radware

HOW TO KEEP APPS AND APIs SECURE IN AN INTERCONNECTED WORLD

INTRODUCTION

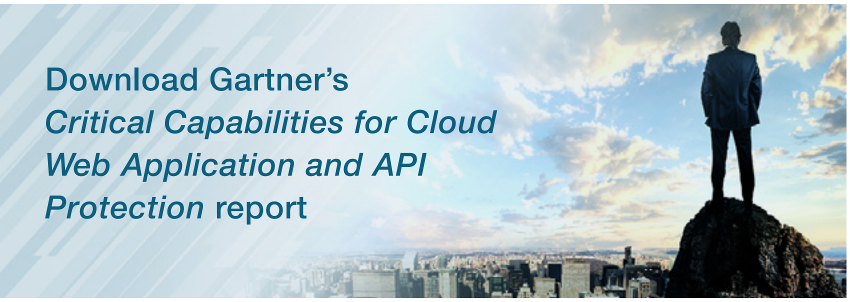
APIs are the quintessential double-edged sword. They are the cement that interconnects systems and applications, but they add security vulnerabilities and complicate protection strategies and application development. According to Gartner, "by 2022, API abuses will move from infrequent to the most frequent attack vector, resulting in data breaches for enterprise web applications."

Migration to the cloud, the adoption of APIs, DevOps, and the increasing loss of visibility into security has left apps increasingly vulnerable. Ensuring app security and data integrity is crucial as businesses continue to rely on applications to connect with customers, partners and staff.

No matter how many APIs your organization chooses to share publicly, your ultimate goal should be to establish a comprehensive application/API security policy that manages them proactively over time. Understanding how to manage application and API security has never been more crucial. Here are six key strategies you should consider to safeguard your applications and APIs in an era of interconnectivity.

1. COMPREHENSIVE, 360-DEGREE PROTECTION

According to Gartner's *Critical Capabilities for Cloud Web Application and API Protection* report, web application and API protection (WAAP) is now the standard when it comes to protecting apps and APIs. It is the preferred choice because it combines both broad scope and comprehensive security with ease of deployment at scale.



Download Gartner's *Critical Capabilities for Cloud Web Application and API Protection* report

When evaluating application/API security solutions, organizations should have the four key capabilities of WAAP top of mind: web application firewall (WAF), bot management, API protection and DDoS protection.

Doing so means building a security strategy that provides comprehensive protection in multi-threat environments. It also helps ensure that your organization is moving beyond best-of-breed, point solutions that might be good at identifying and categorizing attacks, but provide limited mitigation functionality that results in data breaches or a negative digital experience for your customers.

4 Recommendations When Implementing WAAP

Build an application security strategy for the present and the future of your application architecture by using a cloud-first strategy, if possible

Develop WAAP requirements based on the types of web apps, mobile apps and web APIs based on where they are hosted, who can access them and the type of data being accessed

Ensure core security features are covered by any application security solution, including the OWASP Top 10, file and SQL injections, protection against automated and highly sophisticated bot attacks, etc.

Implement products with automated API discovery and behavioral API anomaly detection

2. PRIORITIZE AND ENGAGE SECURITY EARLY

API security should not be an afterthought. Your organization has a lot to lose from a data breach due to unsecured APIs, so incorporate security early into the application/API development process. Yet, this mentality is the exception, not the rule. In 92% percent of organizations, security staff have limited influence on continuous integration/continuous deployment (CI/CD) architecture and, for all intents and purposes, are required to secure it as-is, according to Radware research.[1]

Security development and delivery processes (DevSecOps) should become the cornerstone for prioritizing and engaging security early in web application and API development cycles. It represents a natural and necessary evolution in the way development teams approach security. Historically, security was "tacked on" to the software development cycle (almost as an afterthought) by a separate security team and was tested by a separate quality assurance team. This was manageable when software updates were released just once or twice a year. But as software developers adopted continuous deployment practices, the traditional "tacked-on" approach to security created an unacceptable bottleneck.

DevSecOps should integrate web application and API protection seamlessly into the application development lifecycle. It addresses security issues as they emerge, when they are easier, faster and less expensive to fix by working milestones and "sanity checks" into the process. The last thing any development/operations team wants to play is a game of "patch me if you can."

Additionally, DevSecOps is responsible for ensuring application infrastructure security. Accomplishing this means coordinating with application development, security and IT operations teams. This enables "software, safer, sooner"—the DevSecOps motto–by automating the delivery of secure software without slowing the software development cycle.

[1] The State of Web Application and API Protection

3. SUPERVISE THE UNSUPERVISED

API security is a microcosm for an organization's ability to manage risk and safeguard customer data. In the mad dash to digitally transform, businesses incorporated APIs into their application environments without fully understanding the security risks.

It is imperative to understand how 3rd parties are accessing and leveraging your company's data. You cannot manage what you do not measure, and APIs are no exception. Enterprises need complete visibility into where APIs are hosted, who can access them, the sensitivity of the data being accessed and the scalability that is required.

Always assume that any 3rd-party vendor/cloud provider/partner that is processing your data is not a security expert nor are they prioritizing API security. In addition, ensure your organization understands where the boundaries lie when it comes to who is responsible (either you or a cloud provider) when it comes to keeping data and applications secure. Make sure to inventory and manage your APIs. Conduct perimeter scans to discover and inventory your APIs and then work with DevOps to manage them effectively.

Understand The Cloud Shared Responsibility Model

Additionally, take advantage of emerging technologies and concepts for application development lifecycles, including integrative security tools/Security Orchestration Automation and Response (SOAR) capabilities, Function-as-a-Service (FaaS) capabilities and open-source code. Surprisingly, many organizations have not. For example, one-third of organizations do not use automated provision and testing as part of their application/API development lifecycle.[2]

Lastly, current solutions for APIs fall short on security. API monitoring and management tools are great at providing visibility and monitoring but poor protection. API gateways provide basic authentication and IP filtering, but they don't provide comprehensive, automated protection against an expanding array of attack vectors and bad bots. Moving beyond best-of-breed, point solutions towards comprehensive, adaptive protection (WAAP) is now crucial.

The Move to WAAP

+30%

By 2023, more than 30% of public-facing web applications and APIs will be protected by cloud-based WAAP services

+50%

By 2024, most organizations implementing multi-cloud protection strategies for web applications in production will only use cloud-based WAAP services to safeguard them

[2] The State of Web Application and API Protection

4. FROM RULE- TO MACHINE LEARNING-BASED SECURITY

Many enterprises have responded by implementing the aforementioned API management solutions that provide mechanisms, such as authentication, authorization and throttling. These are long-standing must haves for controlling who accesses APIs across the application ecosystem—and how often. However, organizations also need to address the growth of more sophisticated attacks on APIs by complementing these “point” solutions with machine learning-driven security.

Rule-based and policy-based security checks, which can be performed in a static or dynamic manner, are mandatory parts of any API management solution. API gateways serve as the main entry point for API access and therefore typically handle policy enforcement by inspecting incoming requests against policies and rules related to security, rate limits, throttling, etc.

These policy-based approaches around authentication, authorization, rate limiting and throttling are effective tools, but they still leave vulnerabilities through which hackers can exploit APIs. Notably, API gateways front multiple web services, and the APIs they manage are frequently loaded with high numbers of sessions, making it difficult for a gateway to inspect every request.

Moreover, SAST and DAST testing solutions, while effective at evaluating source code and testing application functionality for security vulnerabilities, only provide reactive insight into API and application vulnerabilities; they do not provide proactive, automated protection.

Machine-learning based application security solutions are adaptive by automatically detecting and responding to dynamic attacks and application/API vulnerabilities. First and foremost, they should automatically detect and protect new web applications as they are added to the network via automatic policy generation.

In addition, machine learning can eliminate API abuse such as token manipulations, parameter tampering, protocol attacks, invalid schemas and more. An enterprise-grade firewall should import, enumerate and catalog APIs to enforce standards and schemas using behavioral protections and positive security.

7 Warning Signs Your Apps/APIs Are Vulnerable

1. Using non-defined/non-allowed HTTP methods for an API endpoint
2. Embedding web attacks in JSON payloads or parameters
3. Excessively utilizing the APIs
4. Attempting to break the API authentication process through an account takeover attack
5. Sending requests not according to the JSON/XML schemas
6. An API key rotation – or a successful login from an unusual source
7. Extremely high application usage from a single IP address or API token

5. SECURITY AND DEVOPS: WHAT TO CONSIDER WHEN CONSIDERING CYBERSECURITY SOLUTIONS

The emergence of new application architectures, cloud-native workloads and the increasing reliance on APIs means organizations now require web application and API protection that can secure at the speed development–without compromising agility, time-to-market or overall productivity. These solutions must be able to “flex” with development environments and adapt to the needs of the business. Before considering any solution, make sure it meets the requirements of both DevOps and security teams.

Here are some key characteristics to consider when evaluating WAAP that integrates well into your CI/CD pipeline.

- **Consistency across hybrid computing environments** – data centers, private clouds and public clouds all require fine tuning and adjustments that result in gaps in your application security posture. Look for security solutions that provide unified, robust and consistent security agnostic where your applications run.
- **Gaining visibility into security events (APIs especially) and performance metrics** – Adopting an integrated approach to security results in an integrated, 360-degree view of security/performance issues via a single pane of glass.
- **Scalability** – This means security solutions that have “elasticity.” They can grow and scale application security alongside development orchestration tools, including auto-learning policies and configuration settings.
- **Effective security (zero-day protection)** — Negative and positive security models are necessary to protect against known and unknown threats, thus maximizing security and minimizing false positives
- **Adaptive security** — Immediate detection of new and modified applications in the CI/CD pipeline is not enough and must be followed by automatic generation and optimization of security policies
- **Risk free integration** with the various tools and systems compromising application development and orchestration solutions to ensure minimal or no delay application development and release cycles

6. HYBRID CONSISTENCY

The overwhelming majority of companies are now hybrid: their applications and/or network infrastructure operates across heterogeneous computing platforms. While this approach provides a multitude of well documented benefits, it also presents a series of challenges when it comes to cybersecurity.

Each environment has its own sets of infrastructure requirements and each typically provides its own set of management/reporting tools. Since your applications are dependent on sending and receiving data from these different environments, this creates two big challenges:

- **Visibility** into security issues and performance across different environments
- **Consistency** of security policy enforcement across different environments

Application and API security are microcosms of both. Having 360-degree visibility into security alerts/performance issues across hybrid environments is challenging enough. Add fluid environments and workflows that are a byproduct of agile development methodologies, and things get worse. Leveraging point management and monitoring solutions and/or manually tuning security policies exasperates these issues and makes keeping applications and APIs secure nearly impossible.

Develop a cross-platform application/API strategy that addresses datacenters, hybrid cloud usage, monolithic apps and microservices. As previously mentioned, automated detection is critical. Implement security solutions with automated API discovery and behavioral API anomaly detection and leverage firewalls that automatically detect new or updated web applications as they are added to the network.

Challenges and Concerns

31%

of organizations say the most significant application security challenge is maintaining security policies across data centers and cloud platforms[3]

30%

of companies are most concerned about visibility into security events impacting their organization[3]

[3] The State of Web Application and API Protection

MOVING FORWARD

The key to application security moving forward will rest on the ability of application development and product teams balancing the need to secure infrastructures while migrating applications to public clouds via automation and governance. Organizations need to change the way they manage security for applications and APIs, both in terms of its role in application development and the security solutions they implement to safeguard them.
In summarizing, secure applications and APIs by:

→ **UNDERSTAND THE THREAT LANDSCAPE**

- Identify what attacks are targeting your applications and APIs
- Classify application vulnerabilities
- Ensure you can distinguish between good and bad bot traffic
- Prepare for API abuse and application denial-of-service attacks

→ **IMPLEMENT NEW APPROACHES TO SECURITY**

- Integrate security into the development cycle
- Develop a cross-platform strategy that addresses datacenters, hybrid cloud usage, monolithic apps and microservices
- Consolidate and unify technologies to limit the use of point solutions
- Select a solution that provides visibility into what is happening across the network
- Leverage automation and machine-learning capabilities to boost mitigation capabilities

Learn More About What Integrated Application Protection Now Means In An Interconnected World

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.