WHITE PAPER

The Changing Face of Web Application Security

neustar

TABLE OF CONTENTS

OVERVIEW

About This White Paper

In this white paper we will:

- Explore how the rise of applications continues to drive a complex threat landscape
- Review application layer attacks and their businesses impacts
- Highlight how web application firewalls (WAFs) can help mitigate exposure to vulnerabilities, missed patching updates, distributed architecture, and legacy systems before the next breach happens

The changing landscape of security threats –from networks to applications, from business disruption to data exfiltration and from single vector to multi-dimensional attacks–is driving an architectural shift in the security industry.

However, the evolution of the modern enterprise has also created precarious interdependencies and security gaps, making it significantly easier to exploit vulnerabilities across the infrastructure, especially at the application layer. Today's attackers live in a target rich environment. They do not need to go after the hardened targets, instead they focus on those left open, vulnerable, and exposed.

Application chaos is leading to opportunities for attackers. It is time to reconsider how we secure them.

APPLICATION CHAOS

The operational challenges facing IT and security teams are immense. On one hand, they have legacy on-premises applications that are critical to back-end business processes, but too dated to migrate to the cloud. These applications require constant care and attention, patching and updating to keep them operational and secure.

On the other hand, there has been a revolution in how applications are developed and deployed. Monolithic application stacks are no longer the default. Modern applications have exploded not just in raw numbers, but in how they are architected, built, and deployed. In the interest of speed, they have been broken into collections of microservices that operate independently, in different languages, which are portable across multiple public cloud environments and managed by orchestration systems like Kubernetes.

For example, a single banking application contains multiple microservices each with a specific function, such as access, account information, balance transfers, support, etc. Each microservice is written, tested, managed, and deployed by different teams in separate locations. The developers use containers to virtualize the application, enabling them to move it from their desktop all the way to production deployment without any involvement from IT, or security.

According to Ed Anderson, Distinguished VP Analyst, Gartner, "The proportion of IT spending that is being allocated to cloud will accelerate even further in the aftermath of the COVID-19 crisis, as companies look to improve operational efficiencies."

"The proportion of IT spending that is being allocated to cloud will accelerate even further in the aftermath of the COVID-19 crisis, as companies look to improve operational efficiencies."

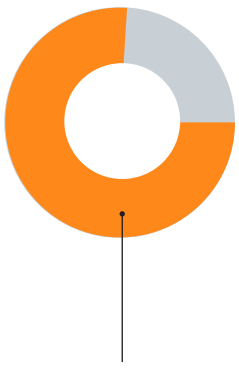
Ed Anderson, VP Analyst, Gartner

APPLICATION INSECURITY

Changes in development process, from waterfall to Agile have been centered around increasing automation, eliminating friction, and most importantly, increasing speed. Veracode's State of Software Security report, released in October 2020, demonstrates the consequences from a security perspective.

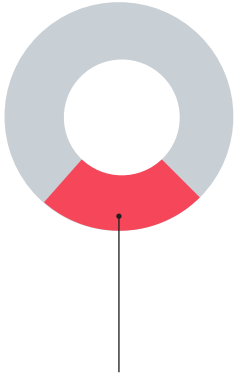
Flawed Applications Are the Norm

As a result, there is a growing movement for organizations to "shift left" and incorporate security earlier in the development process.



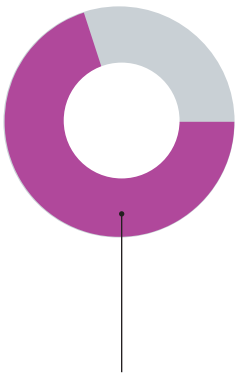
76%

of applications have at least one security flaw



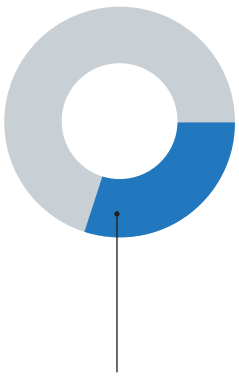
24%

have high-severity flaws



70%

of applications inherit at least one security flaw from their open source libraries



30%

of applications have more flaws in their open source libraries than in the code written in-house

ATTACKERS ARE WATCHING AND LEARNING

There are two immutable laws of cyber attackers:

1 If it is important to you, it is important to them.

2 Attackers are more interested in crimes of opportunity than taking on the most complex challenges.

Attackers live in a target-rich environment. They run, primarily, campaigns of convenience, not targeted sophistication.

A decade ago, when web applications first appeared, they were entirely centralized at one location. This non-distributed infrastructure represented a single point of failure and could result in the application being brought to its knees. What was the straightest line to disruption? DDoS attacks to exhaust resources, often with great success and significant business consequences.

Over the past few years, as the pace of application development and digital transformation took off, attackers saw how applications were being developed and deployed so they diversified their assault on the application layer, expanding from DDoS disruption to ransomware, to data exfiltration, oftentimes gaining access to an enterprise's most critical data.

How are they doing this? It starts with automated scanning that provides broad coverage searching for specific types of vulnerabilities in applications and infrastructure solutions. The exploits they find are then targeted by increasingly sophisticated tools and techniques for advancement and evasion. Attackers may not have targeted the crown jewels, but once inside, they may well gain access to them.

Just as enterprise sales teams like to land and expand within an account, attackers do the same, leveraging a broad set of capabilities that all build off the initial scanned vulnerability. They use distributed networks and multi-cloud deployments to gain a foothold in one application, service, or user account and then move laterally to find valuable information. There are several common attack vectors that put applications and application infrastructure at risk today:

SQL Injection (SQLi)

A SQLi attack uses a web form or other online input mechanism to send active unverified commands to an application's database. A SQLi attack can trigger the backend SQL database to execute SQL commands, allowing attackers to retrieve sensitive information from the database.

Cross-Site Scripting (XSS)

A XSS attack attempts to use JavaScript commands to modify Web page content or obtain information from a website and its users. XSS takes data from one website to pass to another and is an increasingly common form of attack.

Cross Site Request Forgery (CSRF)

A CSRF occurs when an adversary is able to trick or force an end user to execute an action from a third party, in an application where they are already authenticated in a bid to gain unauthorized access or information.

Common Vulnerabilities and Exposures (CVE)

CVE Attacks provide a common way to identify known vulnerabilities. With CVE attacks, attackers will simply scan for known vulnerabilities to identify if a given application target has, or has not, been patched. If the target hasn't been patched, the attacker will deploy a payload to exploit the target.

The demonstrated success of this attack playbook has led to relentless headlines with leaked company information such as intellectual property, customers' personally identifiable information, and salacious emails that were never intended for public consumption. Attackers know from experience that the new generation of applications are rich with potential vulnerabilities and attack vectors.

INDUSTRIES UNDER FIRE

Online businesses rely on information provided by customers to personalize services and reduce the risk of fraud. Unfortunately, the customers you have to worry about won't tell the truth.

IP decisioning and risk data provides independent insights you could be missing. When incorporated into your customer data and log-in flows, IP decisioning data reduces your risk—and allows you to serve good customers more effectively. The attacks in 2020 have not been evenly spread across vertical markets—some industries have been hit extremely hard. These include Gaming, Retail/eCommerce, Healthcare, and Financial Services:

Gaming

The casino side of the gaming sector is reeling from COVID lockdowns and travel restrictions. The situation has gotten so dire that one of the premier gaming companies in the world, Las Vegas Sands, is reportedly seeking a buyer for its Vegas properties, which include Sands Expo Convention Center, the Venetian Resort Las Vegas, and the Palazzo.

However, online gambling is booming, with a 43% increase in the number of daily online poker players and a 255% increase in first-time players.

It is also not surprising that attacks against gaming sites are on the rise. Neustar saw less than 50 attacks targeting gamers in February 2020, the number more than doubled in March then spiked to around 275 by May and stayed at that level in June.

43%

increase in the number of daily online poker players

255%

increase in first-time players

Retail/eCommerce

Digital has become the primary channel for retail. Turning a website into a platform for digital commerce can be complex. Enterprises end up relying on multiple software as a service (SaaS) providers with numerous plugins that enable the back-end commerce and logistics to support the front-end shopping. Attackers often develop payloads that can manipulate the basic call and response between app and user, making it a significant point of risk for the enterprise.

For example, Magento is an open-source e-commerce platform written in PHP. It uses multiple other PHP frameworks such as Laminas and Symfony. A retailer who is not accustomed to using Magento and is not closely following the patching by the other providers used by Magento, is leaving doors open for scanning and exploitation.

Healthcare

As the healthcare sector grew in importance in 2020, it should come as no surprise that it is among the most targeted industries by attackers. In October, the FBI, Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency (CISA) issued a rare joint warning to healthcare organizations being targeted by sophisticated ransomware attacks.

Financial Services

No industry spends more on IT or faces more cyberattacks than financial services. In fact, this sector experiences 300 times more attacks than any other vertical, according to CIO Dive.

According to top-ranked banking analyst Mike Mayo, "Retail customers have been jolted out of the bank branches and forced to use digital banking ... that's going exactly where banks' strategic plans have been going. So, in the last two months, you've accelerated the digital acceleration of the banks by two to five years."

As banks accelerate their digital transformation strategies, the pace of software delivery, and the migration to the cloud, they are at the same time exposing themselves to the risk of attack by bad actors. These culprits are targeting the fast-evolving apps and front-end infrastructure with everything from DDoS attacks to more advanced threats such as crypto mining, ransomware, and zero-day attacks.

Last summer the FBI issued a warning demonstrating how threat actors are creatures of opportunity, presenting defenders with a complex challenge.

"The FBI expects cyber actors to attempt to exploit new mobile banking customers using a variety of techniques, including app-based banking trojans and fake banking apps."

The frequency and size of these attacks has caused many businesses to take a different approach to application security, and many are now looking at WAFs as an extra layer of protection.

WHY WAF?

Key Considerations for WAF

Not all WAFs are created equal. When considering a WAF, there are several critical capabilities that should be evaluated to better prepare for incoming attacks and outbound threats.

- Given that modern organizations use both on-premises and cloud resources, a WAF solution should be resource-agnostic, such that it can work across any type of environment.
- Given the rate of change of applications it should learn — Artificial Intelligence/Machine Learning (AI/ML)
- It should provide coverage for common attack vectors OWASP/Signature while enabling more mature security teams.

When applications moved from on-premises to multiple clouds, the entire notion of perimeter defense went out the window. No longer could applications be protected by a single piece of hardware infrastructure. A firewall at the enterprise perimeter was no longer sufficient. The first generation of WAFs were on-premises and tuned to protect specific applications. Many WAFs today are still deployed that way. The challenge is two-fold; most applications live in the cloud today, and few if any organizations can effectively scale bandwidth to properly scrub and analyze massive volumes of traffic for the applications that remain on-premises.

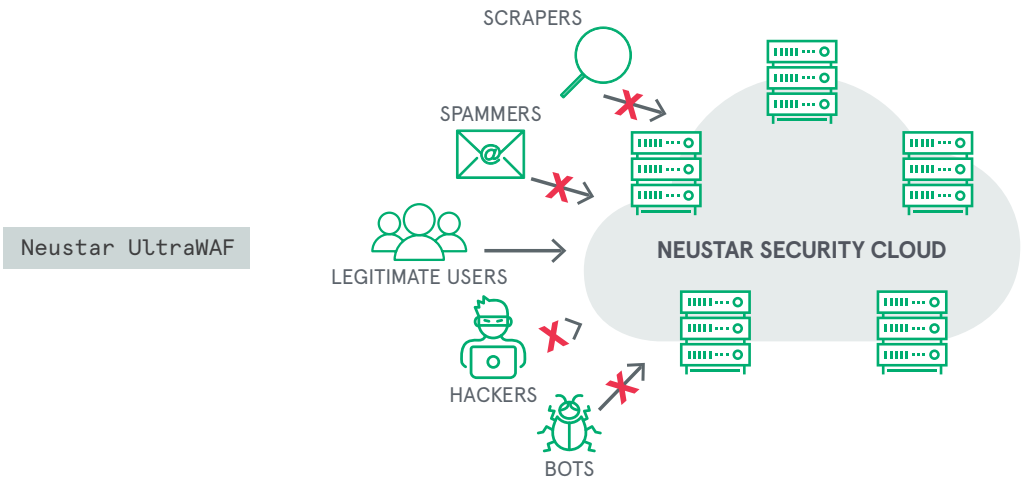
Modern applications are built in containers and microservices, consisting of multiple tiers that make an attractive attack surface for adversaries. These are out of reach of the traditional enterprise security stack. A recent Neustar customer survey found that 40 percent of respondents disclosed that more than half of the attacks targeting their business had managed to get around their traditional firewall solution. Anti-malware technology is focused on endpoints, while identity and access control solutions narrowly address a specific risk, and an Intrusion Protection System/ Intrusion Detection System (IPS/IDS) focuses more network protection.

From SQL injection attacks to Cross Site Scripting, attackers are enjoying success in areas where a WAF would otherwise stop their progression. WAFs serve to enhance the security perimeter by providing an additional barrier between attacker scanners and the application layer. A WAF can help mitigate exposure to vulnerabilities, missed patching updates, distributed architecture, and legacy systems.

In fact, WAFs are so mission-critical that they are mandatory for industries like Finance, Healthcare and E-Commerce that need to safeguard against the leaking of intellectual property and personally identifiable information (PII).

ABOUT UltraWAF

As in most areas of security, providing the right protection begins by analyzing the asset that you are trying to protect. For those organizations that already have an on-premises WAF hardware or software solutions, Neustar's cloud-based UltraWAF can serve as powerful complementary tool.



UltraWAF provides additional coverage and support for existing, highly tuned on-prem WAF deployments by filtering out bad traffic from the public cloud before it ever reaches the local network. By integrating UltraWAF, it is possible to reduce the overall traffic load for on-premise devices, enabling them to be tuned even more precisely.

Neustar UltraWAF is cloud-provider, hardware, and CDN agnostic, delivering visibility into application traffic, no matter where the apps themselves are hosted. Our vendor-agnostic approach simplifies configuration and enables seamless management of a unified policy across complex environments that can be driven programmatically or via a user-friendly portal.

UltraWAF supports custom workflows that can be configured based on policy and application profile. The system can first be placed in learning mode to understand normal traffic patterns and then be switched to automated enforcement and anomaly detection.

LEARN MORE

To learn more about how Neustar UltraWAF can support your security needs **click here**, email us at **security@team.neustar**, or call us at **1-855-898-0036** in the US and at **+44 1784 448444** in the UK.

ABOUT NEUSTAR

Neustar is an information services and technology company and a leader in identity resolution providing the data and technology that enables trusted connections between companies and people at the moments that matter most. Neustar offers industry-leading solutions in Marketing, Risk, Communications, and Security that responsibly connect data on people, devices and locations, continuously corroborated through billions of transactions. Neustar serves more than 8,000 clients worldwide, including 60 of the Fortune 100. Learn how your company can benefit from the power of trusted connections at **www.home.neustar.**

WP-SEC-262567-01.12.2021