SOPHOS

Cloud Security Posture Management Solution Helps Sophos Gain Control Over Its Cloud Estate

Sophos defends the infrastructure and data of its more than 3,000 users and 400,000 customers worldwide. The Sophos internal IT and security teams use multiple Sophos products for the organization's daily security operations. This real-world environment serves as a valuable testing ground, providing the company with insights that inspire continual improvements and advancements to the Sophos portfolio of products.

Sophos
Abingdon, UK

Industry
Information security software provider

Website
www.sophos.com

Number of Users
3,000+

Sophos Solutions
Sophos Cloud Optix

> *'With Sophos Cloud Optix, we significantly minimize alert fatigue. The powerful artificial intelligence built into Sophos Cloud Optix correlates the data and shows us what is truly meaningful and actionable.'*

Ross McKerchar
CISO
Sophos

Challenges

- Gaining visibility across the entire cloud estate
- Preventing alert fatigue and ensuring that alerts are valid and actionable
- Managing cloud accounts and cloud security from a centralized location
- Reaffirming that security controls already in place are working as they should

Sophos defends the infrastructure and data of its more than 3,000 users and 400,000 customers worldwide. The Sophos internal IT and security teams use multiple Sophos products for the organization's daily security operations. This real-world environment serves as a valuable testing ground, providing the company with insights that inspire continual improvements and advancements to the Sophos portfolio of products.

How does Sophos achieve unprecedented visibility across its entire public cloud environment?

Sophos IT and Sophos Cybersecurity team were in search of a visibility, security, and compliance tool for its entire cloud estate, which consists of more than 200 public cloud accounts, using Amazon Elastic Compute Cloud (Amazon EC2), part of Amazon Web Services (AWS) and Microsoft Azure. Sophos CIS Global Operations Manager Andy Joel and Sophos Senior Red Team Lead Dave Davison led the evaluation effort and performed in-depth proof of concept evaluations of multiple products.

Some of the tools they evaluated were cloud management solutions with only a limited set of security functions. Others lacked scalability—they had well-engineered single-pane-of-glass management consoles but could only handle a half dozen accounts at any given time. "Looking at what is available in the marketplace, the big takeaway is that organizations may tend to think that cloud management solutions include cloud security, but that's not the case at all. Adding a simple set of configuration checks doesn't equate to cloud security. In today's dynamic environment when bad guys are using automation and AI to attack, you need a sophisticated solution which analyzes network traffic and user activity logs to proactively inform of potential breaches. For us, that is Cloud Optix." notes Davison.

The team discovered that the only solution that truly checked off all the boxes for them was Sophos Cloud Optix. At Sophos, things move fast and change rapidly, with product teams frequently creating new cloud accounts for development purposes. For Joel, the tool addresses one of his biggest concerns: having visibility across all these highly fluid production environments and ensuring they are secure.

The intuitive and easy-to-use centralized management hub offers an across-the-board view of the highly dynamic Sophos cloud terrain. It includes dashboards with visualizations of the cloud architecture, complete with traffic flows; alert summaries and details; and compliance status.

"Sophos Cloud Optix provides us with unprecedented top-level visibility across our entire estate—way beyond what most cloud management tools claim to offer," he explains. Sophos Cloud Optix provides automatic discovery of the organization's assets across all cloud environments. Through network topology visualization and continuous asset monitoring, the security team can quickly respond to and remediate security risks.

How does Sophos Cloud Optix help improve security processes while offering an extra measure of reassurance?

An example of Sophos Cloud Optix in action is the recent discovery of a handful of user accounts that did not have multi-factor authentication enabled—a direct conflict with company policy. This policy violation occurred in spite of the fact that Sophos had a process in place to enable multi-factor authentication. Because of Sophos Cloud Optix, Joel discovered that the process wasn't quite working the way it should, so it was adjusted accordingly.

"If you don't have complete and continuous visibility into what's going on in your environment, you're blind to potentially suspicious, malicious, or non-compliant activities. Sophos Cloud Optix helps us see everything, protect everything, and take appropriate action," states Joel.

Another revelation that surfaced as a result of deploying Sophos Cloud Optix is that Sophos had a low number of high-priority alerts and zero critical alerts across the entire cloud estate, including the production account for the Sophos Central management platform. As Joel points out, "This is a real testament to the people who have designed and built the production environment. Sophos Cloud Optix gives us a sense of confidence and the reassurance that we have all the right controls in the right places and that they are functioning as they should."

What makes Sophos Cloud Optix alerting stand out among competing technologies?

Davison also notes that, unlike competitive products that deluge security teams with thousands of alerts, Sophos Cloud Optix uses artificial intelligence to power monitoring, detection, and security analytics. All this results in a set of prioritized and correlated "smart alerts" that are both accurate and actionable. It helps the Sophos team remediate security risks faster, with automated alert ranking combined with contextual information. This prevents alert fatigue and helps the security team focus on what's most relevant.

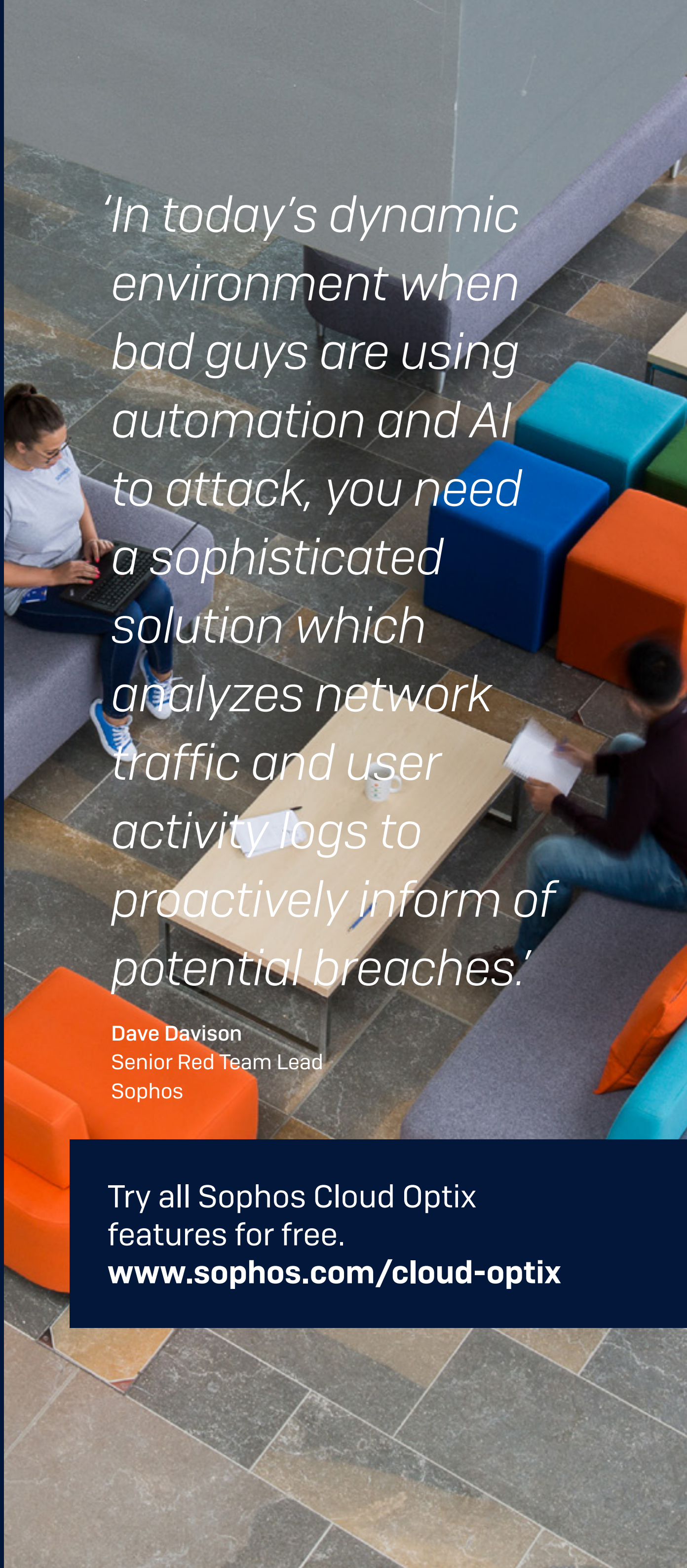
"I found that some vendors try to convince customers that more alerts is better, but that's not really the case. We don't want to filter through hundreds of low priority items. I think Sophos Cloud Optix has really pitched the ball in the right direction on this regard. The critical alerts tend to be things we want to deal with," he asserts.

The flexibility to custom configure alerting and remediation is another big advantage for an organization like Sophos that has so many different groups—each with their own security requirements—creating cloud workloads. For example, in certain accounts, an alert may be classified as "critical," whereas in others, it may be classified as "medium."

Sophos CISO Ross McKerchar further elaborates on this point: "With Sophos Cloud Optix, we significantly minimize alert fatigue. Other solutions play by the numbers, inundating security teams with a massive number of undifferentiated alerts. The powerful artificial intelligence built into Sophos Cloud Optix correlates the data and shows us what is truly meaningful and actionable. This gives us a highly accurate picture of our security posture and risk level, enabling us to prioritize and proactively remediate through automated processes. It's a security product built by security people for security people. We'd be using the technology even if we didn't own it."

In an ever-changing cloud environment, how does Sophos Cloud Optix help maintain continuous compliance?

Compliance is the third requirement that Sophos Cloud Optix satisfies for Sophos. With out-of-the-box templates, automation, custom policies, and collaboration tools, it addresses both standard external compliance regulations and internal governance to ensure consistent best practices across all the organization's cloud accounts. When workloads are created in the cloud, it's often a challenge to determine which compliance processes are applicable and how they should be implemented. Davison and this team are looking forward to using Sophos Cloud Optix in the very near future as a way to reduce the cost and complexity of governance, risk, and compliance in their public cloud environment.



'In today's dynamic environment when bad guys are using automation and AI to attack, you need a sophisticated solution which analyzes network traffic and user activity logs to proactively inform of potential breaches.'

Dave Davison
Senior Red Team Lead
Sophos

Try all Sophos Cloud Optix features for free.
www.sophos.com/cloud-optix