Sophos EDR Secures a Food and Beverages Leader with Advanced Security Empowered with Actionable Security Insights

Hariss International uses Sophos Intercept X EDR and XG Firewall to transform its IT security posture and protect its network and endpoints from an ever-changing threat landscape.

CUSTOMER-AT-A-GLANCE

HARISS INTERNATIONAL LTD

Company Name
Hariss International Limited

Industry
Food and Beverages

Website
www.harissint.com

Sophos Solutions
Sophos Intercept X Advanced with EDR – 300 licenses
Sophos Central Intercept X Advanced for Server with EDR – 35 licenses
Sophos XG Firewall – XG230 Full Guard Plus

> *‘We were very clear that we wanted a complete security package that not only offered an extensive security cover but also better visibility into our network and endpoints. At the same time, we also wanted meaningful insights through investigation and access to rich details that delve deeper into the nature of the security incidents. After extensive research and a threadbare evaluation of various security solutions, we were confident that only Sophos and its portfolio of network and endpoint security solutions could handle our security needs best.’*
>
> **Dani Bachour**
> System Administrator, Hariss International Limited

Hariss International Limited is a leading Uganda-based manufacturer of food and beverages. It was founded in in 2005 and both its food and beverages production are being operated under the brand RIHAM. Through the many years it has been in operation, it has become a trusted household brand and has kept adding to its product portfolio.

The IT Team at Hariss International had a growing realization that the tremendous growth experienced by the company put them in the radar of cybercriminals. The growing number of cyberattacks against organizations irrespective of their size, scale or scope meant that Hariss International had to take proactive steps to improve security.

More importantly, the IT team wanted to move to a security solution that offered exceptional threat hunting and investigative capabilities. This would allow the IT team to get more insights into the threats they were up against and proactively implement security protocols that kept such threats at bay.

Challenges

- A cybersecurity stack made up of different vendors resulting in inconsistent synergies and a lot of time spent trying to make the different solutions work more efficiently together.
- Product management inefficiencies as security solutions were running as a stand-alone solution on each device.
- Inability to get a real-time visibility across all the endpoints resulting in reactive rather than proactive security, leading to a myriad of compliance challenges.
- Inability to quickly zero-in on security vulnerabilities across endpoints in order to plug the security gaps.
- Inadequacy of existing solution to offer behavioural protection in addition to traditional signature-based security approach.
- Lack of threat intelligence made it difficult to get the right threat context thus increasing the incident response time.

A Solution for Growth-Centric Security Challenges

A rapidly growing organization is good news for all stakeholders, and also for cybercriminals. The IT Team at Hariss International was well aware that the growth of an attack surface was directly proportional to the growth of an organization.

Their organization was scaling their IT infrastructure, extending its network and having to manage an increasing number of endpoints. This meant the attack surface was also growing exponentially. "We wanted to enhance cybersecurity both at the endpoint and the network level to prevent cyberattacks and ensure business continuity and process efficiency," reasoned Dani Bachour.

The 15 member IT team was seeing a lot of their time being cannibalized with operational tasks that could be automated. Also, they were suffering from a paucity of information into systemic vulnerabilities and did not have the time to launch investigation into cyber incidents. This lack of visibility meant they couldn't effectively control and manage their cybersecurity infrastructure. The team was unable to detect issues on endpoints and were facing difficulties in pushing updates across all of their computers.

Sophos Security Solutions Emerge the Perfect Choice

"I believe that a critical compliance requirement for any organization is clear visibility into the health of its network and endpoints. Our key focus area while searching for security solutions was their ability to not only give us this visibility but also help us easily apply the rules and policies to reduce the attack surface," explains Dani Bachour. "Other requirements at the top of our list were product efficiency and pricing." Hariss International had deployed the Cyberoam Firewall and while upgrading to the Sophos XG 230 Full Guard Plus they made the decision to switch to Sophos' endpoint security solution in order to partner with just one vendor for all their security needs. They were impressed by the suite of features delivered by the Sophos endpoint solution, and the regular product upgrades and updates that added new features that helped them combat the growing sophistication of cyberthreats. Coupled with competitive pricing, the IT Team was confident that Sophos was the partner they could trust to implement a powerful security roadmap for the future.

Sophos Enforcing Cybersecurity Best Practices

With Sophos XG Firewall, Hariss International gets the full spectrum of features including Sandstorm protection, network protection, web protection, email protection and more. This network security solution delivers both power and performance. The IT team is able to identify hidden risks with superior visibility into risky user behavior and suspicious and sophisticated to take steps that help exercise network control. Technologies like deep learning and intrusion prevention keep the organization secure, and at the same time, automatic threat response, reduces incident response time by identifying and isolating compromised systems on network; the IT team is thus assured that the threats will not spread through the network. With Sophos Sandbox, the IT Team benefits from Sophos Zero-day Dynamic File Analysis to protect against zero-day threats like ransomware and targeted attacks.

What’s more, Sophos Firewall works in tandem with other Sophos products such as Intercept X Endpoint to enable EDR and Synchronized Security. Both the network and endpoint share intelligence to offer better visibility, protection and response advantages.

With Sophos Intercept X Advanced with EDR and Sophos Central Intercept X Advanced for Server, Hariss International gets a security solution integrated with industry-leading endpoint protection and EDR, that offers exceptional endpoint detection and response. Purpose built for IT security operations and threat hunting, Intercept X uses AI-driven analysis to detect and investigate suspicious activity. Active adversaries can be detected and remotely addressed with precision. Empowered with deep-learning, Intercept X detects and remediates never-seen-before threats, and the solution’s anti-ransomware technology identifies malicious encryption processes before they have a chance to wreak havoc across the organization.

The IT Team gets the advantage of end-point protection with centralized management, best placed to address the needs of a growing organization. Since the centralized management solution is hosted on the cloud, the administrative burden is reduced appreciably. With the Threat Analysis Center, EDR’s built-in query mechanism, the team has a better view of possible threats across the network by determining their root cause. EDR decreases the time spent in investigation, thus freeing up the IT Team’s team for other strategic security initiatives

Deployment Results

The Sophos deployment meets all of the organization’s security needs and then some more. The policies and rules applied on the Firewall and Endpoint protection have offered Hariss International and its IT Team better visibility and control over their network and endpoints. The management of the security solution is easier than before and the simplicity of the products has made configurations a breeze. “As a system administrator with a small team, I can easily view my network and determine any possible threats of infection that can harm the organization. We are very happy with our Sophos deployment and as long as Sophos tracks new threats and keeps its product management simple, we shall keep using its products, “signs off Mr. Bachour.

Find out how we can help protect your organization.
Visit www.sophos.com