insight.tech POWERING IoT AND EMBEDDED INNOVATION

API Security Fills Critical Gap in Cyber Protection

Anytime you digitally access your bank account, make an online purchase, or log into a cloud application, you're using an application programming interface (API). Acting as gateways among applications, APIs are the glue of digital connections. Yet they remain poorly understood, and too often unsecure.

Organizations rely on hundreds, even thousands, of APIs, but CISOs, CIOs, and CTOs often lack an accurate inventory. This explains why APIs have become a common cyberattack vector. Problems involving APIs include poor authentication practices, misconfigurations, and lack of monitoring.

API security is a huge challenge and, to a large extent, a consequence of how cybersecurity solutions are applied. Most solutions take a "horse blinders" approach, securing specific parts of the computing environment, such as endpoints, servers, and cloud applications, says Ryan B., Technical Director, Strategic Alliances at Noname, an API security company. "They're only going to see what's in their track and in front of their eyeballs."

The result: a yawning security gap in IT environments that affects a company's internal assets as well as its connections to ever-growing stacks of cloud-based and Software-as-a-Service (SaaS) applications. Noname fills that gap, using AI and ML algorithms to analyze traffic, and identify and block malicious behavior wherever assets reside—in the cloud, on-premises, or a combination of both. "We're purpose-built for the API problem," says Ryan.

Noname approaches the API challenge from the perspective of the enterprise, rather than that of the security vendor or the cloud provider, taking a panoramic view of the entire environment to secure all APIs.

"We find that many solutions out there do not identify malicious activity pertaining to APIs," says Peter Cutler, Vice President, Global Strategic Alliances at Noname. "By the time they find them it's too late. That's why Noname integrates out-of-the-box with cybersecurity solutions such as SIEM (security information and event management) and endpoint protection."

Uncovering API Vulnerabilities with AI and ML

The most common API vulnerabilities, according to OWASP, an open-source foundation for application security, include:

- "Broken object level authentication," which lets a user access data based on the user's role without verifying if the person is authorized to access the data
- "Broken authentication," which occurs when attackers compromise credentials such as passwords, session tokens, and user account information
- "Broken object property level authentication," which involves one user accessing another's data

Malicious bots are often behind the attacks. Humans trying to counter the actions of bots can't compete with their speed and capacity, hence the need for AI and ML.

"This is a superhuman problem to solve. All the people you've hired, all the technologies you've purchased—you thought they were the right solution to the job. You purchased firewalls, hired security consultants, ran some penetration testing. Guess what? It wasn't good enough," says Ryan B.

Noname fights bots with bots. In the first week of implementation at a customer's environment, the Noname

API Security Platform is in learn mode, observing the patterns of traffic moving among applications that use APIs. The platform memorizes API specs, requests, and response schemas, and looks at parameters of communications involving confidential information such as payment card data.

Starting in the second week, the security platform uses this baseline knowledge acquired in the first week to identify activities that stray from normal patterns. AI then determines if the anomalies are malicious. Suspicious activity is flagged and blocked. Noname applies a confidence score to the process. It's based on at least 80% machine learning derived certainty that a specific action is malicious and can be traced to attackers and their known locations, Ryan B. says.

To keep IT defenses up to date, Noname uses Active Testing, a technology that simulates cyberattacks. Whenever customers make changes to their environment, this runtime testing checks if a new software version, endpoint, or other component is properly protected. This prevents introducing new vulnerabilities into the environment.

Without active testing, Cutler says, organizations launch new production APIs "with their fingers crossed that the API gateway or web application firewall (WAF), and other security layers, will identify and protect them. That is very risky and certainly not a good strategy."

API Security Awareness Requires Performant Compute

ML and AI, of course, will continue to play a central role in API security. ML and AI require lots of processing power as traffic volumes grow. "We start out with eight CPUs for about 3,000 messages per second. Our machine learning engine then is hungry for more CPUs as API traffic scales to 7,000; 10,000; 20,000 messages per second," says Ryan B.

Noname works closely with Intel to take advantage of the performance required to run AI and ML. The company benchmarks the 5th Gen Intel® Xeon® processor to benefit from significant performance gains. Work also is underway to leverage Intel embedded encryption to prevent malicious actors from compromising the Noname technology.

As Noname looks into the future, the company wants APIs to be better understood. This requires education, something the company delivers as part of its mission.

"What I see, moving forward into 2024, is people are going to take security even more seriously. They're going to buy the right tool for the job and secure their systems in a way that they haven't even tried to before by leveraging these innovations," Ryan B. says.