APPS ARE ESSENTIAL
SO YOUR WAF MUST BE EFFECTIVE

THE IMPORTANCE OF APPLICATIONS—AND A WAF TO PROTECT THEM—TO BUSINESS TODAY

INTRODUCTION

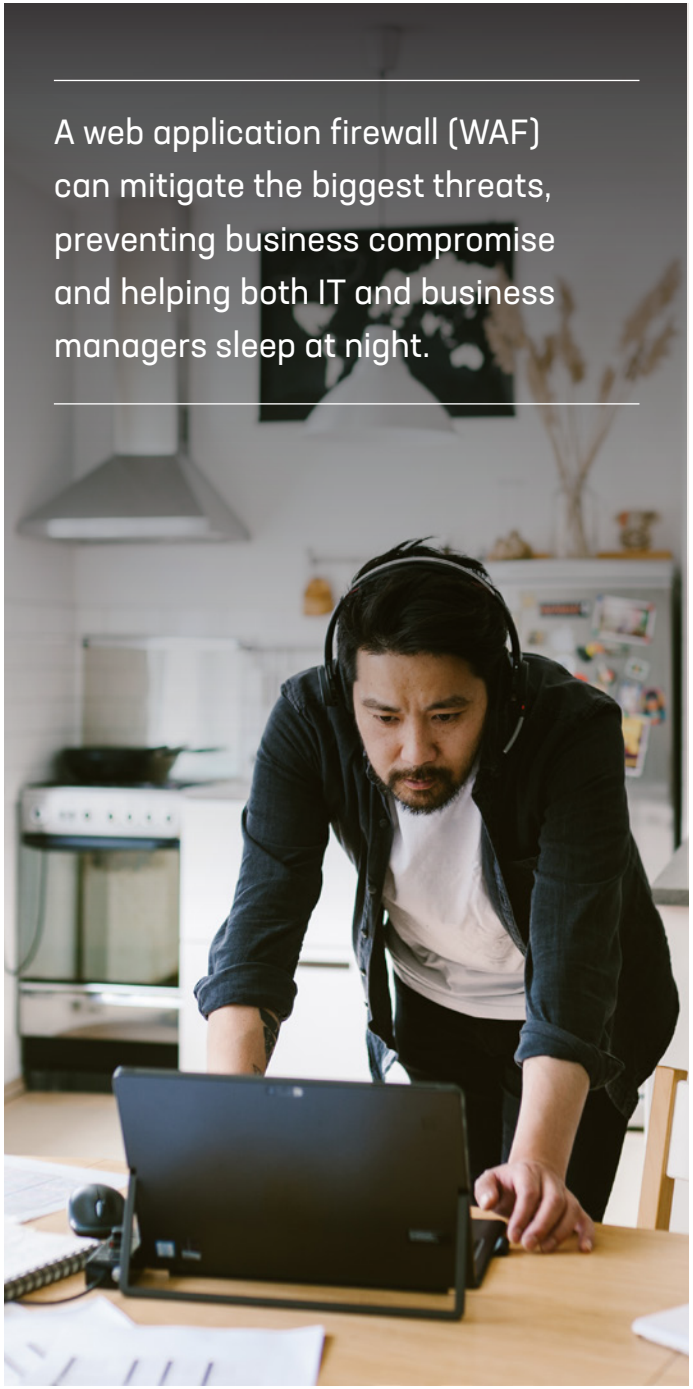
You can't run a business today without applications–whether that means serving customers who want to order online, enabling employees who need to work remotely, or allowing partners to interact with your logistics, financial, or workforce records.

Time to market, revenue, and even an organization's competitive advantage all hinge on the ability for people to quickly and easily interact with applications that do what they need to do without fail.

The flip side? Applications are a primary target for attackers. IT has to make sure the applications people use every day can be accessed reliably—without fear of compromise. And they need to do it while applications are evolving fast across a plethora of architectures, and while attackers are adapting to bypass security controls.

Providing visibility and consistency is challenging for security teams. It also increases the risk of negative business outcomes—from downtime and lost revenue to data breaches to loss of customer trust. For these reasons, threats to applications have become the single biggest risk to business success.

Fortunately, there are things you can do about it. A web application firewall (WAF) can mitigate the biggest threats, preventing business compromise and helping both IT and business managers sleep at night.



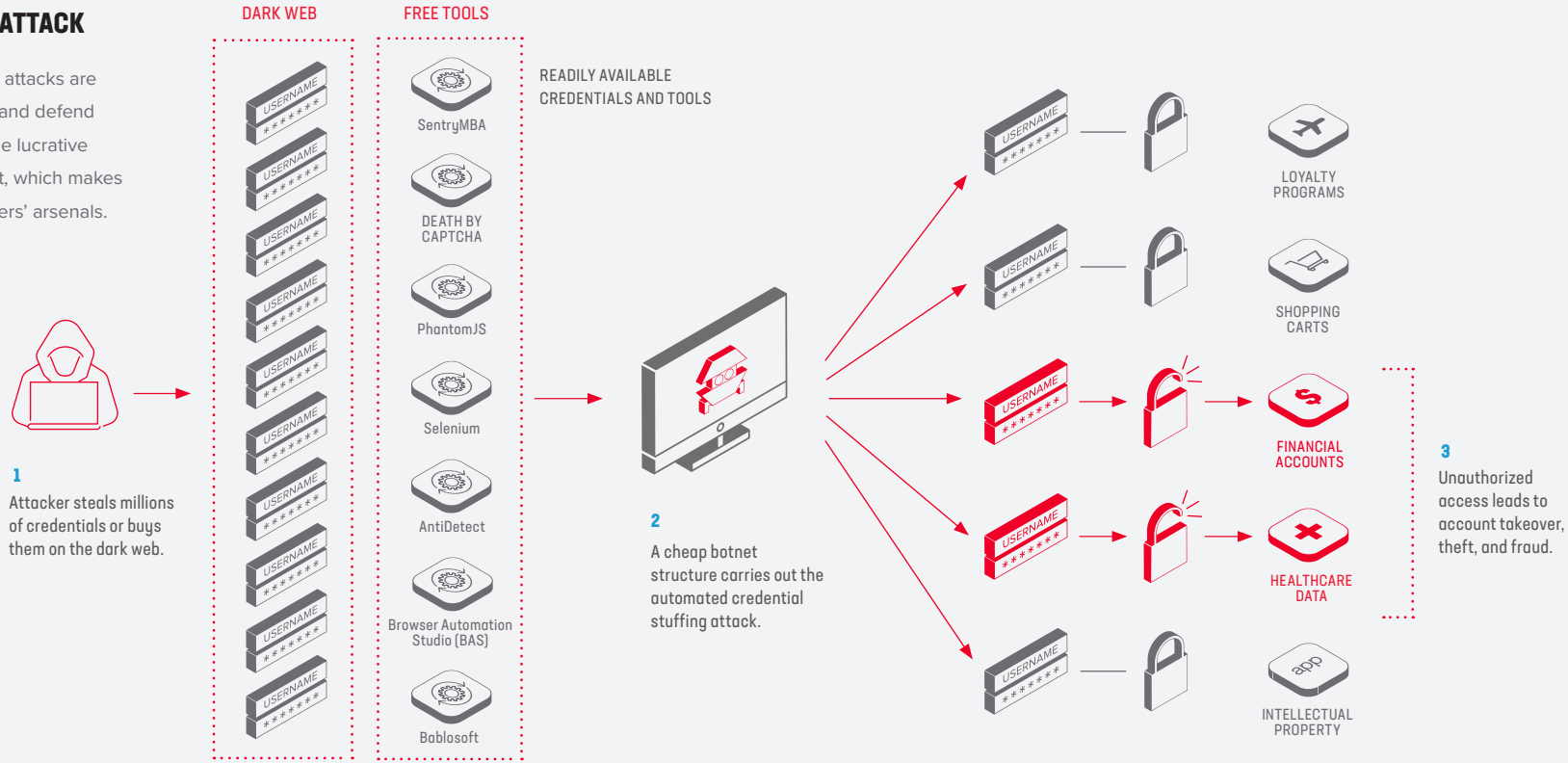
SO... WHY A WAF?

WAFs are commonly used to mitigate application vulnerabilities—typically design flaws or implementation bugs that weaken security. They help organizations comply with initiatives like PCI-DSS and protect sensitive customer data. However, a WAF needs to minimize risk while also safeguarding business goals.

A WAF can do this by preventing application exploits that are weaponized daily and mitigating the kinds of attacks that can result in compromise. Oh, and all this needs to happen at the speed of app development, because a WAF is only effective if it adapts as quickly as the apps it protects.

CREDENTIAL STUFFING ATTACK

Malicious bots and automated attacks are increasingly difficult to detect and defend against. Moreover, they provide lucrative return with minimal investment, which makes them a go-to favorite in attackers' arsenals.



THE EXPANDING RISK SURFACE

Some of the same types of attacks, such as injection and cross-site scripting (XSS), have existed since the dawn of application security. Why then are they so difficult to defend against? For starters:

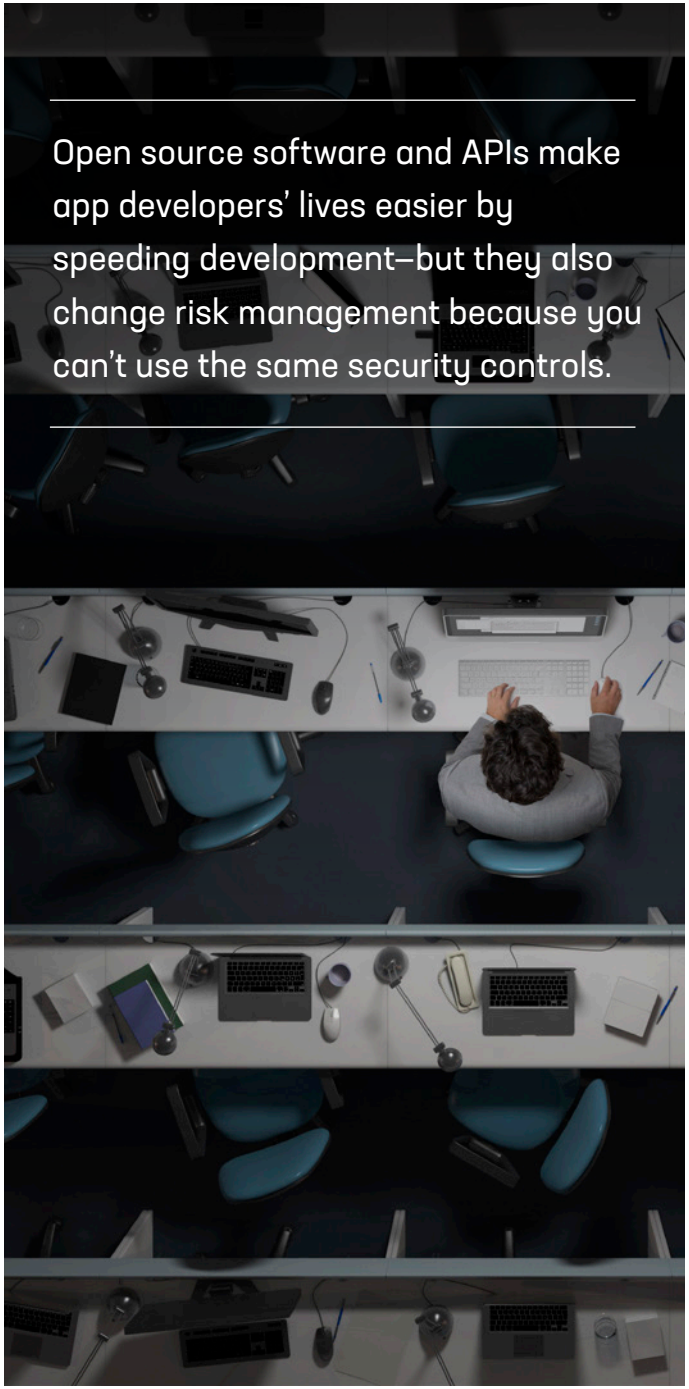
- Diverse and hybrid architectures, including the cloud, lead to inconsistent security.
- Developer reliance on open source software, APIs, and third-party widgets increases unintended risk.
- Application development pipelines often lack security integration.

For example, an injection attack on a popular commercial application in a data center protected by a WAF can be effectively mitigated with a signature. But an injection attack that exploits third-party API widgets needs additional protections.

Additionally, organizations typically adopt multiple cloud providers. The challenge is that cloud environments lack universal security, since cloud providers each have varying security postures (including the shared responsibility model, for instance) and the nuances between them can increase risk for their customers.

Next, open source software and APIs makes app developers' lives easier by significantly speeding development. But they also change risk management, because you can't use the same security controls as those used for software developed in-house (for example, test-driven development).

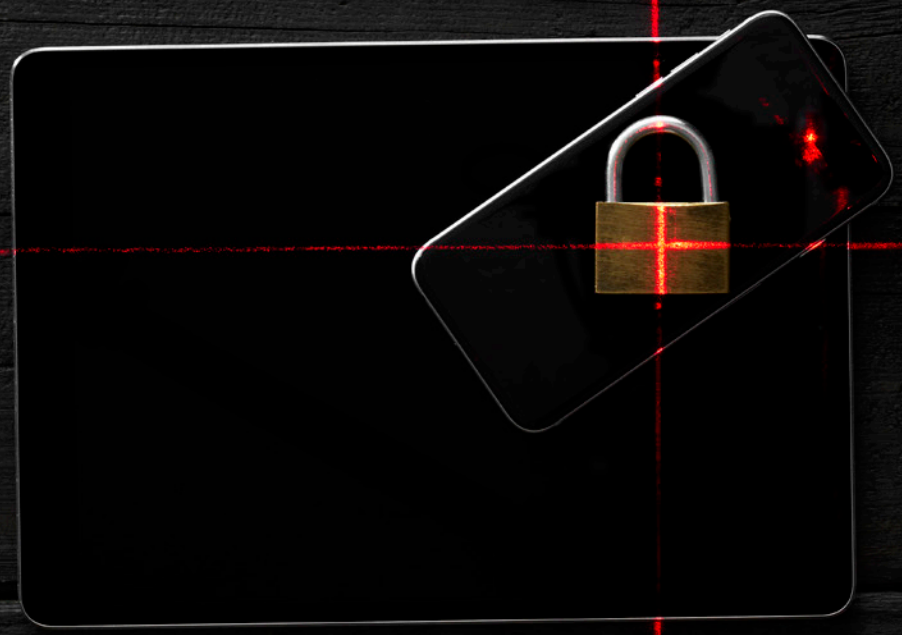
Finally, CI/CD pipelines that automate application development and deployment often lack security, causing friction between app developers and their security colleagues, and leading to a perception of security and time-consuming testing processes as obstacles to business goals.



THERE'S AN APPLICATION THREAT TO EXPLOIT ANY WEAKNESS

Attackers are getting more sophisticated, agile, *and* more creative. Want an example? F5 Labs recently identified threat campaigns that exploit a vulnerability to gain access to cloud-based email servers, send internal phishing emails that link to fake log-in forms, and then harvest credentials for use in credential stuffing attacks.

Tools used for penetration testing are also commonly used in attacks to help beat security challenges and bypass defenses by emulating human behavior. Application threats primarily target vulnerabilities, APIs, and access control.



APP VULNERABILITIES AND INCONSISTENCIES

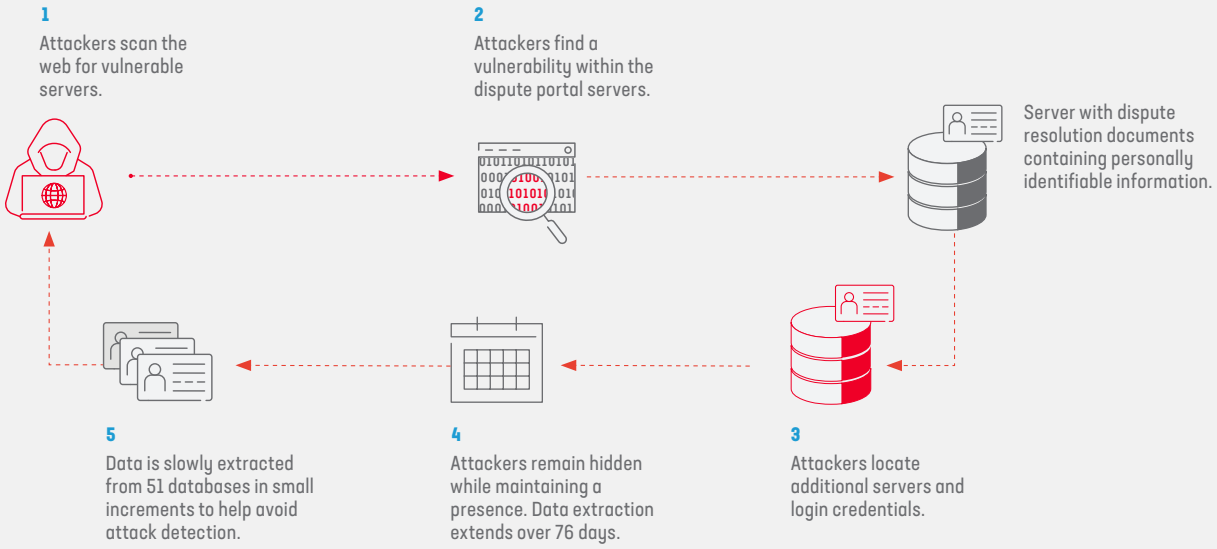
Shortly after a vulnerability has been published, attackers commonly scan for it and try to exploit it using automated tools. For instance, F5 Labs discovered a threat campaign where attackers used automation to find injection vulnerabilities in open source PHP. These vulnerabilities allowed them to exploit weak authentication portals and outdated MySQL databases to set up additional attacks and steal data.

Not all attacks are zero-day threats. If high-value information can be stolen by automating exploits to known vulnerabilities, that's where attackers invest. Attackers may also target valid functionality (for example, XEE attacks on XML), underscoring the need to "shift left" and get more visibility into potential threats earlier in the software development lifecycle.

Ultimately, organizations are responsible for safeguarding customer data because the people in that organization will have to deal with the fallout if a breach occurs. That's where a WAF can help. The only way to make sure a WAF can achieve that level of effectiveness is to get ahead of the vulnerability curve by integrating it with application development tools, frameworks, and processes.

BEST PRACTICE TIP

With the right WAF, well integrated into an organization's app development cycle, security professionals can enable business agility and drive innovation while building in security, rather than bolting it on.



HOW ATTACKERS EXPLOIT VULNERABILITIES

A newly announced vulnerability is often termed a one-day exploit, as in the case of a 2017 consumer credit reporting agency attack.[1] If an organization does not immediately update its servers, they are in danger of being attacked, since cybercriminals will scan for the vulnerability using automated tools.

[1] https://www.gao.gov/assets/700/694158.pdf

HERE COME THE APIS

APIs have become a critical component of modern applications. In some instances—open banking, for example—APIs are the vehicle for monetization.

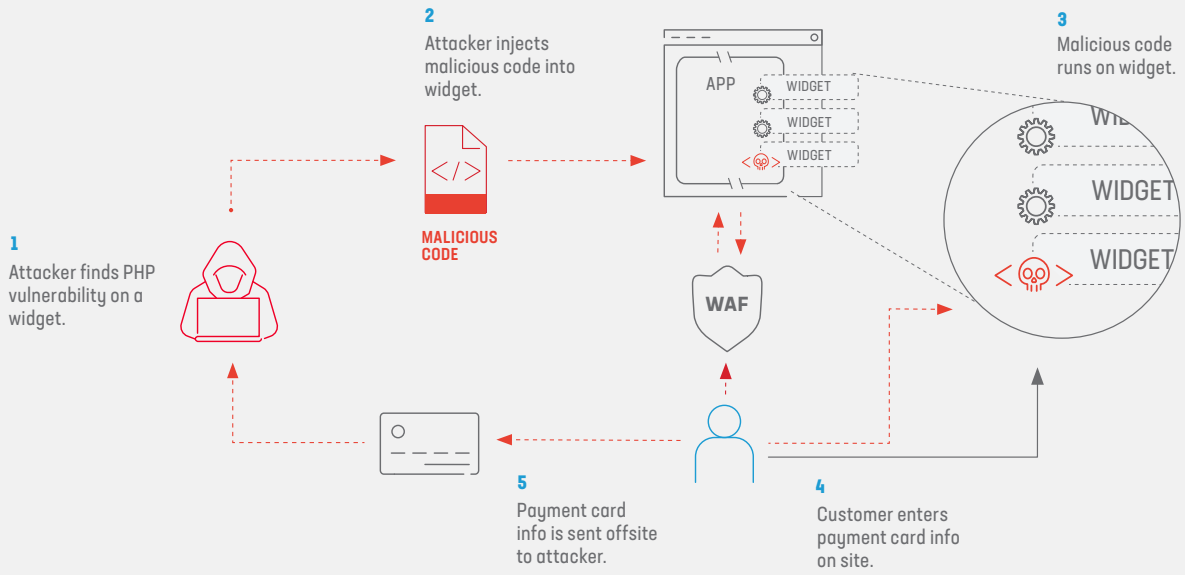
API calls are similar to general web requests, just in a different context. However, like the main page of a website, APIs are susceptible to exploits such as injection and credential stuffing. One key difference is in their structure—the schema, protocol, and content. Because APIs aren't intended for direct user interaction, they may not be in the purview of security teams. That's especially true of third-party API calls buried deep within application logic.

Since people increasingly prefer mobile apps for their personal and business relationships, those apps have become a popular target for attackers. And APIs pose a significant challenge to visibility. Similar to other third-party components like widgets, APIs result in decentralized, often API-to-API communication that bypasses centralized security controls.

Many top API security risks relate to authentication. Access control via integration with an identity-aware proxy or API gateway reduces exposure to potential exploits.

BEST PRACTICE TIP

An effective WAF operates in a distributed architecture to protect API-to-API communication that can bypass centralized security controls.



COMMON INJECTION ATTACK PATH

A standard WAF protects the primary site by examining traffic between the client and the app server. Third-party scripts, however, are loaded directly by the client browser, and bypass perimeter security.

BOTS AND THE BUSINESS

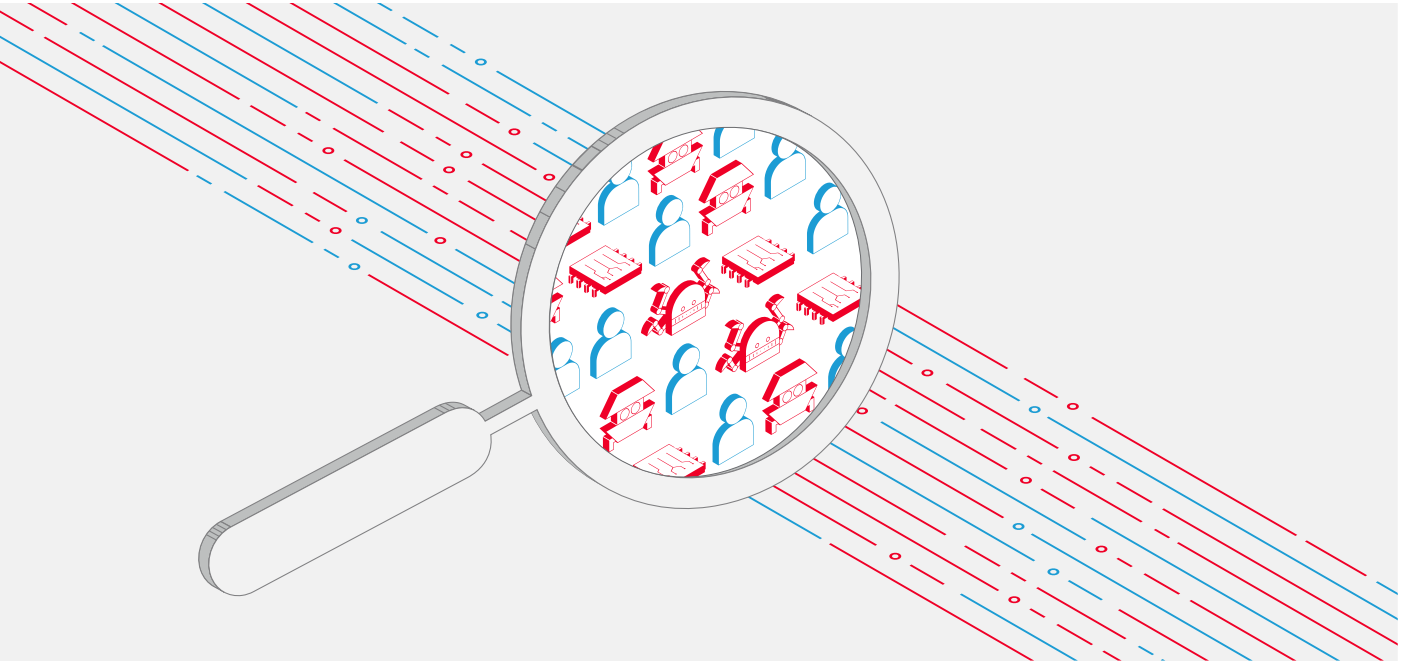
Bots have earned a bad rap, but the reality is far more complicated and nuanced. Bots reduce costs for basic and repetitive tasks and can improve business intelligence and customer engagement. (Hi, chatbot!)

Unfortunately, bots also reduce costs for attackers and help them scale their arsenals. Bots vary from legitimate web crawlers, to simple scripts or headless browsers, to automation that leverages CAPTCHA solvers, browser fingerprint spoofing, and other sophisticated techniques that emulate human behavior. Attackers can also use bots and automation to scale their attacks to achieve a higher ROI.

Skilled attackers will retool and adapt to beat countermeasures. The most sophisticated attackers may eventually abandon automation toolkits and pivot to human click farms or manual hacking to bypass mitigations designed to detect non-human automation.

BEST PRACTICE TIP

An effective WAF integrates with online fraud services to protect the business from sophisticated cybercrime, whether it involves bots or not.



THE KEY IS VISIBILITY

- Is this a potential customer?
- A search engine bot that could improve SEO rankings?
- An automated credential stuffing attack that may lead to compromise?

HOW TO CHOOSE A WAF...

The criteria for a WAF that will best serve your organization can be grouped into three broad considerations: technology, process, and people.

First, an effective WAF must have security controls that align with the organization's goals and the application development lifecycle. Less obviously, third-party APIs and widgets must also be secured. You can't allow API inspection to be bypassed because of the direct interactions between client-side logic and third-party APIs.

Plus, your organization needs to be protected from downtime, abuse, and fraud. The best defense is to detect anomalies using behavioral analytics. For the most sophisticated cybercriminals, only integration with online fraud services that detect human behavior and intent will be effective.

AN EFFECTIVE WAF MUST HAVE:

1. Low false positives and false negatives so the organization can be confident deploying the solution in blocking mode.

2. Comprehensive visibility and reporting so security engineers can demonstrate the value of the WAF to other teams.

3. Integration into an ecosystem of application security so processes can be automated.

...THAT'S BEST FOR YOUR ORGANIZATION

Efficacy and integration with software development are good gauges of WAF effectiveness. That covers the technology and process components of security. Equally important is the people component—specifically, who should implement and maintain the WAF's critical security controls?

One of the biggest obstacles to WAF effectiveness is the operational overhead of deploying and managing the solution. That means the right WAF will be easy to manage, so teams can get value from it without being experts. It will also operate in a purchasing and deployment model that's best for the organization.

Regardless of how it's a deployed, an effective WAF mitigates attacks by operating at the speed of app development, securing APIs, and preventing attacks that can result in compromise.

TYPES OF SOLUTIONS TO CONSIDER

OPTION 1

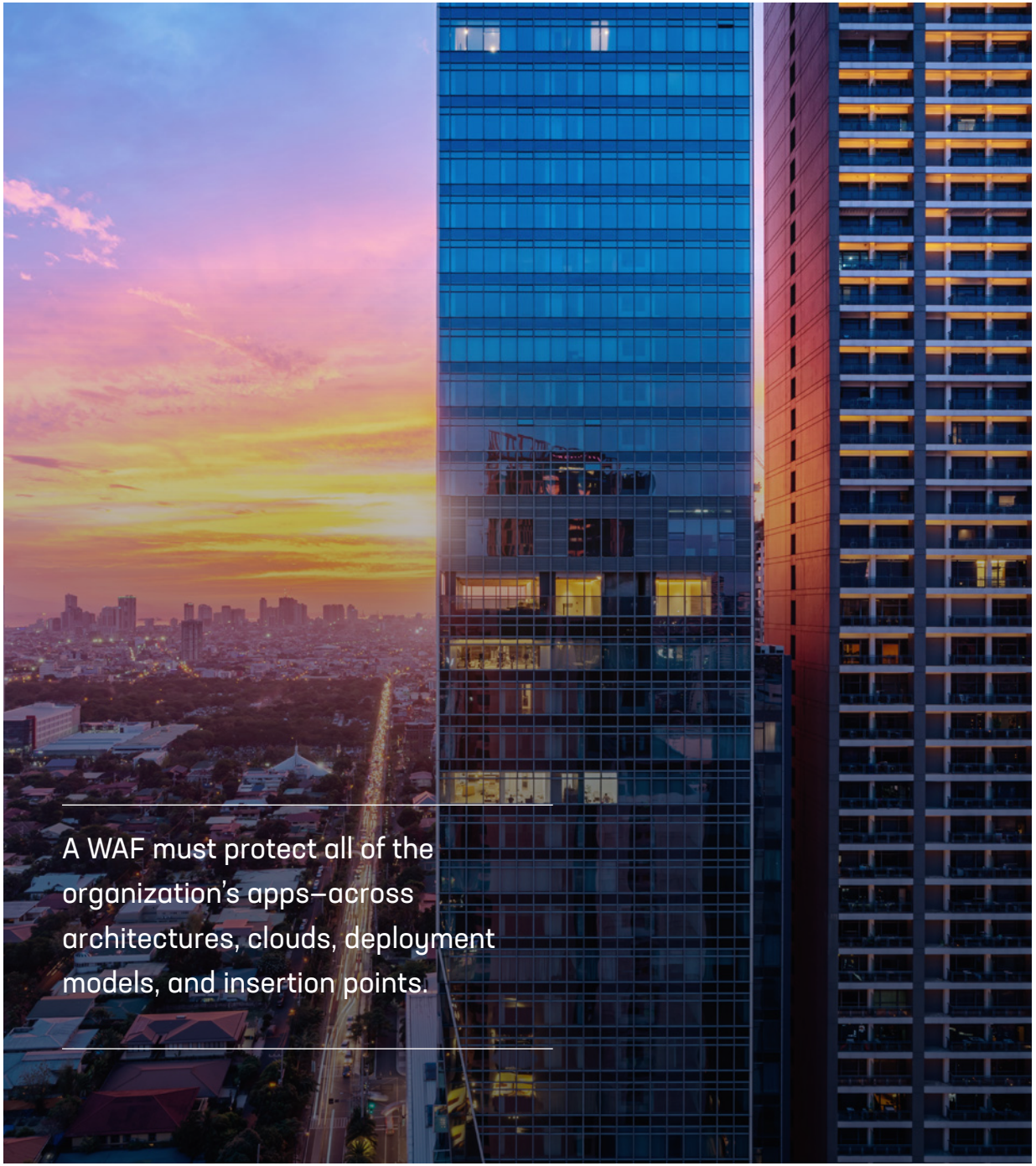
A self-managed solution provides granular control of security policy and customer data–in the application architecture, as a purpose-built appliance in the network, or as a virtual deployment in the cloud.

OPTION 2

A cloud-delivered solution can often be more rapidly deployed and provides robust protection from vulnerabilities in an intuitive and API-friendly interface.

OPTION 3

A managed service solution extends security and incident response capabilities through partnership with a trusted vendor, removing operational burdens from security staff.



MANAGE RISK WITH AN EFFECTIVE WAF

A WAF remains a critical security control for managing risk while supporting business goals. And as digital transformations enabled by apps become business initiatives *driven* by apps, WAFs must protect all of the organization's apps—across architectures, clouds, deployment models, and insertion points.

As a result, organizations should choose the WAF that provides the best combination of:

- Security efficacy—the technology component.
- Integration with development—the process component.
- Manageability, reliability, and visibility—the people component.

Attention to these criteria should deliver a WAF solution that protects your organization and its data while also empowering app-centric business objectives.

Learn more at **f5.com/security/advanced-waf**

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
©2020 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-479727569