SPOTLIGHT

Sponsored by: A10 Networks

Organizations require application security practices to mature beyond a collection of one-off tools — loosely integrated or not — to a more integrated, context-driven, "smart" approach.

Aligning Application and API Security with the Demands of the Modern AI Era

July 2025

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

Introduction

Applications and APIs power the modern digital economy, allowing businesses to reach customers, prospects, employees, and partners. These applications vary widely, as needed, to support a broad range of user types and specialized use cases. However, they share a common requirement — users have high expectations for a positive, reliable, and performant experience. As end-user familiarity with new AI technologies grows, it heightens their expectations for a user experience that is real time, engaging, frictionless, and trustworthy.

Business decision-makers have taken stock of the importance of applications and APIs' contribution to the bottom line and are now looking to leverage emerging technologies to enhance their applications and APIs. The challenge is that new and rapidly changing technologies introduce novel and shifting application security needs. APIs have already expanded the attack surface in recent years by exposing business logic to third parties. Now, AI is introducing a sharp escalation in threat types, volume, and tactics, as the malicious use of AI allows criminals to find zero-day vulnerabilities in mass quantities and write exploits with ease. In recent years, applications and devices have been increasingly interconnected to deliver a richer end-user experience. Now, GenAI and AI-enabled applications are introducing novel risks, such as prompt injection, model manipulation, and data set poisoning.

For many organizations, the cost of poor application security is in the six-figure range each year. In some cases, the damage that attacks targeting applications and APIs cause exceeds $1 million. These organizations must defend themselves against sophisticated, targeted attacks while managing traditional but ubiquitous threats. Unfortunately, defenses now consist of unmanageable, siloed point security products that are difficult to use. As new threat vectors emerge in the AI era, there is a high likelihood that this collection of tools will continue to expand. The point solution approach shifts the burden of event correlation and threat detection onto the enterprise. Worse, this process likely involves the usage of additional third-party tooling such as XDR or SIEM. Organizations require application security practices to mature beyond a collection of one-off tools — loosely integrated or not — to a more integrated, context-driven, "smart" approach.

AT A GLANCE

KEY STATS

According to IDC's 2024 *Web Application and Availability Protection Buyer Insights Survey*:

- 55% of businesses increased security spending in 2024.
- 35% of enterprises increased application security spending specifically to address the emerging needs of AI applications.

According to IDC's April 2025 *Web Application and Availability Protection Buyer Insights Survey*:

- 55% of organizations are taking advantage of existing tools to address GenAI risk or use them in tandem with point solutions.

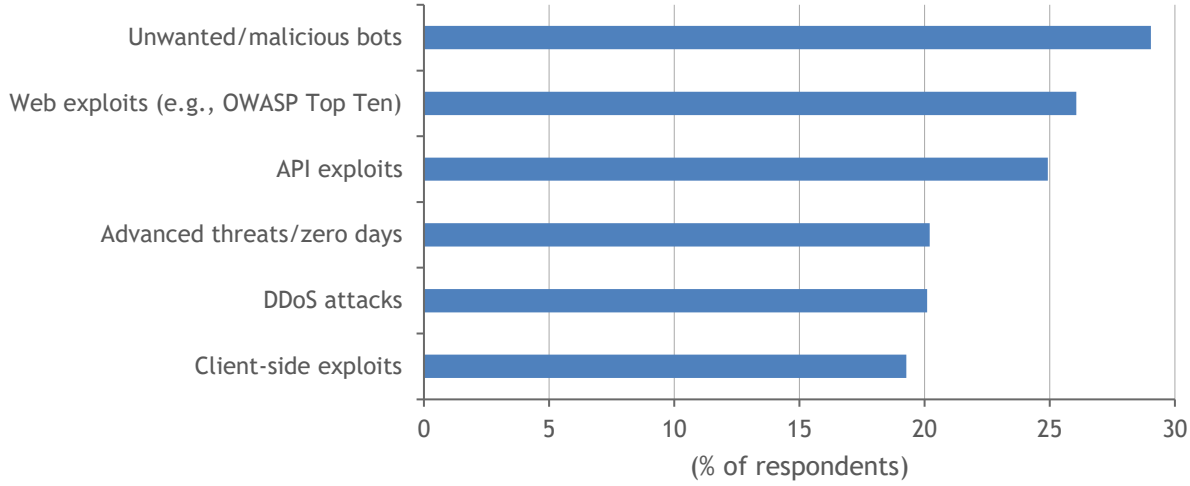
Application and API Security Trends

Application owners must navigate a complex maze of threats and challenges that hamper their efforts to establish a reliable, performant, trustworthy online experience. Among application layer–specific threats, bots were cited as the most common concern for 2025, followed by web and API exploits (source: IDC's *Web Application and Availability Protection Buyer Insights Survey,* April 2025). Notably, the list is rounded out by specialized threats such as DDoS attacks that undermine application availability and client-side exploits that target an overlooked attack vector (see Figure 1).

FIGURE 1: ***Leading Specialized Threats Targeting Applications and APIs***

Malicious and unwanted bots have emerged as a top-of-mind security concern.

Q ***Which of the following security threats associated with web applications and APIs are business leaders at your organization most concerned about for 2025?***



n = 817

Source: IDC's Web Application and Availability Protection Buyer Insights Survey, April 2025

GenAI introduces numerous new risks for business leaders to navigate and complicates existing issues. For example, competitors can use bots to scrape data and content from across the web to train large language models (LLMs). For organizations that employ LLMs in their applications, application security is necessary to mitigate risk — 35% of organizations increased application security spending specifically to address GenAI risks, while 24% of organizations are taking advantage of existing tooling, 41% are investing in new solutions, and 31% are doing both to address GenAI risk (source: IDC's *Web Application and Availability Protection Buyer Insights Survey,* April 2025).

However, the strategy to address each new security challenge with a specialized point solution is producing diminishing returns. When asked to rank the top challenges with their current application security strategies, the top 3 responses were "complexity of solution leading to security gaps," "insufficient integration with broader security architecture," and "complexity of solution leading to incomplete adoption."

When asked what organizations are doing to address the challenges of current security approaches, 29% of businesses cited plans to pursue platform-based solutions over point products. Consolidated, integrated platforms help enterprises

reduce security gaps and management complexity and streamline security inspections. Thus the convergence of multiple security technologies into a single coherent platform is a necessary strategy to address growing security complexity. Web application and API protection (WAAP) platforms were cited as the most popular target for security convergence, and 87% of organizations reported some degree of WAAP adoption already (source: IDC's *Web Application and Availability Protection Buyer Insights Survey,* April 2025).

Organizations also face shifting technical needs and business requirements that will further complicate their application security strategy. First, application infrastructure and network environments have changed. Applications have long since spread beyond the confines of traditional datacenters to the cloud, including edge, containerized, and serverless infrastructure. This migration continues in 2025, as 30% of businesses noted plans to significantly increase spending to migrate applications from on-premises to cloud (source: IDC's *Future Enterprise Resiliency and Spending Survey, Wave 11,* December 2024). As workloads move to the cloud, security must also move to the cloud. Security, enforced at the edge, is an important deployment model to reduce latency for users, and 45% of businesses are relying primarily on cloud services for their application security in 2025. Notably, this shift has not dismissed the need for on-premises security, as only 15% of organizations claimed a total lack of on-premises security; 29% of organizations noted an even balance of cloud and on-premises security (source: IDC's *Web Application and Availability Protection Buyer Insights Survey,* April 2025).

Benefits of Web Application and API Protection Platforms

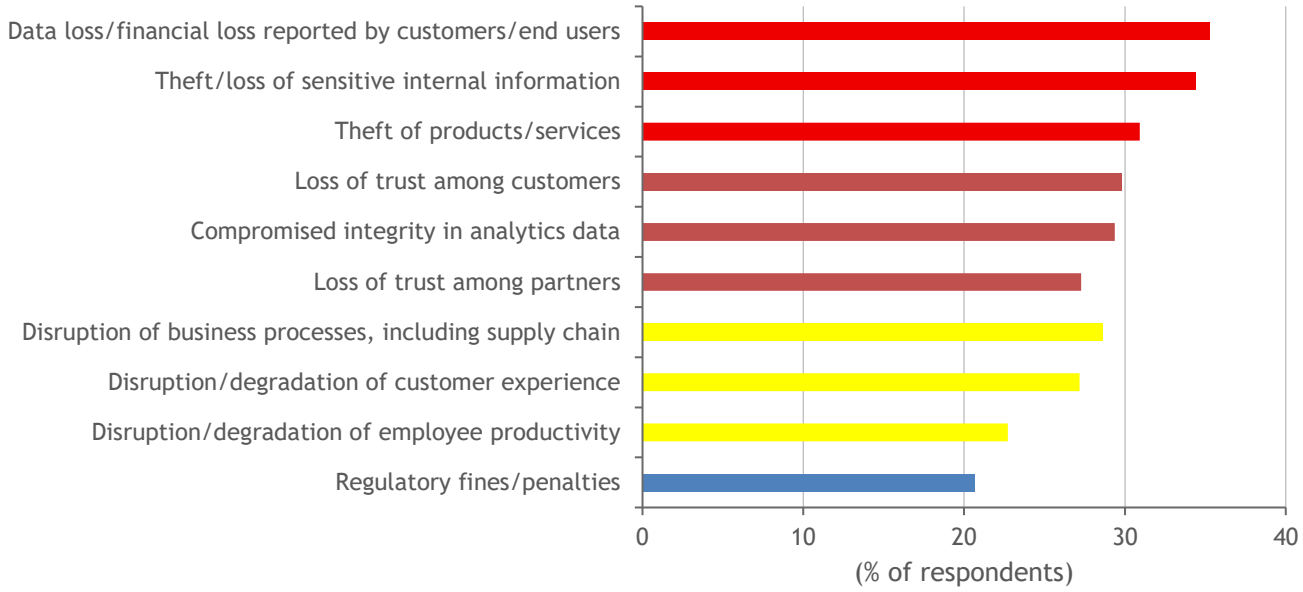
Modern, intelligent approaches to application security are more efficient and effective than legacy solutions that rely on static defenses and databases of known threats. The benefit of modern security technologies is magnified when working in a coordinated, coherent fashion. Purpose-built detections working in concert, rather than silos, is required to detect sophisticated attackers that use multivector attacks. Unsurprisingly, strong security is a key benefit of WAAP platforms: When describing the benefits of WAAP, 39% of organizations cited greater protection against varied threats, 38% reported improved accuracy of threat detection/lower false positives, 36% reported faster time to detection and mitigation, and 35% reported greater protection against advanced threats (source: IDC's *Web Application and Availability Protection Buyer Insights Survey,* 2024).

Strong application security translates to positive business outcomes, as it directly impacts operations and also influences the ability for an online organization to establish trust between partners, customers, and its own data and analytical senses. However, the clearest connection between application security and business health was the effect on the ability to defend against theft and financial losses (see Figure 2).

FIGURE 2: ***Application Security Impacts Business Outcomes***

Application security has profound implications for theft/financial loss, trust, and operations.

Q *What types of damage to your organization did attacks targeting applications, APIs, and availability cause in 2024 (including web/API exploits, DDoS, and bots)?*



n = 817

Note: Red indicates theft-related damages, orange indicates loss of trust, and yellow indicates business disruption.

Source: IDC's Web Application and Availability Protection Buyer Insights Survey, April 2025

Importantly, a modern WAAP solution addresses key requirements — both technical and business related — for application security. For example, the use of fewer specialized security services reduces latency, as multiple security policies and inspections can be applied to application communication in a single pass. By comparison, a point solution approach involving multiple security services may require several additional hops as traffic is redirected to different vendor POPs around the world.

A modern WAAP solution also addresses the need for deployment flexibility, including the reality that web applications and APIs are spread across diverse environments, including on-premises datacenters. By supporting a breadth of network environments, modern WAAPs provide business agility to utilize preferred infrastructure as costs, performance, and other needs dictate while maintaining a consistent security posture. Support for multiple deployment types enables comprehensive security protection without slowing down developers.

Organizations must continue to embrace modern technologies to advance their digital business strategies: 25% of organizations noted microservices as one of the most important technologies for refactoring legacy cloud-based applications in 2025 (source: IDC's *Future Enterprise Resiliency and Spending Survey, Wave 11,* December 2024). The key is to do so without compromising security posture. For example, APIs are increasingly important in modern applications, enabling the adoption of microservices architecture. API protection ensures that businesses receive the benefits of APIs

and microservices architecture without increasing risk by ensuring that cybercriminals do not leverage APIs as a means to evade existing defenses. However, APIs require specialized defenses, as they expose business logic that can be abused if inappropriate defenses, such as WAF or API gateways, protect them. For reference, 42% of organizations noted the security limitations of API gateways and 36% noted the limitations of WAF as top concerns for API security (IDC's *Web Application and Availability Protection Buyer Insights Survey,* April 2025).

WAAP provides a breadth of security capabilities operating as a complete, coherent platform. For businesses that are challenged to do more with less, this offers a simplified approach to application security that addresses the business requirement to streamline security procurement, deployment, and management. All organizations require the functionality that WAAP provides. However, multiple factors, including application type, industry, content and type, and risk tolerance, determine the specific set of security functions necessary to protect a particular application. Positively, WAAP can be tailored to provide the exact protections required for a particular online property.

Considering A10 Networks

A10 Networks has been offering application delivery, performance, and security solutions for high-performance and enterprise security requirements for over 15 years. The company's A10 Defend solution includes ThreatX by A10 Networks, which is a web application and API protection solution, a standalone next-generation WAF for web applications, and a DDoS protection solution.

ThreatX by A10 Networks offers WAAP protection and can be deployed on premises or consumed as a cloud service. It protects web applications and APIs from cyberthreats like bots, Layer 7 DDoS attacks, and all OWASP Top Ten application threats like SQL injection and cross-site scripting. A combination of traffic profiling, collective threat intelligence, and entity-based behavioral analytics enables ThreatX to stop attacks targeting applications and APIs earlier and more accurately than signature-based or rule-based solutions. In addition, a team of security experts is available to provide fully managed application security services including active monitoring, threat hunting, and incident response to reduce the workload on existing security teams.

A10 Defend DDoS Protection is a foundational suite of solutions that work in concert to provide comprehensive detection, prevention, and mitigation of DDoS attacks. It provides organizations with tools to respond quickly to a DDoS threat, reduce false positives with AI-enabled detection, and exert a high degree of control over performance and costs.

The A10 Networks solution offers the flexibility to deploy on premises or natively in the cloud to support business needs and other technical requirements that drive usage in either environment or in a hybrid fashion. The solution allows businesses to maintain a security posture that is consistent and controlled regardless of the location and enables organizations to retain the business agility to shift workloads between environments as needed. This flexibility is important as businesses refine and expand their strategies for supporting AI and AI-enabled applications.

The ThreatX solution includes a managed security operations center that augments existing security teams and helps in threat hunting and incident response services to protect web applications and APIs. The aim of the managed web application security platform is to reduce the burden on security teams by correlating security events to identify threats with high accuracy. A10 Networks offers its A10 Control platform for centralized, single-pane-of-glass management; analytics insights; and automation to help drive the efficiency of operations.

Challenges

While A10 Networks' security solutions are managed centrally through A10 Control, the platform is currently offered as an on-premises solution. IDC notes that a SaaS-based version of the A10 Control management system would provide more flexibility. A10 Networks plans to offer the SaaS version of the A10 Control system in the near future.

Conclusion

Modern application security must help businesses deliver a frictionless, fear-free online user experience. This is a tall order in an era of AI-driven threats and vulnerable LLMs. The effort will require sophisticated security capabilities, along with support for AI applications and diverse IT environments. A10 Networks is positioned to address these market needs, thereby aiding enterprises to embrace the next generation of web application and API technologies while minimizing business risk.

Modern application security must help businesses deliver a frictionless, fear-free online user experience.

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 network infrastructure. IDC's Security and Trust research services to which Chris contributes include network security products and strategies and active application security and fraud.

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
blogs.idc.com www.idc.com