THE PITFALLS OF TRADITIONAL WEB APPLICATION SECURITY

EXECUTIVE SUMMARY

Unprotected web-based applications are often the easiest point of entry for hackers and are vulnerable to a number of attack techniques. Traditional technologies, including firewalls and intrusion prevention systems (IPS), cannot provide complete protection from these threats. Web application firewalls (WAFs) have proven effective in preventing attacks that target known vulnerabilities and detecting zero-day events. However, while WAFs provide behavioral-based capabilities using application-learning methods, they incur a high volume of false-positive detections. This creates an excessive burden on cybersecurity staff, who must manually review all the detections to weed out the false positives and then tune their WAF profiles accordingly. Standalone WAFs can also increase the overall complexity of the security architecture, making it more difficult to manage and less responsive to an evolving threat landscape.

1 in **5** organizations reported malware targeting mobile devices in 2017.[1]

STRUGGLING TO STAY IN CONTROL

As cybersecurity skills shortages persist, network security management remains typically reactive, with teams spending most of their time prioritizing and responding to alerts. Too little time is devoted to the strategic, proactive activities necessary to protect assets effectively and defend against increasingly sophisticated and frequent attacks.

Creating breathing room for strategic thinking is especially important considering the proliferation of mobile devices and the Internet of Things (IoT). These and other aspects of digital transformation are expanding the enterprise's attack surface, creating new

opportunities for cyber criminals and other threat actors. And as the attack surface swells, under current conditions, security infrastructure visibility and control diminish.

Cyber criminals are refining their technologies and methodologies, becoming more sophisticated at matching exploits to their targets. Design attacks where hackers personalize and customize their attack based on the target are on the rise. 73% of organizations experienced a severe exploit during the first quarter of 2018, with web-oriented technologies in the cross hairs of cyber criminals.[2]

Making cybersecurity even more challenging is the fact that zero-day attacks continue to grow more troublesome and difficult to combat. To address the increased sophistication and severity of the threat landscape, including the broader attack surface, security leaders are adding more point security products. But this amplifies complexity, incurring more manual burdens on an already overtaxed cybersecurity team while making it more difficult to defend against attacks that are polymorphic and employ multiple attack vectors simultaneously.

Security complexity is growing from the other direction as well. New and expanded governmental and industry regulations require transparent visibility and centralized controls and adoption. In addition, adherence to security standards and protocols demands real-time tracking and reporting. However, a patchwork of security products that are not integrated thwarts automation of workflows and processes and places the burden to demonstrate compliance on security teams.

70% of security professionals believe the cybersecurity skills shortage has had a negative impact on their organization.[3]

DEFENDING WEB APPLICATIONS IS DIFFICULT

Web-based applications are a rich hunting ground for hackers. Some are public-facing applications and are logical targets for criminals. The majority, whether public-, partner-, or internal-facing, are connected to back-end databases that hold critical business information or personally identifiable information (PII).

When it comes to measuring the impact of the attacks on web applications, the numbers speak for themselves. 48% of all data breaches are caused by hacking of web-based applications.[4] Web applications also offer an attractive attack surface: 42% have at least one severe vulnerability. And the repercussions of a data breach are real. The widely publicized Equifax breach in 2017, for example, was the result of an attack on a reported vulnerability[5] in the Apache Struts web application software that led to the disclosure of PII for more than 147 million Americans.[6]

77% of web application breaches

were caused by automated attacks and botnets last year.[7]

WHERE WEB APPLICATION SECURITY FALLS SHORT

Traditional perimeter security technologies such as IPS and firewalls focus on network and transport layer attacks. In response to the changing web application threat landscape and increasing hacker sophistication, firewall providers introduced application layer enhancements, commonly referred to as deep packet inspection (DPI), which extend the current network signature engine to the application layer.

While this approach is useful in protecting against attacks on the web server infrastructure itself, it lacks the sophistication required to protect against attacks on custom web application code such as SQL injection and cross-site scripting attacks. Further, firewall and IPS solutions cannot protect against zero-day attacks (viz., a signature doesn't exist for something that is unknown).

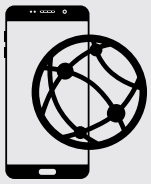
In addition to the above, many web security solutions lack the elasticity and agility to provide visibility and controls into every web application in use. More than two-thirds of organizations indicate they lack requisite visibility into many applications they have deployed.[8]

APPLICATION LEARNING ALONE IS NOT ENOUGH

WAF solutions provide a list of application layer protection, including cookie security, HTTP conformance, bot protection, and security rules. At the heart of many WAF solutions, however, is application learning, which is seen as a means for addressing zero-day threats.

Using application learning, a WAF builds a profile of the application structure and how the application is used. The WAF monitors user access to the application and seeks to understand how elements of the web application are accessed. As an example, a WAF monitors how form fields are being used and the types of values inserted, HTTP methods, cookies that are created, and other activities. Based on these machine-learning behaviors, a WAF automatically updates the profile with new and changed behaviors.

42% of web applications have a severe vulnerability.



80% to 90% of web applications

are built from third-party components that often contain critical vulnerabilities.[9]

Once the WAF determines that it has seen enough activity for an element, it moves that application element into "protect mode," where access to that element must adhere to the profile formulated by the WAF. If the request is different than the profile, the WAF blocks the request. In doing so, WAF solutions are configured to protect against attacks that bypass signatures and zero-day attacks—both automatically and transparently, without administrator involvement.

While application learning certainly advances web application security, it creates a new problem in the form of false positives.

THE FALSE-POSITIVES PROBLEM

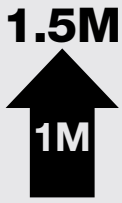
By design, WAFs block anomalies. But many of these anomalies may simply be previously unobserved variations of safe traffic; flagging them as potentially malicious creates false-positive alerts. Dealing with false positives requires two types of resource-intensive manual intervention. First, security teams must review all the blocked packets to determine which are legitimate and which are malicious. Second, to avoid recurring false positives, teams must review every profile before moving it into blocking mode.

With many cybersecurity skills difficult to find and security teams overburdened, this additional work can stretch them to their limits. It also can distract them from working on business-critical initiatives such as supporting digital transformation (DX) projects that elongate time to market and foster reactive security responses.

LACK OF INTEGRATION INTO THE BROADER SECURITY INFRASTRUCTURE

The threat landscape is dynamic, and hackers are leveraging Malware-as-a-Service models that dramatically reduce the amount of time required to develop an attack and provide easy access to polymorphic malware. This type of malware uses polymorphic characteristics to evade detection and employs artificial intelligence (AI) and machine learning to identify new vulnerabilities. Hackers are also unleashing multivector attacks that target multiple security areas simultaneously, making it increasingly difficult to identify and detect malicious intrusions.

To address the dynamic threat landscape effectively and efficiently, security architects must close all gaps between network security



Over 1 million

cybersecurity jobs are unfilled today, a number expected to rise to 1.5 million next year.[10]

elements. This is easier said than done, however, as many WAF solutions don't readily integrate with other security components, such as those protecting email, clouds, endpoints, access points, and other areas. Isolated components result in siloed manual workflows and processes, making it nearly impossible to achieve real-time threat-intelligence sharing, which is essential to outpacing cyber criminals.

CONCLUSION

Web applications are business critical for most organizations in the digital age. Without them, many businesses would be unable to sustain operations, transact business, and communicate and collaborate with customers and partners. But as the attack surface grows and the velocity, volume, and variety of attacks increase, the challenge of protecting web applications from malicious attacks becomes increasingly difficult. Current security approaches to web security, which include IPS and firewall solutions, are inadequate, unable to address zero-day threats and integrate with the broader security infrastructure.

WAFs that use application-learning techniques enable security organizations to thwart zero-day attacks, but they also accumulate excessive false positives that incur substantial resources to identify and eliminate. Additionally, they fail to integrate with the broader security infrastructure and thus are unable to share threat intelligence in real time with other security elements—a requisite in a threat environment where hackers employ multivector and polymorphic attacks. Security architects need an alternative that employs AI and machine learning for precision-point prevention and detection and that integrates with the broader security fabric for real-time threat-intelligence sharing between WAFs and all security elements.

FortiGuard Labs recorded **15,071 new malware** variants in the first quarter of 2018—an average of 167 new pieces of malicious code per day.[11]

1 "Threat Landscape Report Q1 2018," Fortinet, May 14, 2018.
2 Ibid.
3 Jon Oltsik, "The Life and Times of Cybersecurity Professionals," The Enterprise Strategy Group, November 2017.
4 "2018 Data Breach Investigations Report," Verizon, March 2018.
5 Ian Muscat, "Acunetix Vulnerability Testing Report 2017," Acunetix, June 6, 2017.
6 Thomas Fox-Brewster, "How Equifax Kept Its Mega Breach Secret From Its Own Staff," Forbes, March 14, 2018.
7 "2018 Data Breach Investigations Report," Verizon, March 2018.
8 "Application Security in the Changing Risk Landscape," Ponemon Institute, July 2016.
9 "2017 State of the Software Supply Chain Report," Sonatype, accessed on May 21, 2018.
10 "The Global Cybersecurity Skills Gap," Indeed, January 17, 2017.
11 "Threat Landscape Report Q1 2018," Fortinet, May 14, 2018.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

June 15, 2018 2:35 PM