ESTUDO DE CASO DE CLIENTE

Construída para crescer: como a MÚTUA transformou a segurança em vantagem estratégica

Como uma das maiores caixas de assistência profissional do Brasil, a MÚTUA precisava de uma abordagem de segurança capaz de acompanhar a escala e a complexidade de suas operações. Com a Sophos, fortaleceu sua proteção por meio de detecção, resposta e contenção coordenadas em todo o ambiente.

SOPHOS

mútua
Caixa de Assistência dos Profissionais do Crea

Setor
Seguros/Benefícios

Número de usuários
Mais de 133.000 associados atendidos

Estrutura
27 escritórios regionais + 1 sede em Brasília

Soluções Sophos
Sophos Firewall,
Sophos Endpoint,
Sophos XDR
Powered by Secureworks,
Sophos MDR Plus,
Sophos Next-Gen SIEM

Sobre a MÚTUA

A MÚTUA é uma das maiores caixas de assistência profissional do Brasil, oferecendo benefícios reembolsáveis, programas de previdência e suporte a mais de 133.000 engenheiros, agrônomos e profissionais de geociências em 29 unidades em todo o país. Responsável por gerenciar informações pessoais e financeiras sensíveis, a MÚTUA desempenha um papel fundamental na proteção da segurança e do bem-estar de longo prazo dos profissionais que ajudam a impulsionar a infraestrutura, a inovação e o desenvolvimento do Brasil.

À medida que seus serviços digitais se expandiam, a cibersegurança se tornou cada vez mais central para essa missão. A MÚTUA precisava de mais do que controles individuais mais robustos. Era necessária uma forma de visualizar, gerenciar e proteger seu ambiente de maneira consistente entre a sede, as filiais regionais, os endpoints, as redes.

Em parceria com a Security Data, uma Sophos Gold Partner, a MÚTUA fortaleceu sua capacidade de detectar e responder a ameaças, permitindo que sua equipe permanecesse focada em proteger os sistemas, os serviços e a confiança dos associados que estão no centro de sua missão.

Uma organização que superava sua infraestrutura de segurança

Como muitas organizações, a equipe dependia de uma combinação de pontos de controle de endpoint, rede e filtragem que operavam de forma independente. Essa falta de coordenação fazia com que até mesmo incidentes rotineiros exigissem investigação e correlação manuais. A visibilidade era limitada, os tempos de resposta eram lentos e a equipe se via reagindo aos eventos em vez de se antecipar a eles.

Para Emanuel Mota, Diretor de Tecnologia da MÚTUA, a prioridade era clara: detecção mais rápida, contenção automatizada e visibilidade consistente em todas as localidades. A organização também reconheceu que melhorar as ferramentas individualmente não seria suficiente — era necessário mudar a forma como essas ferramentas trabalhavam juntas.

“O principal aprendizado foi que a proteção de perímetro, isoladamente, não é suficiente se as ferramentas operam de forma isolada. A Sophos se destacou por seu ecossistema verdadeiramente integrado, por meio da Synchronized Security. Ter endpoints com XDR, firewalls e pontos de acesso se comunicando nativamente no mesmo sistema, com correlação completa de eventos/logs via Sophos Next-Gen SIEM e monitoramento 24/7 pela equipe de MDR. ” — Emanuel Mota, Diretor de Tecnologia, MÚTUA

> “A Sophos se destacou por seu ecossistema verdadeiramente integrado, por meio da Synchronized Security.”
>
> **Emanuel Mota**
> Diretor de Tecnologia, MÚTUA

Detecção mais rápida. Contenção automatizada. Visibilidade total.

Após a licitação, a Sophos apresentou a melhor opção de mercado, trabalhando em conjunto com a parceira Security Data para unificar suas capacidades de segurança em um sistema único e coordenado. Em vez de continuar gerenciando camadas de proteção isoladas, a organização conectou as capacidades de endpoint, firewall, wireless, SIEM e detecção e resposta gerenciadas, permitindo que os sinais fossem compartilhados, correlacionados e acionados com mais rapidez.

Com a adição do Sophos MDR Plus e do Sophos Next-Gen SIEM ao ambiente, a MÚTUA passou a contar com monitoramento contínuo, correlação de eventos e logs em tempo real, e detecção e resposta proativas a ameaças em endpoints e rede.

O que antes exigia investigação e escalonamento manuais agora é tratado instantaneamente — reduzindo o tempo de resposta e minimizando a exposição a riscos.

Contenção em tempo real, sem intervenção manual

Para a MÚTUA, o desafio não era simplesmente identificar atividades suspeitas. O maior risco estava no tempo entre a detecção e a contenção. Em um ambiente distribuído, que abrange sede e filiais, mesmo um pequeno atraso poderia dar a um invasor espaço para se mover lateralmente, aumentar a exposição e envolver a equipe interna em investigações manuais sensíveis ao tempo.

A Sophos ajudou a fechar essa lacuna ao conectar a proteção de endpoint, a aplicação de políticas no firewall e a detecção e resposta gerenciadas em um único fluxo coordenado. Com o Sophos Endpoint e o Sophos Firewall trabalhando juntos, um comportamento suspeito em um dispositivo pode acionar uma resposta imediata em nível de rede. O firewall isola automaticamente o endpoint, ajudando a impedir a movimentação lateral antes que ela se espalhe.

O Sophos MDR Plus amplia essa proteção com monitoramento ininterrupto e resposta especializada. A equipe de MDR valida as ameaças e atua como uma extensão da equipe interna da MÚTUA, garantindo que os alertas não sejam apenas detectados, mas também investigados e tratados à medida que os eventos ocorrem.

Essa velocidade mudou o modelo de resposta da MÚTUA. Em vez de esperar por um escalonamento manual, as ameaças podem ser contidas assim que surgem. O que antes exigia horas de coordenação agora acontece em segundos, reduzindo a janela de oportunidade do invasor e ajudando a transformar potenciais incidentes em eventos controlados.

> “Com sistemas sincronizados, se um dispositivo apresenta um indicador de comprometimento, o firewall o isola automaticamente. Isso evita a movimentação lateral e reduz o tempo de contenção de horas para segundos.”
>
> **Emanuel Mota**
> Diretor de Tecnologia, MÚTUA

Visibilidade centralizada em todo o ambiente

O que mais mudou para a MÚTUA não foi uma ferramenta específica — foi, finalmente, enxergar todo o cenário de uma só vez.

Por meio do Sophos Fusion, a equipe gerencia todo o seu ambiente a partir de um único local: endpoints, firewalls, pontos de acesso e políticas, de forma consistente em todas as localidades. A adição do Sophos Next-Gen SIEM fortaleceu ainda mais essa visão, reunindo eventos e logs para que a equipe pudesse entender a atividade em todo o negócio dentro de contexto, e não como sinais isolados.

Em vez de buscar informações em ferramentas separadas, a equipe agora trabalha a partir de uma visão mais clara e em tempo real de sua rede nacional. As políticas podem ser gerenciadas de forma consistente, os incidentes podem ser investigados com mais contexto, e a equipe consegue responder mais rápido porque as informações de que precisa já estão conectadas.

Para a MÚTUA, essa visibilidade se tornou mais do que uma melhoria operacional. Ela reduz a complexidade para a equipe de TI, ajuda a acelerar a resposta e dá à liderança mais confiança de que a cobertura de segurança é consistente em todas as localidades.

Desempenho e proteção construídos juntos

À medida que a MÚTUA continuava a evoluir seus serviços digitais, a prioridade não era resolver um problema de estabilidade, mas sim ampliar um ambiente já confiável com mais integração, visibilidade e gestão centralizada. A organização buscava manter a consistência já percebida pelos usuários, ao mesmo tempo em que fortalecia a forma como as capacidades de segurança trabalhavam em conjunto em todo o ambiente.

Na prática, isso significava encontrar uma forma de reunir desempenho, controle e proteção em um modelo mais integrado, preservando a estabilidade operacional enquanto acrescentava a visibilidade e a coordenação necessárias para apoiar as necessidades futuras.

O Sophos Firewall ajudou a eliminar essa tensão ao unir os dois aspectos. Com SD-WAN e inspeção profunda de pacotes operando dentro do mesmo fluxo, o tráfego é gerenciado e protegido simultaneamente — priorizando aplicações críticas e, ao mesmo tempo, identificando e bloqueando ameaças à medida que se movem pela rede.

O resultado é consistência. Os usuários têm acesso confiável aos sistemas na sede e nas filiais, enquanto a segurança é continuamente reforçada, sem ferramentas adicionais ou intervenção manual. À medida que a MÚTUA cresce, a rede escala junto — mantendo o mesmo nível de desempenho, visibilidade e proteção em todos os locais.

> “A visibilidade unificada do Sophos Fusion proporcionou painéis claros e acionáveis para monitorar a saúde da nossa rede nacional em tempo real. Para as operações, isso eliminou a troca constante entre telas e centralizou as políticas, acelerando de forma expressiva a resposta a incidentes.”
>
> **Emanuel Mota**
> Diretor de Tecnologia, MÚTUA

Conectividade segura em todas as localidades

Mesmo com detecção, resposta e visibilidade mais robustas, um desafio permanecia: garantir que a segurança fosse aplicada de forma consistente em cada ponto de acesso. Com 28 localidades espalhadas pelo Brasil, manter o mesmo nível de controle nas redes das filiais e nos ambientes de Wi-Fi era difícil de garantir.

A MÚTUA resolveu isso estendendo sua implantação Sophos até a borda da rede. Com a implantação gradual dos pontos de acesso Sophos AP6 420E junto com o Sophos Firewall, começando pela sede e avançando pelas regionais, a MÚTUA amplia a consistência das políticas e controles de acesso em seu ambiente. O acesso dos usuários passou a ser regido pelas mesmas políticas e controles — seja na conexão na sede ou em um site regional.

O acesso é protegido e gerenciado de forma centralizada, em vez de depender de configuração local, dando à equipe uma visão mais clara de como os usuários se conectam em toda a organização.

O resultado é um controle uniforme em todas as localidades. A segurança não é aplicada apenas dentro do ambiente — ela agora se estende a cada conexão que entra nele, garantindo proteção consistente e uma experiência mais previsível tanto para os usuários quanto para a equipe de TI.

> “Hoje, a equipe pode se concentrar em análise de dados, melhoria contínua e integrações estratégicas. Deixamos de ter uma manutenção reativa para assumir um papel mais consultivo e voltado à inovação.”
>
> **Emanuel Mota**
> Diretor de Tecnologia, MÚTUA

Os resultados: impacto mensurável em segurança e operações

Segurança que escala com a equipe — não contra ela

Para a MÚTUA, o impacto da Sophos foi além de uma proteção mais forte. Ele mudou a forma como a equipe de TI trabalha no dia a dia.

Antes, a equipe gastava um tempo valioso alternando entre ferramentas, correlacionando alertas e coordenando respostas manualmente. Hoje, o Sophos Fusion conecta as capacidades de endpoint, rede, detecção e resposta em uma única arquitetura, permitindo que as ameaças sejam identificadas, correlacionadas e tratadas com mais rapidez. As políticas são gerenciadas de forma consistente, a visibilidade é centralizada, e a resposta é apoiada pela expertise da Sophos 24 horas por dia, 7 dias por semana.

Isso transformou o papel da equipe, que deixou de ser reativo e passou a ter um trabalho de segurança de maior valor agregado.

Para uma organização que atende mais de 133.000 associados em todo o Brasil, essa mudança operacional é significativa. A equipe pode dedicar menos tempo ao gerenciamento da complexidade e mais tempo ao aprimoramento dos sistemas e serviços que sustentam o negócio.

Fechando a lacuna entre detecção e contenção

A MÚTUA também obteve um modelo de resposta mais rápido e confiável. Atividades suspeitas agora podem ser detectadas, correlacionadas e tratadas em tempo real, com dispositivos comprometidos sendo isolados automaticamente antes que as ameaças tenham a oportunidade de se espalhar.

Essa velocidade muda a equação de risco. Reduzir o tempo de contenção de horas para segundos limita a movimentação do invasor, reduz a exposição e ajuda a evitar que eventos de segurança se transformem em interrupções operacionais.

> “Na prática, isso significa automação e inteligência — a capacidade de identificar comportamentos anômalos e isolar riscos antes que se tornem um incidente, bloqueando ameaças de dia zero sem a necessidade de intervenção humana imediata. Trata-se de agir antes do impacto, e não apenas investigar depois.”
>
> **Emanuel Mota**
> Diretor de Tecnologia, MÚTUA

Conformidade consistente em escala

A Lei Geral de Proteção de Dados (LGPD) do Brasil estabelece requisitos rigorosos sobre como as organizações coletam, processam e protegem dados pessoais e financeiros — impondo um padrão elevado de visibilidade, controle e responsabilização.

Para a MÚTUA, que opera em 27 localidades, isso criava um desafio prático: garantir que os mesmos padrões de segurança fossem aplicados de forma consistente em cada endpoint e rede, sem depender de configuração local ou supervisão manual.

Com gerenciamento centralizado de políticas e visibilidade em tempo real, a Sophos permite que a MÚTUA aplique esses padrões de forma uniforme em todo o seu ambiente. As políticas são aplicadas de forma consistente, a atividade é monitorada continuamente e as lacunas entre as localidades são eliminadas.

Continuidade de negócios como vantagem competitiva

Para a MÚTUA, a cibersegurança está diretamente ligada à continuidade dos negócios. Como uma organização que oferece serviços financeiros, programas de previdência e suporte a associados, qualquer período de inatividade ou perda de dados poderia afetar a prestação de serviços, a posição regulatória e a confiança dos associados.

Ao melhorar a visibilidade, acelerar a resposta e reduzir o risco cibernético, a Sophos contribui para fortalecer a estabilidade operacional da MÚTUA e apoiar a continuidade dos serviços.

"É inestimável. Reduzir o risco cibernético contribui para proteger as operações, resguardar a reputação institucional e apoiar a continuidade dos negócios."

"É inestimável — garante a continuidade dos negócios. Reduzir o risco cibernético protege as operações, resguarda a reputação institucional e evita perdas financeiras associadas a violações de dados."

Emanuel Mota
Diretor de Tecnologia, MÚTUA

Uma segurança pensada para sustentar o que vem a seguir

A abordagem da MÚTUA em relação à cibersegurança reflete uma mudança mais ampla na forma como as equipes de TI modernas operam: a segurança deixou de ser um conjunto de ferramentas para se tornar um sistema conectado, integrado ao funcionamento diário das organizações.

Ao integrar a segurança nas camadas de endpoint, rede e gerenciamento, a organização reduziu o atrito operacional e, ao mesmo tempo, fortaleceu a proteção — permitindo que o negócio avance mais rápido sem aumentar o risco.

Com a Sophos, a segurança opera continuamente em segundo plano, detectando e contendo ameaças em tempo real, mantendo a visibilidade e o controle em todo o ambiente.

O resultado é uma arquitetura de segurança que escala com a organização — sustentando novos serviços, requisitos em evolução e crescimento contínuo.

Com gerenciamento centralizado de políticas e visibilidade em tempo real, a Sophos ajuda a MÚTUA a manter controles de segurança consistentes em todo o seu ambiente. As políticas são aplicadas de forma uniforme, a atividade é monitorada continuamente e as lacunas entre localidades são reduzidas. Isso ajuda a apoiar os objetivos contínuos de conformidade da MÚTUA, reduzindo a complexidade operacional para a equipe.

Se você está pronto para iniciar sua jornada com a Sophos, fale com um especialista hoje mesmo.

> “A segurança não deve ser um gargalo — ela deve viabilizar o negócio. Quando a arquitetura de segurança é inteligente e integrada, ela se torna a base para a inovação e o crescimento sustentável.”
>
> **Emanuel Mota**
> Diretor de Tecnologia, MÚTUA

Para começar com as soluções Sophos e encontrar uma solução que escale conforme suas necessidades, fale com um especialista hoje mesmo.

2026-08-17 CCS-EN (MP) CRE-5909

SOPHOS