noname

Financial Services

The financial services industry is rapidly embracing digital transformation in order to stay competitive in an ever-evolving market. By leveraging digital tools like artificial intelligence and big data analytics, financial institutions are able to offer innovative products, reduce costs, and provide more personalized and efficient services to their customers.

At the same time, digital transformation brings with it an increased risk of cyber attacks. To combat this growing issue, cybersecurity is now an essential part of any digital transformation strategy. Financial services firms must ensure that their systems are secure and resilient in order to protect their customers' data and assets from malicious actors.

With that said, one of Asia's prominent commercial banks quickly sought out Noname Security to help fortify their API security posture. API breaches have reached alarming rates, as Tech Wire Asia points out that "today, as many as 1 in every 13 cyber incidents can be attributed to API insecurity." They also stress that, "API vulnerabilities cost businesses up to US$75 billion annually."

Considering our customer has over $700B in total assets, 5,000+ corporate customers, and a world-renowned wealth management reputation, it was imperative that all API vulnerabilities be addressed as soon as possible.

Problems

The institution had already deployed an API management platform for authentication and traffic control, but there were still doubts about preventing API abuse and cyber attacks. Though API gateways provide much needed basic API security controls, they unfortunately are not enough to adequately protect organizations from API-specific threats.

For example, Broken Object Level Authorization attacks, often referred to as BOLA, appear as normal API traffic to gateways. This lack of contextual awareness between API requests and responses enables BOLA attacks to pass through undetected and access critical backend services. Not only can this flaw leave them vulnerable to BOLA exploits, they can also fall victim to other attacks and business logic abuse.

Another visibility limitation involves maintaining an accurate API inventory. As with most large organizations, the bank was struggling with unknown APIs in their environment. The reality is, enterprises manage thousands of APIs, many of which are not routed through a proxy such as an API gateway. These are referred to as rogue or zombie APIs. These APIs were likely deployed by former employees or before the organization got serious about API security. Regardless of the reason, since their API gateway couldn’t see them, it became easy to underestimate just how many APIs they had.

Solutions

The complete Noname API Security Platform with Posture Management, Runtime Protection, and Active Testing deployed across their environment. Almost overnight the customer's security posture improved exponentially as they are now able to detect and remediate vulnerabilities for one the world's most obscure threat vectors.

Now all unknown APIs are able to be discovered and revealed within the platform, enabling complete visibility and risk mitigation. The institution has dramatically reduced its API sprawl and improved compliance, as the Noname platform classifies sensitive data for help with satisfying regulations like GDPR, HIPAA, and more.

They also now have the ability to stop attacks in real-time and protect customer data assets. Noname Security Runtime Protection intelligently detects and prioritizes potential threats while continuously monitoring API activity. By integrating with WAFs, API gateways, SIEMs, ITSMs, and other workflow tools, our platform enables threat remediation manually, partially automatically, or automatically.

Results

APIs have quickly become a preferred attack vector for hackers with no signs of slowing down. As evidence, according to Akamai we saw “a 257% growth in web application and API attacks on financial service institutions year-over-year” in 2022. To avoid becoming a statistic and defend against this trend, the customer will be well equipped thanks to the Noname API Security Platform. Particularly, the customers' security teams will have a better understanding of the dangers APIs present, and be able to create even more secure systems.

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.

nonamesecurity.com | info@nonamesecurity.com | +1 (415) 993-7371