CUSTOMER CASE STUDY

Built to grow: How MÚTUA made security a strategic advantage

Brazil's leading professional benefits association chose the Sophos AI-Native Cybersecurity Defense System to protect against AI-enabled threats through coordinated detection, response, and containment across its environment.

SOPHOS

mútua
Caixa de Assistência dos Profissionais do Crea

Industry
Insurance/Financial Services

Sophos Solutions
Sophos Fusion

Sophos Firewall

Sophos Endpoint

Sophos XDR Powered by Secureworks

Sophos MDR Plus

Sophos Next-Gen SIEM

About MÚTUA

MÚTUA is one of the largest professional assistance entities in Brazil, offering financial services, pension programs, and member support to more than 133,000 engineers, agronomists, and geoscience professionals across 28 units nationwide. Trusted to manage sensitive personal and financial information, MÚTUA plays a critical role in helping safeguard the long-term security and wellbeing of the professionals who help drive Brazil's infrastructure, innovation, and development.

As its digital services expanded, cybersecurity became increasingly central to that mission. MÚTUA needed more than stronger individual controls. It needed a way to see, manage, and protect its environment consistently across headquarters, regional branches, endpoints, networks, and cloud-connected services.

In partnership with Security Data, a Sophos Gold Partner, MÚTUA strengthened its ability to detect and respond to threats while enabling its team to stay focused on protecting the systems, services, and member trust at the center of its mission.

"Sophos stood out with its truly integrated ecosystem through Synchronized Security."

Emanuel Mota
Director of Technology, MÚTUA

An organization outgrowing its security infrastructure

As its digital services expanded and operations scaled across multiple locations, MÚTUA's security environment struggled to keep pace.

Like many organizations, the team relied on a mix of endpoint, network, and filtering control points that operated independently. This lack of coordination meant that even routine incidents required manual investigation and correlation. Visibility was limited, response times slowed, and the team was left reacting to events rather than staying ahead of them.

For Emanuel Mota, Director of Technology at MÚTUA, the priority was clear: faster detection, automated containment, and consistent visibility across every location. The organization also recognized that improving individual tools wouldn't be enough - the way those tools worked together needed to change.

" The key learning was that perimeter protection alone is not enough if tools operate in isolation. Sophos stood out with its truly integrated ecosystem through Synchronized Security. Having endpoints with XDR, firewalls, and access points communicating natively on the same system, with full correlation of events/logs via the Sophos Next-Gen SIEM and 24/7 monitoring by the MDR team, was the decisive differentiator. "
— Emanuel Mota, Director of Technology, MÚTUA

Faster detection. Automated containment. Full visibility.

After evaluating leading vendors, MÚTUA selected Sophos, working closely with partner Security Data to bring its security capabilities together into a single, coordinated system. Rather than continuing to manage separate layers of protection in isolation, the organization connected endpoint, firewall, wireless, SIEM, and managed detection and response capabilities so signals could be shared, correlated, and acted on faster.

With Sophos MDR Plus and Sophos Next-Gen SIEM added to the environment, MÚTUA gained continuous monitoring, real-time event and log correlation, and proactive threat detection and response across endpoints, network, and cloud-connected activity.

What previously required manual investigation and escalation is now handled instantly - reducing response time and minimizing risk exposure.

Real-time containment without manual intervention

For MÚTUA, the challenge was not simply identifying suspicious activity. The bigger risk was the time between detection and containment. In a distributed environment spanning headquarters and branches, even a short delay could give an attacker room to move laterally, increase exposure, and pull the internal team into time-sensitive manual investigation

Sophos helped close that gap by connecting endpoint protection, firewall enforcement, and managed detection and response into one coordinated flow. With Sophos Endpoint and Sophos Firewall working together, suspicious behavior on a device can trigger an immediate response at the network level. The firewall automatically isolates the endpoint, helping stop lateral movement before it spreads.

Sophos MDR Plus extends that protection with around-the-clock monitoring and expert response. The MDR team validates threats and acts as an extension of MÚTUA's internal team, ensuring that alerts are not only detected, but investigated and acted on as events unfold.

"With synchronized systems, if a device shows an indicator of compromise, the firewall automatically isolates it. This prevents lateral movement and reduces containment time from hours to seconds."

That speed changed the response model for MÚTUA. Instead of waiting on manual escalation, threats can be contained as they emerge. What once required hours of coordination can now happen in seconds, reducing the attacker's window of opportunity and helping turn potential incidents into controlled events.

"With synchronized systems, if a device shows an indicator of compromise, the firewall automatically isolates it. This prevents lateral movement and reduces containment time from hours to seconds."

Emanuel Mota
Director of Technology, MÚTUA

Centralized visibility across the entire environment

What changed most for MÚTUA wasn't any single tool - it was finally seeing the whole picture at once.

Through Sophos Fusion, the team manages its entire environment from one place: endpoints, firewalls, access points, and policies, consistent across all locations. The addition of Sophos Next-Gen SIEM strengthened that view even further, bringing events and logs together so the team could understand activity across the business in context, not as isolated signals.

Instead of chasing information across separate tools, the team now works from a clearer, real-time view of its national network. Policies can be managed consistently, incidents can be investigated with more context, and the team can respond faster because the information they need is already connected.

"Unified visibility in Sophos Fusion provided clear, actionable dashboards to monitor the health of our national network in real time. For operations, it eliminated screen switching and centralized policies, dramatically accelerating incident response."

For MÚTUA, that visibility has become more than an operational improvement. It reduces complexity for the IT team, helps accelerate response, and gives leadership greater confidence that security coverage is consistent across every location.

Performance and protection, built together

As MÚTUA expanded, keeping the network running smoothly became more complex. More users, more applications, and increasing reliance on cloud services placed growing pressure on connectivity - while security expectations continued to rise.

In practice, this created a familiar challenge. Improving control and visibility often meant adding friction, while prioritizing performance risked creating gaps in protection.

Sophos Firewall helped remove that tension by bringing both together. With SD-WAN and deep packet inspection operating as part of the same flow, traffic is managed and secured simultaneously - prioritizing critical applications while identifying and blocking threats as they move through the network.

The result is consistency. Users have reliable access to systems across headquarters and branch locations, while security is continuously enforced without additional tools or manual intervention. As MÚTUA grows, the network scales with it - maintaining the same level of performance, visibility, and protection across every site.

"Unified visibility in Sophos Fusion provided clear, actionable dashboards to monitor the health of our national network in real time. For operations, it eliminated screen switching and centralized policies, dramatically accelerating incident response."

Emanuel Mota
Director of Technology, MÚTUA

SOPHOS

Secure connectivity across every location

Even with stronger detection, response, and visibility, one challenge remained: ensuring security was applied consistently at every point of access. With 28 locations across Brazil, maintaining the same level of control across branch networks and Wi-Fi environments was difficult to enforce.

MÚTUA addressed this by extending its Sophos deployment to the edge of the network. By rolling out Sophos AP6 420E access points alongside Sophos Firewall across its headquarters and 27 branches, user access is now governed by the same policies and controls - whether connecting at head office or in a regional site.

This removed a key point of inconsistency. Access is secured and managed centrally, rather than relying on local configuration, giving the team a clearer view of how users connect across the organization.

The result is uniform control across every location. Security isn't just applied within the environment - it now extends to every connection into it, ensuring consistent protection and a more predictable experience for users and IT alike.

The results: Measurable impact across security and operations

Security that scales with the team - not against it

For MÚTUA, the impact of Sophos went beyond stronger protection. It changed the way the IT team works day to day.

Before, the team spent valuable time moving between tools, correlating alerts, and coordinating response manually. Today, Sophos Fusion connects endpoint, network, detection, and response capabilities into a single architecture, allowing threats to be identified, correlated, and acted on faster. Policies are managed consistently, visibility is centralized, and response is backed by 24/7 Sophos expertise.

That has shifted the team's role from reactive maintenance to higher-value security work.

"Today, the team can focus on data analysis, continuous improvement, and strategic integrations. We've shifted from reactive maintenance to a more consultative and innovation-driven role."

For an organization supporting more than 133,000 members across Brazil, that operational shift matters. The team can spend less time managing complexity and more time improving the systems and services that support the business.

"Today, the team can focus on data analysis, continuous improvement, and strategic integrations. We've shifted from reactive maintenance to a more consultative and innovation-driven role."

Emanuel Mota
Director of Technology, MÚTUA

SOPHOS

Closing the gap between detection and containment

MÚTUA also gained a faster, more confident response model. Suspicious activity can now be detected, correlated, and acted on in real time, with compromised devices isolated automatically before threats have the opportunity to spread.

"In practice, it means automation and intelligence - the ability to identify anomalous behavior and isolate risk before it becomes an incident, blocking zero-day threats without immediate human intervention. It's about acting before impact, not just investigating afterward."

That speed changes the risk equation. Reducing containment time from hours to seconds limits attacker movement, reduces exposure, and helps prevent security events from becoming operational disruptions.

Consistent compliance at scale

Brazil's Lei Geral de Proteção de Dados (LGPD) establishes strict requirements for how organizations collect, process, and protect personal and financial data—placing a high bar on visibility, control, and accountability.

For MÚTUA, operating across 28 locations, this created a practical challenge: ensuring the same security standards were applied consistently across every endpoint and network, without relying on local configuration or manual oversight.

With centralized policy management and real-time visibility, Sophos enables MÚTUA to enforce those standards uniformly across its entire environment. Policies are applied consistently, activity is continuously monitored, and gaps between locations are removed.

The result is compliance that scales with the business without adding operational burden to the team.

Business continuity as a competitive advantage

For MÚTUA, cybersecurity is directly tied to business continuity. As an organization providing financial services, pension programs, and member support, downtime or data loss could affect service delivery, regulatory standing, and member trust.

By improving visibility, accelerating response, and reducing cyber risk, Sophos helps MÚTUA keep operations stable and services uninterrupted.

"It is invaluable - it ensures business continuity. Reducing cyber risk protects operations, safeguards institutional reputation, and prevents financial losses associated with data breaches."

"In practice, it means automation and intelligence - the ability to identify anomalous behavior and isolate risk before it becomes an incident, blocking zero-day threats without immediate human intervention. It's about acting before impact, not just investigating afterward."

Emanuel Mota
Director of Technology, MÚTUA

SOPHOS

Security built to support what comes next

MÚTUA's approach to cybersecurity reflects a broader shift in how modern IT teams operate: security is no longer a set of tools, but a connected system built into how organizations run every day.

By integrating security across endpoint, network, and management layers, the organization has reduced operational friction while strengthening protection - enabling the business to move faster without increasing risk.

With Sophos, security operates continuously in the background, detecting and containing threats in real time while maintaining visibility and control across the environment.

The result is a security architecture that scales with the organization - supporting new services, evolving requirements, and continued growth.

With centralized policy management and real-time visibility, Sophos helps MÚTUA maintain consistent security controls across its entire environment. Policies are applied uniformly, activity is continuously monitored, and gaps between locations are reduced. This helps support MÚTUA's ongoing compliance objectives while reducing operational complexity for the team.

If you're ready to start your journey with Sophos, speak to an expert today.

"Security must not be a bottleneck - it should enable the business. When security architecture is intelligent and integrated, it becomes the foundation for innovation and sustainable growth."

Emanuel Mota
Director of Technology, MÚTUA

To get started with Sophos solutions and find a solution that scales to your needs, speak to an expert today.

© Copyright 2026. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2026-07-15 CCS-EN (NP) CRE-5909

SOPHOS