



CUSTOMER CASE STUDY

African + Eastern strengthens security with around-the-clock protection

By deploying Sophos MDR, African + Eastern gained 24/7 monitoring, proactive threat hunting, and expert-led threat response



african+eastern
INSPIRING GREAT BLENDS

Industry

Beverage Distributor

Sophos Solutions

Sophos Managed Detection and
Response (MDR)



About African + Eastern

African + Eastern is a Middle East leader in beverage alcohol featuring a wide variety of spirits, beer, wine, and champagne, tracing its roots back three centuries, first as a general trading company originating in Africa and more recently throughout the Middle East with more than 50 years of expertise exclusively in the distribution of alcoholic beverages in the Arabian Gulf.

The challenges

- No holistic security approach across multiple security products.
- Inability to detect threats and respond to cyberattacks.
- Lack of internal security operations personnel.

Group Information Systems Manager, Santhosh John Thomas, recalled how the organization built its cybersecurity defenses on perimeter firewalls, next-generation firewalls and intrusion prevention systems. As the company grew and added endpoint detection and response technology to its infrastructure, Thomas realized this defense focus on multiple point products was not the holistic security approach African + Eastern needed to stay ahead of threat actors and minimize their organizational risk.

“There came a point where we realized the path we were on might not be the right one,” Thomas said. “We needed to shift our perspective. We recognized the need for a comprehensive cybersecurity portfolio, viewed from a different angle. This promoted us to embark on a new direction: establishing our very own Security Operations Center (SOC).”

The solution

- Deliver around-the-clock monitoring, investigation and response to valid threats.
- Comprehensive visibility and threat detection.
- Proactive, continuous threat hunting.

Given the cost of constructing and operating an internal SOC and the difficult in hiring, training and retaining skilled security resources, African + Eastern determined that building an in-house SOC wasn't feasible. Instead, Thomas said the decision was made to find a robust security solution that could deliver extensive security operations experience and bring in an established SOC from an external security provider.

Sophos Managed Detection and Response (MDR) set itself apart during the company's process of evaluating third-party solutions. Sophos MDR solutions deliver the 24/7 holistic visibility African + Eastern requires, which continuously gathers and interprets telemetry from proprietary and third-party sources throughout a customer's environment,

“There came a point where we realized the path we were on might not be the right one. We needed to shift our perspective. We recognized the need for a comprehensive cybersecurity portfolio, viewed from a different angle.”

Santhosh John Thomas
Group Information Systems
Manager, African + Eastern

Sophos delivered numerous demos and a proof-of-concept to show the skill and expertise of its security operations personnel, threat intelligence, incident response and threat hunting capabilities. Each MDR customer works with a Customer Success Manager (CSM) who collaborates with customers to set and meet goals for security program success, and a Threat Engagement Manager (TEM) who meets with customers every quarter to review overall security posture and areas to improve and reduce overall risk.

“The reliability of Sophos stood out,” Thomas said. “The platform proved to be exceptionally effective during our evaluation. It offers comprehensive threat detection and correlation rules, which impressed us greatly. This level of effectiveness left no doubt in our discussions, making it clear that Sophos could meet our security and business requirements.”

Results and impact

- Comprehensive approach to security monitoring and threat detection.
- Access to security expertise, threat hunting and threat intelligence.
- Combination of global security leader and in-region security operations partner.

A powerful differentiator for African + Eastern is the strong Sophos' presence in region, including incident responders, penetration testers, security engineers, sales support and CSMs.

“Sophos, with its wealth of experience, introduced valuable insights into our discussions,” Thomas said. “We found ourselves in strong agreement on critical aspects such as incident response, threat hunting and the validity of security measures. Their commitment to security aligns perfectly with our vision, making them an ideal collaborator in our pursuit of safeguarding our organization.”

African + Eastern sought a local security operations resource that could work exclusively for its organization. Sophos strategic partner Finesse is based in Dubai and works closely with the company on the delivery of Sophos offerings.

This security operations expert has augmented African + Eastern's team by working directly in the Sophos system, collaborating with the Sophos SOC on alert investigations, escalating incidents to the African + Eastern team and driving remediation and improvement efforts.

“Sophos, with its wealth of experience, introduced valuable insights into our discussions. We found ourselves in strong agreement on critical aspects such as incident response, threat hunting and the validity of security measures.”

Santhosh John Thomas

Group Information Systems
Manager, African + Eastern

“The proficiency of the Sophos platform, combined with this local presence, has contributed immensely to keep us safe and secure,” Thomas said. “Should any security issue arise, we know exactly who to contact first and have a well-defined protocol for escalation.”

Looking ahead

The combination of Sophos and Finesse provides African + Eastern with the perfect solution to enhance its ability to safeguard the organization against cyberthreats and reduce their overall risk. For Thomas, teaming up with Sophos and Finesse represents a necessary next step in his organization's cybersecurity journey.

“In a rapidly evolving security landscape, where new threats and vulnerabilities emerge daily, investing in security is akin to securing insurance for our digital existence,” he said. “It’s an indispensable safeguard that shouldn’t be overlooked.”

“The reliability of Sophos stood out. The platform proved to be exceptionally effective during our evaluation.”

Santhosh John Thomas
Group Information Systems
Manager, African + Eastern

To learn more visit [Sophos.com](https://sophos.com)

© Copyright 2025. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners. (11-2025)

