THINK APP SECURITY FIRST

CHOOSING THE WAF THAT'S RIGHT FOR YOU

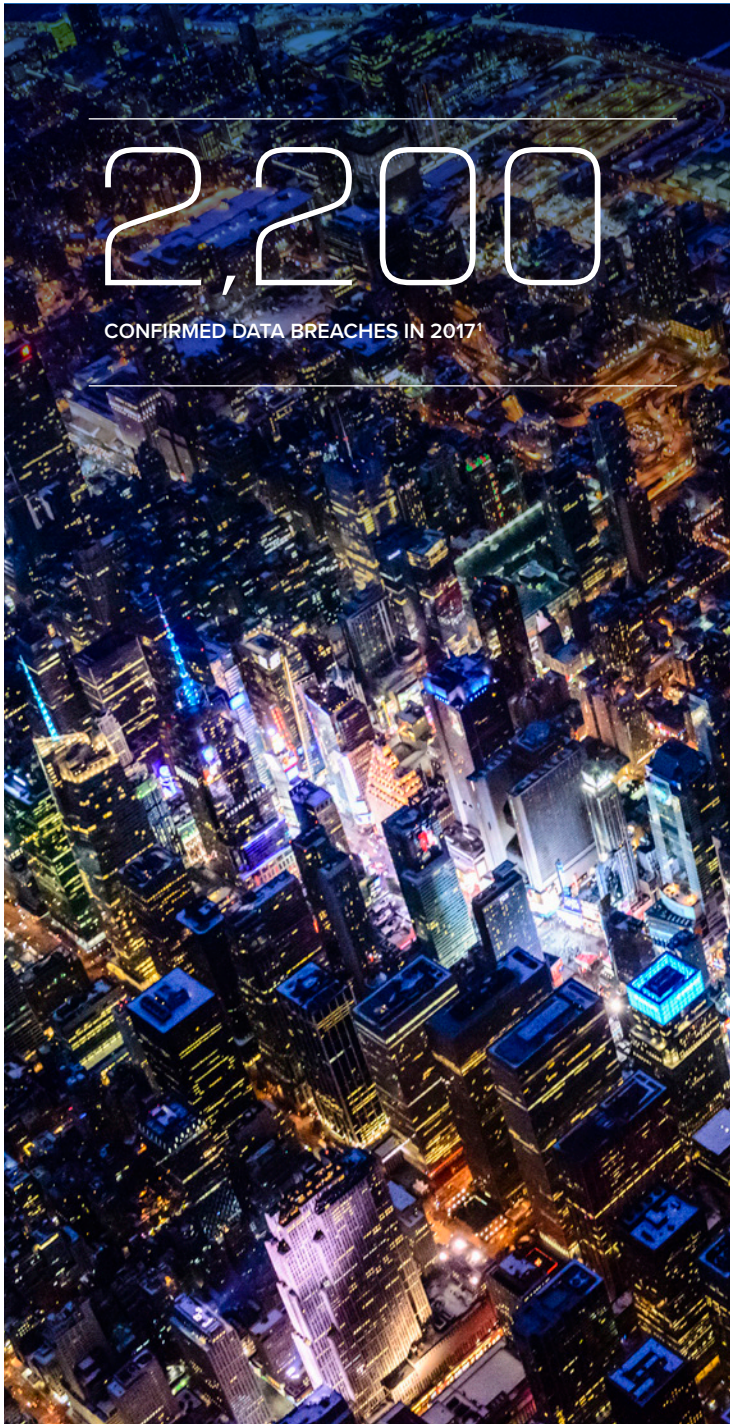
A HOW-TO GUIDE

INTRODUCTION

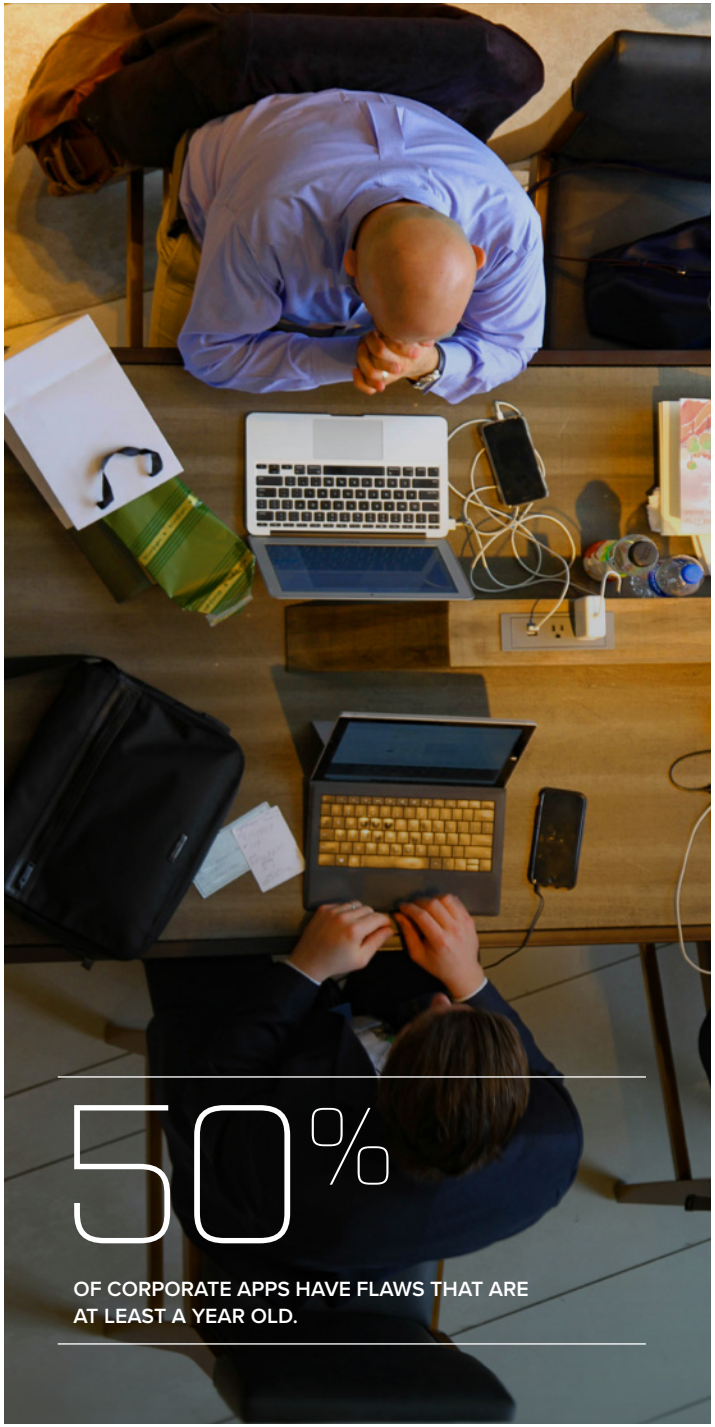
Despite the tech industry's collective best efforts to bolster secure application development practices, half of all applications remain vulnerable to attacks.

The Verizon 2018 Data Breach Investigations Report reveals that in 2017, there were more than 2,200 confirmed data breaches—and those are just the ones we know about.[1] Despite the tech industry's collective best efforts to bolster secure application development practices, half of all applications remain vulnerable to attacks. This isn't too surprising—secure web application development is remarkably difficult.[2]

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 (WAF). A WAF inspects ingress and egress application traffic to identify and block scanners, attackers, and bots, while preserving and accelerating apps for legitimate usage. Whether deployed on premises, leveraged in the cloud, or consumed as-a-service, WAF technology can help defend your organization against web app attacks, which are the primary entry point of successful data breaches.[3]



[1] https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf
[2] https://www.whitehatsec.com/news/half-of-corporate-web-apps-contain-flaws-that-are-at-least-a-year-old/
[3] https://www.f5.com/labs/articles/threat-intelligence/lessons-learned-from-a-decade-of-data-breaches-29035

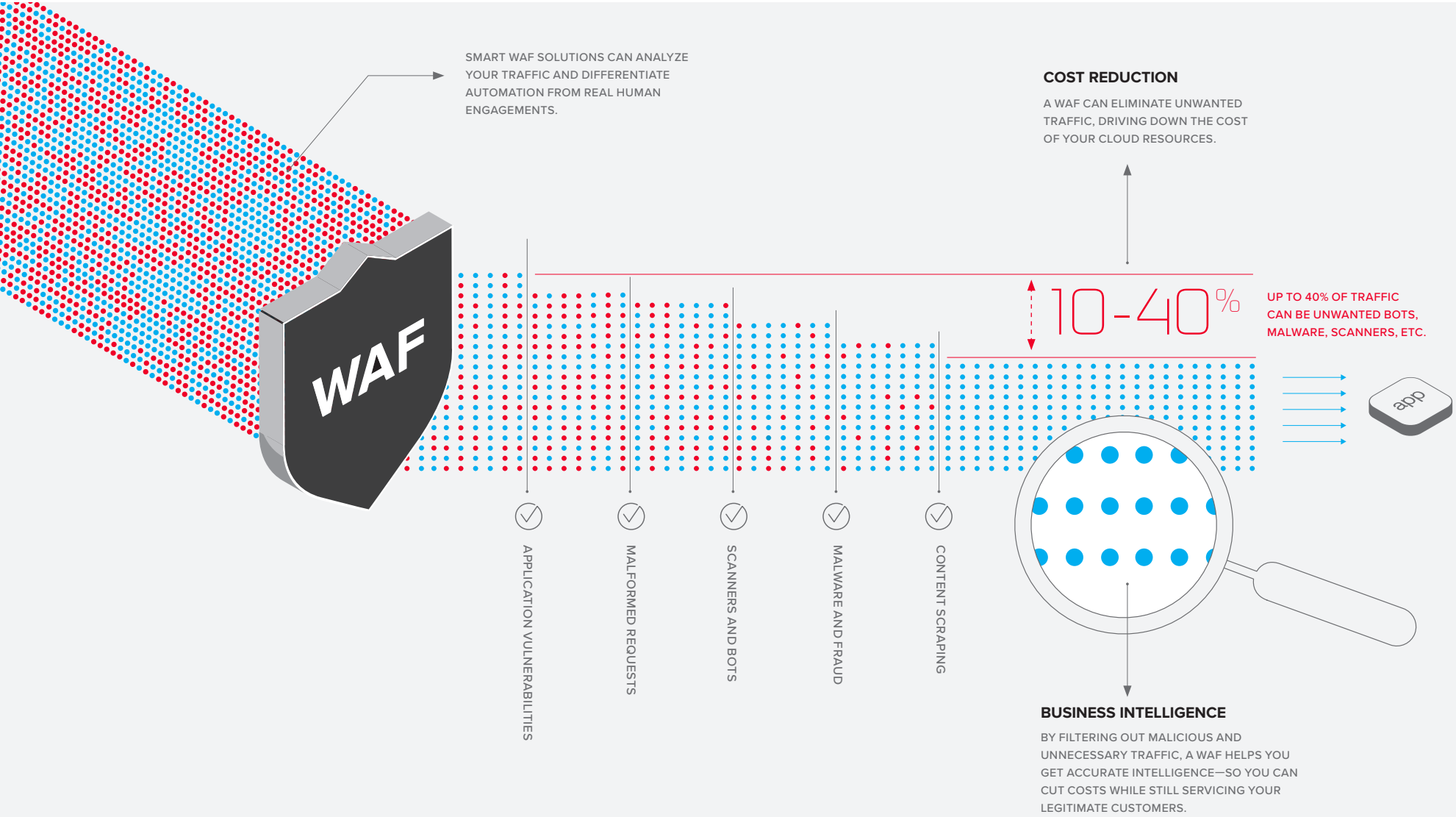


SO, DO YOU NEED A WAF? IT DEPENDS ON SEVERAL FACTORS.

- Do you have a public-facing web property?
- Do you have a high-sensitivity web property?
- 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 leverage legacy web apps?
- Do you need some breathing room from zero-day attacks?
- Do you want to reduce your development time to market?

If you answered “yes” to any of these questions, you should be considering WAF technology when you plan how to protect your apps, your data, and your business from web application attacks and data breaches.

As with any good tool, there are lots of options—and different solutions work better for different situations. Read on to learn how best to choose the WAF deployment model that’s right for your business.



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.

1 CAN SMART 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 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. Smart 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 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, which 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.

IN THE WORLD OF CLOUD COMPUTING AND BIG DATA, GOOD SECURITY SOLUTIONS CAN ACTUALLY *SAVE* YOU MONEY.

OPTIONS TO CONSIDER:

ON-PREMISES ADVANCED WAF (VIRTUAL OR HARDWARE APPLIANCE)

Adds real business value beyond acting as an insurance policy in case of a breach. With proactive bot defense combined with advanced application protection, threat intelligence, and machine learning, this kind of WAF can help you cut costs in the cloud and refine your business intelligence.

CLOUD-BASED + SELF-MANAGED

Allows you to cut costs, refine your business intelligence, and get great business value. With the same feature set as an on-premises WAF, a cloud-based, self-managed WAF gives you proactive bot defense, advanced application protection, threat intelligence, and machine learning.

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

According to the F5 2018 State of Application Delivery (SOAD) Report, the number of breaches has soared over the past year. With more breaches comes less confidence in the efficacy of security solutions to safeguard the confidential data that organizations process and hold.[4] The problem is that unless you're a CISO focused solely on protecting your company's data, you probably don't want to spend all your time managing the minutia of the many web application security risks out there.

You likely want a security solution that just works, so that you can focus on developing and deploying business-critical apps—keeping them online and available.

Fortunately, a variety of WAF options allow you to do just that. And even more good news: according to that same edition of the SOAD report, deploying a WAF has a strong effect on the level of confidence respondents had in protecting their apps. Of those organizations with a very low confidence in protecting on-premises applications, a mere 6% used a WAF. However, of those with very high confidence, 37% used a WAF.[5] It's clear that deploying a WAF can help protect your apps, but different deployment methods are better for different organizations.

[4] https://interact.f5.com/2018_SOAD.html
[5] https://interact.f5.com/2018_SOAD.html

IF YOU ARE LOOKING FOR A SECURITY SOLUTION THAT JUST WORKS, THERE ARE A VARIETY OF OPTIONS THAT ALLOW YOU TO DO JUST THAT.

OPTIONS TO CONSIDER:

CLOUD-BASED + FULLY-MANAGED AS A SERVICE

Can protect your web apps and data from ever-evolving threats while offering 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.

CLOUD-BASED + AUTO PROVISIONED

Gives you the same level of control and customization typically afforded to applications in a private data center while empowering rapid response to threats targeting applications in the cloud.

ON-PREMISES ADVANCED WAF (VIRTUAL OR HARDWARE APPLIANCE)

Offers accessible control levels that can help you meet your protection needs and give you visibility into application traffic while not requiring full-time management.

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.

These 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. 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 44% of organizations reported at least one breach in 2017, the results may surprise you.[6]

[6] https://betanews.com/2018/06/05/organization-data-breaches/

A GOOD WAF ALLOWS YOU TO MEET YOUR COMPLIANCE REQUIREMENTS WHILE ALSO GIVING YOU THE ADDITIONAL SECURITY AND VISIBILITY YOU NEED.

OPTIONS TO CONSIDER:

COMMODITY

Can help you pass an audit, but it won't offer high levels of protection without a significant level of configuration knowledge and continuous maintenance, and perhaps not even then.

ON-PREMISES ADVANCED WAF (VIRTUAL OR HARDWARE APPLIANCE)

Offers better protection, gives you fine-grained analytics, and ensures that you're not just passing your audits—you're actually increasing the security posture of your business.

CLOUD-BASED + SELF-MANAGED

A self-managed, cloud-based advanced WAF offers similar protection to its on-premises counterpart, giving you robust protection and powerful analytics that bolster your overall security posture.

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 feel reasonably confident in the security of the apps you have deployed, you're likely contending with another problem: a large percentage of web traffic to your site or web service is probably coming from autonomous programs 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 the use of 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 stop automated attacks and leverage a combination of challenge- and behavior-based techniques to identify and filter out bot traffic. This is good news for businesses struggling to manage the ever-increasing amount of 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.

ADAPTABLE WAF TECHNOLOGY CAN MITIGATE THE EFFECTS OF UNWANTED BOT TRAFFIC.

OPTIONS TO CONSIDER:

ON-PREMISES ADVANCED WAF (VIRTUAL OR HARDWARE APPLIANCE)

Offers proactive bot protection to defend your apps against layer 7 DoS attacks, web scraping, and brute-force attacks—before they harm your site.

CLOUD-BASED + SELF-MANAGED

A cloud-based, self-managed WAF can also deliver the same level of proactive bot protection, which helps you defend your apps against web scraping and layer 7 DoS and brute-force attacks.

CLOUD-BASED + FULLY-MANAGED AS A SERVICE

Protects your web apps from bot-based threats while offering 24x7 support. By identifying malicious bots that bypass standard detection methods, a cloud-based solution can also mitigate threats before they cause damage.

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 if you put more into it. Also, certain threat vectors—especially attacks targeted against a specific company or digital property—can be challenging to deal with.

Finally, the visibility you gain by deploying an advanced WAF can help inform your decision-making process for both application security and overall business objectives—but only if your organization is set up to leverage that data.

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

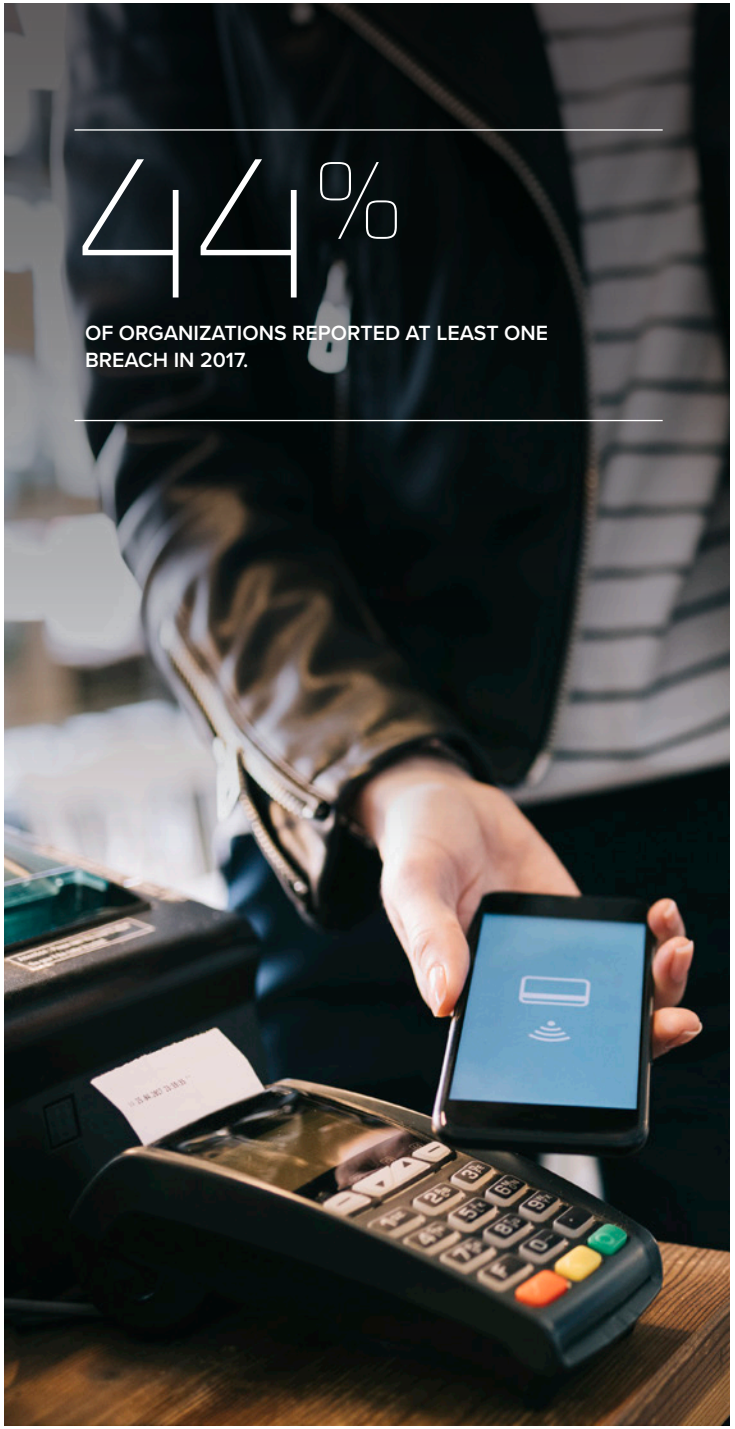
WAF DEPLOYMENT MODES

	PROS	CONS
 **CLOUD-BASED + FULLY-MANAGED AS A SERVICE**	Choose this option if you are looking for the fastest, most hassle-free way to get WAF (and DDoS mitigation) in front of your applications.	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.
 **CLOUD-BASED + SELF-MANAGED**	Get all of the flexibility and security policy portability of the cloud, while retaining control of your traffic management and security policy settings.	Being self-managed, this model requires some involvement from your security team and app owners to deploy and build the security policies applicable to your applications.
 **CLOUD-BASED + AUTO-PROVISIONED**	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 meeting your needs in an easy and cost-effective fashion.	Depending on your application's architecture, this model may not provide as much architectural flexibility as other models.
 **ON-PREMISES ADVANCED WAF (VIRTUAL OR HARDWARE APPLIANCE)**	An on-premises WAF (whether virtual or hardware) can help meet all of your most demanding deployment modes where architectural flexibility, performance, and advanced security concerns are paramount.	This model may require more upfront investment in terms of procurement and deployment than other models, but such investment will pay dividends for those needing the flexibility it provides.
 **COMMODITY**	This low-cost WAF model will give you basic coverage for some known attack vectors and may help address regulatory compliance requirements.	Commodity WAFs may not have the flexibility and resiliency required to defend against the continually evolving threat vectors that threaten today's businesses. Most likely this kind of WAF will not help defend against risks that are not application vulnerabilities, such as bots and fraud.

CONCLUSION

While the choices facing you may seem daunting, the truth is that 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 a good thing, because companies need the protection a WAF offers now more than ever.

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 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.

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com
©2018 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-255258364 08.18