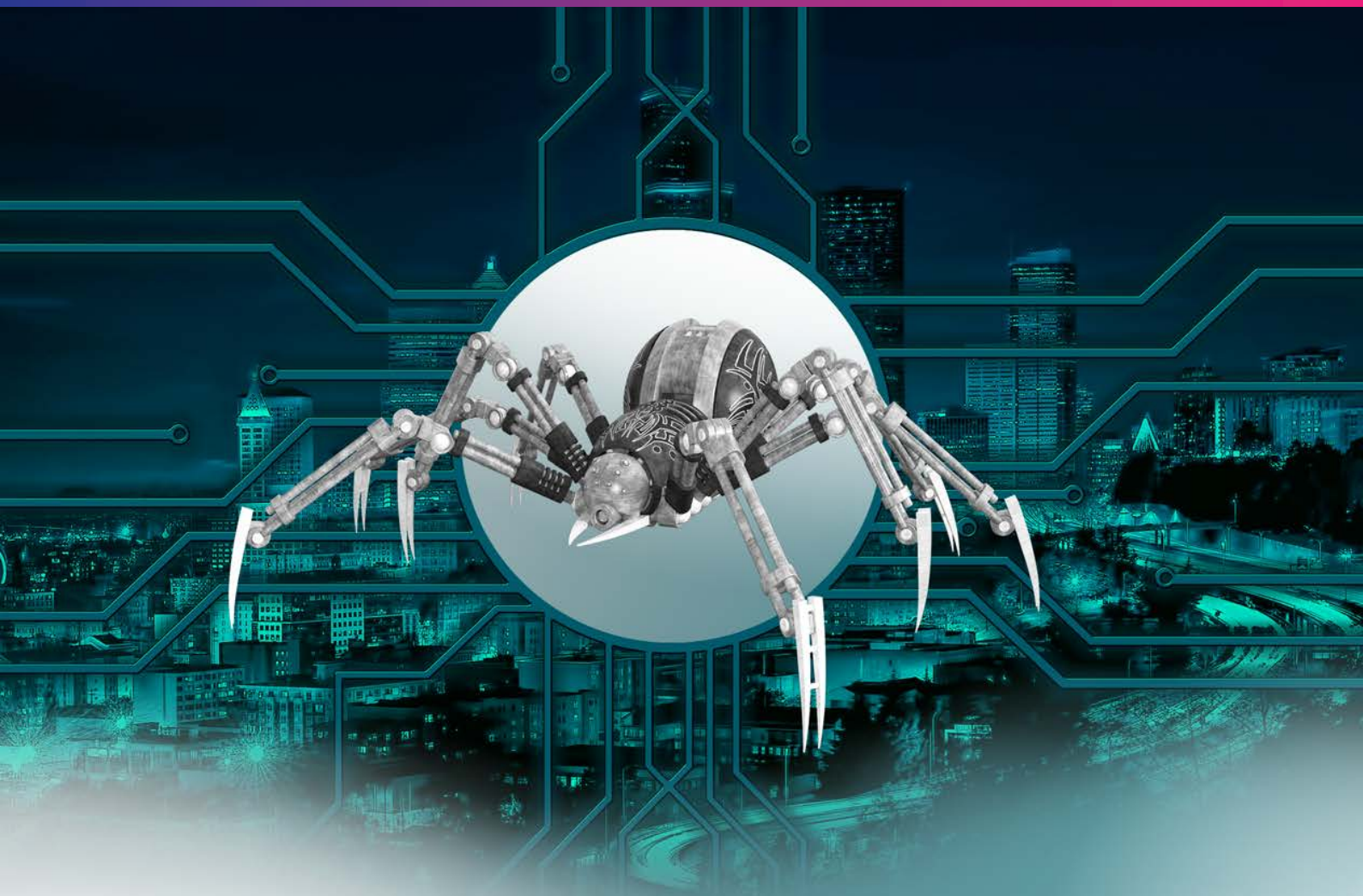
APIs Drive Innovation - How Can You Protect Your Organization?

AI-based API Protection - Intruduction



L7 DEFENSE

Empowering API Security

Introduction:
The Modern API Landscape and its Security Challenges

How often do you think about your corporate APIs, those little bits of code that allow applications to talk to each other and with users seamlessly? You're probably aware of how critical they are to productivity, innovation and agility—but are you aware that their exposed nature also creates high security risks?

This white paper will explore the modern API landscape and the security challenges that have developed as a result.

APIs present businesses with massive opportunities for growth and innovation. But at the same time, they create a myriad of security issues. These are threats that can impact your customers'—as well as your own—reputation.

This new breed of threats calls for disruptive solutions that allow developers to move fast while building in security by design. Similar to living organisms composed of countless systems, wherein each system requires specific defenses – an immune system - to remain immune to threats, the ideal solution addresses APIs as a whole, while securing each one individually tailored to its profile. Continuous machine learning makes such an approach possible, enabling developers and security teams to defend their APIs in an entirely novel way.

The API Economy

Application Programming Interfaces (APIs) have been used in software development since the 1960s, as a way for applications to communicate. APIs are the protocols and definitions that send requests and deliver results between independent websites, apps, users and machines. Similar to how a doorway leads directly into another room, APIs lead directly into another application. The user can take advantage of the functionality of what lies on the other side of the doorway, without ever leaving his or her original position (e.g., website of origin).

Today, businesses need to prove their relevance in an increasingly connected and competitive digital landscape. APIs have become a key strategic business enabler as they allow developers to create new services and richer user experiences. Using APIs, it's simple to share data and digital assets, ending siloed services and expanding innovation.

"APIs allow businesses to monetize data, forge profitable partnerships, and open new pathways for innovation and growth." McKinsey.com

A dramatic shift has taken hold in the last few years as APIs have become even more important. They are now the primary interconnection mechanism to and from systems and applications. Thanks to the move to mobile platforms, the Digital Transformation and some well-timed directives such as the Second Payment Services Directive (PSD2) and Open Banking, as well as imminent directives in other industries such as healthcare, government, transportation, etc., APIs—and the agility, flexibility, and interconnection they enable—are more critical than ever.

Today, APIs are everywhere. For example, they are the backbone of travel websites that exist solely to display data aggregated from other websites. When we log in to websites using social media platforms like Facebook and Twitter, we leverage APIs to get access. The Google Maps API is responsible for the embedded maps on just about every "Contact Us" page on the web. Online retail giants such as Amazon and Walmart use APIs to provide product prices and reviews to other websites.

Far more critical, APIs are transforming industries such as healthcare and banking. Medical APIs enable simple real time exchange of patient information, resulting in better patient outcomes. And APIs have revolutionized the banking industry. The recent PSD2 Directive stipulates that the largest banks in the EU must make their data accessible to other parties, if the user provides consent. The goal is to create new services that may benefit the user. These services include facilitating payments and helping small businesses procure loans. Outside the EU, banks are using APIs to enhance customer experiences in a myriad of ways.

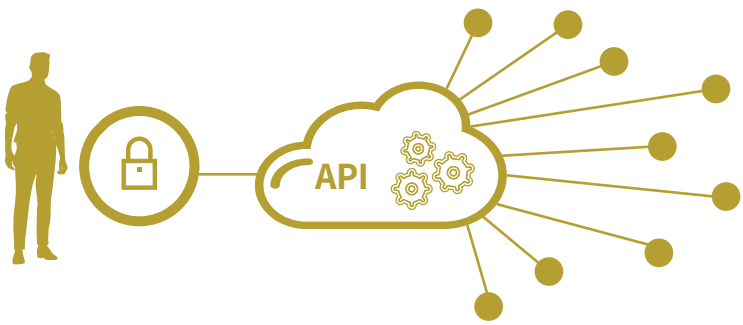
DevOps must secure their APIs

A recent study from Postman.com found that many developers are relatively confident in the API security measures they implement. On the surface, that sounds like a positive trend. But looking at the attacks and breaches that have occurred due to weak API security, it sure seems like it's time for a wake up call.

Why the disconnect between developers and the reality on the ground? DevOps moves fast; security, which requires precision, usually moves slower. This leads to cutting corners and taking the path of least effort where security is concerned. But DevOps without proper security opens organizations up to countless threats.

API security in regulated industries

Regulated industries such as the financial industry are seeing major changes and growth thanks to APIs and the newly established directives mentioned herein. At the same time, the data leveraged by these institutions is subject to strict requirements. Regulated industries must ensure they have the highest levels of API security measures in place—to comply with regulations and moreover, to keep the highly sensitive data they hold secure.



But APIs Create New Security Challenges

APIs may herald innovation, sharing, and enhanced customer experiences—but they have created a slew of new security challenges. APIs, by nature, are transparent and are highly vulnerable, allowing attackers to access the underlying architecture of the application. Thus they have become a new preferred attack vector. This leaves organizations in a frustrating paradox; APIs enable productivity, creativity and drive business—but they create new security problems by definition.

Let's look at some of the specific security challenges APIs create

The sheer volume of APIs to be secured: Consider this - each website contains between tens to hundreds of pages. Each page has dozens of APIs with too many to individually secure. At the same time, as mentioned above, each API is highly sensitive and requires a tailored security approach.

APIs hide attacks: APIs allow attackers to obscure attacks using blended-in noise that helps them bypass traditional security measures. And attacks such as zero-day and SQL injection attacks can easily slip inside organizations, thanks to the varied technologies used in the API landscape. This is exacerbated by an order of magnitude with AI-based attacks.

They increase the potential attack surface: Every API is unique and each one comes with its own risks. In light of these countless APIs, the potential attack surface is sprawling and uncontrollable.

APIs lead to compromised credentials: APIs can publicly expose credentials, allowing attackers to enter networks unnoticed. Using valid credentials means that detection tools cannot find these threats, helping threats move laterally and vertically throughout systems and networks.

Developers and security staff are overwhelmed: Protecting individual APIs requires dozens of rules per API. This customized—yet manual—approach is almost impossible to deliver on, putting undue strain on already-overworked developers and administrators.

Why Application Security isn't Enough

There's a common misconception that organizations can prevent API security problems with the same tools and methods used for application security—as if API security were a mere extension of application security. This is patently wrong. Application security focuses on detecting and mitigating vulnerabilities on the application level to prevent data from being tampered with or stolen. This model, while fitting for application-level threats, does not address the security challenges of APIs.

So how is API security different from application security?
There are a few key factors that separate the two:

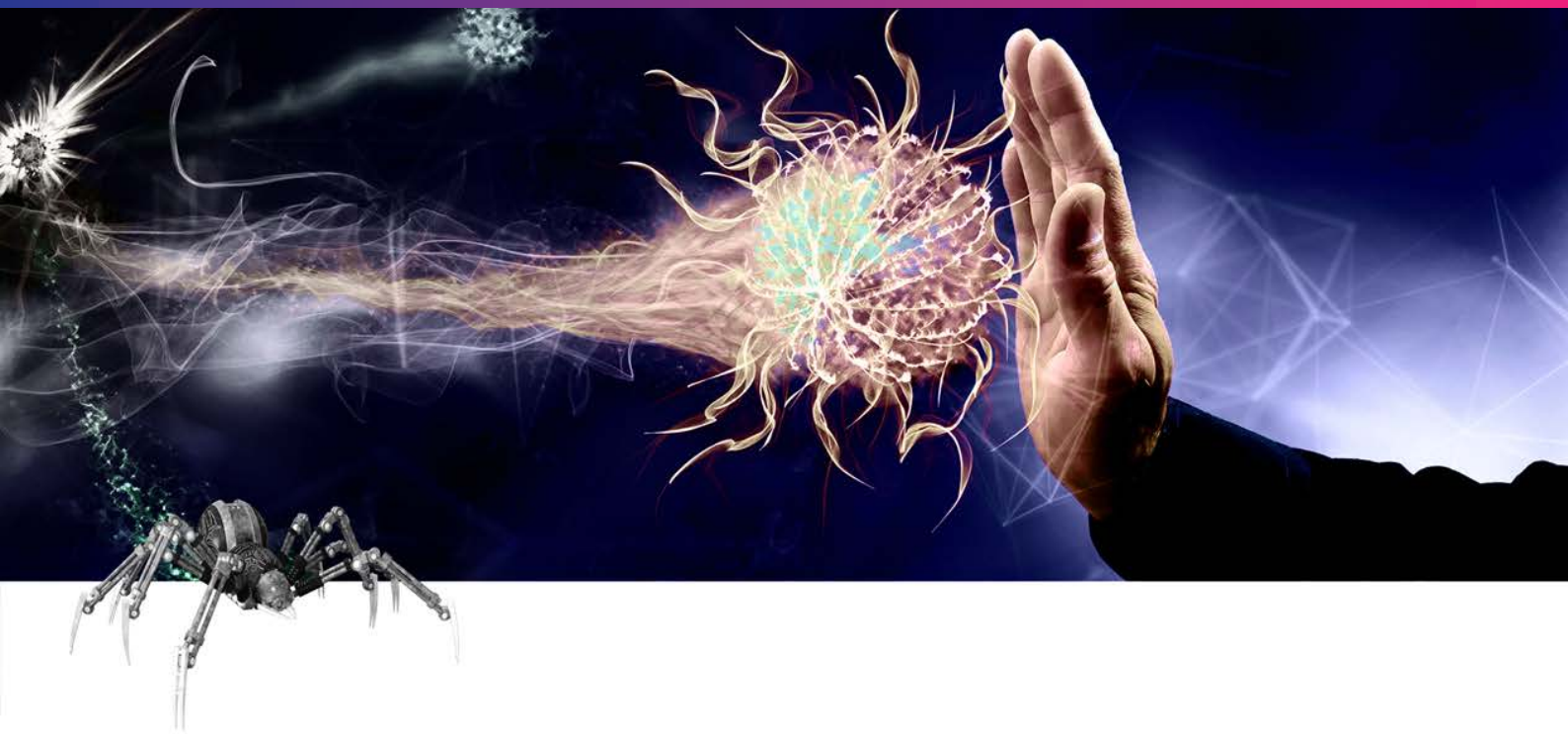
- Each and every API is exposed to a wide range of attacks, stemming from multiple applications and multiple types of users. Application security is focused on a specific range of applications.
- API attacks tend to have a chain-reaction effect. By attacking one single API, attackers can impact many applications. This is typically not the case in application security, wherein the damage is localized to the affected app and ones closely related to it.
- APIs are highly sensitive and the accuracy of defense must be in proportion. Each API on its own can expose businesses to highly damaging attacks and thus must be protected as a standalone application. This high-resolution approach requires a synthesis of automation and customization.

So keeping your APIs secure is not just another aspect of application security—it is its own discipline and requires its own set of tools. Today 30% of all API authentication attempts are fraudulent. And despite the fact that major enterprises such as Amazon, Panera, T-mobile, USPS have all experienced attacks via exposed APIs, many organizations do not conduct extensive API security testing—and some organizations aren't doing any kind of API security testing at all.

This is especially disheartening, considering that The Open Web Application Security Project (OWASP) recognizes API security as a primary concern. In fact, nine of the top ten vulnerabilities in their current OWASP Top 10 report includes an API component.

The L7 Defense Solution:

Ammune™ - Building Immunity into API-borne Threats



Complex challenges require breakthrough solutions. To ensure true, seamless, and automated API security, organizations need simple, inline, and adaptive tools that make the job of protecting their scores of APIs easy.

Ammune™ is the inline AI-based API protection solution that autonomously monitors, detects, and blocks attacks directed at APIs. It's your organization's immune system to defend against API-borne threats, enabling healthy and resilient innovation, agility, and security.

It's a disruptive solution that alleviates the need to manage endless configurations and rules and analyze hundreds of false alarms. This AI-based solution features continuous, unsupervised machine learning technology, enabling organizations to use APIs to maximize creativity, efficiency, and business impact—without compromising your security posture.

How Ammune Works

- It is a novel unsupervised learning core technology utilized for API defense.
- The solution automatically discovers and protect each and every API as a standalone, while it continuously learns the “breathing profile” for every API. It is used to detect and stop emerging threats on the specific APIs that otherwise go unnoticed.
- Ammune does not require previous knowledge a threat or activity pattern in order to understand that it is potentially threatening. It works automatically and autonomously, without prior knowledge or signatures, detecting and fighting back against subtle, stealthy attacks in real time.

The Benefits of Protecting APIs with Ammune

Leverages Unsupervised Machine Learning:

Quick setup, no rules or policies needed

Automatic updates from traffic inspection, no need for rules and constant hand-holding

Does not require additional SOC members to operate the system

Provides Highly Accurate Results:

Minimal to ZERO additional false alarms to handle

Highly accurate at identifying "zero day" payloads and attacks

Yields Rapid Responses:

Sits inline or offline, depending on the user’s choice

Starts to operate immediately after installation as a Plug & Play system

Can operate in detection or enforcement modes, according to the organization policy

Provides Total Interoperability with SIEM/Data:

The system results can be sent to SIEM systems as well as to firewalls and other security systems

Does Not Create GDPR/Privacy Issues

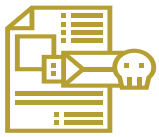
No raw data kept on the system as part of its regular operation

Automatically Detect and Protect all your APIs—At Once

Ammune automatically discovers all APIs and protects against every single threat listed in the OWASP 10 (single request-based threats) and OWASP 20 (bot-related threats, such as data scraping, credential stealing, etc.) and Applicative DDoS.

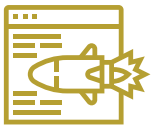
API-WAF Defense

Secures APIs against malicious, single request attacks (OWASP 10) including all types of injection attacks.



API-BOT Defense

Secures APIs against bot attacks (OWASP 20) including identity, transactions abuse and data theft.



API-DDoS Defense

Secures APIs against sophisticated DDoS attacks.

What Makes Ammune Unique?

- **Accurate** - With an error rate close to zero, Ammune delivers an extremely low level of false positives or negatives in real time. It also yields precise performance and accuracy, without negatively impacting the user experience.
- **Defends and detects** - The zero trust solution generates real time applicative transient signatures to mitigate and block a wide array of attacks, whether you're using it inline or in offline mode.
- **Adaptive** - Ammune AI-based auto-policy setting does not require any rules to be set by the user and doesn't use signatures. It continuously self-learns.
- **Easy to deploy** - Deployment is immediate as a Plug & Play solution, with an immediate time-to-value. It's totally scalable to cover all your APIs.

Ammune Compared to Other Solutions on the Market

Other solution available on the market today:

- Require manual discovery of API variations
- Require manual policy creation, setting and maintenance for each and every API
- Require manual threat profiling for each and every API
- Have a high total cost of ownership due to the previous requirements
- Are not automatically scalable
- Have a low rate of discovery, so the False Negative rate is usually high, which can damage customer trust and experience

In Summary
Total Immunity to API Threats with AI-based API Security

APIs are the key to creating today's immersive user experiences. What the future holds for them is yet unknown, but you can bet that they'll further enhance and propel the services and experiences you give your users. AI-based API protection ensures that security threats of today and tomorrow cannot slow down innovation.

To find out more about creating immunity to API-borne threats with leading-edge AI-based defense, click www.L7Defense.com

L7 DEFENSE

Since its inception in 2015, L7 Defense has been helping organizations protect their infrastructure, applications, customers, employees and partners against the growing risk of API-borne attacks. APIs have become critical for data sharing and applications integration – as well as an attractive path for malicious attacks that expose organizations to new, continuously evolving threats.

With a team of experienced leaders and innovators, L7 Defense is poised to revolutionize the way organizations protect their APIs from attacks and exposure using disruptive, AI-based technology. AmmuneTM, L7 Defense's core technology was named the Most Innovative Product in 2018 by Frost & Sullivan, thanks to our novel un-supervised learning AI-based approach to applicative protection at the resolution of discrete APIs.

For more information about L7 Defense and its products,
visit: www.L7Defense.com

You can also follow L7 Defense on LinkedIn.