% no tempo gasto na administração diária da segurança virtual, bem como uma redução de 85% no número de incidentes de segurança.

Para saber mais sobre as soluções de segurança virtual da Sophos e começar o seu teste de avaliação sem compromisso, visite o site [www.sophos.com](http://www.sophos.com) ou fale com um representante da Sophos.

Vendas na América Latina  
E-mail: [latamsales@sophos.com](mailto:latamsales@sophos.com)

Vendas no Brasil  
E-mail: [brasil@sophos.com](mailto:brasil@sophos.com)

© Copyright 2020. Sophos Ltd. Todos os direitos reservados.  
Empresa registrada na Inglaterra e País de Gales sob o n.º. 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.

200612 WPPTBR (NP)

# SOPHOS