AppOmni

CUSTOMER CASE STUDY

Enhancing Visibility & Strengthening SaaS Security: How DLA Piper Leverages AppOmni

DLA PIPER

INDUSTRY
Legal

EMPLOYEES
+4,500

HQ
London, United Kingdom

DEPLOYMENT
ServiceNow
Salesforce
Microsoft 365
iManage

USE CASES
SaaS security visibility
Improve security posture
Ongoing monitoring

ABOUT DLA PIPER

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa, and Asia Pacific. The firm serves corporate clients through a broad range of practices divided into about 15 key groups; specialties include mergers and acquisitions, data, privacy and cybersecurity, franchise, intellectual property, regulatory and government affairs, and technology and commercial.

Matt Finn has over 20 years of experience in senior level IT leadership and Information Security. He is experienced at building high-performing security teams, with a strong reputation for developing and delivering transformation and cyber protection strategy.

APPOMNI'S IMPACT

Enhanced security posture through **improved visibility** into SaaS configurations and compliance gaps

Faster remediation enabled by **automated monitoring** and **prioritised issue resolution**

Stronger collaboration between security, IT, and business teams via **centralised SaaS risk insights**

Operational efficiency gains with a single platform for **proactive SaaS security management**

> AppOmni has allowed us to be more proactive in addressing security challenges. By providing complete visibility into our SaaS environment and automating critical processes, it's another tool in our security armory to automate and orchestrate our response capabilities.

Matt Finn
Information Security Director, DLA Piper

appomni.com

The Challenge

DLA Piper faced challenges in safeguarding sensitive client data as it migrated key operations to Software-as-a-Service (SaaS) platforms. The transition introduced complexities in managing security under a shared responsibility model, compared to traditional on-premise systems. With SaaS, the responsibility shifted, Matt Finn, Information Security Director at DLA Piper, said. In the shared responsibility model of SaaS, companies are accountable for their data, while vendors handle hosting. Companies must understand security, assess risks, and implement measures for visibility and issue management, Finn said.

"When we were on-prem, everything was visible—Patch Tuesday would come around, and you'd know what needed addressing," Finn explained. "Now with SaaS, things have completely changed. The onus is on the SaaS vendors to go public about vulnerabilities that they have."

As the firm accelerated its adoption of cloud-based technologies, SaaS applications became integral to its operations—powering everything from communication to document management. However, this shift introduced a critical challenge DLA Piper hadn't encountered before: ensuring the security of sensitive client data in a complex SaaS environment.

DLA Piper initially relied on service owners and platform-specific tools to manage security, but that strategy proved unsustainable. With so many configurations and data points to manage, the risk of something slipping through the cracks was too high, Finn added.

"We relied on service owners and the built-in capabilities within the systems themselves, but that doesn't scale well," Finn said. "We needed to gain visibility into our SaaS footprint to provide ongoing monitoring capabilities. We needed visibility in one place."

> “We needed to gain visibility into our SaaS footprint to provide ongoing monitoring capabilities. We needed visibility in one place.
>
> **Matt Finn**
> Information Security Director, DLA Piper

Requirements

Finn identified the need for a solution to centralise DLA Piper's SaaS security, enhance visibility, and address vulnerabilities to uphold client trust and the firm's stringent security standards. DLA Piper sought a vendor that offers the following requirements:

- ✓ Easy to use and easy to deploy
- ✓ Automated testing capability
- ✓ Third-party integration oversight
- ✓ Centralised visibility
- ✓ Risk-based reporting and prioritisation
- ✓ Configuration management
- ✓ Compliance and access controls of high-level users
- ✓ Scalability

> “We identified misconfiguration issues almost immediately when we onboarded AppOmni and those SaaS applications. The increased visibility helps us build closer working relationships with the various teams who are leveraging SaaS to deliver their business services.
>
> **Matt Finn**
> Information Security Director, DLA Piper

The Results

Since adopting AppOmni, DLA Piper has vastly improved its SaaS security. During the proof of concept, AppOmni identified security gaps in ServiceNow with over 100 policy issues—leading to immediate improvements, especially in Identity and Access Management (IAM) through enforcement of MFA (multi-factor authentication) requirements.

“We identified misconfiguration issues almost immediately when we onboarded AppOmni and those SaaS applications,” Finn said. The platform’s insights also strengthened cross-departmental collaboration and improved alignment between security, IT, and business units. “The increased visibility helps us build closer working relationships with the various teams who are leveraging SaaS to deliver their business services,” Finn added.

By reducing alert fatigue and manual checks, AppOmni enabled DLA Piper’s security team to focus on strategic priorities. “AppOmni helps the team focus more on strategic initiatives rather than being bogged down by constant alert fatigue or manual and ad hoc security checks,” Finn noted.

This shift has enabled DLA Piper to adopt a more forward-thinking security approach, reducing vulnerabilities, and improving its ability to prioritise critical issues.

“We’ve seen a reduction in the number of misconfigurations across our SaaS platforms thanks to AppOmni’s risk reporting and configuration management,” Finn said. “AppOmni has allowed us to be more proactive in addressing security challenges. It’s another tool in the armory to automate and orchestrate our response capabilities.”

Next Steps

As DLA Piper looks ahead, its collaboration with AppOmni marks a critical milestone in the firm’s SaaS security journey. With a strong foundation in place, DLA Piper is exploring the integration of its SAP-based finance and HR platforms. These systems, combined with those already onboarded, represent what Finn referred to as the firm’s “crown jewels” and will further enhance DLA Piper’s ability to safeguard its most sensitive data. Expanding AppOmni’s coverage to these platforms is a priority for the next year, ensuring comprehensive protection across its SaaS environment.

Looking to the future, Finn reaffirmed the importance of staying vigilant in managing SaaS security. “It’s important to understand that at the end of the day, you are still accountable for your data within that SaaS service,” Finn said.

As DLA Piper continues to expand its SaaS footprint, its partnership with AppOmni remains central to ensuring a robust security posture and addressing emerging challenges in the evolving landscape of cloud security.

“If you’re a big consumer of SaaS applications or systems, as most organisations are, I highly recommend AppOmni because it will help provide both visibility into your SaaS environment and improve your security posture,” Finn said. “The team at AppOmni has been great to work with, always available to work through issues to ensure momentum wasn’t lost.”

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 5 of the Fortune 10, AppOmni specializes in securing diverse SaaS environments.For more information, please visit https://appomni.com.