L7 DEFENSE

Closing the API Gap

Exposing APIs creates a new, attractive path for hackers!

What if you can automate your API security, never writing even a single rule?

APIs exponentially expand the attack surface of the enterprise

Gartner: **“By 2022, API abuses will be the most-frequent attack vector resulting in data breaches for enterprise applications.”**

Nine out of ten top vulnerabilities in the current OWASP report apply to APIs. Denials of service and Botnets attacks can be directed at APIs through websites, apps and related interfaces.

In addition to the OWASP10 vulnerabilities, APIs present a set of new vulnerabilities, not handled by current tools.

APIs require a new security paradigm

Authentication and rate limiting are todays core API security features, ensuring resources are securely accessible by internal groups, partners, and third-parties, but credentials aren’t sufficient to protect APIs – attackers with compromised credentials look exactly like valid clients.

Identifying suspicious activity amidst a sea of API traffic is a big data problem. Attempting to Identify a single malicious transaction amongst tens of thousands of APIs calls is futile.

Can the enterprise protect what is being opened up?
Can it trust what’s coming in?
Can it control what’s going out?

Ammune™ is a Revolutionary AI-Based Solution for API Security

Ammune™ API security platform is an INLINE advanced machine learning solution that protects APIs from the most advanced attack types, hunting down "zero day" attacks with no impact on traffic. Ammune™ API security platform discovers and defends each API automatically. It iteratively builds negative and positive profiles of each API, that spot and stop emerging threats that otherwise go unnoticed. Ammune™ works automatically, without prior knowledge or signatures, detecting and fighting back against attacks in real time.

Detect and Respond - inline security

Traditional signatures, rules and policy-based security tools trigger on a large variety of benign threat indicators. With their limited resources, security analysts can review less than 4% of the alerts, frequently allowing attackers to slip in unnoticed.

Ammune™ is based on a disruptive, accurate threat detection technology with close to zero (<0.001%) false positive alerts, in inline as well as out-of-band modes. Ammune™ not only detects threats, but also actively responds and blocks them. This improves security and reduces the operational overhead of processing a high volume of mostly benign alerts.

Ammune™ Advantages

- **Accurate** – extremely low false positives / negatives rate
- **Automatic monitoring** – auto-discovers every API and continuously monitors it and adapts its baselines
- **Adaptive** - requires no rules, settings or signatures, continuous self-learning mode
- **Zero Trust** - all request are suspicious. No user is trusted, regardless of authentication and authorization checks
- **Elastic** - scales elastically for hi-volume attacks
- **Ease of deployment** - Plug & Play solution, with immediate time to value

L7 DEFENSE

Contact us for more information: Info@L7Defense.com