



Sophos Provides a Resilient and Adaptable Cybersecurity Platform for a Rapidly Expanding Brazilian Restaurant Chain

Madero Group, a Sophos customer since 2017, is a large fast food restaurant chain in Brazil with 276 locations in 18 states. Founded in 2005 by Chef Junior Durski, the award-winning chain grew at the pace of a technology startup — much faster than is usual in the restaurant industry. As one of the first fast-casual concepts in Brazil, Madero Group has enjoyed strong customer demand since the beginning, and, between 2018 and 2022, the organization grew at a 16.6% compound annual growth rate (CAGR). To support its accelerated expansion, Madero Group partnered with private equity companies for growth capital and has built a heavily funded distribution center to supply its restaurants with food and other necessary items. It has also expanded into various restaurant formats and brands to meet a wide range of consumer budgets and preferences.



Grupo Madero

Industry:
Restaurant chain

Number of users:
8,000

Sophos Solutions:

- › Sophos Firewall XGS (128, 2100, 3300, 4500, UNL cores, UNL GB RAM)
- › Sophos Endpoint XDR
- › Sophos MDR (Managed Detection and Response)
- › Sophos Central Email Protection Advanced
- › Sophos Cloud Optix
- › Network Detection and Response (Sophos NDR)
- › Sophos CFR (Central Firewall Reporting)
- › Sophos ZTNA (Zero Trust Network Access)
- › Sophos Device Encryption
- › Sophos DNS Protection
- › Sophos Phishing

“By consolidating security into a unified, resilient, and adaptable platform, we are reducing operational costs, better protecting our infrastructure, and elevating our cybersecurity posture.”

Lucas Dias, Manager of Corporate Infrastructure, Madero Group

Challenges

- › Protecting a wide and highly distributed environment covering 18 states.
- › Freeing an IT team overburdened by rapid growth and increasing operational demand.
- › Optimizing and reducing time and resources for IT.
- › Ensuring business continuity and strengthening customer and stakeholder trust.
- › Complying with constantly evolving complex regulations.
- › Increasing overall security posture to avoid attacks and interruptions of operations.

What security challenges specific to the restaurant industry drove the need for Sophos technologies?

Madero Group has a highly distributed environment, consisting of restaurant branches, data centers, factories, a distribution center, and an administrative office. Rapid growth and increasing operational demand in such a large environment were overloading IT staff and exposing the organization to potential security breaches.

The broad decentralized infrastructure required constant attention to monitor threats, manage security policies, and respond to incidents. The IT team was consumed by intensive manual processes, preventing them from working on strategic initiatives that would contribute to business growth.

As a large-scale organization operating in Brazil, Madero Group was subject to complex and evolving regulatory requirements around data protection, energy use, telecommunications, environmental regulations, and labor laws. The organization needed a way to better protect its digital assets and maintain compliance.

Other strategic priorities included protecting against phishing and targeted attacks and ensuring continued security in the organization's cloud environments.

With billions in revenue at stake, it was vital for the organization to strengthen trust with its business partners, customers, and regulators. Although Madero Group already had deployed several Sophos products in the past, including Sophos XG firewalls and Sophos Central Intercept X Advanced endpoint protection, its rapid growth required additional security investments to ensure stable access to



“Driven by the performance and integration of Sophos solutions, we have transformed challenges into a robust and scalable cybersecurity platform capable of protecting and enhancing the operations of large corporations like Madero Group.”

Willian Tezza, Technical Director, Task TI (Sophos Platinum Partner)

essential resources, mitigate operational risks, and maintain business continuity. Changes, updates, and new solutions had to be implemented in a simplified way that would not disrupt business operations.

It was in this context that Brazilian IT consulting firm and Sophos Platinum partner Task TI helped Madero Group design and implement the project, offering strategic consulting, security architecture planning, technical execution, and ongoing support. This collaboration ensured that security solutions were integrated efficiently, enabling Madero Group to continue to stay secure and resilient in a highly competitive market.

What were the overriding reasons the restaurant chain selected Sophos as its cybersecurity partner?

Madero Group recognized the need to establish a modern, efficient, and centralized security infrastructure aligned with advanced threat protection, regulatory compliance, and business continuity approaches. Evolving threats and regulatory requirements required a more proactive and adaptable model.

“Our vision was to consolidate, automate, and integrate our tools into a unified platform with the goal of improving operational efficiency. We knew it was time to switch from a reactive approach to response and remediation activities to a proactive and preventive approach,” said Lucas Dias, Manager of Corporate Infrastructure at Madero Group.

How does Sophos help a restaurant industry organization achieve its cybersecurity goals?

Sophos products were instrumental in transforming Madero Group’s security posture and boosting its operational efficiency. Working side by side with Task TI, Madero Group replaced Sophos XG firewalls with next-generation Sophos XGS firewalls for faster performance, improved network segmentation, and advanced threat response capabilities.

The new firewalls are fully integrated and managed by Sophos Central Firewall Reporting (CFR). This centralized, cloud-based platform integrates with all Sophos products and allows IT staff to analyze network activity from Sophos firewalls. The platform provides real-time threat protection, automated responses, multifactor authentication, and custom dashboards.

"We were convinced that Sophos was the right security partner for our modernization goals based on our supplier's positive experience and the advanced capabilities of its unified platform."

Lucas Dias, Manager of Corporate Infrastructure, Madero Group

Madero Group also deployed Sophos Cloud Optix to gain complete visibility into its Microsoft Azure and Amazon Web Services cloud infrastructure. This AI-powered cloud security and compliance platform for public cloud environments provides a real-time inventory of cloud-based servers, storage, and network components, making it easier for Madero Group to identify vulnerabilities and comply with regulations.

Sophos Central Device Encryption was implemented to validate the user, application, and security of a device before allowing access to encrypted data. Taking the organization's data protection to the next level, Sophos Zero Trust Network Access [ZTNA] was deployed to ensure secure remote access and authentication throughout the organization's ecosystem. ZTNA tightly integrates with Sophos Network Detection

and Response [NDR], which monitors network traffic for suspicious activities using machine learning, analytics, and rules.

Madero Group was already using Sophos Phish Threat to promote a culture of security by educating and testing users through attack simulations, training, and reporting.

To strengthen its email security, Madero Group upgraded to Sophos Central Email Advanced [CEMA]. This solution leverages AI and integrates with the Sophos Central management hub to protect against phishing, ransomware, zero-day malware, and other malicious email threats.

Adding another layer of security, the organization installed Sophos DNS Protection, which integrates with Sophos Central policy controls

to filter malicious traffic and prevent suspicious communications. Finally, Sophos Managed Detection and Response [MDR], a 24/7 threat monitoring service, reduces the operational burden on the organization's internal staff and ensures uninterrupted protection across the vast ecosystem.

This unified platform provides a holistic view of the environment by bringing endpoint, server, firewall, email, and cloud security controls together in a single centralized console for simplified administration and accelerated investigation and response.

What are the positive results Sophos provides?

Since the deployment of Sophos products, Madero Group has improved its overall security, operational efficiency, and regulatory compliance. It now has a modern infrastructure that is simpler to manage and requires much less time to administer and configure policies.

Task IT played an essential role in the planning, implementation, and validation of these Sophos solutions. The company ensured that each Sophos product was deployed according to best practices and in alignment with the organization's cybersecurity strategy.

"Driven by the performance and integration of Sophos solutions, we have transformed challenges into a robust and scalable cybersecurity platform capable of protecting and enhancing the operations of large corporations like Madero Group," said Willian Tezza, Technical Director, Task TI.

Thanks to Sophos XGS firewalls, Madero Group now has more efficient network segmentation that provides greater performance and more resilient connectivity between data centers, factories, and branch offices. Sophos CEMA reduced the number of phishing attacks and increased the security of commercial communications. Sophos MDR reduced incident detection and mitigation time. And Sophos ZTNA ensures remote access is secure without compromising team productivity.

Overall, Madero Group has seen a substantial ROI on its Sophos investments. "By consolidating security into a unified, resilient, and adaptable platform, we are reducing operational costs, better protecting our infrastructure, and elevating our cybersecurity posture," Dias concluded.



"By consolidating security into a unified, resilient, and adaptable platform, we are reducing operational costs, better protecting our infrastructure, and elevating our cybersecurity posture."

Lucas Dias, Manager of Corporate Infrastructure, Madero Group

To learn more about Sophos solutions, visit [Sophos.com](https://www.sophos.com)