SOPHOS

A carência de qualificação em segurança virtual em PMEs

Explorando o impacto da falta de qualificação em segurança cibernética à linha de frente das pequenas e médias empresas e como lidar com os desafios causados a recursos e orçamentos.

Documento técnico Sophos. Outubro, 2024

Introdução

A carência global de qualificação em segurança cibernética é bastante conhecida e muito bem documentada e não dá sinais de que se dissipará muito em breve, fazendo com que as organizações de pequeno e médio porte procurem formas de driblar os seus efeitos.

Nessa saga, o primeiro passo é entender o tamanho do desafio. Este relatório traz os resultados levantados em uma pesquisa independente realizada com profissionais da linha de frente em todo o mundo e revela como a carência de qualificação afeta as organizações de pequeno e médio porte no dia a dia. Baseado nesses insights, ele oferece diretrizes práticas para tratar desses desafios na contenção de recursos e orçamentos. O relatório também explora as soluções da Sophos que permitem que as organizações menores obtenham melhores resultados na segurança cibernética.

Sobre a pesquisa

A Sophos contratou uma pesquisa independente com 5.000 profissionais da linha de frente em TI e segurança cibernética em 14 países. 1.402 entrevistados trabalham em organizações com 100 a 500 funcionários, o menor segmento de empresas de pequeno e médio porte (PME) neste relatório. A pesquisa foi conduzida no primeiro trimestre de 2024.

As pequenas organizações são afetadas desproporcionalmente pela carência de qualificações

A falta de competências tem grande peso nas PMEs e um impacto desproporcional. A pesquisa revela que as **organizações com menos de 500 funcionários classificam a escassez de especialistas em segurança cibernética nas equipes internas como o segundo maior risco à segurança cibernética**, suplantado apenas pelas ameaças de dia zero. Já entre aquelas com mais de 500 funcionários, ficou em sétimo lugar.

Posicionamento relativo de "escassez de especialistas em segurança cibernética nas equipes internas" como risco à segurança cibernética das empresas

PMEs (n=1.402)	GRANDES ORGANIZAÇÕES (n=3.598)	
100 – 500 FUNCIONÁRIOS	501 – 1000 FUNCIONÁRIOS	1001 – 5000 FUNCIONÁRIOS
Nº 2	Nº 7	Nº 7

Quem ou quais você considera como sendo os três principais riscos à segurança cibernética na sua organização? Posição relativa de "escassez de especialistas em segurança cibernética nas equipes internas" entre as respostas classificadas em primeiro lugar (números de base no gráfico)

Organizações de todos os tamanhos sentem o impacto da escassez de especialistas, mas, com certeza, o maior impacto é nas PMEs. Os riscos mais altos que atingem as grandes organizações, como a falta de ferramentas de segurança cibernética (o 2º risco mais observado pelas empresas com 501 a 1.000 funcionários) e credenciais e dados de acesso roubados (o 2º risco mais observado pelas empresas com 1.001 a 5.000 funcionários), são considerações secundárias para as empresas de menor porte que lutam contra questões mais básicas, como encontrar pessoal para operar seus investimentos existentes.

Carência de qualificação: um duplo desafio

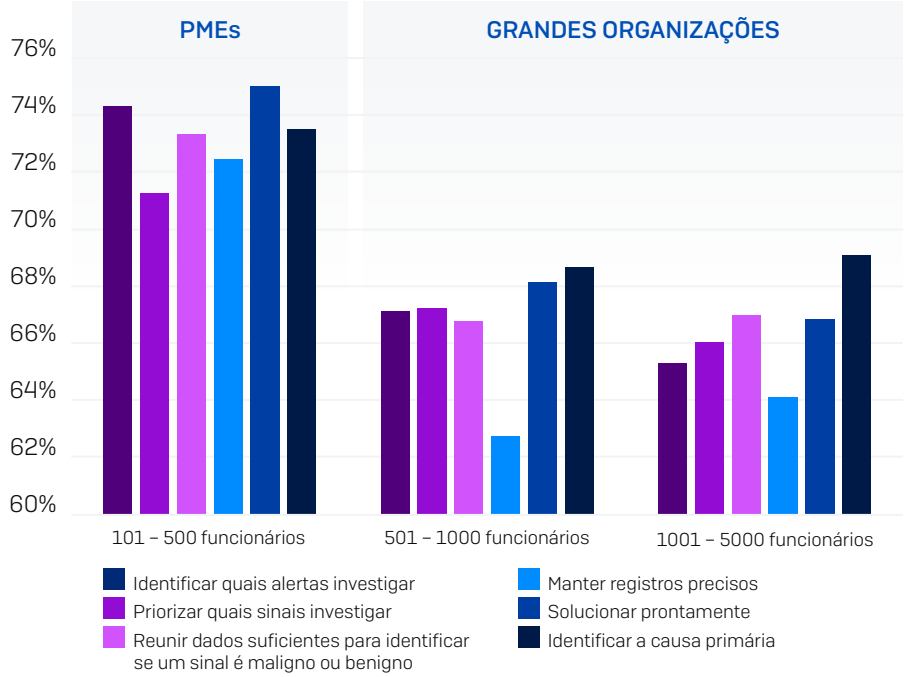
A verdade sobre a carência de qualificação é simples: a quantidade de profissionais qualificados em segurança cibernética é insuficiente, e isso afeta as PMEs de duas maneiras.

Falta de expertise

A tecnologia de segurança e as ameaças cibernéticas são complexas. A capacidade de trabalhar com a segurança cibernética é uma competência avançada que exige um alto grau de especialização — e a linha de referência se mantém em crescente ascensão. Como os ataques cibernéticos continuam a aumentar em complexidade, o nível de expertise necessária para bloqueá-los também aumenta.

Esta pesquisa revela que **96% das pequenas empresas apontam pelo menos um aspecto da investigação de alertas suspeitos que é desafiador**. As grandes organizações geralmente têm dificuldade com as operações de segurança, mas o grande desafio fica mesmo para as PMEs.

Porcentagem de organizações que acham as operações de segurança desafiadoras



Se a sua organização investiga alertas de segurança internamente, qual o grau de desafio que as seguintes etapas representam para a sua organização durante a investigação de alertas suspeitos? "Bastante desafiadora" e "Relativamente desafiadora" (número de base no gráfico)

A praticidade de desenvolver competências em segurança cibernética apresenta um desafio maior para quem trabalha em PMEs. Quando a equipe de segurança e TI é formada por apenas algumas poucas pessoas, fica mais difícil dedicar um tempo regular para os estudos. Além disso, em equipes pequenas, as pessoas têm menos oportunidades para se beneficiar do aprendizado passado pelos colegas de trabalho.

Falta de capacidade

Os adversários não trabalham das 8h às 18h, o que faz da segurança cibernética uma operação 24 horas. Na verdade, 91% dos ataques de ransomware começam fora do horário comercial padrão, quando os invasores tentam se infiltrar nas organizações sem ser detectados[1].

O feedback dos operadores da linha de frente sugere que a cobertura de segurança cibernética 24/7 exige, no mínimo, de quatro a cinco funcionários em período integral para poder cumprir com férias, licença e fins de semana. Para a maioria das PMEs, isso é simplesmente impraticável de se atingir trabalhando apenas com recursos internos.

A pesquisa ilustra esse ponto ao revelar que, durante **um terço (33%) do tempo, as PMEs ficam sem ninguém ativamente monitorando, investigando e respondendo aos alertas**. Sem uma defesa ativa, as pequenas organizações ficam extremamente expostas a ataques.

33%
das PMEs não têm ninguém monitorando e investigando alertas de segurança

Durante o último ano (incluindo noites, fins de semana e feriados), qual foi a porcentagem de tempo em que a sua organização teve alguém ativamente monitorando e investigando alertas? n=1.402 organizações com 100-500 funcionários.

1 Detendo adversários ativos: lições da linha de frente para a defesa cibernética, Sophos

O impacto da lacuna em competências em segurança cibernética nas pequenas empresas

A carência de qualificação afeta as PMEs de diferentes formas. Esse é o segmento com maior probabilidade de ter os dados criptografados em um ataque de ransomware, com 74% dos incidentes resultantes da criptografia de dados. Esse é um provável reflexo da baixa capacidade de detectar e bloquear adversários antes que o ransomware seja detonado.

Porcentagem dos ataques de ransomware que resultaram na criptografia de dados

PMEs (n=1.402)	GRANDES ORGANIZAÇÕES (n=3.598)	
100 – 500 FUNCIONÁRIOS	501 – 1000 FUNCIONÁRIOS	1001 – 5000 FUNCIONÁRIOS
74%	72%	66%

Fonte: O Estado do Ransomware 2024, Sophos. Os criminosos virtuais tiveram sucesso na criptografia de dados da sua organização no ataque de ransomware? Sim. Números de base no gráfico.

Além disso, com menos pessoal para dividir a carga da segurança cibernética, o potencial de esgotamento físico e mental dos especialistas é bastante alto. Em uma pesquisa encomendada pela Sophos e que abrangeu o Japão e a região da Ásia-Pacífico, **85% das organizações disseram ter enfrentado fatiga e esgotamento entre seus profissionais de TI e segurança cibernética**, com quase 1 em cada 4 (23%) tendo problemas "frequentemente" e 62% "ocasionalmente". O preocupante é que 90% das empresas disseram que o esgotamento e a fatiga aumentaram nos últimos 12 meses, e 30% delas disseram que o aumento foi "significativo".

85%
das organizações relataram fatiga e esgotamento entre seus profissionais de TI e segurança cibernética

Como lidar com a falta de qualificação nas pequenas empresas

Contratar mais pessoal não é uma opção viável para a maioria das PMEs. Aumentar o quadro de funcionários de segurança cibernética exige uma grande demanda orçamentária e tem um impacto desproporcionalmente mais alto no orçamento de RH das pequenas organizações em comparação às grandes organizações, além da competitividade que as organizações enfrentam na disputa por um número limitado de bons profissionais. Os profissionais com qualificações em demanda são, em geral, mais seletivos, dando preferência a trabalhar em organizações maiores, que oferecem melhores oportunidades de desenvolvimento e progressão. A solução para enfrentar as dificuldades de contratação de pessoal capacitado é trabalhar com especialistas em segurança independentes e usar as soluções de segurança cibernética projetadas para PMEs.

Trabalhar com especialistas em segurança terceirizados

O engajamento com especialistas em segurança cibernética terceirizados é, geralmente, a forma mais fácil e mais econômica de adicionar capacidade e perícia. As duas abordagens mais comuns são os serviços de detecção e resposta gerenciadas (MDR) e os provedores de serviços gerenciados (MSP).

Normalmente, os serviços **MDR** oferecem busca, detecção e resposta a todo o seu ambiente 24 horas por dia, sete dias por semana. Os analistas monitoram a sua organização, identificando e respondendo a atividades suspeitas, e neutralizando ataques antes que afetem seus negócios.

Procure por um provedor que se enquadre em suas necessidades e forma de trabalhar, seja para terceirizar o processo completo de detecção e resposta ou para colaborar com seus analistas. Considerando também os orçamentos quase sempre apertados, é importante que você trabalhe com um serviço que utilize as suas tecnologias existentes de segurança, evitando assim o custo e a inconveniência de ter que "modernizar" suas operações.

Para ajudar a custear os serviços MDR, você pode usufruir de descontos e facilidades oferecidos por seu provedor de seguro de proteção digital. Os usuários de MDR são considerados clientes "Tier 1" pelas seguradoras, pois estão no patamar de menor risco de sinistro. Consequentemente, acaba sendo uma prática regular entre as seguradoras oferecer descontos substanciais às organizações que utilizam serviços MDR — e esse dinheiro pode ser direcionado para pagar o próprio serviço.

Estudo de caso da Sophos: organização sem fins lucrativos com 350 funcionários

Uma organização sem fins lucrativos na Carolina do Norte, EUA, com um quadro de 350 funcionários conseguiu reduzir o prêmio do seguro de proteção digital em US$ 8.000 porque estava usando o serviço Sophos MDR. Com a assinatura anual do Sophos MDR no valor de US$ 8.467, a economia com o seguro lhes proporcionou 24 horas diárias de detecção e resposta a ameaças por especialistas por um valor incremental de apenas US$ 467.

Há anos os **MSPs** têm dado suporte de segurança cibernética e TI para as pequenas empresas, atuando como suas equipes internas. Com as ameaças cibernéticas aumentando continuamente em complexidade, as organizações de médio porte optaram por trabalhar com MSPs para complementar seus recursos internos.

MDR e MSPs não são mutuamente exclusivos: uma pesquisa da Sophos revela que a maioria dos MSPs (81%) oferece serviços MDR,[2] permitindo que você se beneficie dessas duas camadas de suporte através de um único provedor. Alguns MSPs optam por oferecer serviços MDR apenas internamente, enquanto outros preferem trabalhar com provedores terceirizados especializados em MDR.

Escolha soluções projetadas ativamente para PMEs

A maioria das soluções de segurança cibernética é projetada e desenvolvida para organizações de grande porte com grandes equipes para implantá-las e gerenciá-las. Essas soluções de nível empresarial exercem uma certa atração sobre as pequenas empresas, mas, em realidade, na maior parte das vezes essas organizações não conseguem ver os benefícios em retorno de investimentos ou segurança, pois não são capazes de usá-las de maneira eficiente.

Portanto, busque ferramentas de segurança que sejam tecnicamente avançadas, mas projetadas para facilidade de uso por equipes de TI extenuadas, que é a realidade do mundo moderno. Mudar o seu foco de compra não deve aumentar seus gastos, podendo até mesmo oferecer uma oportunidade de reduzir as despesas com tecnologia e gerenciamento. Ao avaliar as soluções de segurança, considere os recursos do produto e da plataforma.

Plataforma

- Uma plataforma de segurança cibernética é uma ferramenta centralizada que lhe permite implantar, monitorar e gerenciar diferentes soluções de segurança cibernética em um só lugar, como, por exemplo, sua proteção de endpoint e antivírus, segurança de e-mail e firewall.
- Consolidar suas soluções de segurança cibernética em uma única plataforma reduz consideravelmente as despesas gerais com a administração diária, já que não é preciso ficar pulando de um painel para outro para ver o que está acontecendo. Diminuir o número de provedores com quem você trabalha ajuda a reduzir as despesas com o gerenciamento de fornecedores.
- Uma plataforma eficiente também permitirá que as suas soluções trabalhem em conjunto, compartilhando telemetria, insights, políticas baseadas em usuário e mais, elevando suas defesas cibernéticas.

Características do produto

- Os fornecedores apresentam em seus sites uma longa lista de características e recursos. Antes de avaliar as soluções, pondere o que você realmente precisa e não precisa para não pagar por tecnologias que não o beneficiarão em nada.
- Para obter o máximo de seus investimentos em segurança cibernética, você deve poder implantar e usar as soluções com eficiência. Escolha soluções que implementem configurações recomendadas automaticamente desde o princípio, eliminando dessa forma a necessidade de fazer uma configuração manual laboriosa e a possibilidade de equívocos na hora da implantação. Procure também por controles intuitivos projetados para ambientes realistas e que sejam fáceis de usar.
- A configuração incorreta das ferramentas de segurança é o maior risco para as PMEs. Manter uma boa postura é essencial para a sua segurança contínua, o que significa escolher soluções que ofereçam uma visibilidade clara de suas subimplantações e suporte para a correção rápida.
- Sendo uma equipe que cuida de uma pequena empresa, muito provavelmente o seu pessoal não poderá se dedicar apenas à segurança cibernética, o que torna particularmente importante escolher soluções que respondam automaticamente aos ataques até que você possa tomar o controle da situação.

2 Perspectivas para MSP 2024 – Sophos

Como a Sophos pode ajudar

A Sophos tem uma profunda experiência na proteção de organizações de pequeno e médio porte contra ameaças cibernéticas avançadas e oferece uma grande diversidade de produtos e serviços desenvolvidos especificamente para atender a essas necessidades.

Especialistas em segurança terceirizados

MDR

A Sophos oferece o serviço MDR mais confiável do mundo, protegendo mais pequenas empresas do que qualquer outro provedor. Temos excelentes insights dos ataques às pequenas empresas e utilizamos a telemetria de nossa base de clientes para elevar a proteção de todos os usuários.

O serviço Sophos MDR é altamente conceituado por clientes e analistas da área. Recentes reconhecimentos incluem:

- Customers' Choice pela Gartner® Peer Insights™ nos últimos dois anos, com pontuação 4,8/5 obtida em 647 avaliações, 17 de setembro de 2024
- Líder em MDR pela G2, incluindo classificação de Solução de MDR Nº 1 entre os clientes de médio porte
- Líder Mundial em Managed Detection and Response (MDR) pela IDC MarketScape na Vendor Assessment de 2024

"Para as organizações que buscam um provedor de MDR com grande perícia em segurança e com serviços realizados por humanos, que se engajam com a empresa desde o pressuposto até o desfecho, a Sophos é uma escolha sensata."
– Richard Thurston, Gerente de Pesquisa, Serviços Europeus de Segurança, IDC

MSP

A Sophos formou um ecossistema amplo e crescente de parceiros MSP que fornecem produtos e serviços da Sophos, incluindo o Sophos MDR, a PMEs mundialmente.

Soluções projetadas ativamente para PMEs

Plataforma

O **Sophos Central** é a maior e a mais escalável plataforma alimentada por IA e nativa na nuvem do setor. Ela é usada para gerenciar todas as soluções de segurança cibernética Sophos Next-Gen, incluindo Sophos Endpoint, Sophos Firewall, Sophos XDR, Sophos MDR, Sophos Email e Sophos ZTNA. As integrações com a grande diversidade de tecnologias independentes, incluindo Microsoft e Google, garantem que os clientes possam obter total valor de seus investimentos em segurança já existentes.

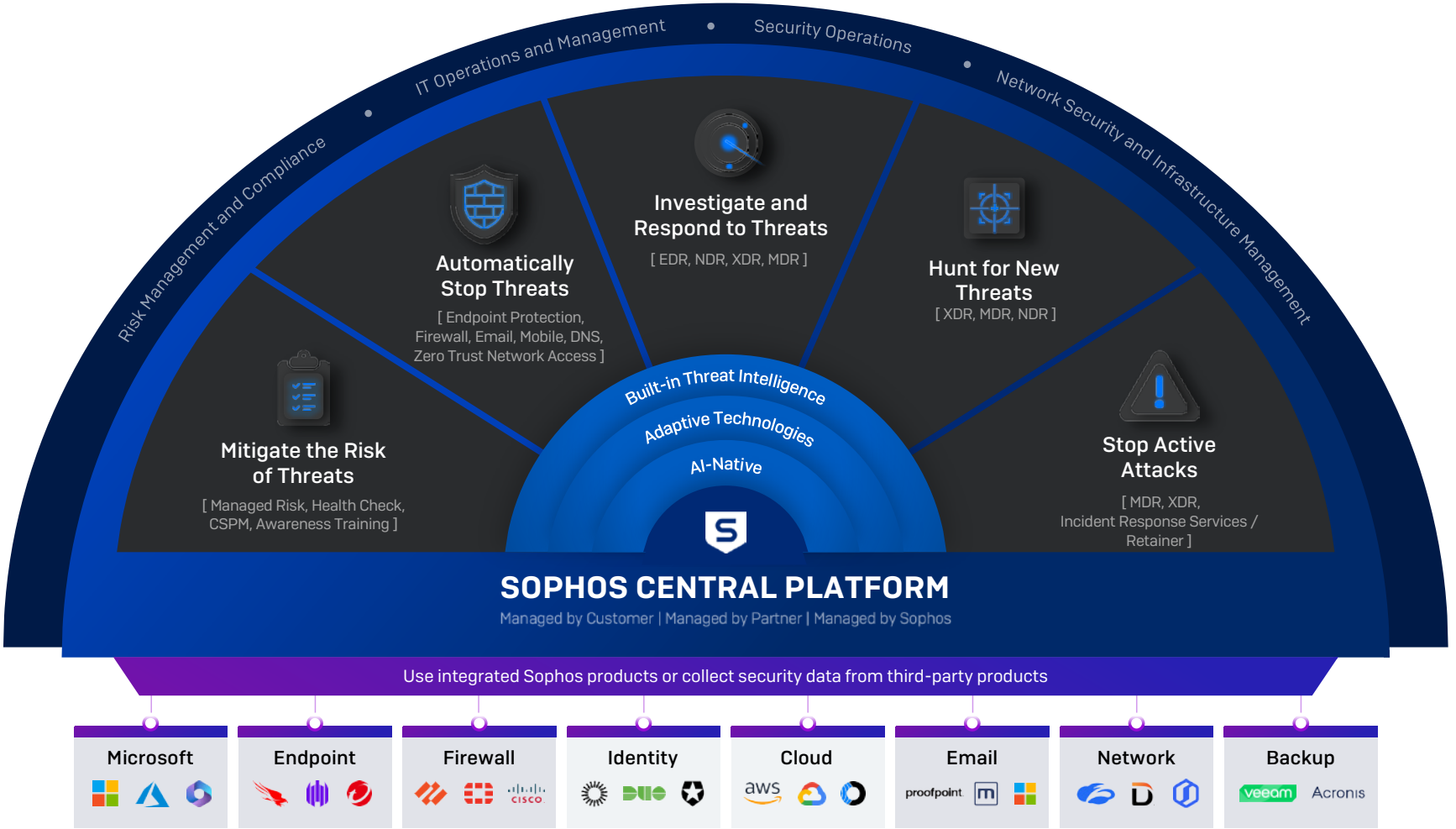
Características do produto

As soluções Sophos são altamente sofisticadas e potencializadas por décadas de experiência no bloqueio de ameaças cibernéticas. Também são projetadas para oferecer facilidade de uso, assegurando que organizações de todos os tamanhos e níveis de operação se beneficiem de suas funcionalidades de defesa líderes de mercado.

Exemplos:

- O **Sophos Endpoint** implanta automaticamente as configurações recomendadas, incluindo nossa proteção contra ransomware líder do setor e recursos anti-exploit, sem a necessidade de ajustes manuais.
- Os relatórios e o gerenciamento centralizado do **Sophos Firewall** permitem gerenciar vários firewalls em um só lugar, o que é particularmente útil para as organizações com unidades dispersas.
- O **Sophos Endpoint** inclui defesas adaptáveis que detectam a presença de adversários no seu ambiente e respondem automaticamente, elevando suas defesas e lhe dando tempo para agir.
- A verificação incorporada de integridade de conta do **Sophos Endpoint** oferece visibilidade clara e em tempo real da postura de segurança, além de um botão para a correção automática que permite reaplicar as configurações recomendadas com um único clique.
- A integração do **Sophos Firewall** com a ampla plataforma Sophos permite bloquear as ameaças ativas automaticamente e coordenar uma resposta entre endpoints e ZTNA, além de switches e pontos de acesso sem fio para prevenir o movimento lateral.

A plataforma Sophos de segurança cibernética



Conclusão

A pesquisa revela que a carência de qualificação em segurança cibernética afeta intensamente as organizações de pequeno e médio porte. A falta de capacitação e habilidades resultante tem um impacto substancial na capacidade da empresa se defender de ataques. Ainda sem perspectivas de encontrar a luz no fim do túnel, as organizações de pequeno porte podem, e devem, mitigar o impacto trabalhando com especialistas terceirizados e escolhendo soluções projetadas especificamente para os seus negócios.

Para saber mais sobre as soluções da Sophos para organizações de pequeno e médio porte, fale com um representante ou parceiro da Sophos ou acesse www.sophos.com.

2024-10-08 PTBR-WP (PC)

SOPHOS