NONAME SECURITY

Securing government data by protecting APIs

Stronger visibility and security controls for APIs can boost the government's efforts to protect sensitive data

Doug Steele | Noname Security

To promote innovation and facilitate faster, more effective decision-making, federal agencies are migrating mission-critical applications to the cloud. Application programming interfaces (APIs) are essential in driving these digital transformations, yet many organizations are not aware of the imminent security risks of an ever-growing API ecosystem.

Organizations are adopting APIs faster than they can secure them. Threat actors are keenly aware of this under-defended attack surface and are exploiting it to steal, disrupt or destroy valuable and sensitive data. Recent API security breaches at Optus, Twitter and Zendesk illustrate the devastating and far-reaching impact on revenue, reputation and operations.

Unprecedented visibility and the power of machine learning

To combat this growing threat, organizations need complete visibility into their API estate and a true "shift left" approach during development to ensure their APIs are built with security in mind.

Many organizations fail to secure their API environment beyond a web application firewall or API gateway. Although these tools are important, they are insufficient in defending against many common vulnerabilities, including those listed in the Open Web Application Security Project's Top 10 API Security Risks.

Using the power of machine learning, Noname Security helps organizations secure APIs by offering unprecedented visibility into their API estates and applying configuration and compliance best practices based on how the organization uses APIs.

4 key pillars of API security

Noname Security's approach to API security and efficiency consists of four key pillars.

1. The platform detects all the APIs on premises and in the cloud, which is often an eye-opening experience for federal customers who lack visibility into the "shadow" or "zombie" APIs running in their environments.

2. We help agencies determine whether those APIs have been configured according to industry standards and highlight any risks in those configurations. Then we provide detailed documentation so the agency can continue to monitor its APIs.

3. We analyze traffic running across the agency's network and look for behavioral anomalies. For example, an API that accesses datasets it's never accessed before or increases its frequency signifies anomalous behavior that should be investigated. Using machine learning to build a baseline of the agency's API fabric, our technology can alert organizations to any potential concerns.

4. Our platform includes a tool that helps teams secure their APIs as they're moving through the development pipeline by conducting vulnerability testing in a controlled environment.

From migrating applications to the cloud to creating innovative digital services for citizens, Noname Security's robust integrations with many commonly used security tools make it easy for agencies to secure the APIs that are essential for achieving their goals. ■

Doug Steele is vice president of federal sales at Noname Security.