SOPHOS

CUSTOMER CASE STUDY **DIANA HOLDING**

Food Industry Major Enhances Protection and Visibility with an Integrated Approach to Cybersecurity

Sophos strengthens network, endpoint and server security for Diana Holding with an industry leading reliable, secure and high-performance firewall, EDR, and email security solution.

CUSTOMER-AT-A-GLANCE

Diana Holding

Industry
Food industry: edible oils, wine making, meat processing, commercial nurseries

Website
www.dianaholding.ma/le-groupe/presentation.html

Number of Users
500-999

Sophos Solutions

45 - XG Firewall (Full Guard)

830 licenses - Central Intercept X Advanced with EDR (CIXA EDR)

79 licenses - Central Intercept X Advanced with EDR for Server (CIXA EDR SERVER)

830 licenses - Central Email Advanced

Diana Holding is a Morocco based food conglomerate with a legacy of more than 40 years in the food industry. It is a fast- growing organization, and this sterling growth means it needs to protect its IT infrastructure, data and employees from cybercriminals. While the organization already had a cybersecurity infrastructure in place, the growing number of employees meant that it wasn't just their network perimeter that was under threat but also their endpoints. They realized existing security solutions weren't giving them the security net needed to guard against rapidly evolving threats. As a result, they decided to build a comprehensive and advanced cybersecurity infrastructure backed by security solutions that could proactively identify and mitigate threats.

Challenges

- A small IT team overwhelmed with the need to secure users on and off the network, protect every endpoint and manage the IT security needs of a fast-growing organization.
- A growing need for better visibility, protection and performance of an increasingly complex and unique network environment.
- Switch from a standard endpoint solution to an EDR one as recommended by an ISO 27001 assessment.
- Difficult to assess the security of the IT environment as a large section of the IT infrastructure was deployed in a third-party standard data centre.
- The existing legacy endpoint solution was difficult manage and proving to be incompatible with the increasing sophistication of the IT environment.
- Growing realization that existing security solutions were woefully inadequate to protect against advanced threats and did not offer, much needed, centralized visibility, control, and management

> *"While we have always been aware about the need for deploying cutting-edge cybersecurity solutions to protect our organization, it was COVID-19 and the numerous cyberattacks targeting organizations across the world during this time, that impressed upon us the need to deploy the kind of solutions that can protect us from threats that cause business disruption, reputational damage and reduce the possibility of incurring fines resulting from data protection violations."*

Reda Loudiyi
Organization and Information Systems Director
Diana Holding

The Case for Improved Cybersecurity

The IT team lead by Mr. Reda is small and dynamic, but over a period of time he noticed the IT team's reactivity to user request's especially from the security perspective was going down. The time to address requests was increasing and with a growing threat landscape the team couldn't take a chance with the reactivity of their cybersecurity posture. Another problem was risk visibility and the inability of existing solutions to identify suspicious or malicious threats and offer insights into network health. There was also a lack of transparency into network traffic.

Diana Holding also had to comply with ISO – 27001 regulation and the company's security framework including the legacy endpoint solution was unable to meet the framework's demand for technical controls from the information risk management perspective.

Also, a critical need was supplementing their endpoint security with three critical security capabilities namely detection, investigation, and response. "While researching the solutions needed for improving our cybersecurity infrastructure, we realized the need for endpoint security empowered with EDR. Our core focus was also on identifying a tool that was not only value for money, but also easy to use, offered sufficient protection capabilities and wasn't resource intensive." explains Mr. Reda.

The existing endpoint was consuming a large percentage of RAM/CPU services and wasn't delivering value on the malware protection front. From the email standpoint, the organization was experiencing spam and phishing attacks, which the legacy endpoint solution wasn't able to prevent. Also, existing email security couldn't address the organization's security concerns around Office 365.

The Road Towards Sophos Deployment

Mr. Reda's key focus area while searching for a replacement for existing solutions was the feature set and its ability to protect the network perimeter and endpoints from sophisticated threats, both known and unknown. Another important criterion was the local presence of the vendor in Morocco and their reactivity in addressing any issues that might crop up. Sophos' deep security roots in Morocco and strong partnerships was one of the key reasons why the client chose Sophos.

Apart from product capabilities, another key attribute the IT team was looking for was an affordably priced product that delivered premier security features, and meaningful ROI. Sophos ticked all the boxes in this regard. And, finally, the team wanted to deploy solutions that ranked well on third party reports, and Sophos has done really well on third-party assessment reports such as AV Comparatives, SE Labs, AV-TEST and more.

Sophos Deployment

There were many moving parts in the deployment process and many holding subsidiaries that the solutions had to be deployed on; complete deployment, therefore, took 3 months. The configuration of Sophos's security solutions also needed to align with the IT architecture requirements.

Sophos's comprehensive cybersecurity evaluation identified a layered and synchronized security approach to bolster the Diana Holding's cybersecurity infrastructure.

Network Security: Sophos Firewall's Xstream architecture delivers exceptional visibility by removing the blind spots resulting from encrypted traffic, through SSL inspection and at the same time, the firewall ensures zero performance disruption.

Also, the firewall's highspeed deep packet inspection (DPI) engine scans the organization's traffic for threats. The firewall stack offloads the complete process to the DPI engine to reduce latency and improve overall efficiency. The high-performance streaming DPI includes next-gen IPS, web protection, app control, deep learning and sandboxing powered by SophosLabs Intelix. This ensures the organization is protected against the latest ransomware and data breaches.

There Endpoint Security with EDR: With Intercept X Advanced with EDR and Intercept X Advanced with EDR for Server Diana Holding benefits from a powerful endpoint detection and response (EDR) combined with top-rated endpoint protection. Purpose built for combining IT security operations and threat hunting, this endpoint solution uses AI-driven analysis to detect and investigate suspicious activity.

It blocks ransomware attacks at the gates by detecting malicious encryption processes and any encrypted files are rolled back to a safe state. This allows Diana Holding employees to work uninterruptedly, minimizing any impact to business continuity.

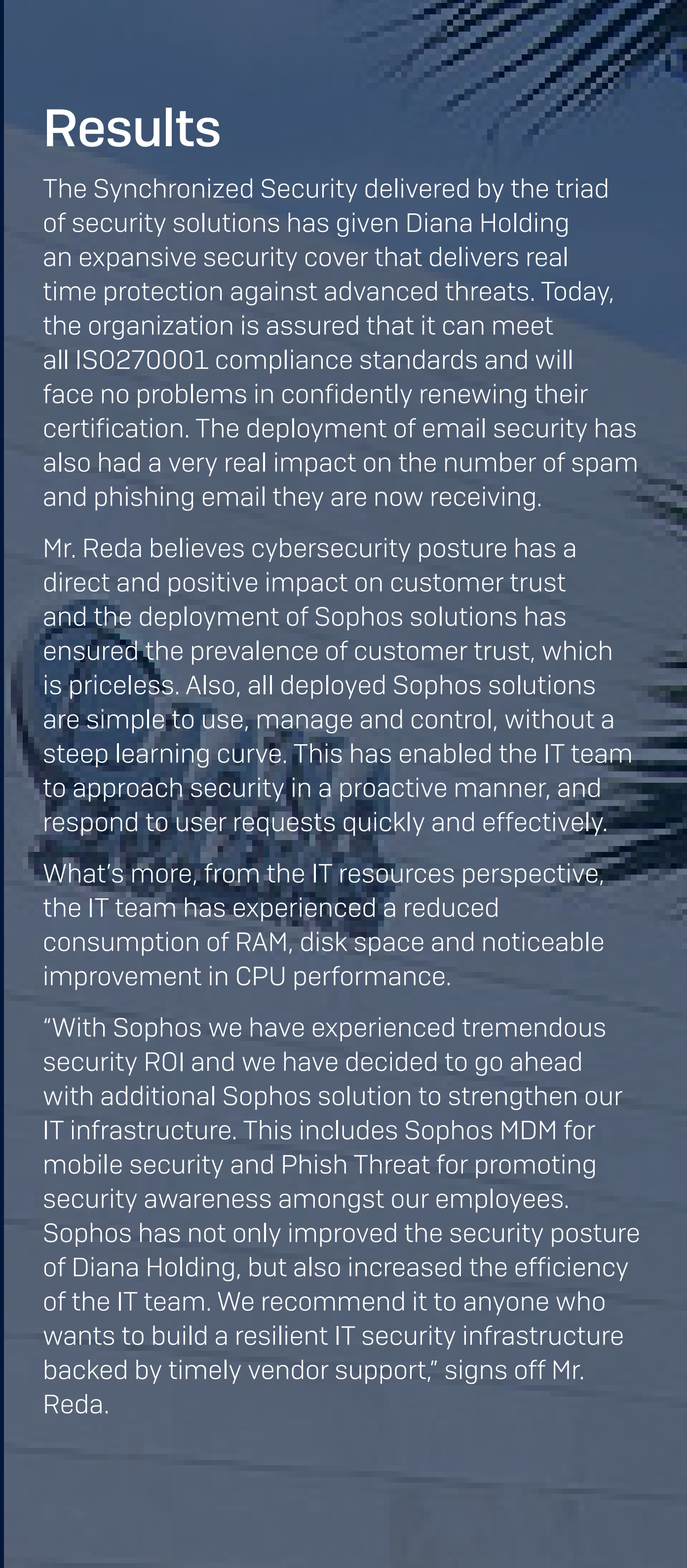
This solution delivers features such as web protection, exploit prevention, download reputation, peripheral control, application control, deep learning malware detection, anti-malware scanning, PUA blocking and more. It offers comprehensive protection that covers attack surface, protection before malware runs on device, stops running threats, and delivers the benefit of detection, investigation, remediation coupled with human-led threat hunting and response.

Server protection automatically detects AWS, Microsoft Azure, and Google Cloud workloads and other critical cloud services to zero in on malicious activities, identify insecure cloud deployment and plug security holes.

Also, the Server Lockdown feature ensures only trusted applications will run on the servers and the IT team at Diana Holding can do this with single click without incurring server downtime.

Email Security: Delivered through a single plane of glass dashboard on Sophos Central, Sophos' email security protects Diana Holding employees from malicious email threats with AI enabled protection. It works in tandem with Sophos Endpoint protection to automatically detect and clean infected computers that are sending malware and outbound spam.

Cutting-edge email protection helps prevent data loss and drives content control with policy-based email encryption. With enforced TLS encryption, messages in transit cannot be intercepted by cybercriminals and push-based encryption helps encrypt the whole email or its attachment. And, the O365 add-in button allows you send secure messages quickly. These features and others have delivered extensive email protection to Diana Holding and its employees.



Results

The Synchronized Security delivered by the triad of security solutions has given Diana Holding an expansive security cover that delivers real time protection against advanced threats. Today, the organization is assured that it can meet all ISO270001 compliance standards and will face no problems in confidently renewing their certification. The deployment of email security has also had a very real impact on the number of spam and phishing email they are now receiving.

Mr. Reda believes cybersecurity posture has a direct and positive impact on customer trust and the deployment of Sophos solutions has ensured the prevalence of customer trust, which is priceless. Also, all deployed Sophos solutions are simple to use, manage and control, without a steep learning curve. This has enabled the IT team to approach security in a proactive manner, and respond to user requests quickly and effectively.

What's more, from the IT resources perspective, the IT team has experienced a reduced consumption of RAM, disk space and noticeable improvement in CPU performance.

"With Sophos we have experienced tremendous security ROI and we have decided to go ahead with additional Sophos solution to strengthen our IT infrastructure. This includes Sophos MDM for mobile security and Phish Threat for promoting security awareness amongst our employees. Sophos has not only improved the security posture of Diana Holding, but also increased the efficiency of the IT team. We recommend it to anyone who wants to build a resilient IT security infrastructure backed by timely vendor support," signs off Mr. Reda.