SOPHOS
Cybersecurity evolved.

# Ecossistema de Segurança Cibernética Adaptativa da Sophos

O Ecossistema de Segurança Cibernética Adaptativa (ACE) da Sophos é um amplo sistema desenvolvido para otimizar a prevenção, detecção e resposta. Ele protege a nova realidade de sistemas corporativos interconectados, além de estabelecer defesas contra o cenário de ataques cibernéticos em constante mudança, que combina a automação à atividade humana dos hackers.

O Sophos ACE mescla automação e analistas, além das informações de produtos, parceiros, clientes e desenvolvedores da Sophos para criar proteção que melhora continuamente – um ciclo virtuoso que aprende e se aprimora constantemente. O melhor de tudo é que você pode começar pequeno e crescer. Comece com a tecnologia de endpoint ou firewall da Sophos e crie a sua base.

*Documento técnico Sophos. Maio de 2021*

# Um panorama em mudança

O panorama de atuação da segurança cibernética está em constante evolução, apresentando mudanças significativas tanto nos ambientes empresarias como na natureza dos ataques nos últimos anos.

## Mudança nos negócios: interconectividade

Na busca incansável a formas de melhorar a produtividade e eficiência, as organizações criaram uma cadeia de fornecimento absolutamente conectada, juntamente com a infraestrutura e a tecnologia que a suporta. A migração de dados e aplicativos para a nuvem oferece muitos benefícios, como habilidade de trabalhar de qualquer lugar, baixos custos de operação e desempenho e escalabilidade melhorados, enquanto catalisa o crescimento da cadeia de fornecimento digital global.

Paralelamente, a COVID-19 acelerou a mudança para o trabalho de casa/remoto e com isso abalou o mito do perímetro organizacional. Hoje, o pressuposto é que pessoas, aplicativos, dispositivos e dados podem estar em qualquer lugar.

Esses sistemas dispersos e interconectados atendem muito bem às nossas necessidades, mas também criam novos desafios de segurança. Muitas organizações têm dificuldades de mapear o alcance de suas redes, que se dirá de proteger todos os sistemas conectados a ela.

Adversários inteligentes e adaptáveis persistem em manter esses sistemas na mira, seduzidos pela oportunidade de incrementar suas ofertas. Uma prova disso foi o recente ataque do SolarWinds, em dezembro de 2020, que fez vítimas variando entre grandes fornecedores de tecnologia, pequenas empresas e órgãos do setor público nos mais altos níveis.

## Mudança de ataque: de automatizado para operacional

Quando você trabalha em segurança cibernética, é fácil perder a noção de um fato pouco considerado: na briga por nossos sistemas e dados críticos, a defesa está vencendo.

As manchetes diárias sobre novas violações à segurança servem a um importante propósito: nos advertir e relembrar de adotar medidas preventivas e ficar vigilantes. Mas essas histórias são uma exceção à regra. Não há manchetes sobre empresas que se defendem com sucesso contra milhares de tentativas diárias de violação.

A eficiência da segurança cibernética não apenas melhorou drasticamente – as novas ferramentas e serviços de segurança gerenciada estão mais acessíveis do que nunca. Tecnologias anti-ransomware, prevenção contra explorações, detecção comportamental e anti-phishing estão disponíveis para todos.

Essas capacidades – que são facilitadas, melhoradas e aceleradas por inteligência artificial e Machine Learning – tratam de táticas, técnicas e procedimentos de adversários conhecidos documentados na estrutura MITRE ATT&CK, bem como de novos e recentes ataques nunca antes vistos em atividade. Ao fechar lacunas, bloquear caminhos e interromper técnicas,

**MUDANÇA NOS NEGÓCIOS**

Cadeia de fornecimento interconectada

Migração para a nuvem de aplicativos e dados

Ambientes de trabalho remoto

**MUDANÇA NOS ATAQUES**

A defesa está vencendo

Automação + operação do invasor

Custos mais altos de violação

essas melhorias deixaram alguns ataques tão onerosos que os invasores tiveram que se adaptar. As melhorias em segurança são tão significativas que o ditado "o invasor só precisa acertar uma vez" já não se aplica mais. Para fazer dinheiro, os invasores precisam acertar várias vezes durante o ataque.

Na verdade, a abordagem mudou de malware automatizado para uma abordagem mais abrangente que combina automação com hackers atuantes. A meta central de um invasor é não ser detectado, e a melhor forma de fazer isso é agir como um funcionário – usando ferramentas locais, dispositivos locais e padrões típicos de tráfego.

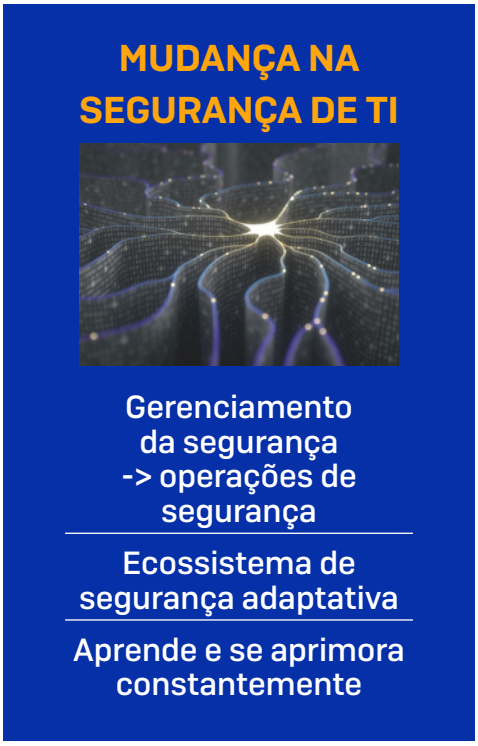
Esses ataques sofisticados, que requerem um investimento humano significativo, são também os mais onerosos para as vítimas. Os invasores são capazes de explorar o conhecimento profundo que têm do ambiente da vítima para causar o máximo de danos – e exigir o máximo de retorno.

## A segurança de TI muda para operações de segurança

Tais mudanças em negócios e ataques precisam de uma segurança de TI que evolua. As organizações enfrentam um adversário inteligente que continuamente reloca o objetivo conforme avança em sua direção, exigindo que as equipes de segurança de TI desenvolvam contramedidas que melhorem suas chances de vencer.

Primeiro, exige uma mudança em etapas de **gerenciamento de segurança para operações de segurança**. Os dias em que definir uma política de segurança e deixá-la cumprir o seu papel já se foram. Conforme os invasores se movem para um estilo mais prático de "atuação", a segurança de TI precisa fazer o mesmo para caçar e detectar comportamentos e eventos suspeitos antes que se tornem uma violação.

Equipes de segurança precisam procurar por atividades suspeitas logo no início da cadeia de ataque para dar aos defensores a habilidade de responder antes que o estrago seja feito. Mesmo os ataques furtivos deixam rastros, e as equipes de segurança precisam encontrar e seguir as pistas para parar o ataque logo no início do processo. Não é mais uma simples questão de encontrar um sinal em meio a ruídos, mas de identificar sinais fracos e críticos antes que se tornem sinais fortes. Quanto mais forte for o sinal, mais perto você estará de uma violação. Com as ferramentas apropriadas, os problemas de TI podem ser proativamente detectados e corrigidos antes que um adversário seja capaz de descobri-los e usá-los em um ataque.




Com as empresas superconectadas de hoje, a segurança precisa seguir o mesmo exemplo. As equipes de segurança de TI precisam mudar dos produtos com pontos de segurança não integrados para um **sistema de segurança adaptativa** que previna automaticamente o máximo possível de problemas, enquanto habilita os operadores a procurar e detectar sinais fracos, como comportamentos e eventos suspeitos, e evitar que se transformem em violações ativas.

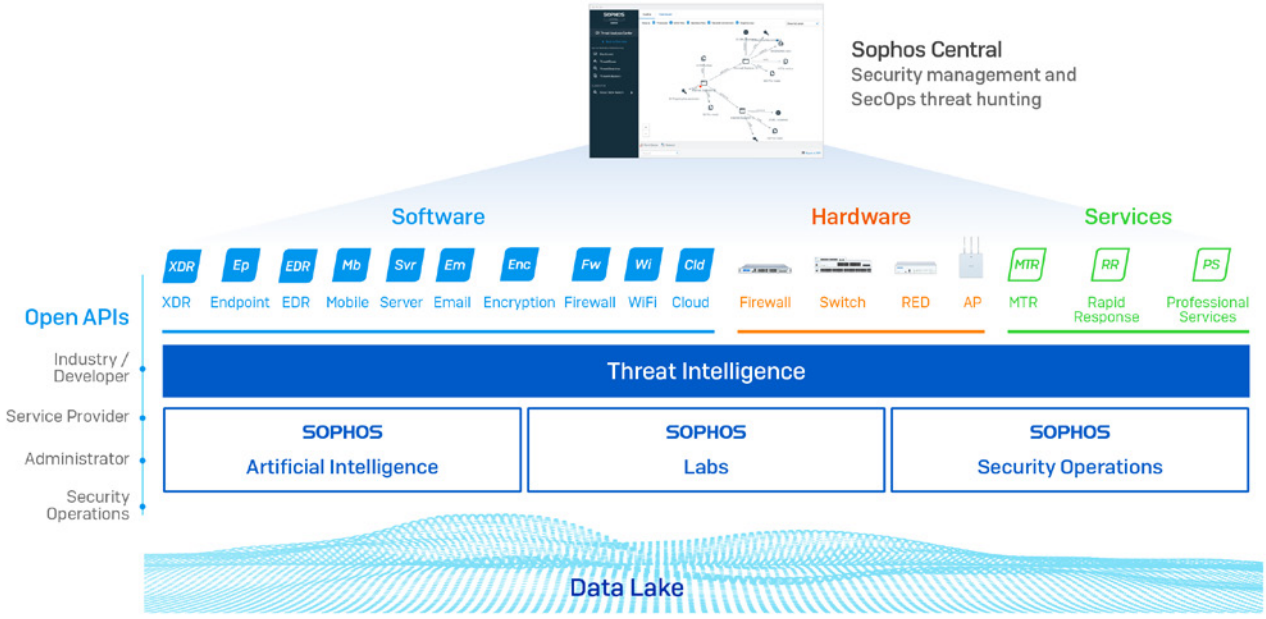
Ambientes empresariais e ataques estão sempre evoluindo. O futuro da segurança de TI é um sistema que possibilite um loop único de feedback, de modo que possa **aprender e se aprimorar constantemente.** Novas informações e eventos detectados pelas equipes de operações podem ser automatizados, melhorando a prevenção e reduzindo o número de novos ataques que entram no sistema. Seguindo o mesmo princípio, conforme a automação do software melhora, os

operadores podem localizar comportamentos e eventos suspeitos com mais rapidez, reduzindo ainda mais o número de incidentes. Esse ciclo virtuoso melhora constantemente a segurança geral da organização e de suas conexões empresarias.

# Ecossistema de Segurança Cibernética Adaptativa da Sophos

Vamos começar com uma boa notícia: esse sistema já existe. O Ecossistema de Segurança Cibernética Adaptativa (ACE) da Sophos aborda essa nova realidade. Ele combina o poder da automação e analistas para acionar a mudança do gerenciamento de segurança para as operações de segurança. A automação pode analisar e reagir com maior velocidade a comportamentos e eventos, enquanto os analistas humanos são exímios na correlação de sinais suspeitos múltiplos e interpretação do seu significado.

O Sophos ACE foi projetado para proteger a interconectividade dos negócios e do mundo online. Ele protege sistemas e dados onde estiverem, aprendendo e se aprimorando constantemente para proteção contra futuras mudanças em tecnologias e ataques.




O ponto de partida do Sophos ACE congrega a **inteligência de ameaças** da SophosLabs, o Sophos Security Operations (analistas humanos que conduzem caça a ameaças avançadas em meio a milhares de ambientes de clientes através do nosso serviço Managed Threat Response) e o grupo do Sophos Artificial Intelligence. Essas funcionalidades com inteligência em tempo real melhoram continuamente as tecnologias next-gen em nossas ofertas de **software** e **hardware** líderes mundiais.

Um único **Data Lake** integrado reúne informações de todos os nossos produtos e fontes de inteligência de ameaças, com análise em tempo real que permite que a defesa impeça violações ao encontrar proativamente sinais suspeitos em meio à grande quantidade de informações. Paralelamente, **APIs abertas** permitem que clientes, parceiros e desenvolvedores criem ferramentas e soluções que interajam com o sistema. Tudo gerenciado através da **plataforma de gerenciamento do Sophos Central**. Toda a sua segurança em um único lugar, oferecendo eficiência sem igual.

Esses cinco elementos – inteligência de ameaças, tecnologias next-gen, Data Lake, APIs e gerenciamento central – trabalham em conjunto para criar um ecossistema de segurança cibernética adaptativa que aprende e se aprimora constantemente. O poder do sistema geral é intenso, e você pode usar o quanto precisar, sem limitações. Muitos clientes começam com a nossa proteção de endpoint ou firewall e depois expandem no seu próprio ritmo.

No ano passado, vários Centros de Operações de Segurança se transformaram em SOCs virtuais. O Sophos ACE pode ser

gerenciado por especialistas em segurança a partir de qualquer local, o que dá às organizações a habilidade de encontrar os melhores profissionais em segurança global. Alternativamente, os nossos peritos podem gerenciar a detecção e resposta a ameaças para você como um serviço.

# A evolução da Segurança Sincronizada

A Segurança Sincronizada – a habilidade dos produtos Sophos de compartilhar informações em tempo real através do Security Heartbeat™ e automatizar a resposta a incidentes – tem sido um elemento fundamental da nossa proteção há muitos anos. Quando foi lançada, em 2015, a Segurança Sincronizada se destacou no mercado pela sua unicidade, e continuamos a oferecer a integração mais completa entre os fornecedores de segurança com insights mais detalhados entre produtos.

*"A Sophos continua a liderar o mercado com suas funcionalidades XDR entre produtos de segurança de endpoint e firewall."*

Gartner
Gartner Magic Quadrant for Enterprise Network Firewalls.
Analistas: Rajpreet Kaur | Adam Hils | Jeremy D'Hoinne | 9 de novembro de 2020

O Ecossistema de Segurança Cibernética Adaptativa da Sophos é baseado na automação e integração da Segurança Sincronizada, ampliando ainda mais o sistema de segurança cibernética da Sophos.

## Mais visibilidade

Ninguém sabe de onde virá o próximo ataque, e é simplesmente impossível para os operadores humanos monitorar tudo. Portanto, você precisa de um sistema que monitore tudo, para poder reagir rapidamente a ameaças emergentes. Por isso, ampliamos nosso ecossistema de modo a incluir uma faixa mais abrangente de tecnologias, como o novo Sophos Extended Detection and Response (XDR) e suas APIs. Os produtos Sophos veem e registram todos os eventos, comportamentos e detecções suspeitos em todo o seu ambiente, de modo que você tenha em mãos todas as informações de que precisa.

## Mais dados

O Data Lake combina e correlaciona informações de todos esses sensores e oferece insights profundos de todos os produtos. Operadores podem consultar o Data Lake diretamente com o Sophos Intercept X with EDR e o Sophos XDR, permitindo a identificação dos comportamentos e eventos suspeitos em todo o seu ambiente – e evitar que problemas se transformem em violações.

## Mais inteligência

Com o rápido crescimento do nosso serviço Managed Threat Response (MTR), somos capazes de adicionar dados em tempo real diretamente das descobertas realizadas por nossos peritos em caça a ameaças para complementar a detecção de dados. Paralelamente, continuamos avançando nossos modelos de IA e dados sobre detecções de ameaças do SophosLabs.

## Mais integração

O SophosLabs, o Sophos AI e o Sophos Security Operations trabalham em conjunto, integrando expertise que beneficia todos os clientes em um ciclo virtual. Por exemplo, o PowerShell é uma ferramenta legítima aplicada ao uso honesto e que também é amplamente explorada pelos invasores. Os operadores do MTR treinam nossos modelos de IA para distinguir entre o "bom" uso do PowerShell e o "mau" uso do PowerShell baseados em suas experiências reais. O sistema inteiro é atualizado com esse aprendizado de IA, elevando a proteção dos clientes.

# Ecossistema de Segurança Cibernética Adaptativa da Sophos em ação

O Sophos ACE é um sistema em tempo real que elevou e estendeu a proteção para o panorama geral do mundo real. Em março de 2021, um grupo adversário chamado Hafnium explorou uma vulnerabilidade ProxyLogon no Microsoft Exchange. Essa foi uma vulnerabilidade de dia zero, quando os invasores se aproveitaram das fraquezas inerentes do Exchange para impedir o disparo de detecções imediatas.

Assim que a vulnerabilidade ficou conhecida, o serviço Sophos Managed Threat Response (MTR) atualizou instantaneamente o monitoramento sensorial para incluir comportamentos associados ao ProxyLogon. Com as informações já depositadas no Data Lake, o Sophos MTR teve acesso instantâneo a todas as entradas de que precisava para identificar e corrigir atividades maliciosas relacionadas a essa vulnerabilidade.

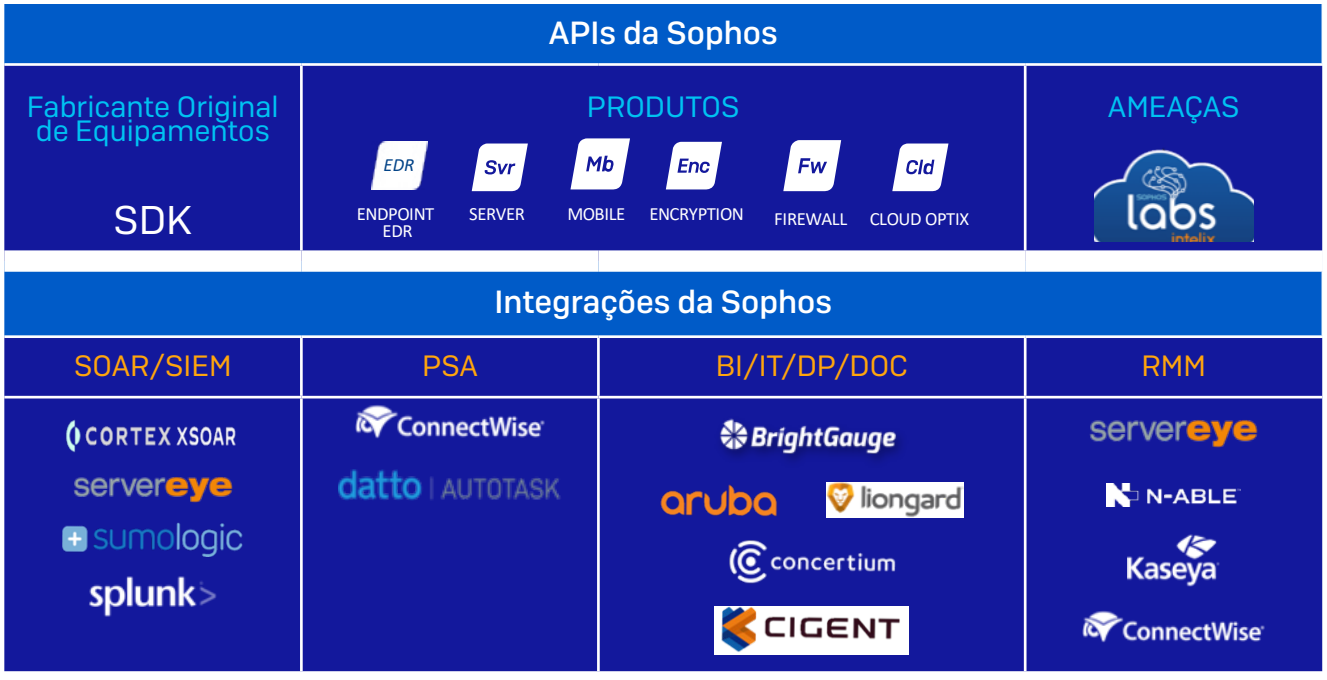
Além disso, combinaram suas habilidades de caça a ameaças com a tecnologia Sophos EDR para desvendar novos artefatos ou indicadores de comprometimento (IOCs) relacionados ao ataque. Esses indicadores foram compartilhados diretamente com o SophosLabs, que os utilizou para publicar IOCs adicionais relacionados com a vulnerabilidade do Exchange, oferecendo proteção extra para todos os clientes da Sophos.

# Uma plataforma com poderosas integrações e APIs abertas

Em nosso mundo interconectado, é essencial que a segurança cibernética possa integrar-se com o ambiente empresarial em toda a sua extensão. A segurança cibernética é multifacetada, e o Ecossistema de Segurança Cibernética Adaptativa da Sophos cobre uma grande parte dessas necessidades de proteção:

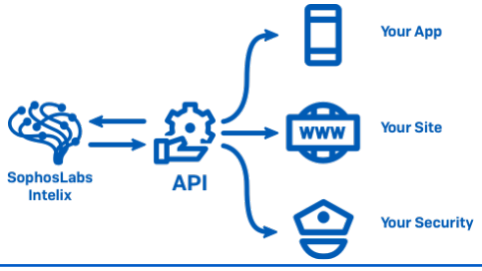
- MSSPs – suporta a entrega de defesas cibernéticas avançadas a seus clientes
- Parceiros de canal – agiliza o processo de negócios
- ISPs – garante a segurança dos serviços de Internet entregues
- Pequenas e médias empresas – facilita a criação de ferramentas personalizadas para controlar e ativar a segurança

Uma infinidade de APIs e integrações já está em vigor – e há mais por vir – com o Sophos ACE manipulando mais de cinco milhões de solicitações de API todos os dias.



### Mostra de API: SophosLabs Intelix™

O Intelix é uma combinação de APIs RESTful simples e de resposta rápida que permite que os aplicativos identifiquem, classifiquem e previnam ameaças, aumentando a segurança que oferecem. Os clientes, parceiros e desenvolvedores integrados ao ecossistema da Sophos podem usar essas APIs para fazer buscas de ameaças na nuvem, análises de arquivos estáticas e análises de arquivos dinâmicas. Mais informações sobre as APIs do SophosLabs Intelix estão disponíveis em https://www.sophos.com/pt-br/labs/intelix.aspx.




## Sophos ACE: criando um verdadeiro impacto nos negócios

Os benefícios do Ecossistema de Segurança Cibernética Adaptativa da Sophos só aumentam. Tecnologias Next-Gen combinadas: a inteligência de ameaças do SophosLabs, Sophos AI e Sophos Security Operations; um sistema integrado, adaptativo e em constante aprendizado; e o gerenciamento centralizado através da plataforma Sophos Central causam um grande impacto à proteção e à eficiência que proporcionam.

| | | | | | | |
|---|---|---|---|---|---|---|
| **Tecnologias Next-Gen** | **+** | **Inteligência de ameaças** | **+** | **Sistema adaptativo, integrado** | **+** | **Gerenciamento centralizado** |

Os clientes com o Sophos Firewall e o Sophos Intercept X já nos disseram que teriam que dobrar o quadro de funcionários de segurança para manter o mesmo nível de proteção se não tivessem um sistema de segurança cibernética da Sophos. Também disseram passar por menos incidentes de segurança e que podem identificar e responder mais rapidamente aos problemas que ocorrem. O Sophos ACE se baseia nisso, avançando na transformação do TCO da segurança cibernética, bem como na proteção.

# Como começar

O Ecossistema de Segurança Cibernética da Sophos é bastante flexível, e sua utilização é tão simples quanto implantar qualquer um dos produtos e serviços de proteção da Sophos. As organizações se beneficiam imediatamente da combinação especializada de inteligência artificial do Sophos AI, SophosLabs e Sophos Security Operations. Você pode expandir o seu ecossistema a qualquer momento, em alinhamento com as necessidades dos seus negócios. Os pontos de partida mais comuns incluem:

Sophos Intercept X, para endpoints ou servidores (com a opção de adicionar a funcionalidade EDR ou XDR)

Sophos Firewall – hardware, software ou virtual

Serviço Sophos Managed Threat Response (MTR)

Para saber mais, fale com um representante da Sophos, visite o site ou faça uma a avaliação gratuita.

Gartner Magic Quadrant for Enterprise Network Firewalls.
Analistas: Rajpreet Kaur | Adam Hils | Jeremy D'Hoinne | 9 de novembro de 2020

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 pesquisa da Gartner consistem em opiniões da organização de pesquisa da Gartner e não devem ser interpretadas como declarações de fato. A Gartner renuncia a todas as garantias, expressas ou implícitas, com relação a essa pesquisa, incluindo quaisquer garantias de comercialização ou de adequação a um propósito específico.

Saiba mais sobre ransomware e como a Sophos pode ajudar a defender a sua organização.

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.



2021-04-26 (SB-NP)

SOPHOS