CUSTOMER CASE STUDY

Royal Media Services: A cybersecurity evolution rooted in trust and visibility

After experimenting with an outsourced Security Operations Centre (SOC), Royal Media Services shifted to Sophos MDR for proactive, global threat monitoring.

SOPHOS

ROYAL MEDIA SERVICES

Royal Media Services

Industry
Television and media

Number of Users
900

Sophos Solutions:
Sophos Central

Sophos Endpoint powered by Intercept X

Sophos Managed Detection and Response (MDR)

Challenges:

- RMS initially relied on Linux-based firewalls and unsecured access points, lacking a unified security framework.
- Without centralized monitoring, RMS struggled to track threats across endpoints, wireless networks, firewalls, and cloud services.
- RMS experienced incidents where user credentials were compromised and leaked online, highlighting the need for dark web monitoring and proactive remediation.
- Previous attempts to outsource their security operations center didn't provide the responsiveness or global threat intelligence the company required.

For Kenya's largest media house, cybersecurity wasn't just an IT concern — it was a matter of public trust.

Samuel Kibacia, head of IT Infrastructure at Royal Media Services (RMS), recalls the early days vividly: "We started off with a Linux-based firewall," he says, "access points that were not security ready."

As Kenya's largest media house — with three television stations, 13 radio stations, and a growing digital and video on-demand (VOD) presence — RMS was rapidly expanding, but its security infrastructure lagged behind.

With millions of viewers and listeners relying on RMS for accurate information, the stakes were high — a single breach could compromise public trust and national discourse.

"Citizen is the biggest TV station in Kenya," Kibacia said. "And our radio stations are the biggest radio stations in Kenya."

With such a prominent public profile, RMS faced a unique challenge: The risk of misinformation.

"If something is broadcast that is not true on one of our platforms, it's almost taken like biblical truth," he said. "So that forms a very serious security threat for us."

Over time, RMS adopted a unified threat management approach.

"We started off with having Sophos at the wireless point, Sophos at the endpoint, Sophos at the firewall," Kibacia said.

RMS unified their defenses under Sophos Managed Detection and Response (MDR) — gaining 24/7 expert monitoring, global threat intelligence, and real-time response capabilities.

"Security is not something you install and then your organization becomes secure. "It requires constant monitoring. You have to continuously see what is happening, meet new challenges, and be able to adapt as threats change."

Samuel Kibacia
Head of IT Infrastructure at Royal Media Services (RMS)

A need for constant monitoring

The shift wasn't just about layering tools — it was about gaining visibility and control.

"Security is not something you install and then your organization becomes secure," he said. "It requires constant monitoring. You have to continuously see what is happening, meet new challenges, and be able to adapt as threats change."

The threat landscape was evolving fast. A decade ago, ransomware wasn't a very common cyber threat for the organization, Kibacia recalled, and about five years ago ransomware was the company's main threat. Today, Kibacia's top concern is AI-generated threats — sophisticated attacks that mimic legitimate behavior and evade traditional protection. As RMS moved more services to the cloud to address these evolving threats, Sophos moved with them.

"We protect our instances also on the cloud, and all of that information comes together on Sophos Central," Kibacia said. "We are able to have clear visibility of any service or application. If there is any threat, we have a 360 view of where it came from, how it moved, and what other services may be affected — including remediation."

The decision to adopt Sophos MDR was driven by the need for proactive, global threat intelligence.

"We realized that there are new threats coming up every single day," he said. "Even if we built a [security operations center] internally, it would be very focused on threats affecting our organization. But with [Sophos] MDR, we have a global organization focused on our security. So threats — even if they come up from other countries — by the time they reach our shores in Kenya, somebody has already seen them, understood them, and actioned them."

Why RMS chose Sophos

RMS had tried outsourcing its SOC before, but the experience didn't compare.

"One of the biggest advantages we got from Sophos MDR was that they are always there for us," Kibacia said. "They are viewing and reporting on threats we haven't even identified. They're a 24/7 service, and beyond that, they work with us to remediate any threat or penetration."

That partnership proved invaluable when one of RMS' users had their account compromised. In this case, the user had their credentials stored on a web browser, and eventually had them leaked online.

"We protect our instances also on the cloud, and all of that information comes together on Sophos Central. We are able to have clear visibility of any service or application. If there is any threat, we have a 360 view of where it came from, how it moved, and what other services may be affected — including remediation."

Samuel Kibacia
Head of IT Infrastructure at Royal Media Services (RMS)

Thanks to a dark web scan from Sophos, Royal Media was alerted of the leaked credentials and allowed the employee to reset their credentials immediately before any bad actor could take advantage of the stolen information.
Sophos Endpoint powered by Intercept X also plays a critical role in ransomware protection.

"We had a ransomware attack on one of our users' computers," Kibacia recalled. "Despite having [legacy] antivirus, it was still ransomed. The ransom engine on [Sophos Endpoint] ensures that any files that are encrypted are decrypted. We've not had a ransomware threat since we started working with them."

Sophos as a complete partner

Today, Sophos MDR is RMS' primary security team.

"In the event that we have a threat, our team actions on the advice provided by the Sophos team," Kibacia said. "We also have quarterly reviews, and during onboarding we did monthly reviews to check for any immediate threats."

Looking ahead, RMS is focused on securing its core switches and gaining full visibility across its network. The company has moved all its logs to cloud storage, which are then covered by Sophos MDR. And as other network access also move to the cloud in the future, the company relies on Sophos Central to monitor everything in one place.

For RMS, cybersecurity is more than just protection—it's about trust, reputation, and resilience.

"Sophos goes beyond a SOC," Kibacia said. "They become a partner. They become one with you, wanting to help your organization grow and achieve your goals."

To get started with Sophos solutions today and find a solution that scales to your needs, speak to an expert today.

© 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.

2025-10-24 CCS-EN (NP) CRE-3685

SOPHOS