SAVE A LIFE: ADD A WAF

Okay, maybe that headline is a bit of an exaggeration. Consistent application security rarely saves a life—but the vulnerabilities you're exposed to without it can cost you time, money, and reputation.

Protecting apps against threats has proven to be a difficult job. Some types of vulnerability are old enough to have graduated high school, and they're still compromising applications—and more importantly, data—today. According to recent F5 research, confidence in protecting apps declined 4% year over year, dropping from 45% in 2017 to 41% in 2018 (SOAD 2018). However, in that same research, 43% of respondents said security is the worst thing to deploy an app without. One in three (36%) plan on protecting less than a quarter of their applications with a Web Application Firewall (WAF). Coverage continues to decline at each quartile, with just over one in ten (13%) indicating protection of 100% of their applications.

CONFIDENCE IN PROTECTING APPS DECLINED 4% YEAR OVER YEAR, DROPPING FROM 45% IN 2017 TO 41% IN 2018.

What do those statistics mean for actual, living, breathing NetOps teams? For one thing, it means a lot more work creating custom security policies and playing Whack-a-Mole as new threats find ways to compromise new apps. It also means less time in the day to accomplish projects that will actually drive the business. This leads to morale issues that slow down productivity, and hurt employee retention.

So, what's the solution? Along with secure coding practices, static vulnerability scanning, and automated penetration testing, the WAF has been a consistent and useful tool in the fight for application security. WAFs are undoubtedly a great idea: they protect your apps by examining application requests and responses for threats, analyzing behavior, mitigating distributed denial-of-service (DDoS) attacks, detecting bots, and preventing sensitive data exfiltration.

The problem for many businesses has been in the implementation. Getting WAF services in front of applications has been difficult, time consuming, and has involved too much friction. In an ideal world, every application, anywhere, would have WAF services rolled out as part of the deployment toolchain, with at least a base level of protection. If you take a close look at data losses, a significant percentage of them—even the truly spectacular ones—might have been prevented with relatively simple security.

SECURITY SERVICES ARE DEPLOYED SEAMLESSLY ALONGSIDE OTHER NECESSARY APPLICATION DELIVERY SERVICES SUCH AS LOAD BALANCING OR NETWORK OPTIMIZATION.

Can we get to the point where all your applications get the benefit of a powerful, secure WAF? Is that a possible and realistic goal? With F5 BIG-IP Cloud Edition, it just might be. BIG-IP Cloud Edition brings a number of innovations that make adding a WAF to every app not just possible, but truly practical. With BIG-IP Cloud Edition, your security team can create a catalog of policies to cover most applications, and your operations team can attach those policies to templates. Better still, your app teams get to choose the template to use for their app from a service catalog, then self-serve the deployment of application delivery and security services. The services are provided by lighter-weight, auto-scaling F5 BIG-IP instances that are deployed on demand and that are dedicated to a single application. The BIG-IP instances are right-sized and right-priced to make this an entirely practical architecture, even for organizations with hundreds or thousands of apps.

With BIG-IP Cloud Edition, security services are deployed seamlessly alongside other necessary application delivery services such as load balancing or network optimization. BIG-IP Cloud Edition also brings enhanced observability and monitoring with customized dashboards—for application owners who care about app performance, and administrators who care about both the apps and the infrastructure.

While there will always be applications that need tailored, hand-tuned security policies (which is perfectly possible with BIG-IP Cloud Edition), most don't warrant the time and effort of creating them. Because the best sort of security is the one you actually use. Wait, scratch that—the best sort is the security you just get, without having to do anything at all.

Learn more at f5.com/cloudedition.