

noname

Aflac

Headquartered in Columbus, Georgia, Aflac is the leading provider of supplemental health insurance in the United States. For more than 65 years, Aflac has provided insurance products for individuals, families and businesses, and now services more than 50 million people worldwide. With such a large global footprint, the company is steadfast in evaluating and investing in the most robust cybersecurity solutions in order to keep sensitive customer data secure.

The company is well aware that cybercriminals have become increasingly sophisticated with Application Programming Interfaces (APIs) quickly becoming the attack vector of choice. APIs increase the attack surface and can make it much easier for hackers to gain unauthorized access to company networks and siphon off sensitive data from customer accounts without being detected. To mitigate the risk of this type of data breach, Aflac turned to Noname Security to fortify their cloud and on-premises environments.

“Noname is a visionary company, fundamentally reshaping how companies approach API security. They are continuing to innovate and solve new security challenges at a remarkable pace. They continually deliver because they listen to their customers and are invested in their success”



DJ Goldsworthy

Vice president, Security Operations and Threat Management, Aflac

Lack of visibility was a top concern at Aflac

Financial services organizations have been tasked with innovating at an accelerated pace as consumers move away from brick and mortar experiences in favor of digital interactions. This has also become the reality for Aflac. However, meeting their digital transformation goals required Aflac to pursue a distributed versus centralized approach to deploying new applications. While it has been beneficial from a resource management perspective, it added complexity to an already challenging asset management scenario.

In addition, the company was also heavily reliant on their existing API gateways to provide visibility into their API estate. This too was a notable issue for leadership. Despite being components of the API delivery stack, API gateways are not designed to provide the security controls and observability required to adequately protect APIs. Additionally, APIs that were implemented outside of a gateway presented even more visibility and security challenges.

“We were aware that our API footprint was large, and we wanted to be completely confident that we had every API accounted for, that we had full visibility into their operation and that they were being continuously tested for security risks. This was essential to our strategy to address the risk of exploit amid the backdrop of an expanding technology footprint,” said Goldsworthy.

Protecting their customers and their legacy

Beyond getting a complete picture of their API estate, Aflac also knew that they needed to be able to defend their APIs against attack. Considering their ironclad reputation and global reach, the company was well aware that they could become a target. They required a holistic API security solution that would not only give them visibility, but an ability to remediate vulnerabilities and attacks to avoid becoming another headline.

“Noname was the most advanced and complete API security solution that we tested, going above and beyond our initial requirements. Not only does Noname have the technology to address our current needs, I was also pleased with what I saw on their roadmap to address emerging security challenges,” Goldsworthy added.

Aflac chooses a market leader

After evaluating the Noname API Security Platform, Aflac decided it was the most comprehensive solution to protect their APIs - many of which reside in their AWS environment. Noname Security will provide both API discovery and API runtime protection. This means the company will have full visibility into every type of API they have, including HTTP, RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC, and gRPC.

The API discovery module, Noname Posture Management, will also provide insight into the types of data that traverse the company's APIs. This provides Aflac with visibility into which of their APIs are able to access sensitive data and identify any anomalies in data access.

This also means the company will have real-time protection to thwart any API attacks. Noname Runtime Protection uses automated AI and machine learning detection to conduct real-time traffic analysis and provide contextual insights into data leakage, data tampering, data policy violations, suspicious behavior and API security attacks.

The Noname API Security Platform runs out of band, leveraging VPC traffic mirroring to copy API traffic from AWS Application Load Balancers in Aflac's environment. This approach enables monitoring without any impact to performance. The data is then forwarded to Noname remote engines deployed on EC2 instances for further analysis. The platform also retrieves information from Aflac's API gateways by sending execution logs and access logs to Amazon Cloudwatch. The breadth of integrations Noname provides across the AWS ecosystem provide Aflac the support they need to confidently address their data security obligations.

How Aflac plans to grow with Noname Security

Aflac is already scoping out how it plans to expand its API security coverage globally, notably in Japan. Asia is a burgeoning market for the company, and they want to ensure that their customers in emerging markets have the same level of security. This will not only continue to differentiate them in the marketplace but also fortify their reputation as a customer-first organization.

The company is also implementing the Noname Security Active Testing solution, which empowers organizations to identify vulnerabilities during development and address them before they reach production. True to the shift left approach, Noname Active Testing provides a suite of API-focused security tests that security operations can run on-demand or as part of a Continuous Integration/Continuous Delivery (CI/CD) pipeline to ensure that APIs are implemented securely. Aflac sees Active Testing as a strategic benefit that will allow them to improve testing and augment their existing application security testing tools with a purpose-built API security testing solution.

“Aflac is excited to have a true market leader securing our API estate. We are confident in the Noname Security platform, their team and their vision. With so much value already recognized and given their impressive ability to innovate, we are excited about what the future of our partnership with Noname Security will offer,” concluded Goldsworthy.

About Noname Security

Noname Security is the only company taking a complete, proactive approach to API Security. Noname works with 20% of the Fortune 500 and covers the entire API security scope across four pillars — Discovery, Posture Management, Runtime Security, and API Security Testing. Noname Security is privately held, remote-first with headquarters in Silicon Valley, California, and offices in London.

