With Great APIs comes Great Responsibility

BLOG IN **PRODUCT UPDATES**

BY **SYDNEY COFFARO**

Evolution of API Development

Enterprises continuously adopt new development methods, techniques and tech stacks to keep pace with evolving technology. We've seen this happen time and time again with the shift from hard drives and floppy disks to solid-state drives, from on-prem hosting to cloud, and now there's a parallel shift underway, from monolithic web apps to API-based web development. There's no doubt that APIs are changing the game for how modern web applications use, store, and transmit data. The change makes it easier on developers–they can build and deploy complex business apps faster than ever. However, this shift also makes web applications the #1 target for data breaches.

What does this mean for organizations?

A commonly used phrase in cyber security is, "you don't know what you don't know ". Unfortunately, for most organizations that blind spot extends to their API attack surface. With the use of APIs on the rise, organizations struggle to manage their layer-7 exposure; that's why API Protection and Discovery is so important. Without proper protection and management, organizations rely on their WAF/WAAP solution for protection, and their vendor choice could mean the difference between winning and losing a battle against Botnet attacks, DDoS, an attacker exploiting a vulnerable endpoint, and many more attack methods.

The Security Paradigm Shift

As Stan Lee once wrote, with great power comes great responsibility. APIs are powerful as a design pattern and as a development tool.

The same concept applies to application security: With great power comes great responsibility.

The power of APIs should not be overlooked or underestimated; attackers know it only takes one deprecated or misconfigured endpoint to gain access to PII, PCI, and many other forms for sensitive information that's used in cybercrime every day.

guys. ThreatX takes a Protection-First approach to API Security starting with our API Threat Assessment capabilities to block attackers from exploiting your production, rogue, and zombie endpoints. But that's only the beginning. ThreatX brings together API Protection with API Discovery by providing visibility into your environment's real-time traffic to understand production API's health, or to discover an endpoint that slipped through the cracks of your organization's CI/CD pipeline.

Security engineers unite, it's time to assemble against the forces of the modern threat landscape. Learn more about how ThreatX can help your organization discover and protect your modern web applications here on our site or by scheduling a demo.

Tags

APIS

About the Author

Sydney Coffaro
Experienced subject-matter expert focused in Cyber Security Automation, Incident Response, APIs, and Application Security with a demonstrated history of working in fast-passed early stage startups. Sydney is a certified Product Manager, Scrum Master, and has led technical sales initiatives for go to customer teams that resulted in the acquisition of hundreds of customers.

Ready to get started?

REQUEST A DEMO

SRC CYBER SOLUTIONS LLP THREATX REQUEST A DEMO

Contact Us
www.srccybersolutions.com
+91 120 232 0960 / 1
sales@srccybersolutions.com

Newsletter Sign Up →

Terms & Conditions

Privacy Policy

Data & Security Compliance

ThreatX Status