Rapid Growth Spurs the Leader in Imaging Products and Services to Adopt Sophos Cloud Optix for Securing its Cloud Environment

aws partner network

Executive Summary

With Sophos Cloud Optix, Shutterfly now has real-time visibility into cloud assets along with a strong security posture built for an elastic cloud environment. This online image-publishing service found a way to reduce manual compliance efforts, assessment, and monitoring, for SOC2 and other regulations in their ever-evolving environment. Now with Sophos firmly in place, Shutterfly has a secure infrastructure at the pace of DevOps by continuously proactively analyzing and monitoring infrastructure code changes.

What impact does growth and expansion have on cloud infrastructure?

Shutterfly is growing their customer base both organically and inorganically. In order to meet the needs of millions of consumers, Shutterfly chose to embrace public cloud to benefit from the agility and flexibility it brings.

What are the security challenges that come with shifts in the business?

From an information security standpoint, this rapid expansion was transformational. The Shutterfly environment currently consists of several AWS accounts and numerous Amazon EC2 Instances, with steady amounts of traffic per day. The server instance count at any given point is not stationary as the organization dynamically spins up and spins down servers to meet seasonal compute requirements. So, the number one challenge was getting real-time visibility of the environment – servers, security groups, user access. The second biggest challenge was to provide continuous compliance of the cloud environment. The last challenge was securing the environment at the DevOps pace where developers are constantly making changes.

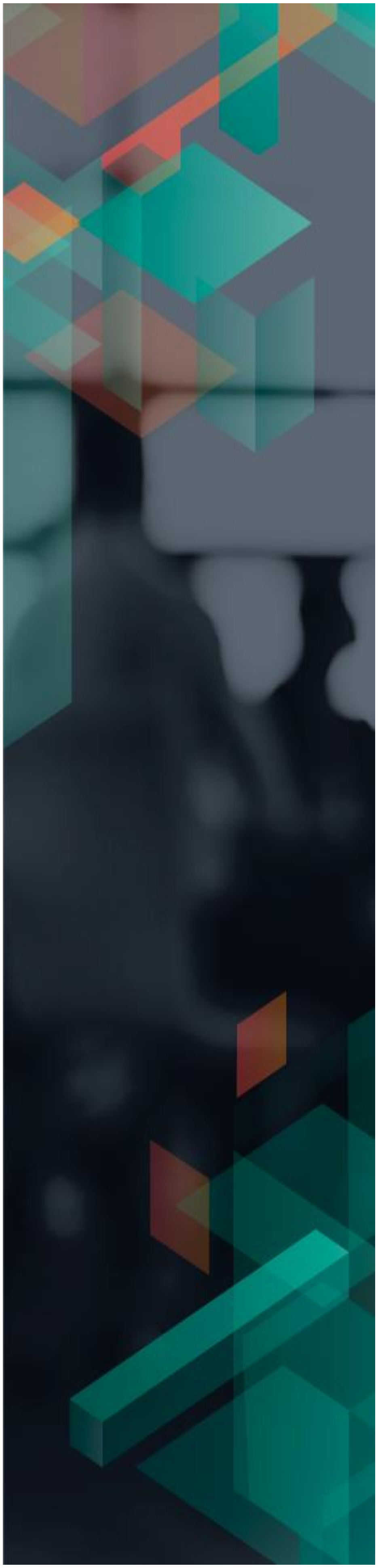
What does a fast-growing company look for in a -cloud security solution?

The solution should provide consistent visibility, security, compliance, and policy enforcement for all workloads in use. The solution also had to be extensible and leverage artificial intelligence and machine learning to make it possible for the teams to secure Shutterfly's dynamic, evolving cloud environment in a process efficient way. It needed to easily integrate with Shutterfly's current security tools and be flexible enough to enable the team to onboard new technology platforms and changes as needed.

About Shutterfly

Shutterfly.

Shutterfly, Inc. is a leader in online personalized imaging products and communications. Founded in 1999, the organization has three diverse business units: Shutterfly Consumer, Lifetouch, and Shutterfly Business Solutions.



Why is visibility so critical to pervasive and proactive cloud security?

You cannot secure what you can’t see.

“One of the things that my team was excited about from day one was the ability of Sophos Cloud Optix to provide an accurate real-time asset inventory, which is the foundation of any security program,” explains Aaron Peck, VP and CISCO for Shutterfly, Inc. “You can build a million controls, and you can deploy them, but if you don't know which assets you're protecting, you have no idea if those assets are actually covered by the controls you're deploying. The level of visibility made available to us by Sophos Cloud Optix is critical for our work.”

Sophos Cloud Optix is also a huge time-saver. When issues arise, the team can quickly search for a resource and receive a risk profile rich with valuable data, such as: Who owns it? What is it attached to? Where does it sit in the environment? What does it communicate with? When was the last time modifications were made to this resource? Is the resource accepting connections from the outside world? The automation provided by Sophos Cloud Optix replaces significant manual effort, aggregating security intelligence from a range of AWS security services including Amazon GuardDuty, AWS CloudTrail and AWS Security Hub in a single risk assessed and prioritized view to get to issue identification and solution paths faster, when every minute matters.

The artificial intelligence technology built into Sophos Cloud Optix drives the accuracy of its findings and its ability to correlate data.

“With Sophos Cloud Optix, not only are the findings as a whole more accurate, it is also capable of proactively informing us about suspicious behaviors it sees. And this is clearly not based on a predefined set of rules, but something that improves over time. Built-in artificial intelligence makes it possible for the solution to actually learn and adapt as it takes in more information,” observes Peck.

Lastly, having a complete understanding of your network topology and traffic is of the utmost importance for securing your environment. A key feature of Sophos Cloud Optix is real-time complete network topology and traffic visualization made possible through a continuous stream of network flow log data from AWS CloudTrail and AWS CloudWatch, including ingress, egress, and internal traffic, which enables the team to respond to and remediate security risks faster than ever before.

How does Sophos Cloud Optix ease compliance efforts?

Compliance needs to be continuous for cloud workloads, and with out of the box templates from Sophos Cloud Optix, the mundane work of extracting the infrastructure status and mapping to the compliance policies was significantly reduced. The control ID feature, which maps common control of the overarching compliance tool with the cloud infrastructure, is a great time savior.

“Our compliance team loves the ability to run reports for compliance audits in seconds,” Peck states.

With the rapid pace of new deployments and changes, how do you deal with configuration drift?

Shutterfly uses a software solution that allows DevOps to release new software or make configuration changes to cloud instances. In Shutterfly's environment, hundreds or thousands of changes could potentially occur on a daily or weekly basis.

Sophos Cloud Optix continuously monitors and detects drift in configuration standards and prevents changes to critical settings that could leave the organization exposed to security vulnerabilities. Team members can now sift through the changes and determine which ones were outside the norm and then take measures to remediate them.

About Sophos

As an AWS Security Competency-approved, AWS Level 1 Managed Security Service Provider and AWS Advanced Technology Partner, Sophos protects more than 100 million users from today's most advanced cyberthreats, helping to build secure and scalable cloud transformations with AWS.

Sophos unique approach fuses automated protection across endpoint, cloud workloads, and networks, with 24/7 managed threat response services to create a single cybersecurity package to secure data, proactively prevent vulnerabilities, and block advanced threats.

Learn more sophos.com/aws-mssp

SOPHOS
Cybersecurity evolved.