The Present and Future of Application Protection

To succeed today, enterprises must broaden their view of security to address all the components at the application level that can expose sensitive data.

White Paper

by F5

Overview

In today's application-centric world, there's truly an app for everything. Organizations offer applications with data access to employees and consumers to drive greater productivity, meet business demands, and ultimately achieve a competitive advantage. But as organizations deliver more and more sensitive data through applications, they're also introducing ever-increasing risk. That's because today's users are everywhere—frequently outside the corporate network—and the apps they rely on can be anywhere, from private data centers to the public cloud. The result is less visibility and control for the organization. It's no surprise that cybercriminals are taking advantage of this exposure by targeting these applications, which exist largely outside the sphere of traditional security protections like firewalls, antivirus software, and TLS/SSL encryption.

Whether it's a volumetric denial-of-service (DoS) attack, browser-based malware, or an advanced persistent threat, today's application attacks are really gambits to obtain or compromise corporate data. As more and more data is encrypted traffic, the majority of today's security tools are running blind, unable to decrypt that data to ensure it's not malicious.

Traditionally, the approach to application security has been focused on the software development lifecycle (SDLC), trying to ensure developers are following best practices for secure coding. While secure code is still a core piece of the overall security puzzle, it's not the whole picture. The old security perimeter continues to dissolve as more endpoints and networks fall outside of conventional enterprise network footprints, while the risks to applications and sensitive corporate data continue to evolve.

Security measures must be enhanced to ensure apps are secured everywhere. The vast majority of attacks today target the application level—but enterprises are not making corresponding security investments at that level. It's time for organizations to come to terms with a new reality: Security needs to be more focused at the app level.

A Risk-Based Approach to Application Security

Looking at application security from this risk-based perspective enables organizations to focus on component failures and helps provide the most robust security for the data that's the ultimate target of most attacks. By analyzing all the components that make up an application, organizations can develop a strategy that delivers the strongest, most appropriate security to the app as a whole. Because compromising one component of an app or the network delivering it —whether a code vulnerability, network availability, or DNS—endangers the entire application, as well as the data it houses.

Critical Components of Application Security

It's vital for organizations to deploy the strongest possible set of application security controls to reduce the risk of sensitive data being compromised by an application-level attack. Key components of a proactive, defense-in-depth security posture for the application perimeter include application security testing, firewall services, access controls, and specific protection against various types of threats.

Application security testing

Software security is still a cornerstone of an overall application protection strategy. Organizations must ensure that new websites and software are coded securely, but they must also address the countless vulnerabilities already present in existing websites that were built without a secure software development lifecycle. It's important to remember that finding and fixing vulnerabilities isn't an academic exercise; it's all about keeping a sentient attacker out of enterprise systems and away from the data those systems protect. But without a clear picture of the adversaries and their tactics, security professionals will have a difficult time developing effective strategies to defeat them. Going forward, it will be imperative that more people working in the security community better understand software—and software security.

Vulnerability scanners help identify and mitigate software issues, whether they are found before or after new websites and web applications go live online. Organizations can obtain the best protection, however, by integrating a robust vulnerability scanner with a full proxy web application firewall.

Web application firewall

Today, a robust and agile web application firewall isn't a luxury—it's a necessity. The growth of cloud-hosted web applications has been accompanied by increasingly sophisticated security attacks and risks that threaten enterprise data.

A hybrid web application firewall can help enterprises defend themselves against OWASP Top 10 threats, application vulnerabilities, and zero-day attacks—no matter where applications are located. Strong layer 7 distributed denial-of-service (DDoS) defenses, detection and mitigation techniques, virtual patching, and granular attack visibility can thwart even the most sophisticated threats before they reach network servers. In addition, having the ability to detect and block attackers before they access an enterprise data center provides a major advantage. A powerful web application firewall that can stop malicious activity at the earliest stage of a potential attack allows organizations to significantly reduce risk as well as increase data center efficiency by eliminating the resources spent processing unwanted traffic.

Enterprises should look for a web application firewall that:

- Provides a proactive defense against automated attack networks.
- Integrates with leading dynamic application security testing (DAST) scanners for immediate patching of vulnerabilities.
- Identifies suspicious events by correlating malicious activity with violations.
- Delivers easy-to-read reports to help streamline compliance with key regulatory standards such as the Payment Card Industry Data Security Standard (PCI DSS), HIPAA, and Sarbanes-Oxley.

SSL inspection

Today, SSL is everywhere. Analysts predict that encrypted traffic will jump to nearly 64 percent of all North American online traffic in 2016, up from just 29 percent in 2015.[1] Organizations are scrambling to encrypt the majority of traffic, including everything from email and social media to streaming video. The level of security provided by SSL is enticing, but at the same time, it has become a vulnerability vector as attackers use SSL as a way to hide malware from security devices that cannot see encrypted traffic.

Enterprise security solutions must gain visibility into this encrypted traffic to ensure that it is not bringing malware into the network. One way to battle these encrypted threats is to deploy an SSL “air gap” solution, which consists of placing an Application Delivery Controller (ADC) on either side of the visibility chain. The ADC closest to the users decrypts outbound traffic and sends the decrypted communications through the security devices. These devices, which can now see the content, apply policies and controls, detecting and neutralizing malware. At the other end of the chain, another ADC re-encrypts the traffic as it leaves the data center. This solution provides the flexibility of keeping security devices in line while ensuring that they can do the job they were built for.

DDoS protection

Today, most apps are Internet based, so a volumetric DDoS attack can cripple—or even take down—an application. DDoS attacks are increasing in scale and complexity, threatening to overwhelm the internal resources of enterprises around the world. These attacks combine high-volume traffic clogging with stealthy, application-targeted techniques—all with the intent of disrupting service for legitimate users.

Organizations must ensure they have a robust DDoS protection strategy in place to ensure the availability of their critical applications. Consider solutions that offer comprehensive, multi-layered L3 through L7 protection and can stop DDoS attacks in the cloud before they reach the network and the data center.

DNS security

While not a part of the traditional, secure-coding view of application security, an enterprise’s DNS strategy plays a huge role in the security and availability of its applications. DNS is the backbone of the Internet, as well as one of the most vulnerable points in an organization’s network. Organizations must protect against an ever-growing variety of DNS attacks, including DNS amplification query floods, dictionary attacks, and DNS poisoning.

An enterprise can ensure that customers—and employees—can access critical web, application, and database services whenever they need them with a solution that intelligently manages global traffic, mitigates complex threats by blocking access to malicious IP domains, and integrates seamlessly with third-party vendors for implementation, centralized management, and secure handling of DNSSEC keys. Some solutions deliver high-performance DNS, which can scale quickly to better absorb DDoS attacks.

Web fraud detection

Fifty years ago, if you wanted to rob a bank, you had to actually go to the bank. Now, you can rob a bank from 5,000 miles away. The global nature of the Internet means that everything is equidistant to the adversary, and financial institutions are some of the highest-value targets on the Internet. To effectively combat the perils of fraud, organizations that offer financial services over the Internet must defend their businesses with a combination of security technologies.

Consider a solution that helps protect against a full range of fraud threat vectors, preventing attackers from spoofing, disabling, or otherwise bypassing security checks. Organizations can thereby reduce the risk of financial and intellectual property loss—and feel secure with proactive protection against emerging web threats and fraud.

Access controls

Some of the most recent and damaging security breaches have been due to compromised user and administrator credentials. These breaches may have been thwarted by authenticating and authorizing the right people to the right information and ensuring secure connectivity to applications with single sign-on and multi-factor authentication technologies. Furthermore, identity and access controls centralized by the enterprise can provide secure authentication between the enterprise network and applications based in the cloud or as Software as a Service (SaaS).

Conclusion: The Future of Application Protection

Application protection is fraught with complexity, and with the exponential growth of the Internet of Things and the applications that go along with it, the issues are only growing. In 2010, there were 200 million web apps; today, there are nearly a billion.[2] In 2020, that could easily be five billion. All those applications are vulnerability vectors—and many of them contain critical data that could be the target of attackers.

By enhancing existing security portfolios with solutions and services focused on the application level, organizations can better protect the applications that can expose their sensitive data. Ensuring that applications are protected no matter where they reside is critical—and the stakes are high.

It’s time to broaden the view of application security so that organizations are in a better position to effectively secure *all* the components that make up their critical apps, safeguard their data, and protect their businesses.

[1] Sandvine, *Global Internet Phenomena Spotlight: Internet Traffic Encryption*, 2015.

[2] Internet Live Stats

F5 Networks, Inc.
401 Elliott Avenue West, Seattle, WA 98119
888-882-4447 f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com