SaaS Provider Leverages Sophos to Provide High-Profile Customers with Visibility into Security Posture and Compliance

CyberMetrics develops software products for the manufacturing industry that help improve quality, reduce costs, and maximize productivity at manufacturing facilities. Its two flagship products are GAGEtrak Calibration Management and Faciliworks CMMS. Headquartered in Phoenix, Arizona, the 25-person software company serves more than 12,000 customers worldwide, including major automotive manufacturers. In addition to automotive customers, it also serves the U.S. Food and Drug Administration (FDA), aerospace industry, and the U.S. military.

CUSTOMER-AT-A-GLANCE

CyberMetrics®

CyberMetrics

Industry
Software products

Web Service
aws

Sophos Solutions
Sophos Cloud Optix
Sophos Intercept X Advanced with Managed Detection and Response (MDR)
Sophos Intercept X

"Sophos came in and actually gave us real manpower that we don't have to hire to help us analyze and review everything for both on premises and AWS, and that was a huge decision-maker for us."

Brian Hertenstein, Systems Operations Manager

Challenges

- Lack of manpower and specialized security expertise
- Need for greater visibility into Amazon Web Services (AWS) environment
- Inability to report on SOC2 and ISO compliance

How does Sophos fit into the picture for a software provider? What pain points does it address?

CyberMetrics is heavily reliant on AWS servers to host its Software-as-a-Service (SaaS) products and leverages many of its services to support its demanding and complex applications, including Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS), Amazon Simple Email Service (Amazon SES), and Amazon ElastiCache.

The company has a hybrid IT environment, with a minimal physical network infrastructure at its corporate office, having moved many internal functions to SaaS applications like Salesforce and Microsoft 365. End-users, such as the sales and support team, do not use AWS.

Prior to Sophos, CyberMetrics had basic antivirus protection onsite and simple firewalls installed on its AWS servers. The primary security concern for CTO Devin Ellis was to provide visibility and reporting on its AWS security posture to customers and security auditors. Although the team had set up the environment to be as compliant as possible, they lacked a solid security incident plan and did not have full coverage when dealing with active threats. This was true both on premises and in the AWS environment.

"With AWS there's a good, solid, and reliable infrastructure, but the security is mostly on you," Ellis pointed out. Following its shared responsibility model for security, AWS demonstrated to CyberMetrics that it was "fantastic in terms of reliability, uptime, and basic security," meaning it ensures security for its infrastructure services, including compute resources, storage, networking,

and related functionality. However, CyberMetrics, like other AWS customers, is responsible for securing its applications and data on AWS servers.

Ellis found the task of measuring, managing, and mitigating threats was spreading his small team too thin. Aside from himself, Systems Operations Manager Brian Hertenstein was and still is the only other person handling security within the company. Given the dynamic and often volatile nature of the cyberthreat landscape, Ellis and Hertenstein knew it was time to upgrade the company's security internally while providing CyberMetrics customers with assurance that their applications were safe to use and their sensitive data was secure in the cloud.

How does Sophos help a small team take security to the next level?

Based on a recommendation, Ellis and Hertenstein decided to look into Sophos. After a presentation and demo of Sophos products, their eyes were open to a way to do security better in both their environments with a small team.

"Sophos came in and actually gave us real manpower that we don't have to hire to help us analyze and review everything for both on premises and AWS, and that was a huge decision-maker for us," says Ellis. As a small company, CyberMetrics is short on specialized security resources. Ellis appreciates how Sophos brings its experts to bear with its "Security-as-a-Solution" model, providing the additional security expertise and in-depth reporting that the small team needed. He says Sophos also gives them peace of mind knowing they have 24/7/365 coverage.

How did Sophos stand out from other solutions in the evaluation process?

Ellis highlights that it was the Sophos Managed Detection and Response (MDR) service that really made Sophos stand apart from other providers. Sophos MDR serves as an instant security operations center (SOC), with a global team of security experts continually monitoring the CyberMetrics environment. If a threat is detected, the Sophos MDR team sends out notifications and acts swiftly to block the threat, investigate the root cause, and communicate guidance on halting similar threats that may emerge in the future.

Hertenstein found Sophos Cloud Optix to be an effective tool to manage the company's security posture, providing visibility into the entire cloud environment and identifying vulnerabilities and risks.

In Sophos Cloud Optix, he can easily access the information he needs to pinpoint compliance risk or remediate security gaps. With software he had used in the past, he had to painstakingly navigate through the software to get where he wanted. In addition, unlike Cloud Optix, previous solutions provided some insights into the AWS environment but did not provide actionable guidance.

"Sophos was built from the ground up to integrate all of the pieces in one place. It doesn't feel cobbled together like some of the systems I've used in the past," he said. "With the Sophos Central management console, everything is right there and easy to use. You just click into it, and it takes you right to where you need to go. It's perfect."

Sophos Intercept X Endpoint was implemented on servers and end-user computers as a replacement for legacy antivirus. It helps reduce the attack surface and combines multiple techniques to stop attacks before they do harm. These include deep learning AI-based detection and prevention of never-before-seen threats, anti-ransomware, anti-exploit technology, and more. It fully integrates with the Sophos MDR service.

Deployment was smooth and straightforward. Hertenstein did the bulk of the work himself and really appreciated having the Sophos Professional Services team standing by to answer questions and double-check the process. "The deployment was a great experience, and it went really quickly," noted Ellis.

How does Sophos as a vendor stand out from the crowd?

In addition to the increased visibility made possible by Cloud Optix and the Sophos MDR service offering, which were unlike anything Ellis and Hertenstein had seen elsewhere, the team was impressed with Sophos as a company. One of Ellis's long-time colleagues, who also works in technology, had a lot of positive things to say about Sophos as a vendor. "The great reputation Sophos has went a long way toward persuading us to embrace its approach to security," he asserted.

In addition to Sophos's reputation, the personalized sales process and comprehensive demo were also instrumental in supporting the team's decision to embrace Sophos. Ellis remarked that the Sophos team did a great job in getting things scheduled, keeping the momentum going, and responding to questions that arose.

"Sophos was built from the ground up to integrate all of the pieces in one place. It doesn't feel cobbled together like some of the systems I've used in the past. With the Sophos Central management console, everything is right there and easy to use. You just click into it, and it takes you right to where you need to go. It's perfect."

Brian Hertenstein, Systems Operations Manager

What security gaps does Sophos solve? How does deploying Sophos MDR and Cloud Optix change business processes?

Sophos has transformed security for CyberMetrics. In addition to vastly increasing visibility into its AWS services, Hertenstein said, "The Sophos MDR alerting system is amazing. It's helped reduce my workload tremendously."

A key part of the visibility gap that the team wanted to close was to determine the company's compliance with SOC2 and ISO standards. Cloud Optix provides that visibility and enables them to show the status of their adherence to those standards to customers. "Even if we don't have the SOC2 certification, we can at least display to a customer that we have these initiatives in place, that we are measuring ourselves against the standards, and that we have a way to show that. Cloud Optix gave us the ability to actually provide that report," Ellis explained.

What other benefits does Sophos bring to the table?

Sophos has freed up time for Hertenstein to work on other tasks—and it has enabled him to take a month off for paternity leave without having to worry. He configured the settings on Sophos Central to have the Sophos MDR team automatically resolve any issues that arise and notify him if there is anything he needs to do.

While he was away on leave, he received a couple of notifications that something was trying to be installed, but the Sophos MDR team isolated the problem and immediately stopped the threat from doing damage. When Hertenstein returned from leave, he felt reassured that things were under control.

"Sophos MDR saves me a lot of time from having to go down the rabbit hole of something that I don't completely understand and that is not my area of expertise," he pointed out.

For CyberMetrics, having Sophos products and the Sophos MDR service in place is like having an extended team. This enables the technical team to focus on strategic projects and provides visibility and peace of mind to customers. "As technical as we are, we're not security experts. We're not forensics experts. So it's really awesome having the Sophos team behind us," asserted Ellis.

"The Sophos MDR alerting system is amazing. It's helped reduce my workload tremendously."

Brian Hertenstein, Systems Operations Manager

Learn more about
Sophos MDR today.
www.sophos.com/mdr

2023-05-31 CCS-EN (PC)