Ugandan Government Organization Chooses Sophos to Build a Reliable Cybersecurity Posture

The Uganda National Bureau of Standards (UNBS) is a statutory body under the Ministry of Trade, Industry and Co-operatives and it's mandate includes formulating and promotion of the use of standards; enforcing standards in protection of public health and safety and environment against dangerous and substandard products; ensuring fairness in trade and precision in industry through reliable measurement systems; and strengthening the economy of Uganda by driving quality assurance of locally manufactured products to improve their competitiveness. As an important government entity, it was concerned that cyber attackers had such entities in their sights and were using advanced attacks to cause data breaches. The IT team was therefore on the lookout for security solutions that not only helped build a robust cybersecurity infrastructure, but also worked in tandem with one another to safeguard the organization's network, endpoints and server. Impressed with Sophos' strong product portfolio across network and endpoint, their search for a security vendor ended at Sophos.

CUSTOMER-AT-A-GLANCE

Company Name
Uganda National Bureau of Standards (UNBS)

Industry
Government

Website
www.unbs.go.ug

Number of Users
420

Sophos Solutions
G310 XG Firewall (Full Guard)

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

16 licenses - Central Intercept X Advanced for Server (SVRCIXA)

'Before switching to Sophos, we experienced plenty of virus attacks despite having deployed top-of-the-line cybersecurity. For the IT team, peace of mind and confidence in the existing security solutions were alien concepts. We decided to look for a solution that was extremely user-friendly, easy to deploy and which gave us the kind of security cover that protected us from advanced threats levelled at our network and the endpoints. Sophos provides both endpoint security and firewall protection meaning both can work together easily to combat security risks and this has given me and the IT team tremendous peace of mind.'

Nkwanga Joachim Charles
Manager ICT

Challenges

‣ A small IT team facing difficulties in coping with remote work challenges during the lockdown.

‣ Inability to get protection again known and unknown threats and better visibility into network assets and traffic.

‣ Failure to get real time insights into critical IT operations and threat hunting questions that can help the IT team take proactive cybersecurity decisions.

‣ Reducing action time on a device even if the device isn't physically present, to drive safety and security when employees are working remotely.

‣ Problems in securing IT infrastructure throughout the country and managing deployments from a single location.

The biggest challenge that UNBS faced is essentially faced by all government organizations across the world. Their data is under constant threat. Also, the organization's need to protect it with cutting-edge security stemmed from the fact that they had suffered from virus attacks in the past. Mr. Charles and his IT team were concerned with the evolving nature of these threats and the fact that they could come from anywhere at any given time. Threat mitigation from a growing and diverse attack surface was the need of the hour. What's more, the pandemic led to a move from an in-office work model to a work-from-home model wherein employees are working remotely. This meant employees were accessing corporate resources remotely, which added another element of risk to the work process. Moreover, as the IT team was also working remotely, it was important that they were able to handle any security issues proactively and remotely.

The overarching challenge was to deploy a robust cybersecurity infrastructure that addressed the security needs of an organization that was working from home; the organization's IT security had to be flexible and scalable enough to protect its employees across distributed locations. "We were looking at a scenario wherein we had to ready our cybersecurity infrastructure for a face off against more advanced cyberthreats that could take advantage of a work environment wherein our employees were not working out of their office," says, Mr. Charles. "While we wanted a cutting-edge security system to bolster our organizational network, we also wanted to offer the best security cover to our employees who were working remotely because of the pandemic."

The Move Towards Sophos

While looking at the various security vendors that could deliver the layered security cover UNBS needed, the IT team evaluated the various options under consideration on four primary parameters – usability, proactive support, customer care, and comprehensive protection. Sophos came good on all these parameters and more. The team was extremely satisfied with the Xstream architecture that Sophos' XG Firewall brought to the table and its ability to offer powerful protection and leading-edge performance. They were are also impressed with Sophos' EDR solution purpose built for simplifying IT security operations and threat hunting. The fact that it is a coming together of EDR with a comprehensive endpoint and server protection means threats are blocked at the door, before they get a chance to infect the organization's endpoint.

A Unified Security Environment with Sophos

With Sophos, UNBS gets a holistic security cover made up of prevention, detection, investigation and response across its network and endpoints. This cover is backed by actionable security intelligence that both the network and endpoints share with each other. This guarantees a more integrated approach towards cybersecurity that is tailormade to protect against sophisticated threats.

XG Firewall offers all-in-one-protection that includes a range of security features that help UNBS stop attacks before they wreak havoc. It's high-performance IPS and ATP are configured to protect against the latest hacks and its superior web and app control enables Mr. Charles and team to configure web filtering policies and user and group-based application controls. Also, it's inbuilt

VPN secure access solution helps extend the network security to employees who are working from home. The internet captive portal prevents unauthorized connections to the UNBS network and the firewall sends daily network statistics e.g., sites visited, volume of internet data used, etc.

Sophos Central Intercept X Advanced with EDR and Central Intercept X Advanced for Server offer UNBS an extensive security blanket that delivers protection across their endpoints and server. With in-built AI, Intercept X deliver signatureless detection to zero in on both known and unknown threats and exploit prevention stops techniques used in file-less, malware-less, and exploit-based attacks.

With EDR, the process of detection and investigation are taken many notches higher as the IT Team can ask for detailed insights into the activities on UBNS' server and endpoint. They get the advantage of proactive security, backed by threat hunting that detects active adversaries; protection is a potent mix of defensive and offensive capabilities. The fact that breaches are stopped before they start, the number of items to be investigated goes down, which saves a lot of time for the IT Team.

All Sophos solutions coordinate effectively to identify isolate and cleanup compromised devices. Upon threat neutralization, and when the risk of lateral movement is zero, network connectivity is restored. This happens automatically without any admin intervention. Also, the solutions deployment by UNBS can be managed and monitored from Sophos Central, the cloud-based management platform for all Sophos deployments. Mr. Charles and team can investigate potential threats, craft and implement policies and get drill-down visibility into all installations from a single unified console.

Deployment Results

With Sophos, Mr. Charles and his team have been able to easily secure and control their countrywide IT infrastructure. What's more, they have got immediate and actionable support, which has saved a considerable amount of time and effort for their team. Since, the time they started using Sophos, they haven't experienced any virus attacks and more importantly both their network and systems are performing much better than before.

"Sophos solutions are user friendly and have good support, which ensures a lot of time is saved that will otherwise be spent on managing the different security solutions deployed. What's more, EDR features such as automated threat identification, Live Response and Live Discover, has made life simpler for us when it comes to responding to, and solving all manner of security incidents," signs off Mr. Charles.

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

SOPHOS