nononame

Pharmaceutical Industry

Healthcare providers, insurers, and pharmaceutical companies alike have been transitioning to digital business models over the last decade. However, this transition has accelerated rapidly over the last few years as the pandemic drove the masses to consume more services digitally. At the root of this evolution lies Application Programming Interfaces, or more commonly known as APIs. By allowing healthcare organizations to share data via APIs, we've been able to usher in a new era of medical innovation that creates tailored patient experiences.

Some of the more popular healthcare related APIs involve continuous monitoring, clinical trial data, illness tracking, prescription pricing, and patient access, to name a few. These services are swiftly becoming more widely adopted with no signs of slowing down. According to Deloitte, "more than 80% of biopharma executives surveyed agreed that digitalization of operations will likely continue even after the pandemic ends."

Though this exponential growth of APIs is projected to do wonders for the patient experience, the risk landscape is rapidly evolving. And while cyber risk is not new to the healthcare industry, it has taken on a new dimension.

Most notably, Gartner predicted API attacks would become the most-frequent attack vector by 2022. And despite investments in perimeter, network, and application security, without the proper API security, healthcare providers put patient and financial data at risk.

The first step to securing your APIs is knowing how many you have. Which is exactly why a Global 500 pharmaceutical company sought to partner with Noname Security.

You Can’t Protect What You Can’t See

Few businesses have a good handle on their API or application inventory. This information helps application security teams identify high-priority security risks. Without an accurate API inventory with context-based threat details, it is impossible to know where to effectively apply security efforts.

Our customer had inadequate visibility into their API environment and grossly underestimated just how many APIs they had. The general consensus internally was about 50 APIs. Much to their surprise, the actual number was over 10x what they originally anticipated.

Discovering the Unknown with Noname Security

The Noname API Security Platform provides granular API inventory, behavioral analysis, real-time attack detection, and vulnerability management. It allows users to discover and catalog data type classifications for all APIs. You can find and inventory every type of API, including HTTP, RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC, and gRPC. As well as identify legacy and rogue APIs not managed by an API gateway.

With the Noname platform, our customer found over 500 previously unknown APIs. Once identified, they were able to ensure these APIs were adequately inventoried, secured, or decommissioned. This new level of visibility allows the organization to dramatically improve their API security posture and address the increased scrutiny in compliance and regulatory adherence. They now have more control over how well their business and personal information is protected when dealing with vendors, hospitals, doctors, and 3rd party medical services.

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