



Salesloft Increases Its Security Visibility and Efficiency

Customer Problem

Salesloft is a leading sales engagement platform focused on helping B2B sales teams run more efficiently and close deals faster. With rapid growth over the past several years, the company has scaled up in size in terms of its employees and infrastructure. As a result, the cloud-native company has generated a large and complex cloud infrastructure environment that relies on workloads running in containers and Kubernetes.

The security team at Salesloft was created with a clear mission in mind—to protect the company’s systems and data against unauthorized use, disclosure, modification, damage, and loss. The team is given strict SLAs to meet each quarter, such as reducing the mean-time-to-resolve (MTTR) for vulnerabilities in order to keep systems secure. Historically they used a cloud security tool that focused on anomaly detection, which they realized did not provide complete visibility into their growing environment to keep their operations running efficiently. Therefore, in order to harden their security posture and keep pace with innovation, the team decided to upgrade support for their cloud security.

The Increased Cybersecurity Solution

To kick off this process, Salesloft’s Lead Security Engineer began looking for a tool that would help them better manage their complex environment and drive down the time and effort it took to achieve the outlined SLAs. The most critical items he was evaluating in a new cloud security vendor were increased visibility and better support. He was looking for a tool that provided a holistic view for everything going on in his cloud environment and gave his team increased visibility and management over the cloud security controls put in place.

Additionally, the team wanted a partner to support in managing their daily security operations. Given the scope of their goals, they were looking for a partner that could provide human expertise and monitoring for the environment, and provide context and remediation recommendations for high priority threats. To this point, they had not found the right combination of both advanced software and human expertise.



Founded

2011

Headquarters

Atlanta, GA

Industry

Sales Engagement

Employees

400+

With this, the Lead Security Engineer chose the F5® Distributed Cloud App Infrastructure Protection (AIP), formerly known as Threat Stack, solution to achieve their security operations goals.

“The [Distributed Cloud AIP] team has done a great job of digging in with us and giving us an understanding of more efficient ways to tune and act on priority alerts.”

Lead Security Engineer at Salesloft

Results

With Distributed Cloud AIP, the team is now able to meet and exceed its SLAs like MTTR thanks to increased visibility and efficiency in identifying potential vulnerabilities. Our combination of industry-leading rules for known threats and machine learning (ThreatML) for anomalies provides Salesloft with the data and context needed to quickly remediate threats to their cloud security. The increased visibility also helps the team efficiently investigate any assumptions they have about the security controls in place and adjust as needed. Distributed Cloud AIP's approach to aggregating alerts in a tiered system allows the team to stay organized and focused on the highest priority threats helping them to clearly prioritize and take action on what matters most to achieve their security goals.

The security team also takes advantage of Distributed Cloud AIP 24/7/365 managed security service to alleviate pressure from their team, helping them to focus on the biggest security priorities and drive greater business value for the organization. “The most important thing that [Distributed Cloud AIP] gives us is uninterrupted sleep. The team's human element means more confidence in understanding the threats to our environment, and that we can take the necessary action to remediate,” said the Lead Security Engineer. “The team has done a great job of digging in with us and giving us an understanding of more efficient ways to tune and act on priority alerts. We feel great about the effortless support this managed security service provides us.”

Distributed Cloud AIP has also enabled the security team to have a positive impact on the larger organization by opening up cross-functional communication. With increased visibility and a deeper understanding of the environment, the Salesloft security team has worked with engineering to raise security awareness and provide guidance on how to operate more securely without being intrusive to the daily engineering team's tasks and goals. Distributed Cloud AIP's visibility has also helped the team show Salesloft's leadership the value of investing in security and how it's helping to push the company's mission and values forward.

A Secure DevSecOps Future

The security team at Salesloft is looking to continue growing its partnership with Distributed Cloud AIP, working to learn more about how to strategically run their cloud security operations and secure its complex infrastructure. In the near future, the team also plans to leverage Distributed Cloud AIP's compliance capabilities to help pass audits for both SOC 2 and ISO 27001.

Threat Stack: Now Part of F5

Threat Stack is now F5 Distributed Cloud App Infrastructure Protection (AIP). If you'd like to learn more about this solution, the company's Security Operations Center (including Distributed Cloud AIP Managed Security Services and Distributed Cloud AIP Insights), and more, feel free to contact our cloud security and compliance experts.

Let our experts take your cloud security worries off your shoulders, so you can get down to business. To learn more or to schedule a demo, [visit our website](#) today.

