FINDING A BETTER SOLUTION FOR WEB APPLICATION SECURITY

EXECUTIVE SUMMARY

Web applications are a favorite attack target because they can provide access to valuable data and are relatively easy to exploit. The growing number of new application-related threats requires additional security capabilities that a firewall or intrusion prevention system (IPS) can't provide. Signature-based detection, IP reputation, and deep-packet inspection (DPI) can stop some of these advanced threats, but even they have limitations. Thus, organizations need to expand their existing security architecture to include solutions such as web application firewalls, secure application delivery controllers, and distributed denial-of-service (DDoS) mitigation appliances to address these new threats to the data center and users.

The **Open Web Application Security Project (OWASP)** has consistently reported since 2010 that almost every web-based application has one or more vulnerabilities listed in their **Top 10 application security risks**, and that **95% of all websites** are attacked annually using cross-site scripting and injection techniques.[1]

Acunetix—an industry-leading web application vulnerability scanning provider—noted that **42% of their customer websites** had at least one critical vulnerability in 2017.

ATTRACTIVE TARGETS OF HACKERS

Web applications are attractive to hackers because they are open to the public-facing Internet. Since web applications include a large number of ecommerce and tools used for business operations, they often contain sensitive personal and/or financial information. A successful attack (such as the 2017 Equifax breach[2]) can have devastating consequences, including monetary costs, damage to brand reputation, and loss of customer trust. Some organizations never recover from a major security breach, and web applications top the list of attack vectors leading to data breaches.[3]

In 2017, the Russian hacker Rasputin compromised 63 federal, state, and local government agencies and universities via SQL injection.[4]

The lines of exposure that lead to data breaches break into four main use cases:

1. Application Vulnerabilities.
Many web applications allow the uploading of files, which introduces risk. Antivirus scans can check for previously identified attack types, but previously unknown threats can circumvent traditional antivirus detection. While perimeter security technologies such as IPSs and firewalls traditionally focused on network and transport layer attacks, many security vendors have added application layer enhancements to extend signature detection. And although this is useful in protecting against attacks on the web server infrastructure (IIS, Apache, etc.), it cannot protect against things like injection attacks on custom web application code such as HTML and SQL.

2. DDoS Attacks.
While DDoS attacks are one of the oldest security threats, they have evolved over the past decade to target application-level services. The fastest-growing category of DDoS attacks are Layer 7 events that only take a few megabits of packets to do as much harm as a large-scale attack in the hundreds of gigabits. Data-center managers continue to rank DDoS as a top concern over other disruptions like infrastructure outages or bandwidth saturation.[5]

3. Advanced Malware.
Advanced persistent threats (APTs) are custom-developed, targeted malware that can be introduced by attachments sent through web-based applications. They can evade straightforward detection by using previously unseen (also known as "zero-day") attack methods and by coming from brand-new or seemingly innocent hosting URLs and IPs. They're often designed to seek out opportunities like unpatched security updates. An APT's goal is to compromise the target system with advanced code techniques that circumvent security barriers—and then to go unnoticed for as long as possible.

4. Unsecured Web Applications.
Enterprises are aggressively expanding secure sockets layer (SSL) and transport layer security (TLS) encryption for web-facing applications to protect sensitive application traffic. Combined with explosive growth in applications, the complexity of moving to more advanced encryption keys effectively doubles secure packet sizes. Because of these conditions, organizations are struggling to keep up with the demands of traffic inspection in their current application delivery infrastructures. If security becomes a bottleneck for network performance, many organizations will forgo inspection—potentially leaving undiscovered threats hidden in encrypted file attachments.

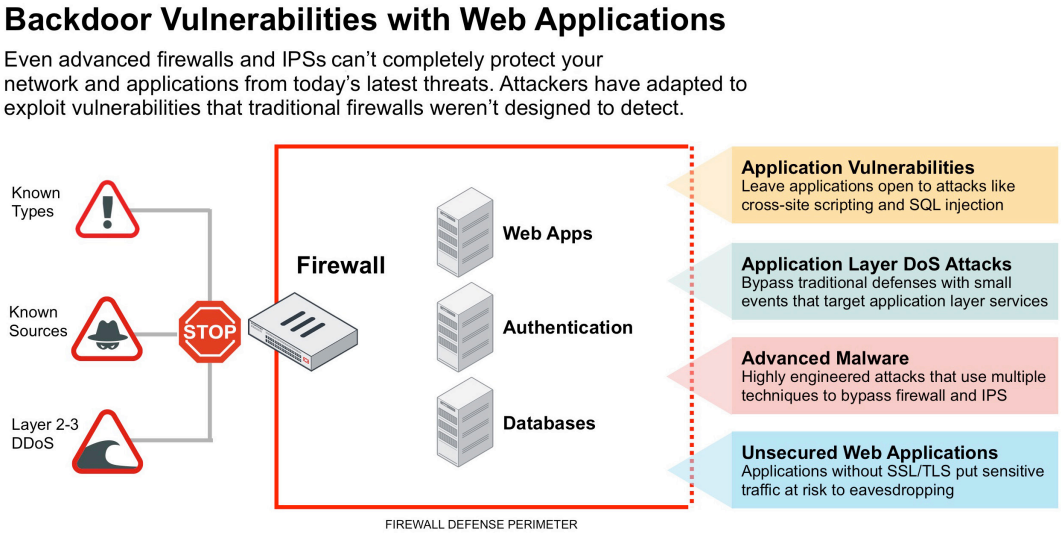

FIGURE 1: WEB APPLICATION VULNERABILITIES

WHY WEB APPLICATION SECURITY NEEDS MORE ATTENTION

The most commonly used application-level protection features of firewalls are IP reputation and signature detection. Usually, subscription-based services, IP reputation, and attack signatures are very effective measures for blocking attacks before any processing is applied by the firewall. If an attack is from a known source or it matches a predefined signature, it is blocked automatically without the firewall having to perform further inspection.

Although these are very effective controls for blocking known attacks, zero-day threats and unknown sources can get past these detection systems. Application code-based vulnerabilities have almost unlimited ways to bypass predefined signatures and IP reputation. Current APTs are customized as such so that their malicious code has never been seen before and offers no known threat signature for security to intercept. Services such as DPI and data loss prevention (DLP) can also be enabled, but there are still security loopholes and performance impacts that need to be considered in enterprise deployments.

To address each of the aforementioned vulnerability use cases and provide complete protection against zero-day attacks, additional security capabilities—beyond those of traditional firewall or IPS solutions—are required. Here, there are three different security solutions that can address each of these outstanding vulnerabilities within an integrated, complementary security architecture.

WHAT TO INCLUDE WHEN PROTECTING WEB APPLICATIONS

1. Web Application Firewalls (WAFs)

WAFs supplement the signature-based defenses provided by firewalls and IPS platform protection. Unlike any other solution deployed across the security architecture, a WAF can provide complete application protection by understanding application logic and what elements exist in the web application, such as URLs, parameters, and the cookies it uses.

Using behavioral monitoring of application usage, a WAF provides deep inspection of every application in your data center to build a baseline of normal behaviors and trigger actions to protect your applications when anomalies arise. WAFs provide bidirectional defenses against malicious sources, DDoS attacks, and sophisticated threats such as SQL injection, cross-site scripting, buffer overflows, file inclusion, cookie poisoning, and many others.

2. Application Delivery Controllers (ADCs)

Users have come to expect applications that are highly available and reliable. But in order to secure ever-expanding application traffic, SSL encryption incurs a cost in user capacities, speed, and latency.

ADCs offer organizations the ability to offload SSL traffic from servers to the ADC solution itself. Most manufacturers can do this using software encryption and decryption—but only hardware-accelerated appliances have dedicated security processing units (SPUs) to handle the speeds of a modern data center. Software-based devices can typically handle a few hundred to a few thousand transactions per second. Hardware-based appliances can manage tens of thousands of secure transactions per second. In this case, encrypted application traffic can be thoroughly inspected for hidden threats without creating a performance bottleneck for users.

WAF SOLUTION: WHAT TO LOOK FOR

- **High protected WAF throughput (not just L4 or L7 throughput)**
- **Multiple threat detection methods, including protocol validation, AI-based behavioral identification, and reputation/ antivirus/web attack signatures**
- **Vulnerability scanner, including support for virtual patching with third-party scanner integration**
- **Sandbox integration**
- **Simplified deployment with automatic setup tools**

ADC SOLUTION: WHAT TO LOOK FOR

- **L4 and L7 throughput to meet your needs**
- **Complete L4 to L7 server load balancing**
- **Intelligent policy-based routing**
- **Scripting for custom load balancing and content rewriting rules**
- **Antivirus and sandbox integration**
- **SSL forward proxy for increased secure traffic inspection with NGFWs**

3. DDoS Mitigation

DDoS attacks target Layer 7 services to slowly exhaust resources at the application level. They can be very effective using small traffic volumes, and they may appear to be completely normal to most traditional DDoS detection methods. Most Internet service providers (ISPs) don't have sophisticated detection tools for intercepting these smaller application-level threats, so they can frequently pass through to your network.

DDoS attack mitigation appliances are dedicated, in-line devices that block Layer 3, 4, and 7 attacks. They come in both carrier and enterprise-grade options. Most organizations seeking to protect their private data centers usually look at the enterprise models to provide cost-effective DDoS detection and mitigation. Many current solutions include capacities that can handle large-scale volumetric attacks for 100% protection across all three layers, or they can be used to supplement basic ISP-based bulk DDoS protection with additional advanced Layer 7 detection and mitigation.

COMPREHENSIVE APPLICATION PROTECTION ACROSS YOUR ORGANIZATION

While firewalls remain the first line of defense in your data center, many new threat trends targeting web applications require new capabilities to be added to your security infrastructure. Signature-based detection, IP reputation, and DPI can stop some—but not all—advanced threats, but they are limited in what they can offer. Additional products like WAFs, ADCs, and DDoS mitigation are needed to protect your data and users from a rising tide of sophisticated attacks.

DDOS MITIGATION: WHAT TO LOOK FOR

- **High bidirectional throughput**
- **Hardware-based L3, L4, and L7 DDoS attack identification and mitigation**
- **Behavior-based DDoS detection**
- **Complete invisibility to attackers (no IP or MAC addresses in the data path)**
- **Advanced DNS DDoS mitigation**
- **Hybrid on-premises/cloud capabilities**
- **Continuous threat evaluation to minimize false-positive detections**
- **IP-reputation scoring and continuous attack re-evaluation to reduce false-positive detections**

[1] "OWASP Top 10 – 2017," OWASP, March 27, 2018.

[2] "Equifax blames known web app glitch for hacking." Financial Times, September 17, 2017.

[3] "2018 Data Breach Investigations Report," Verizon, April 10, 2018.

[4] Setu Kulkarni, "Web application security: Creating a strong digital battlefront," GCN, June 26, 2018.

[5] Warwick Ashford, "DDoS a top security and business issue, study shows," Computer Weekly, May 2, 2017.

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
8 Temasek Boulevard #12-01
Suntec Tower Three
Singapore 038988
Tel: +65-6395-7899
Fax: +65-6295-0015

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

283234-0-A-EN
September25,201810:17AM
wp-web-application-security