**SPOTLIGHT**

*Sponsored by: Fastly*

**Applications power the all-important online experience. Now, security modernization is required to keep pace with the innovation of the digital-first era.**

# Securing a Modern Online Experience That Demands Performance and Value

*June 2023*

**Written by:** Christopher Rodriguez, Research Director, Security and Trust

## Introduction

For many modern businesses, a digital presence is a key channel for reaching audiences and customers around the world. The online experience is a critical concern for these organizations and is a make-or-break factor for businesses that are built entirely around a digital presence.

Applications are the engines that power user experiences, providing the interactivity that enables countless innovative use cases across web and mobile. These applications are designed to be exposed to users around the world at any time of day via common web browsers.

Thus, the importance of applications to the modern digital business cannot be overstated and continues to expand. Enterprises are embracing a similar online experience strategy to empower worker productivity as well. Web and mobile applications provide benefits such as allowing employees to utilize their own devices for work purposes and simplifying contractor access.

Despite the value of such functionality and widespread, easy access, the concomitant increase in business risk is one key drawback. Threat actors also benefit from uninhibited access, allowing them to scan and probe for vulnerabilities and gaps in defenses. As a result, weak or nonexistent security practices have driven an increase in data breaches in 2023. There are many reasons behind this increase, including simple misconfigurations and supply chain attacks. However, many of the breaches noted involved well-known threat vectors such as code injection and cross-site scripting, both of which increased year-over-year as well. Legacy approaches to application security have proven to be overly brittle and static in nature, forcing businesses to make trade-offs between steady security states and aggressive development of new applications, features, and functionality.

Overall, businesses must deliver powerful functionality and user experiences that are trustworthy and frictionless to compete in the digitally transformed era. Thus, application security is paramount to the risk mitigation efforts of the IT organization as well as broader business goals. There remains room for improvement, however, as businesses identify and rectify the weaknesses of legacy tooling in their security architecture. For application security, an updated, modernized approach to security is required.

## AT A GLANCE

### KEY STATS

Businesses are focusing on secure, edge, and cross-ecosystem digital strategies. Business leaders prioritized the following as themes for digital-first strategies:

- » Unified security
- » Cross-ecosystem
- » Edge data

However, applications are an emerging weak point in security defenses:

- » Application security breaches have grown drastically from 2022 (57% of businesses) to 2023 (78% of businesses).

(source: IDC's *DevSecOps Adoption, Techniques, and Tools Survey,* January 2023, April 2022, n = 311)

## Definitions

**Web application firewall (WAF):** A specialized security gateway that protects web application traffic against a variety of attacks, including automated bots, code injection, and application layer denial of service. WAF leverages a variety of techniques to protect applications including positive and negative security models, access policies, and client/IP reputation. WAF solutions are offered in a variety of form factors including appliances, virtual, and SaaS.

**API security:** The practice of protecting API communications from misuse, abuse, and exploits through secure design, testing, identity management, policy enforcement, and threat detection. Some functions are aspects of established practice areas and technologies such as application testing, identity management, WAF, and API management. However, specialized solutions exist to fully address the unique security requirements of APIs.

**Bot management:** Specialized solutions to detect, categorize, and control automated bot activities affecting a web application. Bot management solutions offer a variety of methods for detection as well as multiple options for response depending on the nature of the bot activities.

**Distributed denial-of-service (DDoS) mitigation:** Solutions and services designed to detect and mitigate the impacts of a DDoS attack.

**Web application and API protection (WAAP):** A converged security solution that provides essential protections for application front ends and APIs. WAAP solutions offer a foundation of WAF and add various capabilities across API security, bot management, and DDoS mitigation.

## Benefits of Application Security Modernization

### Streamlining Security for Strong Security

The web application firewall, as a security technology, was introduced nearly two decades ago as a dedicated tool for providing specialized protections for the unique needs of web applications. However, during the digital transformation era, application development and infrastructure changed at a rate that challenges the traditional application security models and tools. Furthermore, developer teams are increasingly leveraging microservices architecture to accelerate time to market. As a result, DevOps teams can deliver new features and updates rapidly and often. Developers that use microservices deploy code weekly in most cases, and some deploy code multiple times a day or even hourly.

Legacy WAFs cannot completely provide a critical level of protection across the many new computing environments, design practices, and use cases introduced in the digital-first era. Security teams must make a choice between basic WAF capabilities designed for specific infrastructure or deep security functionality that is difficult to implement in edge and cloud environments.

A new generation of WAF solutions are emerging to bridge the gap caused by modern application technologies, infrastructure, and practices. By providing security rules that adapt to the constantly changing nature of applications, business leaders can ensure that security does not inhibit CI/CD pipelines. These solutions provide dynamic protections to replace the traditional approach of regex rules, tuning, and adjusting protections to prevent false positives. Essentially, modern solutions provide security that "just works," blocking threats, but without the time-consuming requirement for constant tuning and learning cycles.

## Flexible Security Lowers Hurdles to Innovation

Flexibility in deployment options and integrations is crucial to meet security and developer teams where they are currently and where they go next. The approach of investing in several one-off solutions designed to support a particular environment is increasingly unfeasible because businesses now leverage multiple cloud providers to gain benefits of cost advantages, business agility, or performance. This heterogeneous environment leads to security complexity, which leads to gaps, conflicts and, eventually, breaches. As each organization moves to cloud on a different path and at a different pace, the ability for modern WAFs to provide consistent protection across all environments is more important than ever.

Furthermore, developer teams are embracing APIs and microservices architecture and aggressive development practices to ensure speedy time to market and innovation. Applications are increasingly integrated now, using APIs to connect applications internally and externally for delivering new functionality and enhanced user experiences. The strategy ensures a strong degree of competitiveness in the marketplace but also drives business risk if security processes cannot match the pace.

IDC found that organizations are interested in DevSecOps strategy as a method to ensure continuous security throughout the development life cycle due to benefits of improved security posture (34%), improved compliance (20%), and ability to improve the pace of application development while maintaining an existing security posture (15%). However, a lack of collaboration between application development teams and security teams was a top concern (17%) (source: IDC's *DevSecOps Adoption, Techniques, and Tools Survey,* January 2023, n = 311).

Furthermore, modern WAF solutions add functionality to integrate with these "shift-left" strategies to support businesses in their efforts to empower innovation while continuing to mitigate risk. IT buyers cited the ability to integrate security tooling into the DevOps CI/CD pipeline as a top 3 technical challenge for DevSecOps adoption (23%).

## Edge Protection Enables the Performant Experience

Modern security solutions must operate across the internet, offering seamless integration with multiple public clouds, edge compute, CDNs, and private cloud and on-premises environments. Cloud and edge services enable earlier detection of threats, stopping attacks as close to the threat as possible. This edge security approach reduces latency and prevents the need for a compromise between security and performance. Performing security at the edge, in combination with general compute capabilities, is key to enabling cutting-edge use cases such as autonomous fleets and augmented reality. Modern WAF solutions are designed to provide a consistent security posture across cloud, edge, and on-premises environments.

## Smart Security Drives Business Value

Dynamic protections that do not require tuning are becoming table stakes in an era when speed to market and cutting-edge functionality are top business priorities. This dynamic approach to security offers efficiencies that free security teams from having to spend time investigating false positives or adjusting WAF features to prevent breaking an application. Instead, modern WAFs generate fewer false positives and actionable alerts, which leads to better security outcomes with less wasted time.

Simplified security is also essential to improve adoption among developers, with modern WAF solutions better aligned with modern workflows. More importantly, accurate security improves the trust that security goals will not hinder application performance or break applications, leading to better, more productive relationships between security and DevOps teams.

However, the value of modernized application security must be recognized in the broader business advantages that are enabled by smart, adaptive, and flexible security approaches. Strong application security is mutually beneficial for both digital businesses and consumers. By protecting the confidentiality and privacy of personal data, including health information and payment information, businesses can foster strong lifetime relationships with customers. For businesses, eliminating unwanted bot activity will ensure that products are delivered only to genuine customers, and blocking fraudsters will reduce costly chargebacks. While the value of trust can be challenging to quantify, business leaders are keenly aware of the benefits. 46% considered "digital trust programs" to be a priority investment, whereas 38% considered them to be a top priority investment (source: IDC's *Future Enterprise Resiliency and Spending Survey, Wave 6,* July 2021, n = 791).

## Key Trends in Application Security

### Multicloud/Hybrid Cloud Practices Present Operational Challenges for Traditional Security Approaches

Applications are emerging as critical control points in the cybersecurity architecture. WAF remains a vital part of the application security strategy, providing a base level of protection across all application communications. While these solutions were once exclusively on premises, new form factors have been added to allow IT organizations to extend protections and policy enforcement to multicloud and hybrid cloud environments. Early approaches to adapting WAF to the cloud focused on virtual appliances that presented bottlenecks that hindered cloud scalability.

Cloud service providers also tend to offer WAF capabilities of their own as easy add-on services. These solutions are typically limited to essential protections such as well-known threats described by OWASP, such as code injection and misconfigurations. More importantly, the usage of one-off security tools for specific environments leads to security complexity, inconsistent policies and protections, lack of portability, and business agility.

As a result, businesses found limitations and trade-offs associated with both cloud-specific WAFs and legacy WAF approaches. IDC research confirms that security across multiple cloud environments is both the biggest risk addressed by DevSecOps and the biggest technical challenge (source: IDC's *DevSecOps Adoption, Techniques, and Tools Survey,* January 2023, n = 311).

### Modern Threats Use Automation for Scale

Threat actors are creative and clever, using automation to test defenses regularly and to cast a wide net. Bots are used to automate attacks of all kinds and all severity, from anti-competitive, disruptive, and nuisance activities to malicious, fraudulent, and criminal actions. Malicious activities such as account takeovers and data theft are top concerns. However, IT organizations prioritize other issues as well, such as scraping, data aggregation, and other forms of automation, depending on the nature of the business.

This is a growing area of concern for enterprise security teams. 20% of security professionals noted malicious bots as a top 5 concern for securing business operations and IT environments (source: IDC's *Global Outsourced Cybersecurity Services Survey,* December 2021, n = 517).

### APIs Lead to New Security Risks

54% of organizations cited microservices and APIs as key for enabling easy integration of new products and features as well as integration with other applications (IDC's *Future Enterprise Resiliency and Spending Survey, Wave 12,* January 2022, n = 810). However, APIs are vulnerable to the same attacks that target application front ends. APIs also introduce new threat vectors and vulnerabilities, including business logic attacks. Given the low level of maturity around the threat vector, API threats continue to focus on simple attack vectors. Unauthorized access via an API was a popular attack method in 2022, representing 21% of reported application security breaches (source: IDC's *DevSecOps Adoption, Techniques, and Tools Survey,* January 2023, n = 311).

Legacy WAF solutions lack visibility into or understanding of API communications. This can lead to gaps in security visibility, and threat actors are continually leveraging their botnets to find unprotected or underprotected APIs. As a result, specialized API security solutions have emerged to fill the gap left between API management and legacy WAF solutions. Modern WAF solutions offer the ability to inspect and apply policy and protections to API traffic.

## Considering Fastly

Fastly is a provider of cloud services for application and media delivery as well as security services. The company offers Next-Gen WAF, a comprehensive application security solution it gained through the acquisition of Signal Sciences in 2020. Fastly provides essential protection against known threats as well as capabilities to address emerging security needs for APIs, bots, and DDoS risk.

### Performance

The Fastly Next-Gen WAF is architected for scalability and performance and is built on a cloud-native architecture that leverages containerization to apply full-stack application security at scale. The company leverages a combination of lightweight agents, optional modules for performance, and a centralized cloud analytics engine to balance speed and security. As such, the Fastly Next-Gen WAF service offers low-latency, rapid security decision making at the edge.

At its core, Fastly leverages the Signal Sciences SmartParse technology to deliver a high degree of security performance for applications and APIs. The SmartParse approach avoids the requirement for learning and tuning time associated with machine learning approaches. As a result, the Fastly Next-Gen WAF provides very low false positive rates as well as consistent protection across application versions and updates. As such, Fastly ensures a consistent, high level of security that is not a hindrance to or degraded by aggressive CI/CD pipelines. Fastly claims that 90% of customers use the WAF in blocking mode because of its SmartParse technology.

To tailor security based on unique business or application needs, the Fastly Next-Gen WAF allows for business-specific or application-specific logic through custom rules that leverage systems signals or custom signals based on customer-created labels and tagging. Signatures can be automatically added or customer-created depending on use cases or the nature of the applications they are protecting. The signals approach offered by the Fastly solution allows teams to gain more visibility and take greater control over the application traffic.

### Flexibility

To protect applications across complex, heterogeneous hybrid IT environments, the Fastly Next-Gen WAF supports multiple deployment options, including edge, cloud, virtual appliances, containerized images including proxy and sidecar patterns, and service meshes. Fastly's Next-Gen WAF secures and supports emerging application and API protocols such as WebSockets, GraphQL, and gRPC, to further assist the evolution of web applications to power enterprise use cases. Furthermore, the company invests heavily to support modern compute, cloud, and edge environments. For example, the Fastly Next-Gen WAF can secure applications in cloud edge containers. The solution also supports Arm processors to empower businesses to architect their edge compute deployments based on the unique balance of power and energy efficiency required.

Importantly, the Fastly Next-Gen WAF is designed to integrate with DevOps workflows and tooling to streamline operations and to deliver metrics that aid DevOps in troubleshooting. The Fastly Next-Gen WAF can be deployed with Terraform to further simplify deployment at DevOps scale.

### Value

The Fastly approach to value is centered on security that is low effort, but high efficacy. The SmartParse engine provides a dynamic set of protections that ensure a consistent security posture across versions and updates. The edge delivery options offer a high-performance application experience to support innovative use cases. The combination of detection accuracy, security insights, and asynchronous design offers protection without inhibiting performance or breaking applications.

The company places a high priority on customer support, citing strong NPS and customer references. To further aid businesses along their security modernization journeys, the company offers managed security services that reduce the strain on overtaxed IT and security teams.

### Challenges

Fastly specializes in application security, with an ability to provide purpose-built capabilities for the unique needs of the threat vector. Fastly's competitors are also at varying degrees of integrating application security offerings, such as zero trust network access (ZTNA), cloud access security broker (CASB), and secure web gateway, into enterprise security suites. Generally, these remain two separate competitive landscapes, but some cross-pollination is already available that may change buyer requirements.

## Conclusion

Application security is a powerful but often overlooked enabler for the all-important online experience. However, in recent years, there have been rapid changes in the way applications work as well as where they exist, how they are made, and the threats they face. IDC has noted rapid growth in the market as security vendors race to develop a new generation of WAF solutions that can meet the complex needs of modern applications and APIs. Fastly is working to define the next generation of WAF, and to the extent that the company can address upcoming challenges, Fastly can help organizations deliver on the full promise of the digital-first era.

Security at the edge, in combination with general compute capabilities, is key to enabling cutting-edge use cases.

# About the Analyst

### ***Christopher Rodriguez,*** *Research Director, Security and Trust*

Christopher is a Research Director in IDC's Security and Trust research practice focused on the products designed to protect critical enterprise applications and infrastructure. IDC's Security and Trust research services to which Chris contributes include Active Application Security and Fraud, where he covers web application firewall, DDoS mitigation, bot management, and API security.

## MESSAGE FROM THE SPONSOR

### More About Fastly

Fastly's programmable edge cloud platform helps the world's top brands deliver the fastest online experiences possible, while improving site performance, enhancing security, and empowering innovation at global scale. With world-class support that achieves 95%+ average annual customer satisfaction ratings, Fastly's suite of edge compute, delivery, security and observability offerings have been recognized as leading solutions by industry analysts. Compared to legacy providers, Fastly's powerful and modern network architecture is one of the fastest on the planet, empowering developers to deliver secure websites and apps at global scale with rapid time-to-market and industry-leading cost savings. Thousands of the world's most prominent organizations trust Fastly to help them upgrade the internet experience, including Reddit, Pinterest, Stripe, Neiman Marcus, The New York Times, Epic Games, and GitHub. Learn more about Fastly at www.fastly.com.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

**IDC Research, Inc.**
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

**This publication was produced by IDC Custom Solutions.** The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.