A Combination of Advanced EDR and Firewall Delivers Advanced Protection to a **Tanzanian Bank**

Amana Bank is a full-fledged, licensed, and registered commercial Islamic Bank in Tanzania, operating under Sharia Compliance. Since it began its operation in 2011, the bank has experienced tremendous growth and has assumed a prominent role in the banking and finance industry in Tanzania. This growth is backed by a continuously scaling IT infrastructure to meet the demands of the business and its clients. This has meant the bank now has to secure its network and endpoints from a growing attack surface, made worse by the sophisticated nature of attacks. The small, but supremely efficient IT Team at Amana Bank, therefore wanted to build a cybersecurity posture that protected them from known and unknown threats, in real-time and at the same time was easy to control and manage. Sophos emerged as the perfect security vendor for their needs.

CUSTOMER-AT-A-GLANCE

Amana Bank
Together, on the right path

Amana Bank
Tanzania

Industry
Banking and Finance

Website
www.amanabank.co.tz

Sophos Solutions
XG430
Sophos Central Intercept X Advanced for Server with EDR
Sophos Central Email Advanced

"Threat detection, visibility, and automated response are the three primary qualities we were looking for from a cybersecurity perspective. Also, we did not want to work with different vendors but a single security partner who could offer security solutions for the network, as well as, endpoints. Sophos ticked all the boxes."

ABDUL BANDAWE, HEAD OF ICT, Amana Bank

Challenges

- Addressing the prospect of ransomware attacks being launched against the bank
- Inability to filter user activities and gain insights into risky user behavior
- Protecting employees from phishing attacks
- Difficulty in keeping track of, and managing numerous security initiatives and data coming from diverse security solutions
- A small IT team tasked with optimizing the performance of the IT infrastructure, as well as, managing the security protocols

Dependence on traditional security solutions was limiting the cybersecurity posture of Amana Bank. The IT team recognized the importance of transitioning to a far more mature security approach than they currently had, the kind of approach that offered comprehensive security across the network and endpoint.

"We were working with different security vendors and were finding it difficult to manage the disparate security solutions. Analyzing and evaluating data from different sources was a time-intensive task. What's more, we were still not getting the depth of security we wanted," states Mr. Abdul. The IT team set about exploring the various options available on the market, preferably from a single vendor, that not only delivered excellent protection but wherein all the installations could be managed from a single console.

Mr. Abdul was also concerned about the rise of phishing attacks and their increasing levels of sophistication. He wanted to deploy smarter email security that stopped ransomware and all manner of stealth and phishing attacks.

Also, the overarching approach to security transformation had to focus on creating a security ecosystem that talked to one another and worked in tandem to identify threats, isolate infected endpoints and remediate threats in an automated manner, thus saving the IT Team's time that could be spent elsewhere.

"Along with the best endpoint protection available on the market, its EDR functionality purpose-built for IT security operations and threat hunting is a big plus. As a small team, we wanted to support in answer questions around security incidents and maintain security operations hygiene and EDR has answered this need, in its entirety."

ABDUL BANDAWE, HEAD OF ICT, Amana Bank

A Centralized and Mature Approach to Security with Sophos

The IT Team evaluated a range of security solutions and what differentiated Sophos and its powerful security portfolio from the competition, is that this portfolio spanned both network and endpoint. Also, the adaptable and advanced nature of the solutions coupled with a core focus on performance and cutting-edge technology, encompassed by the power of Synchronized Security, left no room for doubt that Sophos was perfectly placed to address the Amana Bank's security needs and challenges.

With Sophos Firewall, the IT Team gets tremendous visibility and control over all applications on the network and any malicious activity impacting performance. "We are also impressed with Security Heartbeat that links the Sophos Firewall to the Sophos Managed Endpoint and isolates threats before they move laterally through the network," says Mr. Abdul.

With the Advanced Threat Protection feature, the firewall detects bots and any other advanced threat launched against the network. Also, the team can now configure user identity-based policies and make use of unique user analysis to control users and their activities on the network. The team now has complete visibility and control over the web traffic and can exercise enforcement based on user activity, schedules, quotas, and traffic shaping. Mr. Abdul is now confident that they have full control over their network as they can now keep a watch on traffic, users, and apps.

With Intercept X for Endpoint, the Bank's endpoints are protected with best-in-class endpoint security that offers features that stop unknown threats, block ransomware, and prevent exploits. The endpoint protection leverages deep learning AI to detect and block never-seen-before malware; and its anti-ransomware capabilities not only detects and blocks ransomware but also roll back changes to files, thus ensuring business continuity.

Also, features like application lockdown, web control, data loss prevention, and signature-based malware detection, ensure Mr. Abdul and his team can rest easy knowing all-encompassing endpoint security has got their back.

Also, features like application lockdown, web control, data loss prevention and signature-based malware detection, ensure Mr. Abdul and his team can rest easy knowing an all-encompassing endpoint security has got their back.

"Along with the best endpoint protection available on the market, its EDR functionality purpose-built for IT security operations and threat hunting is a

big plus. As a small team, we wanted to support in answer questions around security incidents and maintain security operations hygiene and EDR has answered this need, in its entirety," says Mr. Abdul.

For the team, EDR baked into Intercept X ensures the team now has access to historical endpoint data that offers answers to drive informed decision-making. All the team needs to do now, is ask specific questions around performance and security and get data-backed answers. When the team confirms a security issue, the device can be remotely accessed to take necessary action.

With Sophos Email, Amana Bank and its IT Team are able to maximize the potential of the solution's deep learning neural network to stop zero-day malware and unwanted applications. They also get the benefit of behavioral analysis to stop ransomware threats and boot-record attacks at the gates.

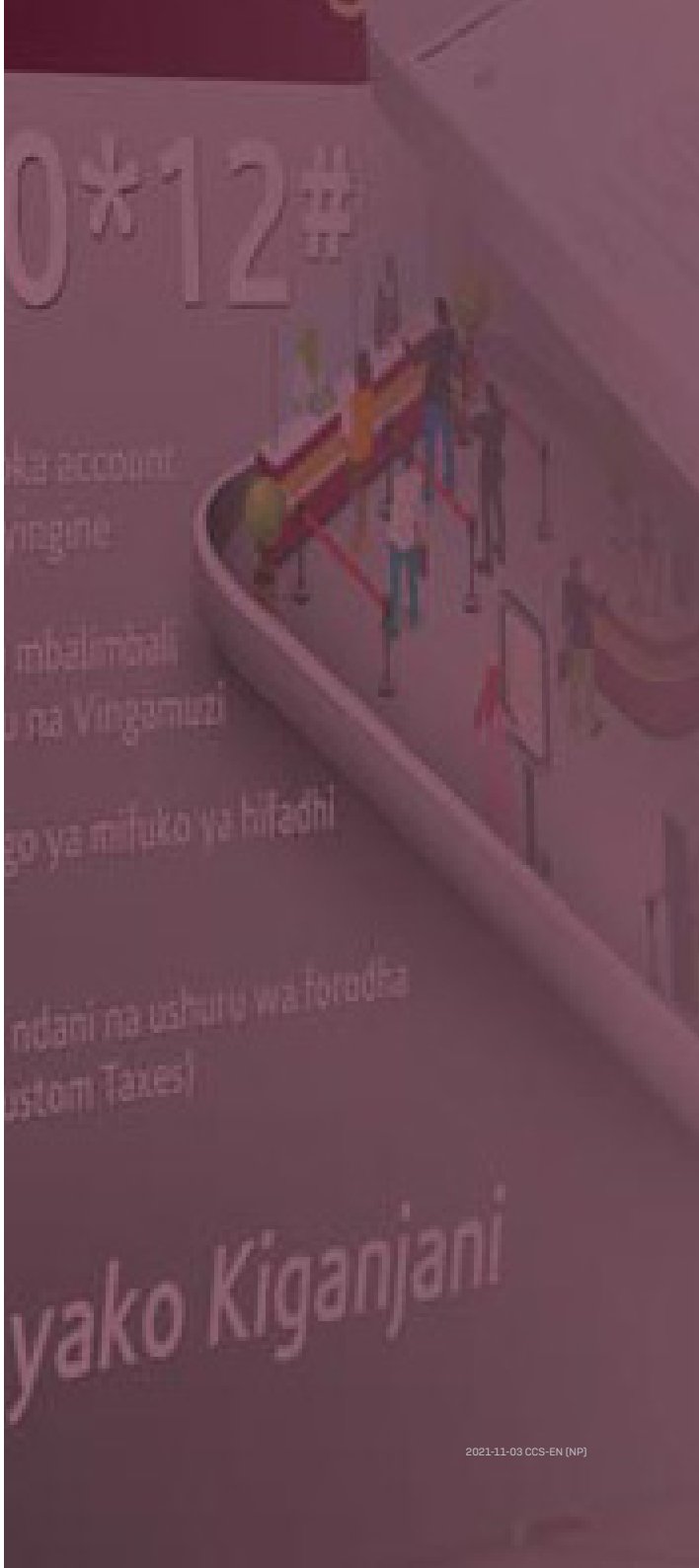
"The biggest benefits of using Sophos Central Email Advanced is that it easily and comprehensively blocks phishing attacks using a range of techniques including SPF, DKIM and DMARC and analyses such as email header anomaly, display name and lookalike domains. Sophos Email blocks, quarantines and tags suspicious messages with a warning," explains Mr. Abdul. I now have confidence that employees won't fall a victim to phishing attacks.

The Bank now benefits from a Sophos ecosystem, wherein products are connected to each other via Synchronized Security and all of them can be managed from a single management console – Sophos Central.

Deployment Results

Sophos has delivered on all Amana Bank's security needs and has allowed the IT Team to address all security challenges in an end-to-end manner. Post Sophos deployment, the bank benefited from immediate security ROI through easier management and control and quicker support. With Sophos Central, the team now has complete visibility, management and control of all the security installations, and can easily push security policies and make sense of all the security data coming their way.

"We are happy with all aspects of Sophos implementation and have a special word of praise for its EDR as it has given us new insights into security incidents and enabled us to build a better cybersecurity posture. With Sophos, we were able to build cutting-edge cybersecurity infrastructure, that is extremely easy to manage. So yes, we recommend it to any organization that is challenged by the evolving cyberthreat landscape," signs off Mr. Abdul.



© Copyright 2021 Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is a registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

SOPHOS

2021-11-03 CCS-EN (NP)