

API Security

Beyond Gateways & Web Application Firewalls

Summary Abstract

The majority of enterprises now develop new applications and infrastructure solutions based on a combination of private and public APIs. While the use of these APIs dramatically accelerates development and deployment, it has also created an abundance of new attack surfaces that bad actors now exploit to steal confidential information and impair critical enterprise infrastructure.

While API gateways and Web Application Firewalls offer some basic protection from API attacks, they are neither designed nor deployed in a way to address the current API threat landscape. Specifically, they do not offer the discovery, compliance, or protection functionality now required to block currently active API attacks.

An effective API security solution enables organizations to:

- Discover the plethora of APIs now in use by the enterprise, even those third-party and hidden APIs they do not yet have cataloged
- Test currently active APIs to determine compliance with functional specifications and perform dynamic risk assessment of each one
- Protect enterprise information and infrastructure from malicious bot networks and fraud schemes designed to attack active APIs

Read on to learn more about the security gaps left by API gateways and Web Application Firewalls and how dedicated API security significantly improves enterprise security posture.

Application Programming Interface Threat Landscape

Of all the changes that have affected the enterprise IT landscape in the last decade perhaps none of have had more impact than the proliferation of Application Programming Interfaces (APIs) upon which nearly all enterprise applications are now based. More than 75% of enterprises surveyed by the Enterprise Strategy Group claim that an average of 26 APIs are included in each new application now being deployed. While only about 1/3 of applications currently in use include APIs, enterprises believe that fraction will grow to more than half as legacy (non-API based) applications are replaced.¹

The majority of enterprises also report using publicly-accessible APIs for connecting applications with partners, and/or connecting microservices in support of new web applications.¹ The reasons for this increase in API usage aren't a secret. Companies are increasingly recognizing the value of APIs as a way to expose their data and application functionality to external developers. Enterprises have also discovered that APIs can unlock new revenue streams, improve customer experiences, and dramatically streamline internal development processes.

The proliferation of new APIs has created an abundance of new attack surfaces for adversaries to exploit.

As if these benefits weren't enough to drive increased API usage, the development and deployment of APIs is no longer solely the realm of experienced developers. With the rise of low-code and no-code platforms, even non-technical users can utilize pre-built templates and drag'n'drop functionality to participate in API creation and usage, often adding even more unknown/unmanaged APIs to the organization's attack surface.

While the benefits of building new applications on APIs are numerous and compelling, they also have created an abundance of new attack surfaces for adversaries to exploit. 35% of organizations reported at least one security incident due to insecure APIs including data exposure, account takeover (ATO), automated content scraping, and/or denial of service attacks.¹ Further, more than half reported experiencing multiple such incidents. As stated by Gartner® in one of their Strategic Planning Assumptions, "By 2025, less than 50% of enterprise APIs will be managed, as explosive growth in APIs surpasses the capabilities of API management tools"² indicating this problem will get worse for most enterprises before they get it under control.

¹ Enterprise Strategy Group, Securing the API Attack Surface, August 2023

² Gartner, Innovation Insight for API Protection, Dionisio Zumerle, Jeremy D'Hoinne, et al., Validated 02 February 2024 | Originally Published 10 Oct 2022. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission.

"Successful API attacks lead to at least 10 times more breached records than an average cybersecurity breach."

– Gartner, How to Respond to the Threat Landscape in a Volatile, Complex and Ambiguous World, Jeremy D'Hoinne, John Watts, et al., 30 Apr 2024

Some of the most recent data regarding the prevalence of attacks on APIs is found in research conducted by Cequence Security.³ In an analysis of 10 billion API-based application requests, Cequence found:

70% of app requests are via automated requests to APIs

53% of orgs are impacted by three or more API attacks per month

The retail segment saw a 50% increase in bot attacks in the 2nd half of 2023

Despite the relative⁴ novelty of cyber-attacks aimed specifically at API vulnerabilities; a number of enterprises have already experienced their effects. In September 2022 Optus, the second largest telecommunications carrier in Australia, revealed that 10 million of its users had personal data stolen in what was then the worst data breach in Australian history.⁵

Earlier in the year 5.4 million Twitter users had their account details stolen due to a previously reported vulnerability in their user authorization API. This particular vulnerability had been in production for 18 months before it was discovered.

API vulnerabilities are common enough that the Open Worldwide Application Security Project (OWASP), well known for their Top 10 software vulnerabilities list, started publishing an API Security Top 10 vulnerabilities list in 2019. Their [2023 Top 10 list](#) includes the following vulnerabilities.

OWASP Top 10 API Security Risks – 2023	
Vulnerability	Title
API1-2023	Broken Object Level Authorization
API2-2023	Broken Authentication
API3-2023	Broken Object Property Level Authorization
API4-2023	Unrestricted Resource Consumption
API5-2023	Broken Function Level Authorization
API6-2023	Unrestricted Access to Sensitive Business Flows
API7-2023	Server Side Request Forgery
API8-2023	Security Misconfiguration
API9-2023	Improper Inventory Management
API10-2023	Unsafe Consumption of APIs

3 Cequence Security, 2022, https://www.cequence.ai/wp-content/uploads/2022/02/Cequence_Infographic_APIs-tool-of-choice-for-devops-target-of-choice-for-attackers.pdf

4 Compared with conventional viruses, malware, Denial of Service, dictionary password attacks, etc.

5 Tiffanie Turnbull, "Optus: How a massive data breach has exposed Australia", BBC Australia, 28 September 2022, <https://www.bbc.com/news/world-australia-63056838>

API Tools With Security Functionality

Because building new applications atop existing public and private APIs is so popular, multiple categories of tools are now available to help teams develop and deploy new API based applications quickly and reliably. The primary two categories of tools that support development of API based applications are API Gateways and Web Application Firewalls (WAFs). API Gateways were not originally designed as security solutions to anything, but have evolved to include basic security functionality. Web Application Firewalls, which started to appear in the early 2000s were designed from the ground up as security solutions, but only address a rather narrow class of threat. Only more recent solutions that are focused on identifying and addressing the entire current API threat landscape can provide comprehensive protection from this growing category of cyber-attacks.

API Gateways

API Gateways were originally designed to provide traffic management between user applications and the remote API based services they depend upon to function. Over time they also started to provide a communications path between API based applications (sometimes referred to as east-west traffic). In both of these roles they provide traffic control including traffic prioritization, quota management, caching, throttling, and the imposition of rate limits. Historically, they have also provided policy management, protocol conversion, and bulk data transfer. Some API Gateways also offer API composition, virtualization, versioning and request auditing in support of the development process.

In terms of security features API Gateways typically only offer:

- Access control to publicly available services
- Authentication of users requesting access to services
- Traffic blocking based on user IP address
- Message-level security (SSL/TLS)
- Manual inventory management

While these features are important to maintain process and data security, they do not by themselves address the current API threat landscape. Perhaps the biggest security limitation of API Gateways is that gaining benefit from this functionality requires the enterprise to KNOW what APIs are deployed and to onboard them to their inventory and monitoring systems. APIs that aren't explicitly onboarded are unmanaged by the API gateway.

In order to use the security features of an API Gateway the enterprise must know which APIs are in use and have them under active management.

Web Application Firewalls

While the first Web Application Firewall (WAF) was released by Perfecto Technologies in 1999, they didn't really take off until the Payment Card Industry Data Security Standard (PCI DSS) Requirement 6.6 was released in September 2006. The credit card industry realized that the internet was both the biggest opportunity and the biggest threat it had ever faced. The industry concluded they needed to standardize the security requirements of the burgeoning number of service vendors and applications that wanted to access their services. Specifically, PCI Requirement 6.6 declared "that all custom application code must be professionally reviewed for vulnerabilities or a web application firewall must be installed in front of web-facing applications". As such, WAF solutions have historically been very focused on addressing the needs of the PCI industry and less concerned about the needs of other sectors and *their* growing dependence upon API-based applications.

A WAF basically operates by monitoring HTTP traffic for known malicious patterns and reroutes "good" traffic while blocking "bad" traffic. Most WAFs will then block all incoming traffic from the source of the bad traffic based on the rules it has in place. Internally, a WAF works very much like legacy antivirus software in that it uses signatures to identify known vulnerabilities based on the OWASP Top 10 Application security risks list.⁶ It's not terribly sophisticated but it performs its limited role reliably. Most WAFs cannot identify or block newer threats that haven't yet been cataloged by OWASP or address the visibility, inventory tracking, risk assessment, and threat prevention requirements necessary to comprehensively protect APIs across the entire API security lifecycle.

Most WAFs cannot identify or block newer threats that haven't yet been cataloged.

Architecturally, a WAF's most significant limitation is that it's purely an application (OSI layer 7) protection appliance. It has decent visibility on the contents of the HTTP traffic going to and from a web application, but little else. As a segment WAF products are in the same position today that the network firewall products were in before the advent of "Next Generation" firewalls that included much richer security functionality. Some products are only now starting to see features like faster rules updates, rate limiting, and DDoS protection. Like API gateways, Web Application Firewalls are a necessary, but insufficient tool for addressing the current API threat landscape.

API Gateways and WAFs definitely do provide a level of API security, but they neither architecturally or functionally were designed to "see" all of the APIs enterprises now depend upon, assess the risks associated with those APIs, or to defend applications and infrastructure from the associated threats. Providing comprehensive API security requires an entirely different approach.

⁶ Note: This is a different project and list from the OWASP API Security Top 10 risks list.

Cequence Unified API Protection Platform

The Cequence Unified API Protection (UAP) Platform takes a completely different approach to the legacy API gateway and application firewall products based on three core tenets of API security:

Discover | Comply | Protect

Discover

Management guru Peter Drucker famously said, “You can’t manage what you can’t measure”. The cybersecurity corollary to Drucker’s observation is that, “You can’t stop what you can’t see”. The first step in effective API security is “seeing” all of the APIs currently present on organizational infrastructure even if all of them are not currently in use by one application or another. We noted previously that enterprises report an average of 26 APIs are involved in each new web application they develop. But these are just the APIs they know about. That number does not include the shadow and third-party APIs that are unknown, undocumented, unmanaged, and unprotected in nearly all enterprises.

Using nothing more than a domain name, Cequence is able to perform a non-invasive discovery crawl that provides an “attacker’s view” of an organization’s externally-facing API attack surface. The Cequence UAP crawls all of an enterprise’s domains, catalogs the APIs found, and classifies them for immediate action through user-customizable algorithms. The Cequence UAP is agentless and even identifies APIs that aren’t currently transacting data.

In an average enterprise scan, Cequence UAP discovers 326 API servers spread across 37 hosting providers. The vast difference in numbers found versus commonly reported indicates that most enterprises don’t have a complete picture of the API services upon which their business runs. The Cequence platform goes well beyond simply building a database of the APIs it discovers. It leverages that repository to establish and maintain an enhanced API security posture and to protect those APIs from malicious actors.

Cequence UAP is agentless and identifies the unknown shadow and third-party APIs in deployment regardless of whether they are transacting data.

None of the currently available API Gateway products or Web Application Firewalls include anything like the Cequence API discovery capabilities.

Comply

The Cequence UAP Platform Comply functionality includes three key components:

- API functional testing
- Comparison of those test results with known specifications
- Dynamic risk assessment

In the case of discovered APIs for which there is not a current specification, Cequence UAP automatically builds an OpenAPI-compliant spec. The subsequent risk assessment is based on predefined and customizable OWASP API Security and Automated Top 10 Risk categories. Further, Cequence UAP can also create a complete API test plan, speeding the process by orders of magnitude. APIs in development can even be tested and assessed using synthetic traffic to determine if they will introduce any OWASP, business logic abuse, or other risks.

Like the Discover functionality, none of the currently available API Gateway products or Web Application Firewalls include anything like the Cequence API Comply capabilities.

Cequence UAP improves API security posture through functional testing and risk assessment of currently deployed APIs.

Protect

The most common types of attacks on APIs include, but are not limited to:

- Account takeover (ATO)
- Broken Object Level Authorization (BOLA) attacks
- Attempted expropriation of sensitive data
- Gift card and loyalty program abuse
- Business logic abuse
- Inventory fraud/hoarding
- Fake account creation

Cequence UAP identifies and blocks attacks from bot networks and sophisticated fraud schemes.

Cequence UAP utilizes two modules to address specific types of attack strategies. The Bot Management module identifies and blocks the most sophisticated types of attack payloads regardless of how the adversary attempts to hide their true intent. Historically, WAFs could block most bot traffic based on IP source address, session ID, or HTTP user agent. However, the miscreants perpetrating these attacks have become quite good at circumventing the algorithms WAFs use to identify malicious traffic. Cequence UAP provides a superior level of API security by using a proprietary correlation engine that is able to see through attempts to disguise the source, content, and metadata profile of malicious traffic. Unlike the currently available WAFs, Cequence UAP compares API requests with normal user behavior benchmarks and can even examine the request payload to assess its legitimacy.

The other module that provides superior protection when compared to API Gateways and WAFs, is the Fraud Prevention module. This module allows security teams to define and deploy very granular fraud policies based on their business practices and risk profile. Besides deploying enterprise specific policies, security teams can establish repositories of known rogue and high-risk users to be blocked or filtered before they can interact with any of the enterprise's API infrastructure. Once the policies and undesirable user lists are in place the security team can leverage them to establish customized alerts and remediation actions to address any attempted fraud in real time.

Like the Discover and Comply functionality, none of the currently available API Gateway products or Web Application Firewalls include anything like the Cequence API Protect capabilities.

Cequence Unified API Protection solution capabilities compared with WAFs and API gateways

		Cequence Unified API Protection	Web Application Firewalls	API Gateways
API Discovery & Inventory	Unmanaged (shadow) API discovery	Yes	No	No
	API usage analysis	Yes	No	Yes
	Assign/track API by owner	Yes	No	Limited
API Risk Assessment & Categorization	Data governance	Yes	None	None
	Weak/missing authentication	Yes	None	None
	API specification conformance	Yes	None	None
	Custom risk criteria	Yes	None	None
Threat Detection	Threat database of billion+ records	Yes	No	No
	Vulnerabilities	Yes	Yes	Yes
	Automated attacks	Yes	Limited	Limited
	Business logic abuse	Yes	Limited	None
Mitigation	Block on Behavioral Fingerprint	Yes	No	No
Response Options	Deception	Yes	No	No
	Forward to third party	Yes	No	No

With enterprises moving to API-based applications and infrastructure solutions and the adversary developing ever more sophisticated techniques to exploit those APIs, the need for secure development and deployment of these mission critical IT systems will only increase. API Gateways and Web Application Firewalls are not designed to meet the current threat landscape nor architecturally capable of evolving to address new threats in a timely manner. The Cequence Unified API Protection (UAP) Platform empowers enterprises to discover and catalog active APIs, test those APIs for functional integrity and compliance, and protect sensitive data and systems from malicious bot networks and fraud schemes.