Best Practices for API Security

What security practitioners, DevOps, and DevSecOps need to know

What's Inside

API Security is a Growing Concern

Many organizations scramble to maintain their competitive foothold amid rising costs and security skills shortage. All the while, customer behaviors and expectations are forcing businesses to bring new capabilities on board quickly. Web applications and APIs are surging to support new business-critical workflows.

APIs help businesses get work done. End-users today expect to be able to access sensitive business data from any internet-connected device. A salesperson needs to access customer records from a CRM system on their phone while en route to a customer. An executive needs to quickly check inventory levels by accessing their supply chain management tools from their web browser. From end-users to the executive teams, APIs have become essential for line-of-business functions, and 83% of organizations today consider API integration a critical part of their business strategy.[1]

APIs have become fundamental to business agility. Because developers build new apps and enhance existing ones so rapidly, the APIs are constantly changing — as fast as a company's DevOps and CI/CD practices allow. Yet centralized and consistent security controls are often not yet in place, and 62% of businesses have delayed app rollouts because of API security concerns.[2] DevSecOps face the challenge of securing against API exploitation.

In this eBook we will examine the best techniques to defend your APIs against security threats.

1. "API Sprawl a Looming Threat to Digital Economy," DevOps.com, 2021.
2. "Concerns Over API Security Grow as Attacks Increase," DARKReading, 2021.

The New Security Reality

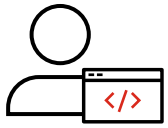
In an ideal world, DevOps write code without distractions, and security professionals are involved throughout every project, from inception to deployment. The reality is that many DevOps professionals are often forced to take on the responsibility for security, in part or holistically, leading to software development delays. Further, many security teams don't have full visibility into the APIs in their environment. The reasons vary and may include the rapid pace of developing apps without time to identify security vulnerabilities before production, the inheritance of unfamiliar applications, web apps and APIs from acquired companies, or security staff shortages or turnover.

Cybercriminals leverage scripted attacks and new technology to increase their speed and scale, and cybercrime groups have the funding and organization to launch advanced attacks and conduct detailed reconnaissance of the attack surface. In 2021, 43% of organizations confirmed they had experienced application breaches or compromises in the past, and more than a third of respondents did not know when the last breach occurred.[3]

Let's not forget to mention the shortage of skilled professionals. The world is lacking three million cybersecurity professionals, according to the latest report by the World Economic Forum (WEF).[4] A lack of skilled personnel tops the list of barriers organizations face when securing their web applications (46%).[5] Sometimes companies are forced to move forward with their digital projects with insufficient security resources, creating more risk.

3. "Application Security Report," Cybersecurity Insiders, 2021.
4. "Shortage of cybersecurity professionals a key worry for firms in '22" Livemint
5. "Application Security Report," Cybersecurity Insiders, 2021.

You Are Not Alone in Facing These Challenges in Your Workplace:



DevOps
Every developer manages security for their app independently
Each app handles its own API keys
New apps are deployed quickly and with security as an afterthought
It's challenging to keep track of every app's own set of APIs
Independent departments manage applications according to their own application preferences and requirements

Security Practitioner
Lack of visibility into and control of each app's security
Decentralized app security management
Overseeing subcontractors' access to multiple systems
Security alert fatigue
Increase in malicious bot activity

From Static to Dynamic

Gone are the days when web apps just delivered static content such as images, video, and website information. Today's web apps are dynamic, and content is customized for each user. Web apps generate pages based on each request by pre-fetching data through APIs to deliver a responsive experience to users.

APIs provide an entry point to an organization's business-critical information. They interact with backend systems and open access to enterprise apps as well as data, partners, suppliers, and customers.

APIs enable modern web applications to:

Improve user experience

Connect different systems

Share information across a B2B environment

Deliver data to mobile apps

The API market offers nothing but growth

There are over 2 million API-related repositories on GitHub, and APIs are fundamental to organizations' digital transformation efforts.

Over **90%** of developers use APIs[6]

68.5% of developers expect to rely on APIs more in 2022[7]

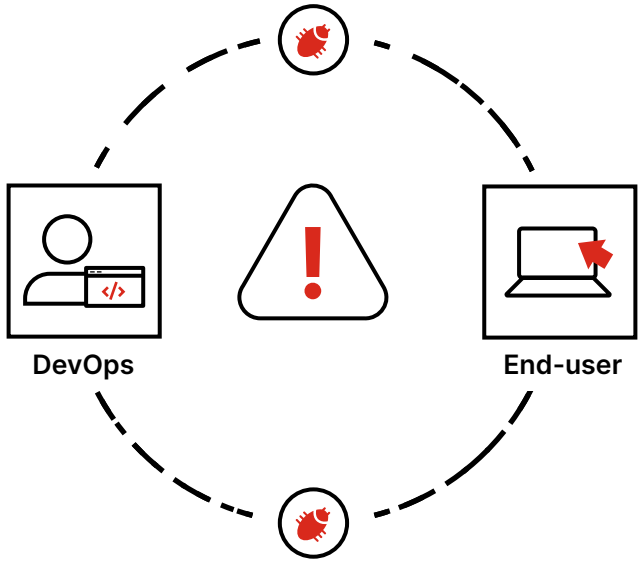
56% of developers find APIs help build better digital products[8]

6. "20 Impressive API Economy Statistics," NordicAPIs, 2022.
7. "State of APIs 2021: 'Great Resignation' leading challenge, security remains a top focus," Developer, 2021.
8. "20 Impressive API Economy Statistics," NordicAPIs, 2022.

More Code. Bigger Attack Surface.

The attack surface is rapidly changing with every iteration of code. Organizations use DevOps methodology to speed time to market and accelerate software release cycles. GitLab's latest survey revealed that, almost 59% of respondents deployed code multiple times a day, once a day, or once every few days.[9]

This cadence leaves little time for deep security investigation on every code iteration. DevSecOps tools are enabling developers to release code faster than ever — yet testing, code review, and disagreements on who oversees security remain sticking points within organizations.



Application proliferation

48% of organizations have 100 or more unique apps in their environment.[11]

Companies publish **25** software updates into production every month on average.[12]

9. "DevOps is getting code released faster than ever. But security is lagging behind," TechRepublic, 2021.
10. "DevOps is getting code released faster than ever. But security is lagging behind," TechRepublic, 2021.
11. "Application Security Report," Cybersecurity Insiders, 2021.
12. "Application Security Report," Cybersecurity Insiders, 2021.

APIs: The Next Big Cyberattack Vector

The prevalence of APIs is astonishing — 77% of organizations develop and consume APIs. Whether you are developing new APIs or using existing RESTful APIs they may be the most serious security threats your organization faces. This is because they provide direct lenses into highly sensitive data and functionality.

The Peloton Breach: A Real-World Example

Security researcher Jan Masters revealed a vulnerability in Peloton's user account API whereby requests for personal data could be made without the system checking for authentication. This allowed access to a Peloton rider's private data, including the user's age, weight, location, gender, workout data, and more.[13]

The breach was caused by failing to authenticate and validate access so that only trusted identities have access to the API at every step of the transaction process, from client to server. For Peloton, the exposed infomation may have included user PII and user behavior intelligence that could have been validated against accessed data stores.

Peloton has since resolved the API issue, but this is one example of many. Almost all web app attacks come from external threat actors, and financial gain is the primary motive for the attack 89% of the time.[14]

Why API Security is so Problematic

When your environment was a bit simpler, managing API security was easier. Every app handles controlling access to APIs differently. For example, you may have 30 apps with different approaches to API security. This would require you to become an expert in each approach to maintain your security posture.

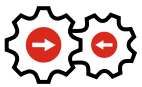
Since APIs expose sensitive data such as Personally Identifiable Information (PII), they have increasingly become a target for attackers. Given the high cost of a security breach and a shortage of security professionals, trying to secure every app in the environment becomes a huge undertaking and risk.

13. "Peloton's API exposes riders' private data," Security Magazine, 2021.
14. "2021 Data Breach Investigations Report," Verizon, 2021.

5 Common Myths About API Security

API security isn't widely understood, and the following myths add to the confusion, creating a false sense of security. Learning the truths about API security can help strengthen your overall strategy.

My cloud provider supplies API security protection.



My web application firewall (WAF) automatically protects against API threats.

All of my apps — whether open source, commercial off-the-shelf, or custom — handle API security in the same way.

API schema validation is sufficient to protect my apps.

APIs automatically update to block attacks.

Best Practices to Secure APIs

The guidance Open Web Application Security Project (OWASP) provides for security APIs is helpful, but most organizations lack the tools, resources, or time to identify all API vulnerabilities in the development or testing/staging categories. And thus, security teams find it difficult to exert much influence over these first two phases.

Taking a centralized approach to API security provides the efficiency and scale security teams need to identify and address API security risks quickly. By monitoring all web apps and APIs with one security solution, you can centralize responsibility instead of scattering it among multiple app development teams. With a unified view of the attack surface, the security team no longer needs a deep knowledge of each application.

Prevent Adversaries from Exploiting APIs with These Five Best Practices:

☑ **1. Perform API discovery.** Often companies are unaware of the full extent of their API attack surface. They may have deployed undocumented shadow APIs that are not visible to the security team. A vulnerable API opens the door to attacks that can compromise sensitive data, so ongoing API discovery should be performed to inventory all externally exposed APIs.

☑ **2. Rewrite API calls.** Sophisticated attackers find ways to attack APIs even if the underlying API is not visible to the outside world. Malicious actors analyze API structures and identify ways they can exploit API security flaws. You should rewrite API calls so that public-facing components don't reveal clues about the rest of the API that can expose sensitive data.

☑ **3. Detect anomalies.** Machine learning (ML) will model how your APIs are typically used in real life and how your users interact with your app. ML-based anomaly detection improves threat detection and reduces the false positives that drive administrative overhead. ML also helps identify behavior anomalies that can indicate credential stuffing, brute-forcing, or scraping attempts by attackers.

☑ **4. Provide visibility and policy control to the security team.** Deploy centralized API security solutions that enable the security team to see the full API attack surface, set policies, and manage incident response. Give your security team the tools they need to define an API security posture across all exposed applications and to orchestrate security policy changes without touching each application.

☑ **5. Optimize resources.** Provide security practitioners with an API security tool for comprehensive visibility over all APIs to accelerate the ability to identify API vulnerabilities early. You can reduce manual processes by using automation for routine activities such as the configuration of signatures or rules. This frees security practitioners to focus their efforts on establishing proven API security practices instead of being burdened with mundane security tasks.

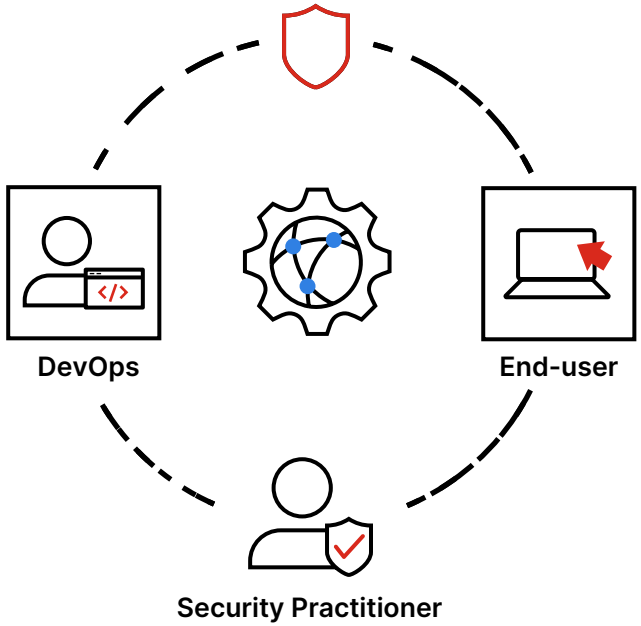
From WAF to WAAP

Organizations deploying API-based applications expose a new attack surface. The traditional WAF evolved into a modern WAF to protect APIs. Gartner refers to the modern WAF as a Web Application and API Protection (WAAP) solution. A WAAP solution protects internet-facing APIs, eliminates alert fatigue without compromising critical data security flowing through your web applications and APIs, and uses ML for advanced protection. Since APIs support critical line-of-business functions, and the number of APIs is growing so rapidly, automation is key with ML. ML learns how apps and users behave, to detect anomalies and minimize false positives. This is essential for protecting APIs that enable B2B communication and support mobile applications. ML is also used to block the full range of malicious bot activity (e.g., content scraping, denial of service, data harvesting, transaction fraud).

Boost Your App and API Defenses

Fortinet's WAAP solution, FortiWeb, takes a multilayered approach to comprehensively protect web apps and APIs. FortiWeb leverages Fortinet's in-house global threat research team, FortiGuard Labs, that monitors and analyzes security threats from various sources. FortiGuard Labs provides near real-time threat intelligence to create signatures and block known malicious sources.

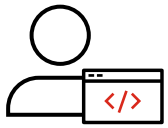
FortiWeb helps DevOps teams deliver new code without delay and enables security practitioners to protect their APIs everywhere they are deployed.



Equip Your Team for Success

Using FortiWeb, DevOps and security practitioners can deliver new software capabilities on time and securely. DevOps pushes code faster to the end-user, and security practitioners protect APIs along the way.

FortiWeb Improves Productivity Across Teams:



DevOps

Push code faster to end-users without slowing down the development process.

Spend more time developing code without worrying about security.

Improve retention by keeping developers doing what they love — writing code.

Security Practitioner

Focus on high-value and meaningful activities using a centralized security solution that protects apps and APIs.

Improve threat detection and reduce the false positives that drive administrative overhead.

Enhance API security by identifying shadow APIs and hiding internal API structures from potential attackers.

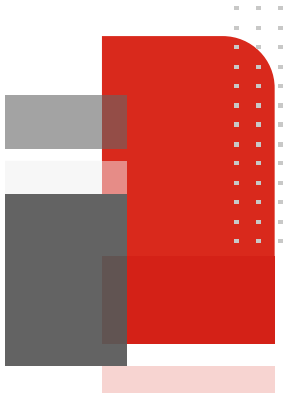
Protect applications from bots to enhance security:

- Block malicious bots without blocking users or interfering with legitimate bot activity such as search engines.
- Lower or eliminate reliance on user verification techniques such as ReCaptcha that degrade the user experience.

Protect Your APIs with FortiWeb

FortiWeb helps businesses speed up their time to market and deliver new apps while maintaining a strong security posture amid growing API sprawl. Fortinet's centralized and comprehensive cybersecurity solution helps organizations release new software capabilities to move fast, stay resilient, and remain competitive.

Learn more about FortiWeb Cloud and test drive it for free



April 2022