CUSTOMER STORY

Unlocking the Power of Real-Time Detection: Sprout Social's Partnership with Sysdig

Founded in 2010, Sprout Social is a leading social media management and optimization platform. They offer a suite of deep social listening and analytics, customer advocacy, customer care, influencer marketing, and comprehensive publishing and engagement tools. Integrated with all major social networks, the company helps its customers drive growth and cultivate deeper relationships.

Sprout Social is trusted by marketing teams across the globe, including Atlassian, Yamaha, and Procter & Gamble. Since its initial public offering in 2019, the company has continually evolved to stay ahead of the rapidly changing social media landscape.

sproutsocial

INDUSTRY

Software Technology

CHALLENGES

- Complex infrastructure required defense in depth
- Lack of real-time visibility into cloud workloads and containers
- Difficulty prioritizing and investigating incidents and threats

OUTCOMES

- Significant improvement in speed to detection
- Highly consolidated threat monitoring and vulnerability management toolkit
- Streamlined management of security alerts, events, and vulnerabilities

CHALLENGES

An Opportunity to Achieve More Visibility

For several years, Sprout Social partnered with the same managed security service provider (MSSP), which supported a wide range of use cases, including threat monitoring, vulnerability management, posture management, compliance, event prioritization, and host intrusion detection. However, that partnership came to an unexpected end in 2023 when the MSSP was acquired by another company, which decided to discontinue the product.

“Suddenly, we needed a platform to take over everything the MSSP used to handle,” said Brayden Santo, Senior Security Engineer at Sprout Social.

Facing a firm end-of-life date for their existing solution, Sprout Social began searching for an alternative that was more than just a direct replacement. Recognizing opportunities for improvement, they sought a platform capable of addressing persistent cloud security challenges while also bridging the gaps left by their MSSP.

Although Kubernetes had been part of Sprout Social’s infrastructure for some time, visibility into those environments was an area they wanted more focus on. A new solution posed an opportunity to find a tool that provided more visibility and insight into their expanding Kubernetes deployment.

Navigating Complexity and Seizing Opportunities to Consolidate

Sprout Social’s security team is organized into specialized units, with Santo and his colleague overseeing monitoring, including security operations and incident response. Additionally, the company has dedicated teams for application security, infrastructure engineering, and employee security. Describing their security infrastructure as complex would be an understatement.

“We have around 30 different use cases related to security and visibility, vulnerability management, configuration, and audit monitoring,” Santo said. “Previously, we were using five or six tools just for vulnerability and posture management. We realized that by finding the right platform, we could consolidate many of these use cases into a single solution.”

To achieve this, Sprout Social needed a platform capable of monitoring multiple containers, Amazon Web Services (AWS) instances, and cloud logs for vulnerabilities and threats. Additionally, the platform had to be flexible enough to integrate with their other security tools.

CHALLENGES

Too Many Alerts, Not Enough Time

Sprout Social's ecosystem generates hundreds of thousands of security events and alerts each week. This wasn't an issue with their previous MSSP, as the vendor's analysts handled most of the heavy lifting.

However, with the MSSP no longer in place, the responsibility for managing these alerts would soon fall entirely on the company's monitoring team.

"Our environment is extremely busy and equally noisy," Santo said. "We realized that if we handled notifications manually, we'd likely need at least two more full-time employees just to manage the volume."

Fulfilling Business-Critical SLAs

Alert fatigue wasn't the only challenge Sprout Social faced. Vulnerability management was also a concern. They needed a way to identify and remediate vulnerabilities in both production and preproduction environments, as streamlined as possible. Preventing critical vulnerabilities from entering production required a precise, error-free, and flexible solution.

"Our service-level agreement (SLA) mandates that we remediate high-severity vulnerabilities within seven days and address critical vulnerabilities as quickly as possible," Santo said. "We also need to generate reports on these vulnerabilities, not only to ensure security but also to avoid reputational damage and potential penalties for missing an SLA."

> "We have around 30 different use cases related to security and visibility, vulnerability management, configuration, and audit monitoring. Previously, we were using five or six tools just for vulnerability and posture management. We realized that by finding the right platform, we could consolidate many of these use cases into a single solution."
>
> **Brayden Santo**
> Senior Security Engineer, Sprout Social

SOLUTIONS

Detected in Seconds vs. Hours

Sprout Social narrowed their options to two solutions: **Sysdig** and one of its leading competitors. They ran a comprehensive proof-of-concept for each platform. By the end, the two were similar in many ways, with one exception.

"We ran atomic red team testing against our environments, and Sysdig detected and alerted us to the anomalies within seconds," Santo said. "The competitor, however, lagged behind by about an hour or two. That real-time response is what tipped the scale for us."

Convinced that they had found the ideal replacement for their MSSP, Sprout Social deployed Sysdig for **cloud workload protection** (CWP) and **cloud detection and response** (CDR).

> "We ran atomic red team testing against our environments, and Sysdig detected and alerted us to the anomalies within seconds. The competitor, however, lagged behind by about an hour or two. That real-time response is what tipped the scale for us."

Brayden Santo
Senior Security Engineer, Sprout Social

SOLUTIONS

Unifying a Complex Deployment

Given the complexity of Sprout Social's environment and infrastructure, the company expected a challenging implementation.

They managed over 900 nodes, comprising virtual machines and containerized hosts, all running on AWS. Monitoring AWS was critical, as it generated two distinct sets of logs – one for auditing and another for performance and availability.

With support from the Sysdig team, Sprout Social successfully deployed, implemented, and integrated Sysdig, despite the unique challenges of their implementation.

"The support we received from the Sysdig team throughout implementation has been incredible," Santo said. "And as we've progressed, having direct Slack access to our account manager feels like having him on our team. That kind of instant communication has been invaluable."

Santo worked side by side with Sprout's infrastructure teams to accomplish the initial deployment. Several teams worked together to configure security policies for various events and alerts across Sprout Social's environment and automate the deployment.

"Sysdig makes it incredibly easy to segment our monitoring and scanning layers," Santo said. "The platform delineates things clearly, so I can focus on specific areas like AWS or dive into containers or hosts. It's simple to compartmentalize and visualize exactly what I need."

> "In the past, a lot of communication just didn't happen. We now use Sysdig alongside Snyk, integrating the two—Snyk for image scanning and Sysdig for runtime security. This has brought us into closer collaboration with infrastructure engineers, software developers, and other various business units across the company."
>
> **Brayden Santo**
> Senior Security Engineer, Sprout Social

No More Noise

Sysdig has dramatically streamlined Sprout Social's management of security alerts, saving the company valuable time. Santo's team now operates with the efficiency of a team twice its size, with time and resource savings equivalent to adding two full-time analysts.

"Sysdig's ability to group events, assign policies, and manage alerts enables us to handle a massive workload with far fewer people than you'd expect," Santo said. "It's also helped us prioritize vulnerabilities more effectively. For example, the Sysdig interface allows us to focus on the 2% of the most important vulnerability signals, while reducing 98% of the noise."

Building a Secure Future Through Collaboration

When security tools are introduced into cloud environments, they often become siloed within specific teams or provide value only in limited areas. However, because Sysdig is purpose-built for the cloud, this hasn't been the case. Instead, the platform has enabled Sprout Social to enhance communication across multiple business units.

"In the past, a lot of communication just didn't happen," Santo explained. "We now use Sysdig alongside Snyk, integrating the two—Snyk for image scanning and Sysdig for runtime security. This has brought us into closer collaboration with infrastructure engineers, software developers, and other various business units across the company."

Beyond that, Sprout Social is already expanding its use of Sysdig, focusing on building out vulnerability management, compliance, and posture management.

"Sprout Social has always been focused on risk management — helping companies mitigate risks to their brands," Santo concluded. "That's why Sysdig is such a great fit for us. It helps us manage our own cybersecurity risks, so we can focus more on driving success for our clients."

To learn more about Sprout Social, visit **sproutsocial.com**.

sproutsocial

INDUSTRY

Software Technology

INFRASTRUCTURE

AWS

ORCHESTRATION

Amazon EKS

SOLUTION

Sysdig Secure

About Sysdig

In the cloud, every second counts. Attacks move at warp speed, and security teams must protect the business without slowing it down. Sysdig stops cloud attacks in real time, instantly detecting changes in risk with runtime insights and open source Falco. We correlate signals across cloud workloads, identities, and services to uncover hidden attack paths and prioritize real risk. From prevention to defense, Sysdig helps enterprises focus on what matters: innovation.

Sysdig. Secure Every Second.

To learn more about Sysdig, visit **sysdig.com.**

REQUEST DEMO →

CS-SPROUTSOCIAL
REV. A 12/24