

Companies that establish strong security foundations today will be in a better position to adopt new AI capabilities tomorrow with confidence, resilience, and speed. A cloud-centric approach to AI security can help, especially with the right partners that have the expertise to deliver against the desired outcomes.

Strategies to Address Emerging AI Security Needs with a Cloud-Centric Approach

November 2025

Written by: Philip D. Harris, CISSP, CCSK, Research Director, GRC Solutions, and Christopher Rodriguez, Research Director, Security and Trust

Introduction

AI adoption has reached an inflection point. Organizations can no longer afford to experiment cautiously as competitors are already deploying AI at scale to streamline operations, accelerate decision-making, and unlock new revenue streams.

Yet, despite growing awareness — 35% of organizations told IDC they increased security budgets in 2024 specifically for generative AI (GenAI) risks — most remain unprepared for AI-specific threats like prompt injection attacks and model poisoning. Defending against such threats requires both new technologies and fundamental shifts in security architecture.

In the age of AI, organizations around the world will be challenged to ensure they have adequate protection from external disruptions and/or cyberattacks. What they need is a robust AI security program that will require new technologies as well as a greater breadth of existing capabilities and practices.

Establishing a common external cybersecurity layer that works in concert with AI applications on the back end can reap many benefits, such as simplifying and protecting AI application development efforts. While laying the foundation for appropriate AI control structures can be expensive, the right guidance can empower organizations to move their projects forward.

Organizations will need assistance with navigating the new AI requirements. They also need help in clearly defining their strategic approach, understanding the key requirements, and effectively liaising with internal and external technical teams to ensure that they build the requirements into the resulting applications.

Organizations starting their AI journey have much to consider architecturally, even before the design and implementation stages. Having qualified partners that can support this journey can help simplify development efforts, reduce the risk of cost overruns, create strategic plans, and accelerate customer outcomes.

AT A GLANCE

KEY STATS

- » 35% of organizations increased spend in 2024 to address GenAI risks (source: IDC's *Web Application and Availability Protection Buyer Insights Survey, 2024*).
- » 41% of organizations primarily plan to invest in dedicated solutions for protection of AI applications (source: IDC's *Web Application and Availability Protection Buyer Insights Survey, 2025*).

Benefits

Securing AI requires a cloud-centric approach. A modern cloud architecture not only delivers immediate protection but also ensures the flexibility and scalability needed as AI adoption accelerates. Key benefits include:

- » **Flexible deployment:** The cloud is pervasive and provides low-latency, edge-based connectivity that eschews the need for hairpinning traffic from end-user devices back to a local datacenter. Ideally, organizations can apply protections directly in the environments where developers work, whether workloads are in the cloud, on premises, or moving between the two.
- » **Future-proof architecture:** Security practices have typically followed the adoption of new technologies and business practices. However, the strategy of adopting one-off point products to secure the latest threat vector is falling out of favor as organizations recognize the eventual inefficiencies that emerge from siloed security strategies. Instead, they seek to adopt application security solutions that are part of or can be easily integrated into comprehensive security platforms such as web application and API protection (WAAP). When asked by IDC how they would address key application security challenges, organizations noted plans to prioritize platform-based solutions ahead of best-in-class solutions. However, a pragmatic approach was most popular, with 34% of organizations noting plans to follow a balanced approach that consolidates some functions while utilizing point products as needed, according to IDC's 2025 *Web Application and Availability Protection Buyer Insights Survey*. A cloud foundation supports ongoing expansion, making it easier to integrate emerging AI-specific capabilities and specialized tools into a unified platform, as the provider naturally expands the platform's capabilities over time.
- » **Continuous innovation:** Security delivered as a managed service ensures that defenses are always up to date, incorporating the latest threat intelligence and enhancements without added operational burden.
- » **Improved performance and visibility:** Cloud-based defenses provide a global perspective on attack trends, enabling organizations to identify and respond to threats faster. The ability to detect and respond quickly to novel threats is a function of broad signals intelligence and expert analysis. The initial detection of a novel exploit fuels the intelligence that organizations need to propagate protections to defensive positions worldwide.
- » **Developer focus:** Embedding an interoperable security layer into AI development allows organizations to free their teams to focus on building applications that deliver business value without the constant worry of catastrophic disruptions or cyberattacks.

Key Trends in Addressing AI Risk

As organizations adopt AI at scale, their understanding of risk is maturing. Several key trends are shaping how businesses secure AI. Initial concerns focused on how employees would interact with AI applications, including the potential exposure of sensitive data. However, the ability to rely on output from large language models (LLMs) has also been an open question. AI outputs may include hallucinations, biases, and toxicity, which could undermine the value of insights and knowledge that LLMs provide. These outputs can be extremely detrimental if users are caught unaware.

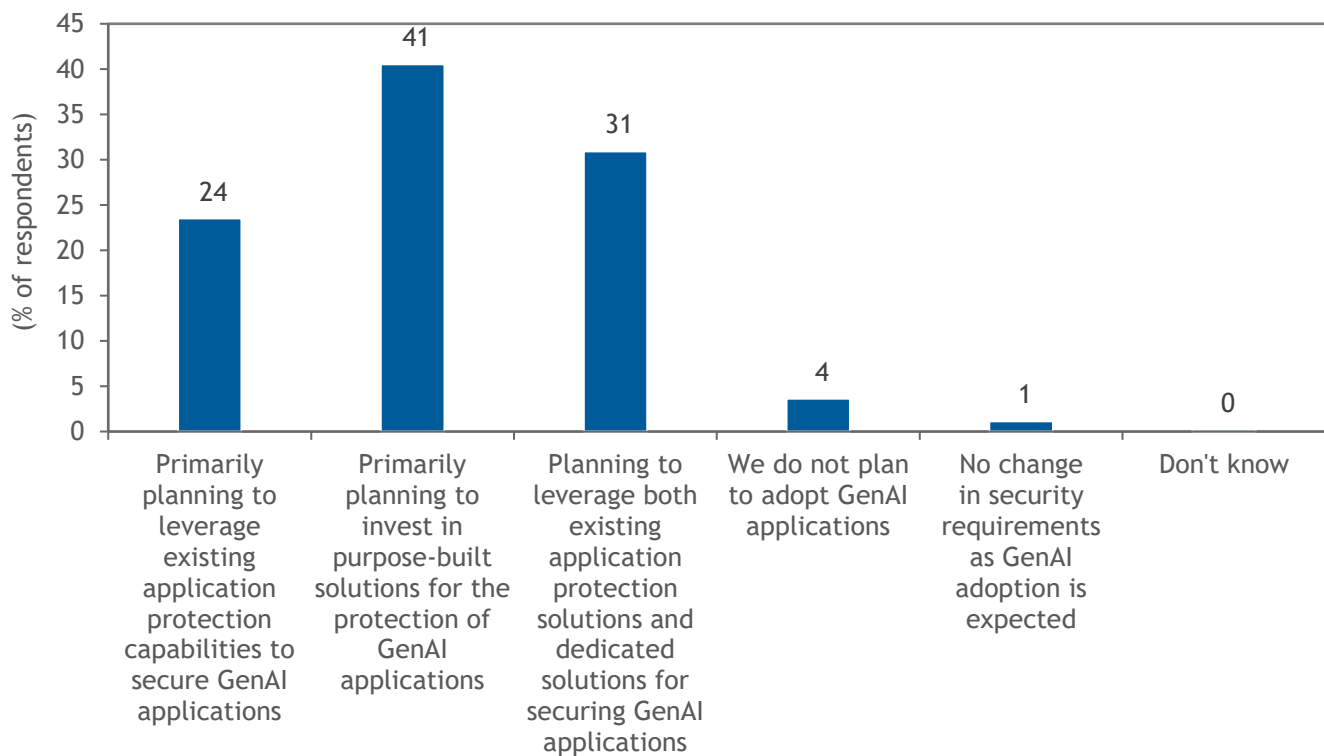
Today, attention is expanding to include crafted attacks that undermine the unique capabilities and characteristics of LLMs and LLM-powered applications. These include prompt injection attacks, model manipulation, and the poisoning of training data sets. On the other hand, cybercriminals are also looking to leverage LLMs to develop new exploits or improve existing tactics, such as crafting more convincing social engineering efforts.

Two schools of thought have emerged in the effort to determine AI security best practices. While comprehensive security platforms are widely seen as the ideal long-term approach, emerging requirements are being addressed as one-off solutions in the interim. IDC's research finds that enterprises are bracing for the near-term reality of deploying point products to address urgent risks. When asked about plans to address AI-related risk, the top response was to invest in purpose-built solutions (41%), according to IDC's 2025 *Web Application and Availability Protection Buyer Insights Survey*. This approach overshadowed plans to leverage existing application protection capabilities (24%), thereby demonstrating the need to invest in new technologies to address the unique security requirements that AI imposes.

However, 31% of organizations indicated plans to leverage existing security investments while layering on AI-specific protections (see Figure 1). This approach represents a hybrid strategy that maximizes value without adding unnecessary complexity. The expectation is that the hybrid approach will increase in popularity over the years as companies evolve their practices beyond disjointed one-off solutions that operate in silos.

FIGURE 1: **How Organizations Are Applying Application Security to AI Requirements**

Q How does your organization plan to address the risks associated with GenAI applications?



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

Essentially, organizations are looking for security solutions that help mitigate the risk of AI adoption while maximizing value. They can do so by considering the relevant protections provided by existing security tooling, such as web application firewall (WAF) or API security, when determining what new security solutions may be required. IDC research shows that organizations are most commonly pursuing a pragmatic application security strategy that prioritizes the implementation of specialized solutions when needed, such as in the case of AI, and then consolidating functions into a

common platform, such as WAAP, as possible. Furthermore, 38% invest in a commercial WAAP solution, while 52% of organizations tap a managed security service provider (SP) for their WAAP needs, according to IDC's 2025 *Web Application and Availability Protection Buyer Insights Survey*.

Considering the Accenture and Cloudflare Partnership to Reduce AI Risks

Cloudflare and Accenture have partnered to help organizations adopt AI securely and at scale while shielding them from the external risks AI poses. Cloudflare provides the protection and performance capabilities that are foundational for enabling a successful AI application strategy, ranging from foundational zero trust networking capabilities to AI-specific security controls.

AI applications face a range of familiar and new threats. Cloudflare offers DDoS mitigation services, ensuring that AI and AI-connected applications remain accessible and deliver maximum value to the business. In particular, DDoS mitigation is an important practice for ensuring that costly AI inferencing is not wasted on inauthentic requests. In March 2025, Cloudflare announced the beta release of its Firewall for AI solution, an integrated inline security capability included in its Cloudflare Web Application Firewall (WAF) service. Firewall for AI is designed to defend against LLM-specific threats, such as prompt injections, manipulations, abuse/misuse, and unsafe content. The combination of Cloudflare's DDoS protection, WAF, and Firewall for AI enables businesses to ensure that their applications, including AI and AI-powered applications, are reliable and trustworthy, ultimately improving business outcomes.

Zero trust controls, including data leakage prevention (DLP), are fundamental to preventing the exposure of sensitive data. This is particularly true in the case of third-party LLMs, where clawing back data or requesting deletion may not be possible after its inclusion in AI training data sets. Organizations that build their own applications need a high level of security control to limit access to only the users and use cases required to complete their assigned tasks. This granular level of access control minimizes the possibility of abuse or misuse, data theft, and other nefarious activities. The Cloudflare One SASE solution provides these capabilities, including DLP and ZTNA services, for the complete inbound and outbound control of AI-related communications. Cloudflare's ZTNA includes support for post-quantum encryption to further protect the communications privacy.

Cloudflare security solutions are supported by its global edge infrastructure consisting of peering points and network interconnects delivering over 400Tbps of edge capacity. This architecture ensures a high degree of reliability and scale, including CDN services to further enhance the performance of web and AI applications. Cloudflare continues to introduce multiple capabilities to address emerging AI-specific security challenges. One recent example is its new Cloudflare AI Crawl Control solution, which helps publishers that need to manage how AI crawlers collect and use digital content. Collectively, these capabilities form the foundation of Cloudflare's AI Security Suite, which is designed to protect AI models, data, and applications throughout their life cycle, from training to inference and compliance. Built on Cloudflare's global network, this suite helps organizations adopt AI securely and at scale while maintaining visibility, data integrity, and compliance.

While Cloudflare has made progress in delivering new capabilities to secure AI, the company also leverages AI to enhance its security solutions.

Accenture applies its broad service capabilities to help organizations adopt AI modernization with minimal disruption to their business operations. By leveraging its deep expertise in innovation, integration, and implementation, Accenture helps companies move their applications and services closer to end users. The firm collaborates closely with

organizations to define critical requirements, build tailored strategies, and evolve those strategies over time to meet changing needs.

For AI initiatives, Accenture employs a use case–driven approach to ensure targeted and effective outcomes. Through its partnership with Cloudflare, organizations benefit from proactive prevention, detection, and mitigation of AI-related vulnerabilities and threats. The implementation of these protections at the front end allows the application of security measures, even after an attack has occurred, helping safeguard applications and maintain operational continuity.

Accenture brings the following capabilities to the table:

- » **AI security governance and risk management:** Accenture brings in-depth expertise and experience assisting organizations design actionable AI risk assessment and control framework capabilities. These are foundational capabilities needed to ensure a secure AI foundation incorporates the appropriate policy, industry, and regulatory considerations and can, in turn, inform implementation of controls.
- » **Business-driven security design:** Accenture's framework for secure AI capability design and deployment is anchored around enabling business outcomes through trusted and secure AI systems. Partnering with Cloudflare, Accenture designs control deployment with business process outcomes in mind, ensuring security is embedded by design and does not create friction.
- » **Speed to market:** Accenture's expertise with cutting-edge AI technologies, as well as security capabilities, can help organizations take advantage of AI innovations.
- » **Health check services:** As part of its services, Accenture leverages AI to further enhance automated application health checks, not only in dealing with immediate issues but also in bringing the ability to predict future issues based on conditions in applications and potentially offering self-healing or bringing issues to the forefront for immediate resolution.
- » **Accelerated enhancements:** With Accenture, Cloudflare offers organizations the ability to receive enhancements on an accelerated basis and be shielded from the typical SaaS or on-premises migration and integration disruptions.
- » **Total cost of ownership:** The partnership between Cloudflare and Accenture can help organizations realize more consistent and/or reduced costs than they would experience by doing the work themselves.
- » **Portfolio rationalization:** Accenture will work closely with Cloudflare and customers to rationalize their various application portfolios — from cybersecurity to application development to infrastructure technology — to ensure that AI modernization efforts do not create redundancies in the overall portfolio.
- » **Adjacent capabilities:** Accenture brings deep expertise in the comprehensive and methodical execution of processes to ensure the timely delivery of customer outcomes.

Accenture and Cloudflare will also manage various industry and regional issues in an expedited manner:

- » **Requirements for regulated and controlled industries:** To manage these requirements, the partners offer the implementation of a consistent set of front-end protections that will shield applications from needing to integrate industry-specific controls individually.

- » **Regional compliance and sovereignty requirements:** Cloudflare offers a vital layer of protection that can be easily deployed across industries and geographies, especially useful for accommodating sovereignty requirements.

Customers can benefit from the partnership in the following ways:

- » The combination of Accenture and Cloudflare provides organizations with strategic and tactical services that enable immediate use of AI while based upon a secure foundation.
- » Transformations involving AI, while beneficial, can have risks that potentially impact the end customer. Accenture and Cloudflare shield customers from the risks resulting from AI transformations.

Organizations can build a secure foundation for responsible AI modernization by combining Cloudflare's platform capabilities with Accenture's governance expertise.

Challenges

Cloudflare's application security portfolio, enhanced by AI-driven capabilities, aims to provide full inline protection of API traffic. However, the company's multitiered packaging is currently tailored for mature enterprises that have a clear understanding of their API security use cases. By simplifying packaging and leveraging AI to guide configuration and deployment, Cloudflare could better serve organizations across the full maturity spectrum of application security.

Accenture's challenge lies in ensuring the fine-tuning and rigorous testing of the company's AI-powered modernization services. Success will depend on how effectively these services accelerate speed to market, improve operational efficiency, and deliver measurable ROI for clients navigating digital transformation.

Conclusion

The business implications of AI are undeniable because opting out is no longer an option. As adoption accelerates, security is emerging as a defining factor that will determine whether organizations realize AI's potential or expose themselves to new vulnerabilities.

Success will require a holistic approach to AI risk, one that addresses data protection, model integrity, and evolving threat vectors while enabling innovation at scale.

Companies that establish strong security foundations today will be better positioned to adopt new AI capabilities tomorrow with confidence, resilience, and speed.

AI is transforming how applications and APIs support the modern digital economy, enabling businesses to interact seamlessly with customers, employees, and partners while safeguarding their investments. As organizations rapidly adopt modern cloud-based applications to meet global scale and performance demands, AI-powered solutions, especially when integrated with cloud SPs, play a critical role in accelerating modernization. These intelligent application systems help tailor strategies, optimize resources, and drive security transformation, making it easier to identify the right cloud SP partner and achieve cost-effective, efficient outcomes.

In short, securing AI is not simply a technical requirement; it is a strategic imperative.

Securing AI is not simply a technical requirement; it is a strategic imperative.

About the Analysts



Philip D. Harris, CISSP, CCSK, Research Director, GRC Solutions

Philip Harris is responsible for developing and socializing IDC's point of view on governance, risk, and compliance services and software across people, processes, and technologies focused on creating a foundation of privacy and trust with enterprises, IT suppliers, and service providers.



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 active application security and fraud and trusted access and network security.

MESSAGE FROM THE SPONSOR

Accenture and Cloudflare are at the forefront of AI technology innovation. Through their partnership, the companies are developing a collaborative blueprint for capitalizing on AI for security, while bolstering defenses against AI powered threats. With combined expertise in infrastructure and security, Accenture and Cloudflare can design, build, and run projects that will help organizations achieve better protection and faster growth with AI. Read the Accenture State of Cybersecurity Resilience 2025 report for additional information <https://www.accenture.com/ca-en/insights/security/state-cybersecurity-2025> or visit <https://www.cloudflare.com/en-ca/ai-security/>.



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

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. This IDC material is licensed for external use, and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

©2025 IDC. Reproduction is forbidden unless authorized. All rights reserved. [CCPA](#)