IDC

**SPOTLIGHT**

*Sponsored by: Radware*

**Applications have evolved rapidly over the years, and security practices must evolve, too, toward a more integrated, context-driven, "smart" approach.**

# A Modernized Security Approach to Overcome Risks of New Application Technologies

*June 2023*

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

## Introduction

Web applications power the online experience, allowing businesses to reach broad, new audiences. As such, the importance of these applications cannot be overstated. Businesses invest heavily in numerous delivery and security technologies to ensure a performant, user-friendly experience.

Similarly, IT organizations have deployed layers of protection such as DDoS mitigation and web application firewall (WAF) solutions, that protect against disruption and data theft. But application security is a tightrope act as businesses prioritize user experience and speed to market over application security.

Furthermore, application security has changed over the years. Now, applications face a range of threats, from zero-day exploits to business logic abuse. Application security is further complicated by the many new technologies that businesses leverage to improve agility, scalability, and delivery of new features. Highly specialized security tools have come into prominence as a result, with each one requiring additional time and training to deploy and manage.

Enterprises need solutions that can help them deliver a frictionless, fear-free user experience. This goal will require application security practices to mature beyond a collection of one-off tools to a more integrated, context-driven, "smart" approach.

## AT A GLANCE

### KEY STATS

- "Cybersecurity threats" was cited as the risk that will have the greatest impact on technology investment plans (IDC's *Future Enterprise Resiliency and Spending Survey, Wave 11,* December 2021, n = 858).
- 29% of organizations leverage cybersecurity to enable sharing of data, applications, and operations with partners (IDC's *Future Enterprise Resiliency and Spending Survey, Wave 9,* October 2022, n = 817).

## New Technologies and Development Practices Move the Application Security Goalposts

Security practitioners are already very familiar with the "cat and mouse" game that cybercriminals play. With potentially lucrative payouts at stake, hackers are continually inventing new methods of circumventing defenses. Application infrastructure and the applications themselves have changed as well. Every new technology introduced into the development and deployment of applications requires an accompanying adjustment to security strategy.

## Applications Have Evolved

Applications have evolved in design, purpose, and execution. Applications are no longer monolithic compilations of millions of lines of code deployed on a mainframe in a datacenter. Instead, developers now focus on microservices architecture, designing applications as a suite of loosely coupled services that implement specific functions. Businesses are embracing microservices architecture because it offers composability, code reuse, and API usage. 54% of organizations cited microservices and APIs as key technologies enabling easy integration for new products and features and with other applications (IDC's *Future Enterprise Resiliency and Spending Survey, Wave 12*, January 2022, n = 810).

Most importantly, applications are developed for new use cases every day. As a result, applications must support a spectrum of client types, including web, mobile apps, IoT devices, APIs, and even other applications. In recent years, developers have embraced client-side code to make applications faster, which is particularly useful in cutting-edge use cases such as autonomous vehicles and smart factories.

## Application Infrastructure Has Changed

Modern design principles and technologies enable portability and flexibility of deployment, while infrastructure changes, such as cloud and cloud-native infrastructure, offer further benefits for application performance, stability, and portability.

The combination has enabled applications to leave the confines of private datacenters to public cloud environments, containers, and even serverless. For many organizations, applications and workloads are often distributed across multiple cloud environments or hybrid deployments across public and private cloud. Businesses often leverage multiple clouds for specialized capabilities, redundancy, business agility, and cost management.

These changes have also introduced new security concerns. In the past, there was a high degree of correlation between the physical perimeter of the organization and the security perimeter of the web application. As applications have become more distributed, this perimeter has disintegrated. Organizations following a legacy network perimeter approach to security are increasingly susceptible to attacks. The usage of point products or built-in security functionality may also lead to inconsistent policies and protection gaps.

Such changes are often driven by business needs and so may not be unavoidable either. For example, businesses have demonstrated an eagerness to share applications and data with industry ecosystem partners: 29% of organizations are relying on cloud applications and infrastructure to enable sharing of data, applications, and operations (IDC's *Future Enterprise Resiliency and Spending Survey, Wave 9,* October 2022, n = 817). APIs offer extensive business benefits by facilitating easy integration with partners and third-party systems. Unfortunately, these API integrations also decrease visibility for legacy security tools, drive risk of lateral movement, and introduce unknown entry points and expanded attack surfaces. Rising API-related risk is readily visible in the headlines as cybermiscreants regularly find new unprotected APIs to exploit with ease.

## Audiences Expanded, Expectations Increased

Security teams, developers, and business leaders are all challenged to do more with less, to produce at a higher level, or to drive value. As a result, modern application design, technologies, and infrastructure have offered appealing benefits to businesses. Code reuse and third-party libraries help developers deliver on time. Business leaders commission new applications to support a broad spectrum of users, from anonymous users to employees.

With these changing audiences and use cases, risk tolerance and performance requirements will vary. Security teams are also challenged to do more with less because of a lack of available security expertise in the labor market. With new threat vectors and security tools added each year, 45% of businesses are looking to outsource cybersecurity to managed security services providers, as evidenced by IDC survey research (IDC's *Security ServicesView Survey*, February 2022, n = 1,400).

Certainly, new use cases will continue to drive new security requirements and considerations. These objectives are not mutually exclusive but are real-world considerations and trade-offs that factor into security strategy. Because applications are designed to provide a legitimate user with functionality, some business logic abuse concerns may not be evident beforehand and will be identified only through trial and error. Innovation is an inherently risk-prone process.

## Application Security Strengthens Trust in the User Experience

The modern digital business relies on numerous applications to convey, capture, and create data. For many organizations, web and mobile applications are the first or only point of contact with customers. By definition, web applications must be exposed to the world community, leading adversaries to perceive these applications as lucrative or easy targets.

### Security as the Foundation for Trust

IDC research shows that extensive efforts have been made to secure applications, with the global market reaching $3 billion in 2022 investments across solutions such as WAF, bot management, DDoS mitigation, and API security (IDC's Security Products Tracker, 2H22). These established approaches to application security continue to play a foundational role because digital transformation is an ongoing evolutionary process. However, modernization of application security architecture offers key benefits, such as reducing risk and increasing threat detection rates.

### Smarter Detections Reduce Risk

Web applications face a high degree of risk by design. Enterprise applications are typically protected by layers of network security, such as firewalls, threat prevention systems, and authentication systems for credentialed users. By comparison, web applications are intentionally exposed to a wide range of end users, including anonymous users. As most web application users are unauthenticated, this glaring security blind spot has been widely accepted as unavoidable.

However, identity-aware information is the foundation for understanding user behavior in the context of intent. A deeper understanding of identity, behavior, and intent is necessary to detect sophisticated attacks including fraudulent, malicious, or otherwise unwanted activities. Identity context and behavioral trust decisions must be able to factor in the anonymous nature of users and address it while identifying insights where possible.

Alignment with this new approach to application security will require orchestration of signals and contextual information spanning persistent identity insights, identity proofing, behavior-based detection, and device security posture. By establishing the new security perimeter of web applications based on identity and intent, digital businesses will be better positioned to establish a proper level of trust with their audience.

### *Modern Applications Need a Modern Security Approach*

Given these changes in the design and deployment of modern applications, traditional web application security tools no longer provide sufficient coverage to protect them against up-and-coming threats. Rather, a modern security approach is required, based on the following tenets:

- **A comprehensive, modular platform.** While WAF remains a vital part of the application security strategy, a WAF on its own is no longer enough. Rather, modern application security requires comprehensive protections across WAF, bot, API, and DDoS attack vectors. As modern web applications increasingly leverage client-side functions for code execution or data storage, client-side security is also becoming more of a requirement. A comprehensive, modular platform, which combines all these protections in a single solution, should be the foundation of any application defense strategy.
- **Cross-ecosystem protection.** As organizations increasingly adopt hybrid cloud deployments consisting of microservices, Kubernetes, and multiple cloud environments, cross-ecosystem application protection becomes more and more important, enabling organizations to protect their applications in a consistent, uniform, and centralized manner.
- **Identity-aware, intent-based analysis.** Whereas in the past there was a high correlation between the security perimeter of the web application and the physical perimeter of the organization's datacenter, the new cross-cloud, containerized, and client-side centric application design means that this perimeter has largely dissolved. This moves the foundation of application defense from inspecting communications via an inline-deployed WAF to being focused on the identity of the host making the request and discerning the intent behind it to distinguish between legitimate and malicious requests.

As IT budgets tighten in 2023, few organizations have the luxury of scaling back their investments in cybersecurity. In fact, businesses continue to rely on traditional applications for certain use cases, and these use cases are well served by a traditional on-premises WAF. Instead, businesses benefit from modern application security solutions that support existing investments. These existing WAF investments can and should be incorporated into a modern application security strategy to ensure consistent protection across all environments. Furthermore, a modernized application security strategy will offer improved accuracy of threat detection with lower false positive rates, which will block with a high degree of fidelity and make alerts actionable.

## *Considering Radware*

Radware provides purpose-built application and infrastructure protection solutions. The company's approach to application security leverages a cloud-based portfolio that is broad and includes purpose-built solutions for WAF, DDoS mitigation, API protection, bot management, and client-side security. Radware recently announced a new holistic, 360-degree vision for application protection in the modern digital transformation era, emphasizing three key principles: leveraging identity and intent insights; supporting modern application designs, technologies, and infrastructure; and addressing security team needs.

### *Leveraging Identity and Intent Insights for Enhanced Application Protection*

Radware is focusing on offering identity-based controls that are designed to provide insights and attestation of unknown, unauthorized users. The solution, recently introduced in its Bot Manager, builds a single source of truth for user identity spanning numerous signals such as IP address and device fingerprinting. Identity persistence is established via new blockchain-based crypto ID to ensure stateful analysis of user risk.

Radware aims to combine this identity-aware context with behavior-based detection to understand intent. Radware security mechanisms are based on a "positive" security model, which uses behavior-based learning to study the behavior patterns of legitimate web application users and discern the intent-based activity to understand whether a client's behavior is legitimate or not.

### *Supporting Modern Application Designs, Technologies, and Infrastructure*

Radware's vision for holistic application protection requires a model that is agnostic to underlying environments and infrastructure. As a result, Radware solutions are offered in a variety of delivery models for customer flexibility and consistent protection.

The company's cloud-based SaaS suite integrates WAF, bot management, Layer 7 DDoS protection, API security, and client-side protection for defense of cloud-based and hybrid environments. The SaaS suite also offers Kubernetes WAAP deployment options running as a Kubernetes sidecar for Kubernetes-based applications in air-gapped environments as well as for east/west lateral protection within organizational networks.

To support multicloud and hybrid cloud deployments, Radware developed its SecurePath architecture, offering an API-based, out-of-path deployment option that does not require changes to DNS redirection and provides consistent security across on-premises, private cloud, and public cloud environments.

### *Addressing Security Team Needs*

The Radware solution leverages AI and machine learning technologies for threat detection. The approach is designed to provide accurate, actionable alerting and automated protections. In addition, the new service is offered as a fully managed security service, which helps with ease of deployment as well as reducing the friction required to operate.

### *Challenges*

Radware faces a number of competitors that are positioning essential capabilities as easy add-on services or built-in capabilities. Generally, these strategies focus on lower-friction options for deploying security, with advanced security capabilities as a secondary consideration or unavailable. Partnerships may help alleviate the competitive pressures. Similarly, broader industry frameworks may be necessary to establish appropriate divisions of responsibilities between application and infrastructure providers and security providers.

Enterprises require application security solutions that can help them deliver a frictionless, fear-free user experience.

## *Conclusion*

IDC believes that applications are emerging as a critical control point in the modern cybersecurity architecture. Overall, enterprises require application security solutions that can help them deliver a frictionless, fear-free user experience. To the extent that Radware can address the challenges described in this paper as it positions itself appropriately and looks ahead to the next iteration of web application development, the company will have a significant opportunity to help customers succeed in their application security journeys.

# About the Analyst

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

Christopher Rodriguez 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 Radware

Radware helps organizations stay ahead of emerging threats by combining state-of-the-art protection, frictionless integration, and industry-leading knowledge and expertise.

Radware offers a comprehensive, cloud-based security platform which includes a web application firewall (WAF), bot management solution, API protection, DDoS protection and client-side security. This comprehensive platform is centrally managed through an intuitive management portal, with robust management, reporting and analytics capabilities.

Radware's state-of-the-art security mechanisms are based on a 'positive' security model using advanced machine-learning and artificial intelligence algorithms. This helps provide Radware's customers a higher level of protection, with lower rates of false positives.

In addition, Radware offers frictionless integration for today's multi-cloud and microservices-based environments with flexible deployment options and a dedicated Kubernetes edition.

Finally, Radware's security tools and services are backed by our Emergency Response Team (ERT), one of the industry's largest and most experienced teams in application security.

Visit us at www.radware.com to learn more.

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