

Spencer Fane Establishes Firmwide SaaS Security and Risk Management Program

APPOMNI'S IMPACT



Fine-grained security insights for M365, ServiceNow, and Salesforce



Immediate visibility into policy violations and misconfigurations



Security administrators can prioritize changes and set up change meetings as needed



Improved understanding of security posture via exports of normalized logs from applications to their SIEM



I needed to get a better understanding of the overall attack surface, our portfolio of applications, and their configurations and data exposure risks."

Wai Sheng Cheng

Information Security and Risk Manager, Spencer Fane



SpencerFane®

INDUSTRY

Legal Services

EMPLOYEES

900+

HQ

Kansas City, MO

DEPLOYMENT

M365

Salesforce

ServiceNow

Webex

Smartsheet and Others

USE CASES

Configuration Management

SaaS Security Visibility

Manage Identities and Access

ABOUT CASTLE VENTURES

Spencer Fane is a law firm in the U.S. with offices in 26 cities around the country. The firm has over 900 total headcount, including more than 510 attorneys, and recently completed an acquisition of another law firm in Salt Lake City, UT. Spencer Fane is one of the highest-performing law firms nationally in workplace satisfaction, client satisfaction, diversity traction, and growth.

Wai Sheng Cheng serves as the Spencer Fane Information Security and Risk Manager, where he draws on his many years of experience as a security and IT professional in the financial services and healthcare industries. Wai Sheng has been at the firm for more than three years and currently leads a small internal security team.

The Challenge

Wai Sheng was tasked by Spencer Fane CIO, Allen Darrah, to build and manage the firm's security and risk management program. Many of the firm's clients are in highly regulated industries, including financial services, healthcare, and defense contractors, and information security is therefore a significant client requirement.

Spencer Fane handles sensitive data that is stored across its private cloud and SaaS applications.

Wai Sheng said that he "needed to get a better understanding of the overall attack surface, our portfolio of applications, and their configurations and data exposure risks."

In addition, the security team did not have sufficient identity and access management controls to know "who was doing what" in their applications. The firm uses a wide variety of operational and productivity-oriented SaaS applications from Salesforce to ServiceNow, M365, Monday.com, Webex, and Smartsheet. The distributed ownership and management of applications meant that the security team had very little input into configurations and controls. To get basic visibility into their environments, the team had to look at one application at a time, signing into each individual application to first identify configuration baselines and then suggest policy guidance to application owners. For example, Salesforce was onboarded by the marketing organization, the IT team owned ServiceNow, and the firm's partners used Smartsheets.

Wai Sheng said that "each of these application owners had varying security controls and some teams were more receptive than others to raise awareness about security issues and make changes."



There is always going to be some friction when it comes to security. But the important thing is to establish a shared commitment and understanding of security issues."

Wai Sheng Cheng

Information Security and Risk Manager,
Spencer Fane



Requirements

The Spencer Fane security team knew that they needed a better mechanism to both gain visibility into the SaaS attack surface and understand their policy baselines so that they could set up better risk management and governance practices. Wai Sheng's team established the following general, high-level requirements for their security products and solutions.

Each solution needed to:

- A single solution that secures their entire SaaS estate
- Have high availability at 99.999% uptime
- Provide the option to be deployed either on-premises or in the cloud
- Be easy to deploy, requiring one to two administrators and at most 30 minutes
- Have low overhead, requiring at most two administrators to manage
- Not be disruptive to critical systems and business processes
- Have rich and mature API for integrations
- Integrate with closed and open-source SIEM
- Have low to no noise for alerts and be easy to tune
- Auto-remediate critical and high risks
- Deliver responsive and timely U.S. support
- Provide metrics and reports
- Be compatible with both Linux and Windows OS
- Have optional AI capabilities



Our administrator was able to on-board the M365 application over lunch. ServiceNow took a couple of more hours to bring both the development and production environments under management. But we were up and running within a few hours."

Wai Sheng Cheng

Information Security and Risk Manager, Spencer Fane

Wai Sheng worked with the AppOmni team to set up a proof of concept (PoC) starting with M365 – without the Microsoft Teams Windows container – and ServiceNow. Wai Sheng and team found that AppOmni was not cost prohibitive and was easy to both set up and integrate with these initial applications. Wai Sheng summarized their experience by saying, "our administrator was able to on-board the M365 application over lunch. ServiceNow took a couple of more hours to bring both the development and production environments under management. But we were up and running within a few hours."

The PoC gave the security team immediate visibility to the application configurations. AppOmni gave the team a single, centralized system to review configurations so that they no longer needed to look at applications individually. Wai Sheng explained that "it was about the convenience of understanding our policy baselines. Is MFA even enabled in this application? What tweaks can we apply to make it more secure? The more I looked into it, the more I realized that there isn't a product like AppOmni out there."

The Results

The security team has since brought more applications under management with AppOmni. The security insights available for M365, ServiceNow, and Salesforce are fine-grained and help the team evaluate security issues thoroughly. In addition, the security administrators are now able to use AppOmni Findings to prioritize changes and set up change meetings as necessary to raise awareness with the application owners. AppOmni replaced time-consuming processes that could take many days with a quick summary of policy violations and misconfigurations. Wai Sheng said, "I have attended more change control meetings since I brought in AppOmni, but that's a good thing because it has helped us become more mindful of security controls needed to meet client requirements and remediate issues faster."

The visibility with AppOmni has been a big win for Spencer Fane. The security team is also able to export normalized logs from the applications to their SIEM to review metrics, access patterns, and gain a better understanding of their security posture. The team sees value in AppOmni's ability to surface third-party SaaS-to-SaaS connections into their managed SaaS environment and expects to use the capability as part of their risk management and governance processes.

Next Steps

Now that they've completed the heavy lift, the Spencer Fane security team is self-sufficient in managing their SaaS environment and plans to bring more applications under control with AppOmni. They continue to take the steps necessary for compliance and provide risk mitigation at an acceptable level to the firm's partners and clients.

Asked about his advice to other cloud security professionals in the industry, Wai Sheng cautions that security professionals should know their attack surface thoroughly and not be constrained by tunnel vision, which can all too easily prevent teams from seeing the full picture. He explained, "There is always going to be some friction when it comes to security. But the important thing is to establish a shared commitment and understanding of security issues. Rather than trying to force these requirements on people, I take the approach of surfacing issues, making suggestions, asking questions to validate configurations and policies, and make the necessary adjustments."



I have attended more change control meetings since I brought in AppOmni, but that's a good thing because it has helped us become more mindful of security controls needed to meet client requirements and remediate issues faster."

Wai Sheng Cheng

Information Security and Risk Manager,
Spencer Fane

About AppOmni

AppOmni, the leader in SaaS Security, helps customers achieve secure productivity with their applications. Security teams and owners can quickly detect and mitigate threats using unmatched depth of protection, continuous monitoring, and comprehensive visibility. Trusted by 4 of the Fortune 10, AppOmni specializes in securing diverse SaaS environments. For more information, please visit <https://appomni.com>.