Choosing the WAF That's Right for You

A how-to guide

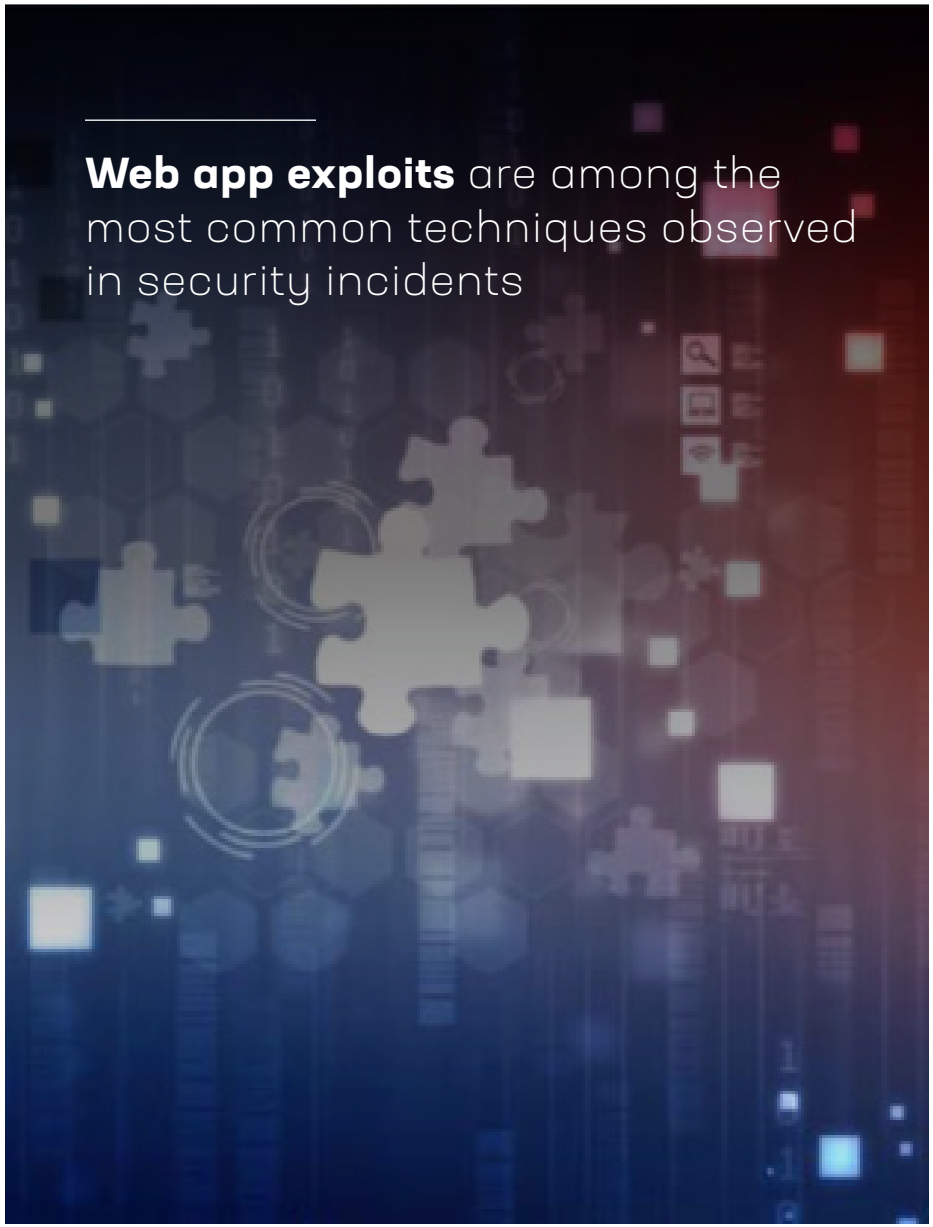
Introduction

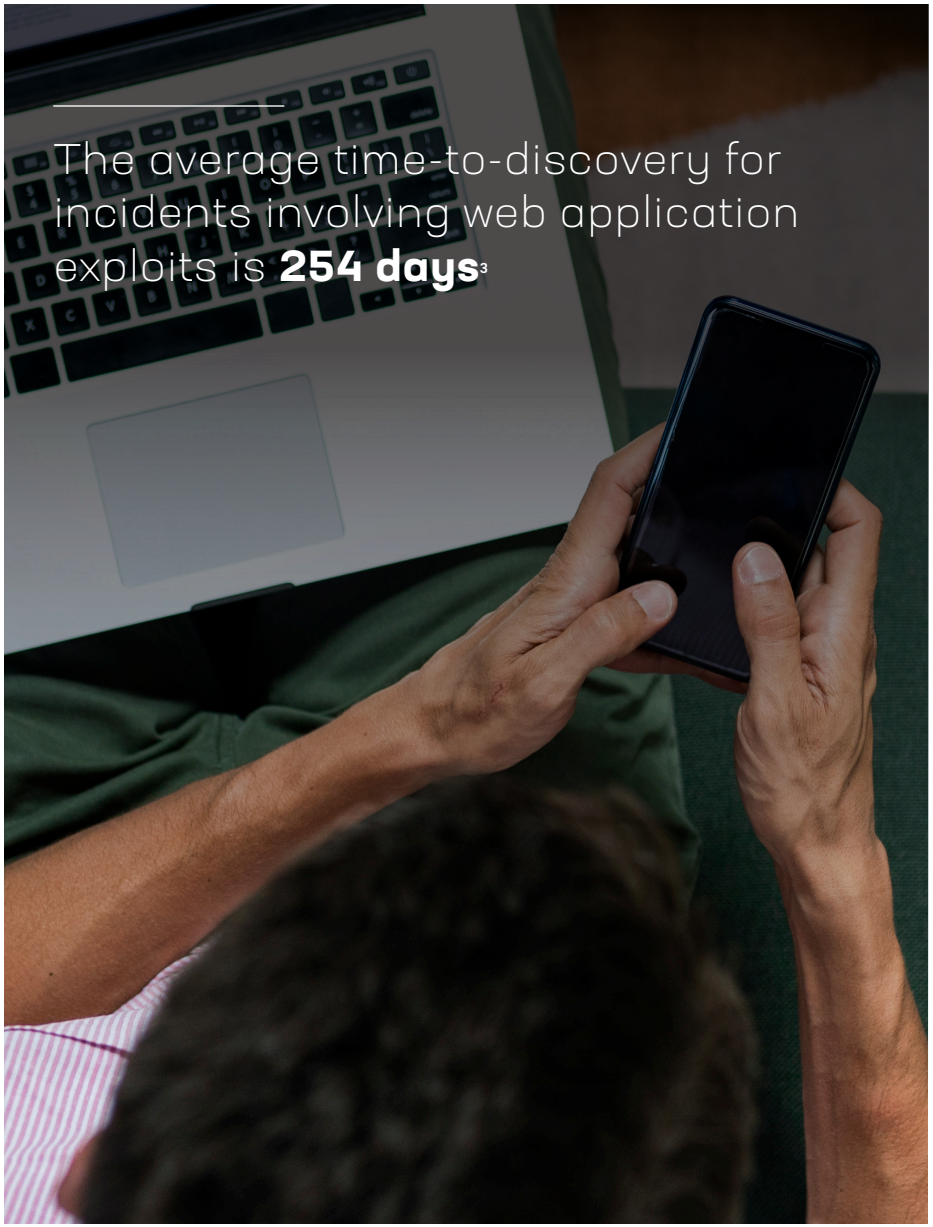
Despite the industry's best efforts to bolster secure application development practices, the growing decentralization of infrastructure has resulted in complex application deployments that are by nature more difficult to protect.

The State of the State of Application Exploits in Security Incidents corroborates what F5 Labs learned from the IRIS-X and Verizon DBIR reports: Web app exploits are among the most common techniques observed in security incidents.[1] This should not be surprising, since today's decentralized multi-cloud environments, third-party integrations, and modern, distributed architectures based on APIs and containers increase complexity that intrinsically put apps at higher risk.

The good news is that there are tools to help shield your apps from risk by mitigating vulnerabilities and preventing compromise—specifically, web application firewalls (WAFs). A WAF provides a stop gap against insecure code and software-level vulnerabilities, and inspects ingress and egress application flows to identify and block malicious traffic while preserving and accelerating the experience for customers. A WAF can also extend security to your APIs and mobile apps, which have become a foundation of modern applications and target for attackers.[2]

Regardless of your application architecture and its respective threat surface, a WAF can be leveraged in a variety of forms to help defend your organization against attacks, including physical and virtual appliances managed by your security teams, cloud-delivered self-service solutions, and dedicated, outcome-based managed services. To help manage the complexity and risk of distributed, multi-cloud apps, Web App and API Protection (WAAP) solutions provide effective security through integrated and easy-to-operate WAF, API security, bot defense, and DDoS prevention technology.





So, Do You Need A WAF? It Depends On Several Factors

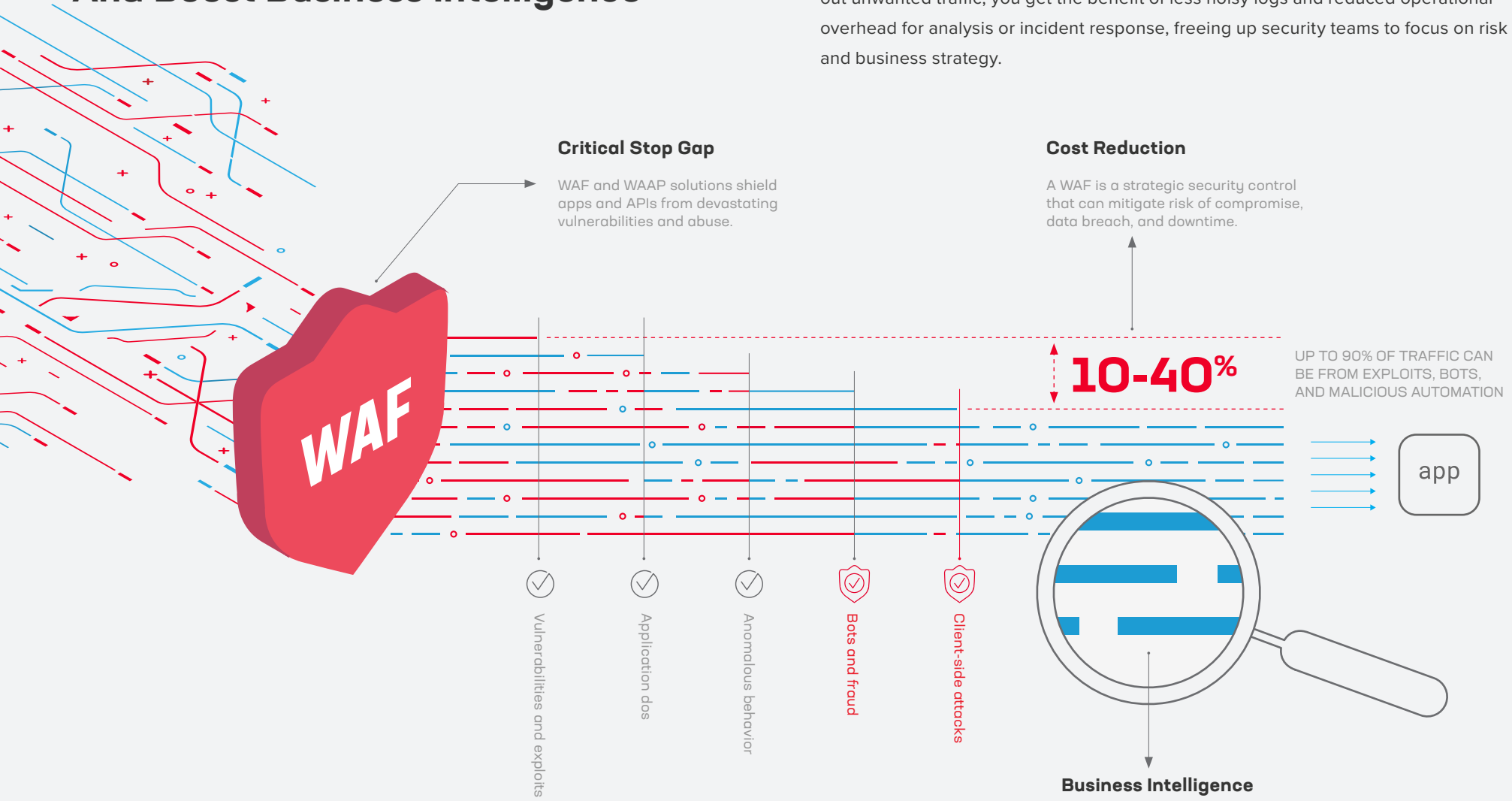
- **Do you have public-facing web or mobile apps?**
- **Do you have overwhelmed or strained security teams?**
- **Do you have compliance obligations?**
- **Do you have software stacks that are difficult to upgrade?**
- **Do you leverage third-party APIs or ecosystem integrations?**
- **Do you maintain legacy and modern web apps?**
- **Do you need some breathing room from zero-day exploits?**
- **Do you want to streamline security policy and testing through CI/CD pipeline integration?**

If you answered “yes” to any of these questions, consider WAF technology when you plan to protect your apps, your brand, and your business from compromise, data breach, and downtime.

As with any good tool, there are lots of options—and different solutions work better for different situations.

A WAF Can Reduce Operating Costs And Boost Business Intelligence

Deploying a WAF in front of your apps and APIs can save you money while making it easier to get the data-driven insights your business requires. Since a WAF filters out unwanted traffic, you get the benefit of less noisy logs and reduced operational overhead for analysis or incident response, freeing up security teams to focus on risk and business strategy.



1. Can Security Tools Add Real Business Value?

It can be hard to justify spending money on security solutions. Sure, we all know we should have robust defensive measures; and we hope we'll be protected if we get attacked. But you never know if you're going to be attacked, much less whether that firewall or IPS will be able to effectively protect your business if you do. This is especially true when it comes to exploits that target application vulnerabilities, which, left unaddressed, can allow cyberattackers to take over websites and online applications, steal money, harvest data, and access customer accounts.[4] While security is often regarded as a necessary evil with no quantifiable ROI, clearly that is no longer the case in the new digital economy.

In the era of cloud computing and big data, security solutions can actually provide business value by mitigating risk and reducing costs—saving you money and helping you optimize your web applications and digital properties. Effective WAF solutions can filter malicious traffic, helping you differentiate between bots and attackers looking to exploit new application vulnerabilities and real customers trying to transact. This is important because as more and more commerce shifts online, delivering secure digital experiences will become the vehicle for customer and revenue growth.[5]

If you use a WAF to shield your apps and APIs from a variety of attacks, you'll be able to optimize your web properties, resulting in a significant cost savings, by ensuring that you're only serving your current and potential customers. That means that your security tools are providing real value by helping you control your costs and protect your brand.

In the world of cloud computing and big data, **security solutions can actually save you money.**

In addition, your customer interaction data will be further refined, resulting in stronger business intelligence. When you have solid, actionable data that you trust, you'll be in a better position to market effectively to your real customers.

Options to Consider:

Self-Managed

Deployed on premises or in a cloud environment, a self-managed WAF gives you control to protect your applications as you see fit while leveraging a robust set of security defenses. A self-managed WAF supports any application architecture, from legacy three-tier web stacks to containers, and adds real business value by blocking emerging threats without constraining app team innovation.

Cloud-Delivered (Saas)

An as-a-service WAF enables you to cut costs and operating overhead while maintaining high security effectiveness. With a similar feature set as an on-premises WAF, this option provides out-of-the-box protection from application vulnerabilities, reducing risk and remediation costs. Cloud-delivered WAAP includes integrated WAF, API security, bot defense, and DDoS prevention technology to deliver consistent security across clouds and architectures.

2. Do You Want To Manage Your Business–Or Manage Your Security Solutions?

According to the F5 State of Application Strategy in 2021 Report,[6] IT is evolving from supporter to enabler to business partner. Security is becoming a competitive advantage for delivering digital experiences quickly and safely. However, a longstanding cybersecurity skills gap has been exacerbated by the challenge of maintaining consistent security across all application architectures—in many cases, across multiple cloud providers that host both legacy and modern apps. Plus, certain threat vectors—especially attacks targeting common software packages or digital integrations—are becoming commonplace. The problem is that unless you've got a security team with unlimited resources, you probably don't want to spend all your time managing the minutia of the many application security risks out there.

You likely want a security solution that just works, so you can focus on other business-critical objectives.

Fortunately, there are WAF options that allow you to do that. Even more good news—deploying a cloud-delivered WAAP solution provides the technical controls necessary to protect against many threats that lead to data breaches, including attacks in the OWASP Top 10, automated threats like credential stuffing, and denial-of-service that evades traditional network-based defenses—without straining precious security team resources.

It's clear that deploying a WAF can help protect your apps, but different deployment methods are better for different organizations. Fortunately, there are multiple options.

If you are looking for a security solution that just works, **a variety of options provide that.**

Options to Consider:

Cloud-Delivered (Saas)

Easily activate a SaaS WAF for robust protection and minimal false positives. Without infrastructure overhead like hardware or software or updates to manage, this is a perfect fit for letting your dev teams integrate security with little effort. Cloud-delivered WAAP provides integrated WAF, API security, bot defense, and DDoS prevention to deliver consistent security across clouds and architectures in a self-service model.

Managed Service

Protect your web apps and APIs from ever-evolving threats with continuous monitoring and oversight. Augment (or replace) your own in-house resources with a service that's wholly set up, deployed, and maintained by experts in a 24x7x365 Security Operations Center (SOC).

3. Do You Want To Go Beyond Basic Regulatory Compliance?

Many organizations feel comfortable with their existing security posture but might be considering WAF technology as a result of a compliance mandate or audit finding. Several different entry-level WAFs can certainly help you check that box and fulfill the lowest-common-denominator requirements, but organizations that go this route often find that deploying such basic measures comes at a cost. Specifically, risk of compromise, fines, and tarnished brand.

Basic WAFs may help you pass an audit, but they're not built with operational manageability in mind and often cause more headaches than they cure (that is, false positives or, worse, false negatives). Also, because they don't offer the full feature set of an advanced WAF, you may not find that you're fundamentally better protected—despite the level of investment you made.

There's a better way. If you need a WAF to meet compliance requirements or check a box from an audit perspective, why not get one that provides more than a modicum of protection? An effective WAF allows you to meet your compliance requirements while also giving you the visibility you need to properly assess your actual vs. perceived risk. And given that a 2021 study[7] found a 259% increase in the use of open source software and that 84% of code bases contain at least one vulnerability, this risk is not theoretical.

A WAF allows you to meet your compliance requirements while also giving you the additional security and visibility you need.

Options to Consider:

Self-Managed or Cloud-Delivered (SaaS)

These options may be implemented and managed by your team directly in traditional or CI/CD pipeline-driven environments, or delivered through a self-service WAAP platform. Regardless, you get fine-grained analytics, ensuring that you're not just passing your audits—you're actually increasing the security posture and competitiveness of your business.

Managed Service

The most hands-off option, of course, is one where you don't have to worry about your WAF's compliance obligations or the security of your apps and APIs. That responsibility is offloaded to the team of experts protecting your business from attacks—providing continuous monitoring and protection for your entire application portfolio.

4. Do You Want To Get A Handle On Bot Traffic While Focusing On Your Customers?

Even if you already have a strong, secure application development process in place and reasonable confidence in the security of the apps you've deployed, you're likely contending with another problem—a large percentage of traffic to your site or APIs is probably coming from automation or bots. While this traffic may look legitimate at first glance, clicks from bots are not the same as clicks from humans. Unwanted and unprofitable traffic can skew your analytics and distort your market intelligence by flooding your systems with spurious data.

In addition, attackers have embraced automation to scan your applications for vulnerabilities, attack business logic such as logon, create account, and add to cart functions, and inflict denial of service (DoS). Increasingly, attackers inject malicious scripts directly into the browser to avoid detection by centralized security solutions.[8] By deploying an advanced WAF and integrating specialized anti-bot, anti-fraud, and client-side protection technology, you can focus on serving your real customers without burdening your security teams.

WAF can mitigate the effects of malicious bots, automation, and scripts.

Options to Consider:

Self-Managed

Deploy proactive protection to defend your apps against bots that scan for application vulnerabilities, launch denial-of-service attacks, scrape your content, and attempt to compromise customer accounts through brute-force attacks—before they harm your business's reputation.

Cloud-Delivered (Saas)

Cloud-delivered WAAP provides specialized technology to mitigate bots and abuse from automated attacks that exploit business logic intended to enable your customers to transact and your business to collect revenue.

Managed Service

Protect your web apps from bot-based threats while receiving 24x7x365 monitoring and support. By identifying malicious bots and automation that bypass traditional detection methods, an outcome-based service can also protect against fraud from account takeover (ATO), new account creation and loyalty abuse, inventory hoarding, and more.

5. Do You Know About Your APIs, And Are They Secure?

Because of the business value unlocked through partnerships and integrations, virtually all new applications leverage APIs. This improves time to market and allows organizations to quickly enhance digital capabilities—but introduces significant unintended risks and opportunities for API abuse.

API security needs to be implemented at strategic points within the development pipeline. An advanced WAF can protect APIs from exploits, abuse, and misconfiguration, and a cloud-delivered WAAP service can dynamically discover and protect APIs with automated and adaptive security.

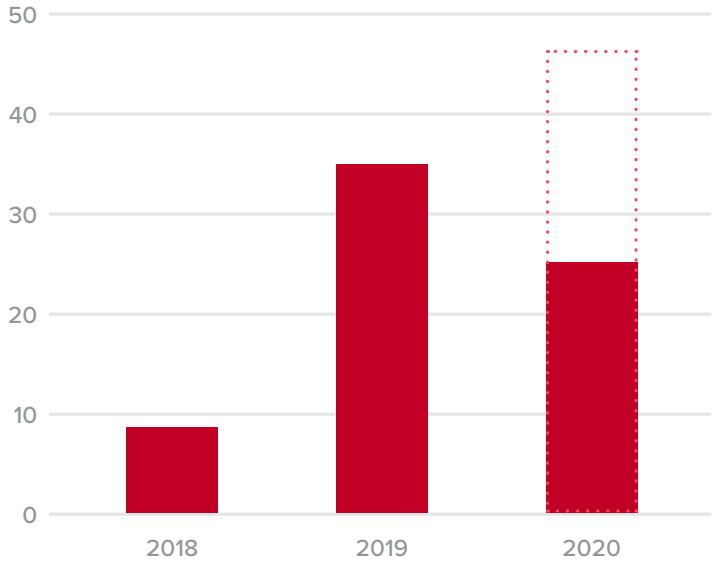


Figure 1: API incidents, 2018–mid-2020. At the current rate, a greater number of API incidents will occur in 2020 than in the previous two years combined.[3]

Options to Consider:

Self-Managed

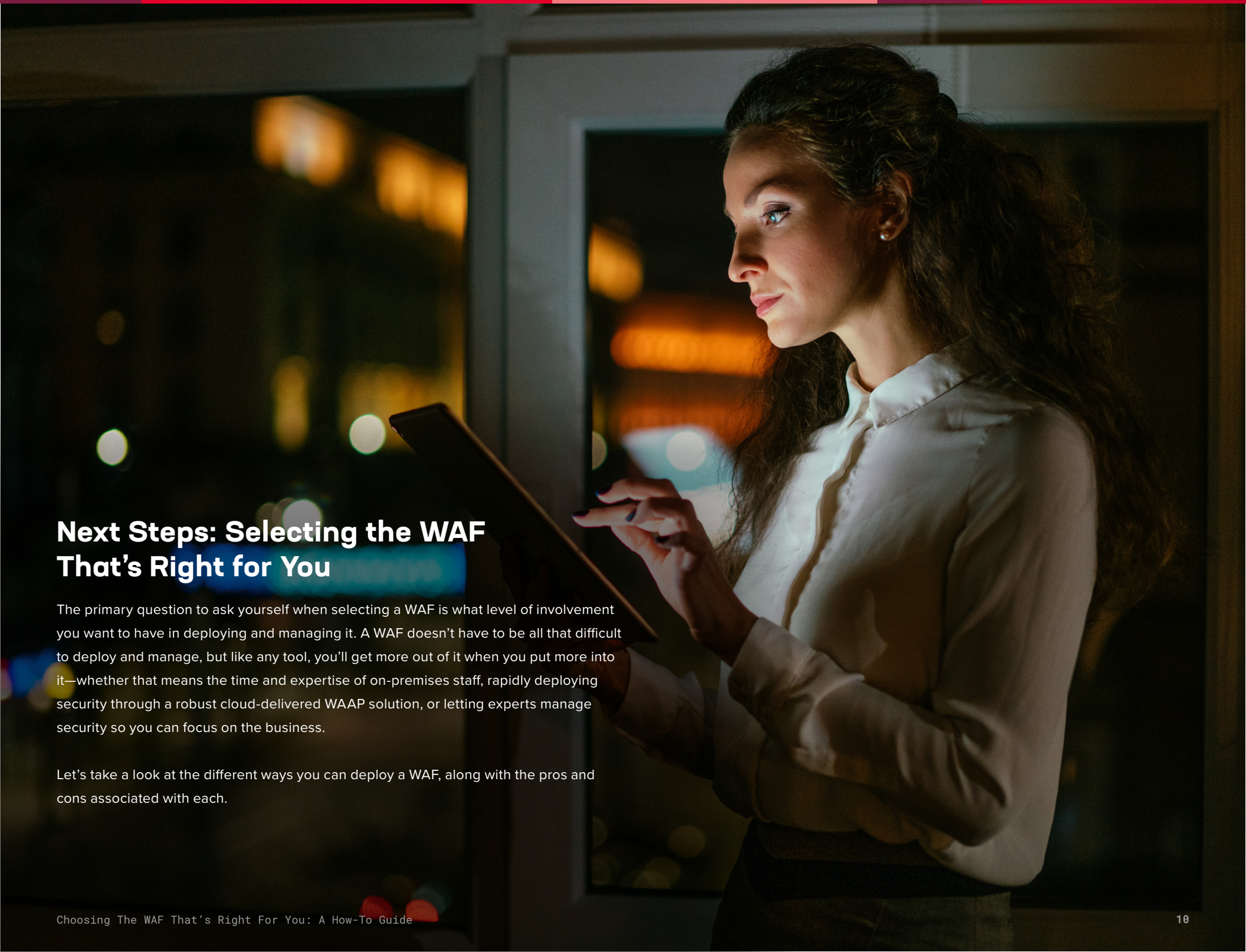
Provide robust protection against exploits and abuse while automating the creation of custom rules specific to each exposed API. An advanced WAF deployed in front of your application or integrated into a distributed containerized infrastructure allows you full control of API security and access policy.

Cloud-Delivered (Saas)

Cloud-delivered WAAP provides dynamic API discovery, automated protection, and adaptive security with visibility across architectures and consistent schema enforcement.

Managed Service

Automatically ingest published API configuration files and protect your integration ecosystem with 24x7x365 monitoring for your applications and their associated APIs—extending your security team with experts that help manage unintended risk.



Next Steps: Selecting the WAF That's Right for You

The primary question to ask yourself when selecting a WAF is what level of involvement you want to have in deploying and managing it. A WAF doesn't have to be all that difficult to deploy and manage, but like any tool, you'll get more out of it when you put more into it—whether that means the time and expertise of on-premises staff, rapidly deploying security through a robust cloud-delivered WAAP solution, or letting experts manage security so you can focus on the business.

Let's take a look at the different ways you can deploy a WAF, along with the pros and cons associated with each.

WAF Deployment Modes

	PROS	CONS
Managed Service	Choose this option if you prefer to focus on the business and leave the protection of your applications and APIs to the experts. A collective defense network with highly trained AI and continuous oversight provides maximum efficacy in addition to access to always-on experts.	Although fully managed service offerings reduce risk by partnering with experts for dedicated support and continuous oversight, you may not have as much architectural flexibility. Some offerings might not give you direct administrative control over your security policies. This is typically a more expensive option; however, it should still be cheaper than hiring the full-time staff required to keep your applications secure.
Self-Managed	Provide flexibility while retaining control of your traffic management and security policy settings. This option can help meet your most stringent security demands with architectural flexibility, high performance, and granular security controls.	The self-managed model requires involvement from your security team and app owners to deploy and build the security policies that should apply to your applications, but the investment will pay dividends for those needing the flexibility this model provides.
Cloud-Delivered	This is one of the easiest ways to protect applications and APIs. Rapid deployment, dynamic API discovery, and automated protections allow you to deploy consistent security policy that adapts to changing apps and attacks in an easy-to-operate and cost-effective self-service model.	Depending on your organization's staff, you may benefit from the continuous monitoring and bespoke protection of a managed service that maximizes business outcomes.

Conclusion

While the choices may seem daunting, there's never been a better time to shop for a solution to secure your applications and APIs. WAF technology is now more accessible, affordable, and manageable than ever before—which is good, because companies need the protection a WAF offers more than ever to deliver secure customer experiences and get ahead in the digital economy.

For more information about choosing the WAF that's right for you, visit f5.com/security.

Appendix

[1] https://www.f5.com/labs/articles/threat-intelligence/the-state-of-the-state-of-application-exploits-in-security-incidents

[2] https://www.f5.com/labs/articles/threat-intelligence/2020-apr-vol1-apis-architecture

[3] https://www.f5.com/labs/articles/threat-intelligence/the-state-of-the-state-of-application-exploits-in-security-incidents

[4] https://www.f5.com/labs/articles/threat-intelligence/explaining-the-widespread-log4j-vulnerability

[5] https://www.f5.com/solutions/the-new-business-imperative

[6] https://www.f5.com/state-of-application-strategy-report

[7] https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html

[8] https://www.f5.com/company/blog/holiday-formjacking

THINK APP SECURITY FIRST

Always-on, always-connected apps can help power and transform your business–but they can also act as gateways to the data beyond the protections of your firewalls. With most attacks happening at the app level, protecting the capabilities that drive your business means protecting the apps that make them happen.

Find more security resources at **f5.com/solutions**

US Headquarters: 801 5th Ave, Seattle, WA 98104 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com
©2022 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com.
Any other products, services, or company names referenced herein may be trademarks of the irrespective owners with no endorsement or affiliation, expressed or implied, claimed by F5. EBOOK-SEC-798087620