Guide

Why API Gateways Are Not Enough to Secure APIs

In an attempt to address the increased use of application programming interfaces (APIs), the marketplace is now littered with a variety of API gateway solutions designed to facilitate all aspects of managing the API lifecycle. Certain API gateways can also process basic signature-based API protection, leading many organizations to assume their APIs have comprehensive protection through their API gateway. Unfortunately, that is not the case.

What Is an API Gateway?

An API gateway is a single entry point for all API calls made by client devices to a particular set of back-end services. The most important role of an API gateway is to ensure the reliable processing of every API call. In addition, API gateways cover a variety of operational tasks, including controlling access, translating protocols (for example, from RESTful to SOAP), or scaling resources if there is a traffic spike.

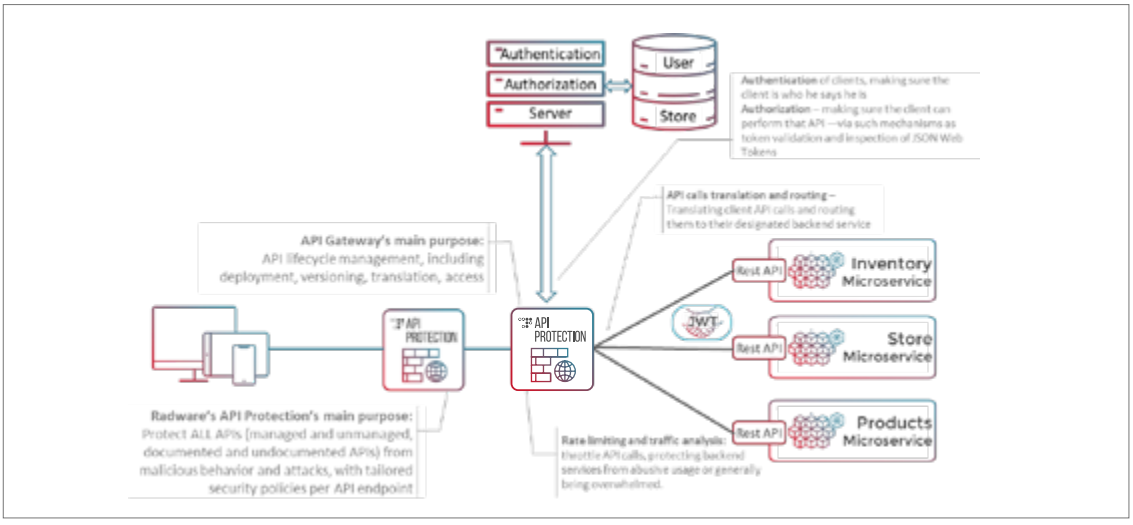

Figure 1

The roles of API gateways and of API protection solutions

Many API gateways also provide basic API protection capabilities, including authentication and authorization, encryption, rate limiting, transaction logging and rudimentary signature-based security policies.

Do API Gateways Provide Effective Protection?

The modern API threat landscape has become highly diverse and sophisticated. Most attackers can easily evade traditional security signatures and rate-based rules. According to research findings published by Security Magazine, 94% of organizations have suffered from an API security incident and API attack traffic has grown at more than triple the rate of overall API traffic.[1] Basic signature-based rules can create more harm, such as false positives, than actual effective protection.

The OWASP API Security Top 10[2] identifies numerous attack vectors that require effective security policies that go far beyond signature-based defenses and negative security models. For example, the #1 threat listed on the OWASP Top 10 are malicious bots, which can create different type of attacks through an application's API – from account takeover (ATO) to application distributed denial-of-service (DDoS) attacks and web scraping. While each unique call a bot sends may look legitimate and harmless, it's the sequence and sum of all API calls that must be detected and blocked.

API Security Stats

- Unmanaged and unsecure APIs create vulnerabilities that can accelerate multimillion-dollar security incidents.
- By 2025, more than 50% of data theft will be due to unsecure APIs.
- By 2025, fewer than 50% of enterprise APIs will be managed, as explosive growth in APIs will surpass the capabilities of API management tools.

Source: Predicts 2022: APIs Demand Improved Security and Management, Gartner Research, December 6, 2021.

Another example is the proliferation of east-west traffic via internal APIs between the different application components. API gateways are placed between the user and an application's front-end server so they can monitor API calls coming from the outside (north-south traffic) but prevent them from monitoring API calls running between the different application components (east-west). Only an enterprise-grade API protection solution integrated into the various application microservices can protect east-west API calls.

The security functions of the API gateway (such as client authentication and authorization) are an important part of any API deployment strategy. However, API gateways were never designed to provide advanced security capabilities, which is why many API vendors provide integrations with more comprehensive API security solutions.

1 API Attack Traffic Has Grown at Triple the Rate of Overall API Traffic, Security Magazine, July 28, 2021

2 OWASP API Security Project.

Comprehensive API Protection

Radware's approach to comprehensive protection is based on a dedicated API protection solution that is part of a larger, holistic application security solution. It protects the application and API as a singular entity, in addition to any underlying infrastructure.

Radware's API protection starts by mapping the API attack surface and tailoring an API-specific security policy that is able to effectively detect and block the ever-growing spectrum of modern API threats. Underscoring these capabilities are machine-learning algorithms that automate the discovery of all active APIs, their structure and parameters as well as their value types and ranges. Based on this discovered information, an accurate security policy for all discovered APIs is automatically generated.

"Frictionless" API Security

To ensure the security policy is accurate enough to block attacks while avoiding false positives, Radware's API protection solution continuously runs a machine-learning-based policy optimization to automatically suggest and apply security policy adjustments to correct and eliminate false-positive events. The result is state-of-the-art API protection while making API management and security "frictionless".

API Protection Against Automated Threats

Radware's API protection solution also includes machine-learning algorithms to detect malicious bot activities targeting APIs, such as ATO attacks, content scraping and data harvesting, fraud, and more:

- API Flow Control – Machine-to-machine API protection from access to bad bots
- API Client SDK – Unique source identification of machine-to-machine APIs (fingerprinting)
- Invocation Context Analysis – Web and mobile APIs
- Authentication Flow Analysis – ATO protection for APIs, such as credential stuffing or token cracking

Radware's API Protection Solution Versus API Gateways

USE CASE OR TYPE OF PROTECTION	RADWARE API PROTECTION SOLUTION	API GATEWAY	COMMENTS
Schema Enforcement, Applicable for Documented APIs	Supported; protects all aspects of the API, including API parameter, header and full body	Supported	It is considered bad practice to trust API documentation in the security field. Handling the service exposition, it can disclose deprecated APIs and open shadow APIs with a new attack surface. An independent layer of security provides the best and strongest mitigation solution that can be tailored at the level of the API definition.
API Discovery	Advanced; automatically discovers documented and undocumented APIs and managed and unmanaged APIs, with all their endpoints, schemas and allowed value ranges	No protection	While API gateways can perform "API discovery," they are limited to performing it to dynamically link the API definition in the API gateway to what is existing and evolving on the server side.
Authentication and Authorization	Not provided	Advanced	A basic function of an API gateway, it protects against unauthorized API call execution.
Token Verification, Validation and Policy Access	Available with specific API gateway vendors	Available by design	Radware also allows a security policy configuration per user context (extracted from the authenticated token).
Negative Security Model: Injection, XSS, Known Vulnerabilities	Advanced; strong protection with a low false-positive rate, with machine-learning-based optimization of security policies	Basic	Leverages a basic negative security model engines often require severe security compromises to avoid high rate of false positives
Zero-Day Attack Mitigation	Advanced	Weak or no protection	Zero-day attack mitigation can't rely on a negative security model. It requires both negative and positive security models for effective protection, in addition to a strong vulnerability research team that can release protection within a few hours for zero-days attacks, such as with the Log4j vulnerability.

Advanced API Attacks – XML Bomb, XXE, and Others	Advanced	No protection	
SSRF, LFI, RFI	Advanced	No protection	
Account takeover	Advanced	No protection	Radware's Bot Manager solution's bot detection engine analyzes every API request, including payload and HTTP headers, to identify anomalous behavior patterns. It leverages intent analysis to understand the actual intent behind an API request to filter malicious API calls.
Application Distributed Denial of Service	Advanced	No protection	
Web Scraping	Advanced	No protection	

Conclusion

While API gateways are an essential component for effectively managing the life cycle of APIs, their protection capabilities don't provide comprehensive protection against the array of threats targeting APIs. Moreover, application protection requires a holistic approach in which the API is only one aspect.

Radware's API protection solution is part of a holistic architecture that protects against a wide range of API and application threats.

Learn More about what comprehensive application and API protection must now encompass to keep your organization secure in an interconnected, digital environment

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare,
YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.