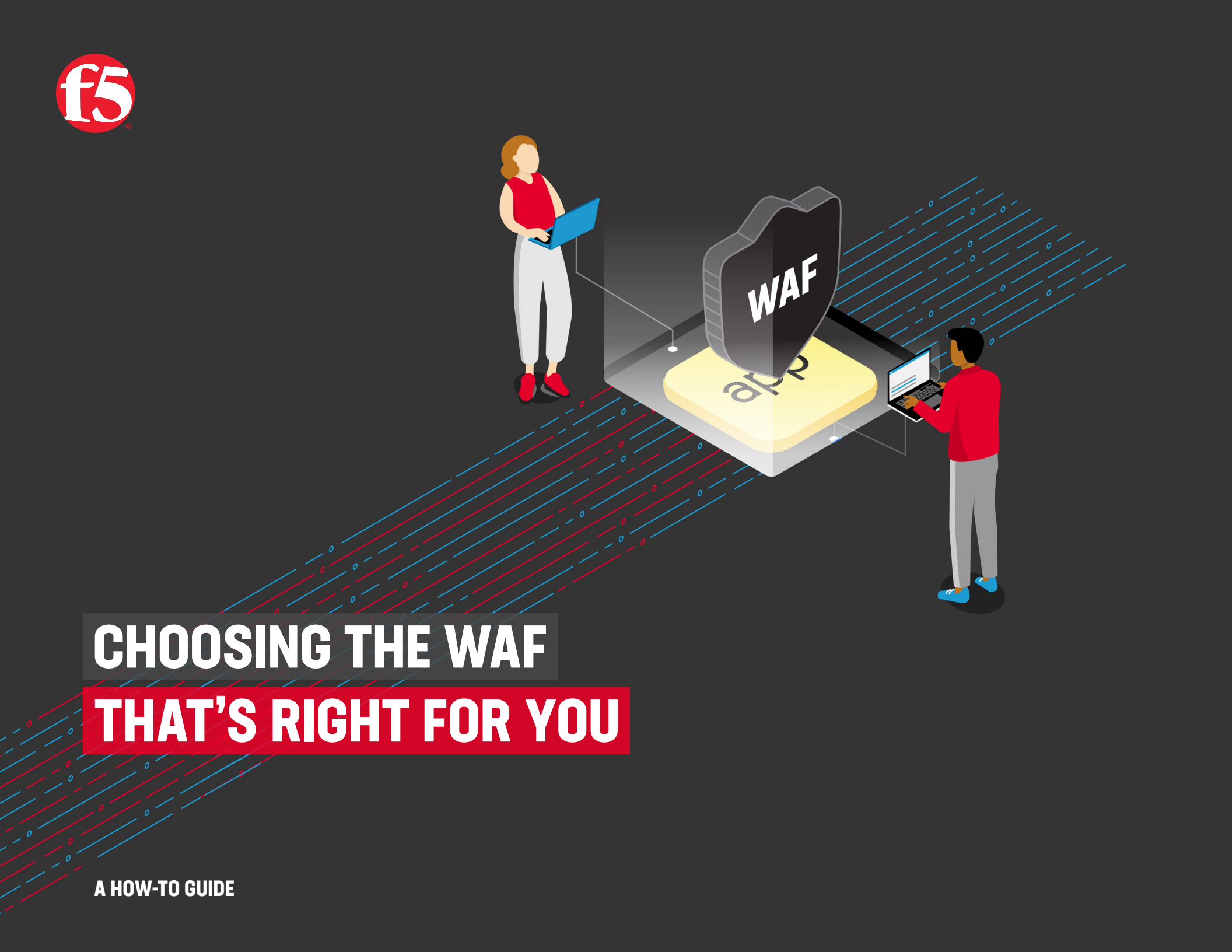



# CHOOSING THE WAF THAT'S RIGHT FOR YOU

A HOW-TO GUIDE

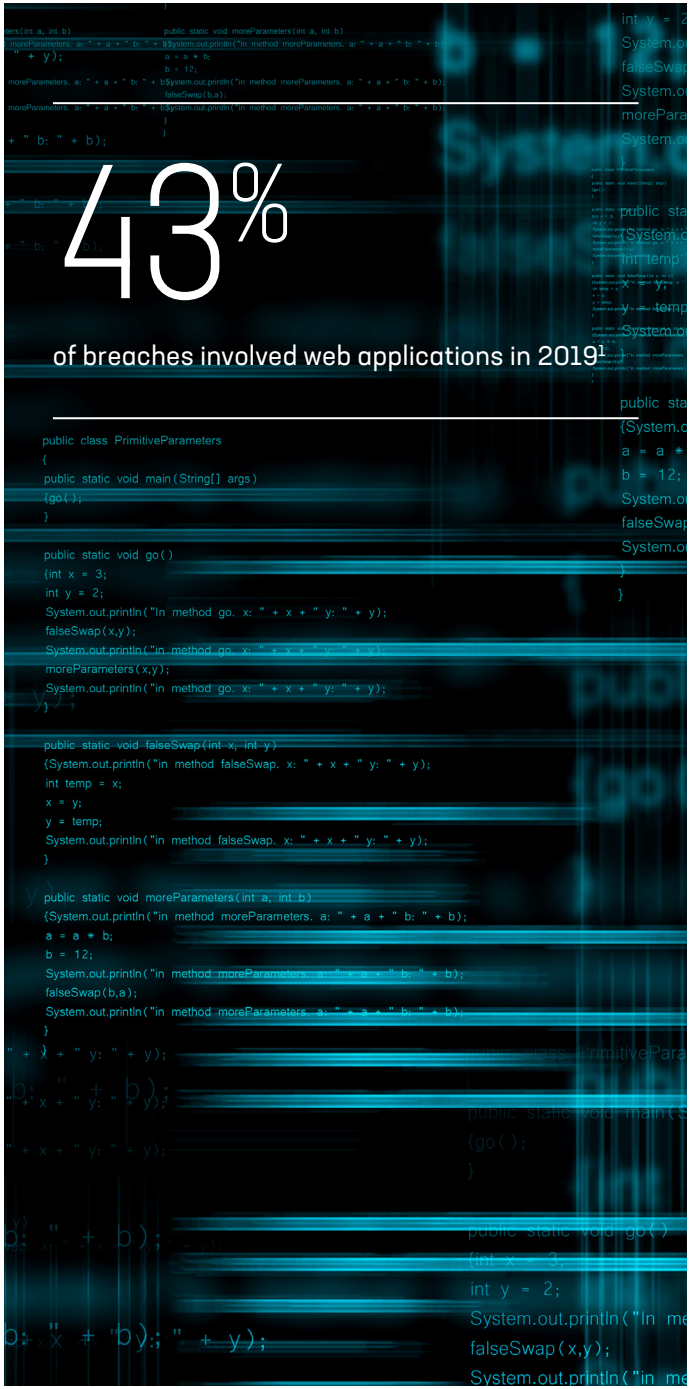
# INTRODUCTION

**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.**

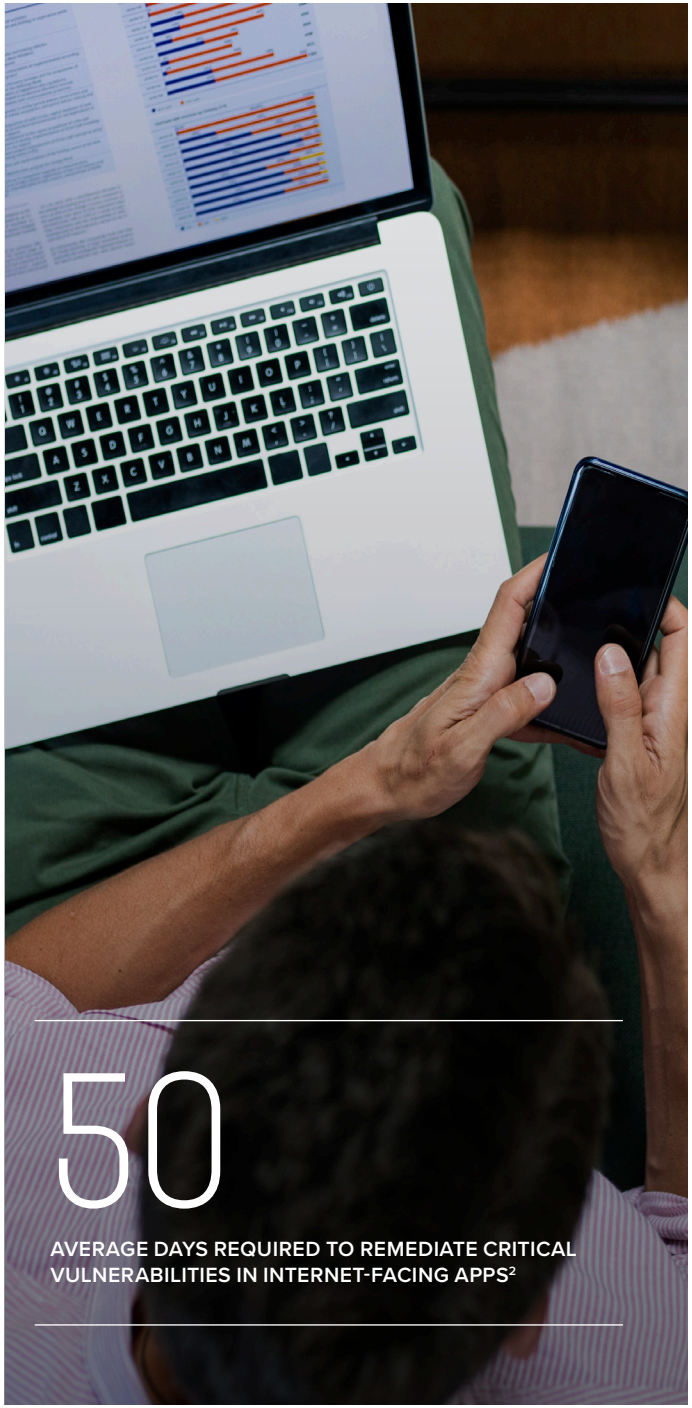
The Verizon 2020 Data Breach Investigations Report reveals that in 2019, nearly half of all breaches involved web applications. This should not be surprising, since today's decentralized multi-cloud environments, third-party integrations and content, and new architectures such as serverless and container environments require complicated deployments that intrinsically put apps at risk.

The good news is that there are tools to help you bolster your apps against breaches by mitigating vulnerabilities and stopping attacks—specifically, web application firewalls (WAFs). A WAF provides virtual patching for code and software-level vulnerabilities, but it also inspects ingress and egress application traffic to identify and block scanners, attackers, and bots while preserving and accelerating apps for legitimate users. A WAF can also provide security to your APIs, which have become foundational in the building of modern applications and are a favorite target of attackers (with much success).

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. Those forms include a physical or virtual appliance managed by you, cloud-delivered, containerized, or outsourced to a dedicated managed service.




[1] https://enterprise.verizon.com/resources/reports/dbir/



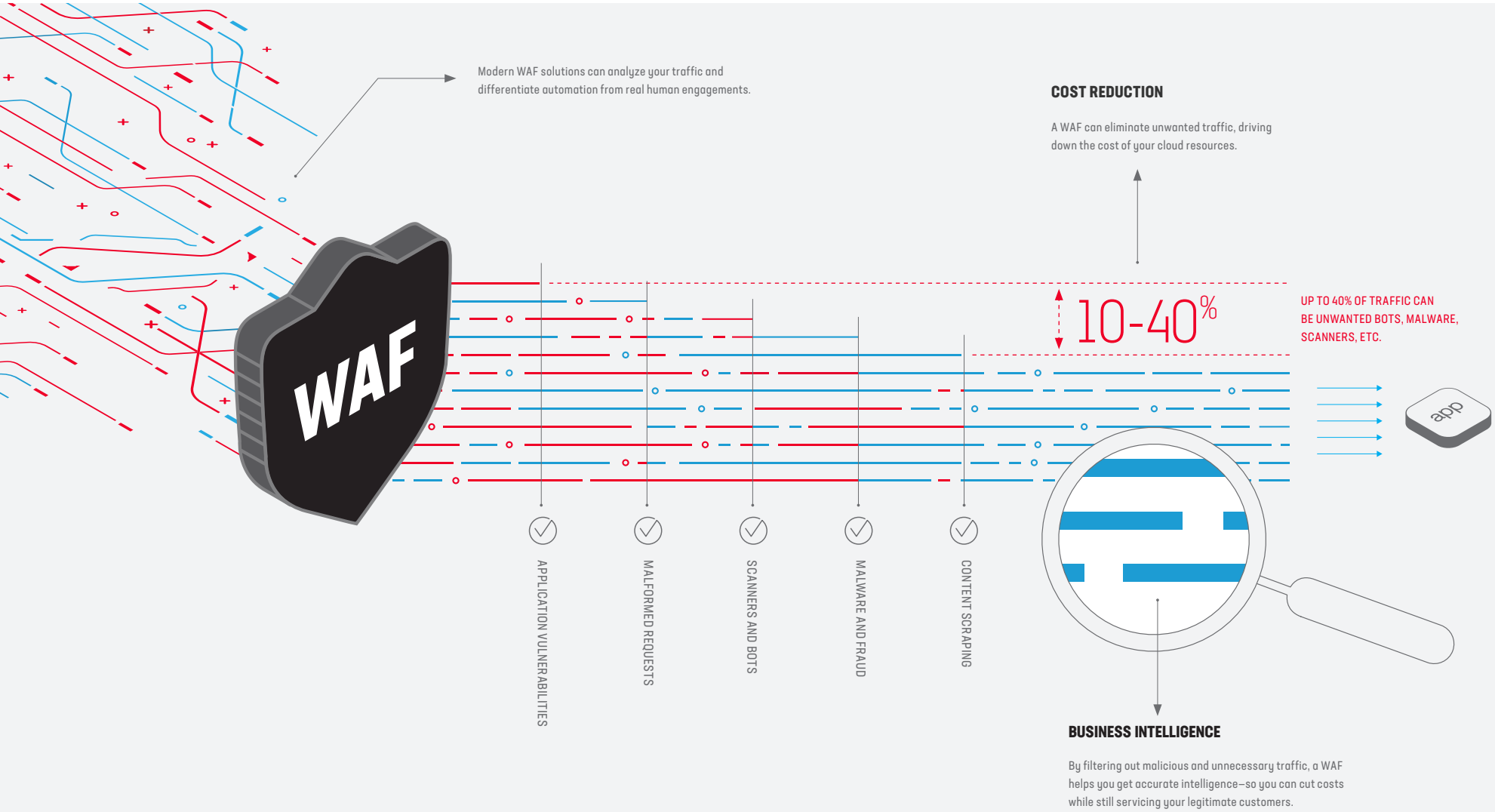

## SO, DO YOU NEED A WAF? IT DEPENDS ON SEVERAL FACTORS.

- Do you have a public-facing web property or mobile application?
- Do you have a high-sensitivity web property or mobile application?
- Do you deal with bots and unwanted automated traffic?
- Do you have compliance obligations?
- Do you have software stacks that are difficult to upgrade?
- Do you need API security?
- Do you leverage legacy web apps?
- Do you need some breathing room from zero-day attacks?
- Do you want to reduce your development time to market through CI/CD pipeline integration?

If you answered "yes" to any of these questions, consider WAF technology when you plan how to protect your apps, your data, and your business from application attacks and data breaches.

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

[2]https://techbeacon.com/security/30-app-sec-stats-matter




## A WAF CAN REDUCE CLOUD COSTS AND BOOST BUSINESS INTELLIGENCE

Deploying a WAF in front of your cloud-based app can save you money while making it easier to get the data-driven insights your business requires. As a WAF filters out unwanted traffic, you also get the benefit of less noisy logs and reduced operational overhead for analysis or incident response.

A few more key questions can help you choose the WAF deployment model that's right for your business, with the WAF features most valuable for your organization.

# 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 network if you do. Security is often regarded as a necessary evil with no quantifiable ROI, but that doesn't always have to be the case.

In the world of cloud computing and big data, good security solutions can actually save you money by helping you optimize your web applications and digital properties—and they can do it while still protecting your business from attacks. Modern WAF solutions can filter your traffic, helping you better differentiate between automated bots and actual humans. This is important because as more and more cloud-based service providers offer a utility billing model, bot traffic can drive up your infrastructure costs without providing any business value.

If you use a WAF to eliminate much of that bot traffic, you'll be able to optimize your web properties for your intended customer base by reducing useless or malicious traffic, resulting in a significant cost savings. You can ensure that you're only serving your real and potential customers. That means that your security tools are providing real value by helping you control your costs in the cloud.

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 full, granular control so you can tune it to best protect your applications. A WAF that supports any application architecture, whether traditional or containerized, adds real business value beyond acting as an insurance policy in case of a breach. Block emerging threats with dynamic signatures to allow your security to adapt to the threat landscape.

### CLOUD-DELIVERED (SAAS)

An as-a-service WAF enables you to cut costs and operating overhead, providing great business value. 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.

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

# 2 DO YOU WANT TO MANAGE YOUR BUSINESS– OR MANAGE YOUR SECURITY SOLUTIONS?

According to the F5 2020 State of Application Services Report, 71% of organizations report a skills gap in security. A shortage in skills to operate the necessary security tools can justifiably weaken confidence in how well those tools will safeguard confidential data. The skills gap is further exacerbated by the challenge of providing security parity across all application architectures and infrastructures—in many cases, across multiple cloud providers. Plus, certain threat vectors—especially attacks targeted against a specific company or digital property—can be challenging to deal with. 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: According to the 2019 F5 Labs Application Protection Report, deploying a WAF provides the technical controls necessary to protect against many threats that lead to data breaches like injection attacks or credential stuffing.

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.

## OPTIONS TO CONSIDER:

### CLOUD-DELIVERED (SAAS)

Easily activate an SaaS WAF so your applications can be instantly protected from thousands of threats identified by F5 and corroborated with probability scores to minimize 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.

### MANAGED SERVICE

Protect your web apps and data from ever-evolving threats while receiving 24x7 support. Augment (or replace) your own in-house resources with a service that's wholly set up, deployed, and maintained by certified experts in a Security Operations Center who are constantly monitoring your traffic.

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

# 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.

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 a robust 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? A good WAF allows you to meet your compliance requirements while also giving you the additional visibility you need to properly assess your actual vs. perceived risk. And given that a 2019 study found that 75% of organizations' codebases contained vulnerabilities (n=1,253), the results may surprise you.

## OPTIONS TO CONSIDER:

### SELF-MANAGED OR CLOUD-DELIVERED (SAAS)

These options may be implemented and managed by your team directly in traditional or automation pipeline-driven containerized environments, or partially managed through an as-a-service offering. Regardless, you get fine-grained analytics, ensuring that you're not just passing your audits—you're actually increasing the security posture 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. That responsibility is offloaded to the team of experts protecting your applications from attacks—providing real protection on top of compliance requirements.

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

# 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 web traffic to your site or web service 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 account credentials, or inflict denial-of-service (DoS) attacks. By deploying an advanced WAF with proactive bot defenses, you can adapt to automated attacks by leveraging a combination of challenge- and behavior-based techniques to identify and stop bot traffic. This is good news for businesses struggling to manage ever-increasing bot activity on their digital properties. Adaptable WAF technology can help you offload this onerous duty, so you can focus on serving your real customers.

## OPTIONS TO CONSIDER:

### SELF-MANAGED

Deploy proactive bot protection to defend your apps against layer 7 DoS attacks, web scraping, and brute-force attacks—before they harm your business's reputation.

### MANAGED SERVICE

Protect your web apps from bot-based threats while receiving 24x7 support. By identifying malicious bots that bypass standard detection methods, a cloud-based solution can also protect against application fraud like account takeover, new account creation abuse, loyalty account fraud, and more.

Adaptable WAF technology can mitigate the effects of unwanted bot traffic.

# 5 DO YOU KNOW ABOUT YOUR APIS, AND ARE THEY SECURE?

Because of the true business value in unlimited partnerships and integrations, virtually all new applications are built with accessibility via an API. But if the rapidly growing volume of recorded incidents due to misconfigured APIs is any evidence, APIs need to be prioritized for protection.

API management and security need to be implemented at strategic points within the development pipeline. To ensure all APIs are secured, automate the publishing of your Swagger or OpenAPI files to the WAF so protection can be integrated from the start. A full-featured WAF can protect APIs from all of the common web attacks, such as injection or cross-site scripting, but can also handle additional attacks on server resources by restricting exposure, enforcing protocol conformance, and rate limiting.

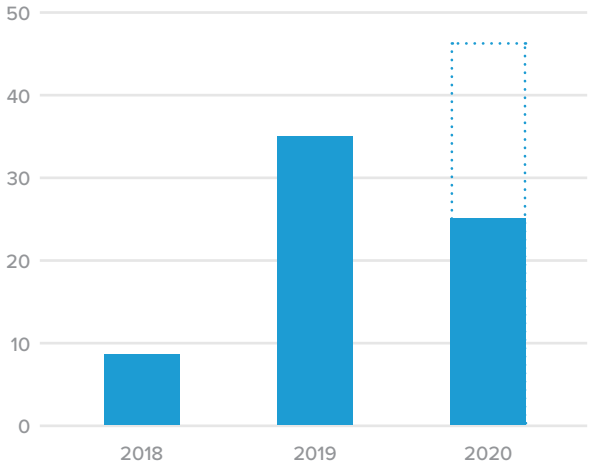



**Figure 1**: API incidents, 2018–mid-2020.
At the current rate, a greater number of API incidents will occur in 2020 than in the previous two years combined.[3]

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

## OPTIONS TO CONSIDER:

### SELF-MANAGED

A WAF can protect APIs from all the same attacks that web applications face, but it needs to automate the creation of custom rules specific to each exposed API. An advanced WAF deployed in front of your application or integrated into several components of a containerized application can allow you to manage API security effectively.

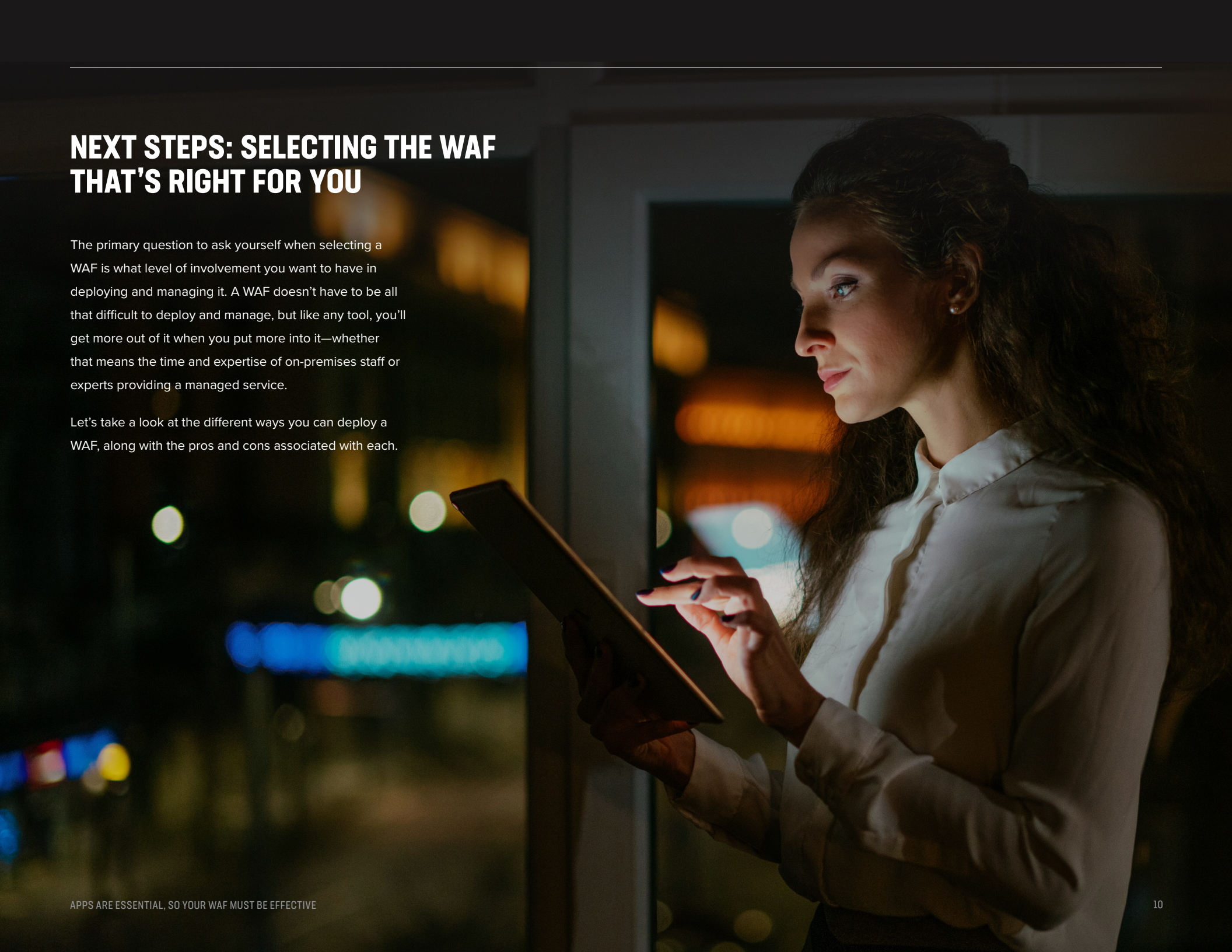
### MANAGED SERVICE

A similar integration can apply to a managed service scenario, with the managed service automatically ingesting published API configuration files. As a result, you'll get 24x7 protection and support for your applications and their associated APIs. Close attention to application health and performance ensures that policy changes can be made as necessary by the resident experts.

# 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 or experts providing a managed service.

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 are looking for the fastest, most hassle-free way to get WAF, DDoS, and fraud defenses in front of your applications. This can also be the best option for detecting and stopping application fraud as intelligence based on attack profiles and risk surfaces provides maximum efficacy in addition to the always-on experts. | Although fully managed as-a-service offerings can get you up and running faster than other models, 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 and security policy portability for multi-cloud deployments, while retaining control of your traffic management and security policy settings. This option can help meet all your most demanding deployment modes where architectural flexibility, performance, and advanced security concerns are paramount. | 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 get started with a WAF in the cloud. Auto-provisioning allows you to deploy a security policy that meets your needs in an easy and cost-effective fashion to get instant protection. | Depending on your application's architecture, this model may not provide as much architectural flexibility as others. |

# CONCLUSION

While the choices may seem daunting, there's never been a better time to shop for a web application firewall. WAF technology is now more accessible, affordable, and manageable than ever before—which is good, because companies need the protection a WAF offers now more than ever, too.

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

## 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