Cybersecurity
INSIDERS

2025

Web Application Security Report

Evolving Threats, Strategies, and Best Practices

FORTINET®

Introduction

Web applications are the backbone of modern organizations, enabling digital transformation, customer engagement, and business operations. However, rapid development cycles, complex cloud environments, and increasingly sophisticated threats expose critical security gaps. Weak access controls, insufficient visibility, and delayed threat detection leave applications vulnerable to attacks, leading to data breaches, compliance failures, and operational disruptions.

Compounding the challenge, attackers now leverage AI, automated bots, and API vulnerabilities to exploit these weaknesses, underscoring the urgent need for more robust application security measures.

The 2025 Web Application Security Report is based on a comprehensive survey of over 600 IT and cybersecurity professionals. The survey explores organizations' biggest challenges, strategies for responding to them, and the evolving role of automation, AI, and consolidated platforms to provide a nuanced understanding of the application security landscape.

Key findings from this report include:

- **60% struggle with application visibility** – Blind spots in workloads, APIs, and cloud environments make it difficult for security teams to detect threats before they escalate.
- **58% cite API security as a major concern** – API-driven services require robust anomaly detection, firm authentication, and real-time monitoring to prevent data theft.
- **49% rank DDoS as the top bot-driven attack** – Advanced bots pose severe operational risks as a prolonged outage can cost organizations thousands of Dollars per minute of downtime. Yet 62% remain uncertain about their readiness to defend against human-like bot activity, underscoring a significant gap in organizational preparedness.
- **30% or organizations have experienced a breach tied to stolen credentials** – Weak identity protections expose organizations to account takeover attacks, such as credential stuffing for instance, reinforcing the need for multi-factor authentication and strong access controls.
- **61% are using AI for threat detection** – Organizations increasingly rely on AI-powered security tools to identify anomalies and respond to attacks more effectively. Many organizations report that AI-driven threat detection has improved speed and accuracy in identifying malicious activity.
- **43% plan to consolidate security tools** – With rising complexity and tool sprawl, nearly half of organizations aim to streamline their security stack to improve efficiency and integration.

We extend our sincere gratitude to Fortinet for their valuable insights and contributions to this report. We hope the findings and recommendations presented in the report will provide actionable insights to help security teams strengthen their application security defenses, close security gaps, and protect applications from evolving threats. With the right tools—those capable of discovering and enhancing visibility of digital assets while employing sophisticated measures like machine learning and threat analytics—businesses are better equipped to safeguard applications and APIs against advanced threats.

We trust that our readers will find this report helpful in their journey towards improved application security and in navigating the complexities of modern digital landscapes with confidence.

Thank you,

Holger Schulze

Founder, Cybersecurity Insiders

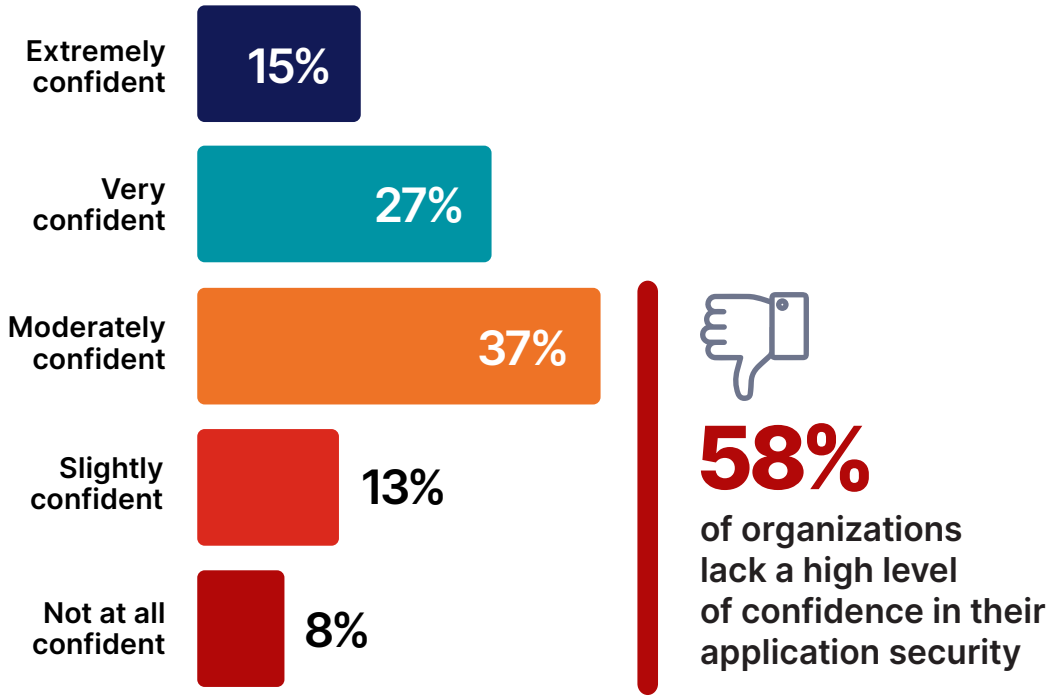
Confidence in Application Security: A Mixed Picture

Confidence in an organization's application security posture provides a critical indicator for its readiness to defend against emerging threats.

The responses show that only 42% of respondents are confident in their application security measures. The majority, 58%, do not feel confident, marking a continued decline in confidence from last year (53%).

The increase in respondents reporting a lack of confidence could be driven by persistent uncertainty. This highlights ongoing challenges in addressing vulnerabilities, scaling protections, and navigating increasingly complex security landscapes.

How confident are you in your organization's application security posture?



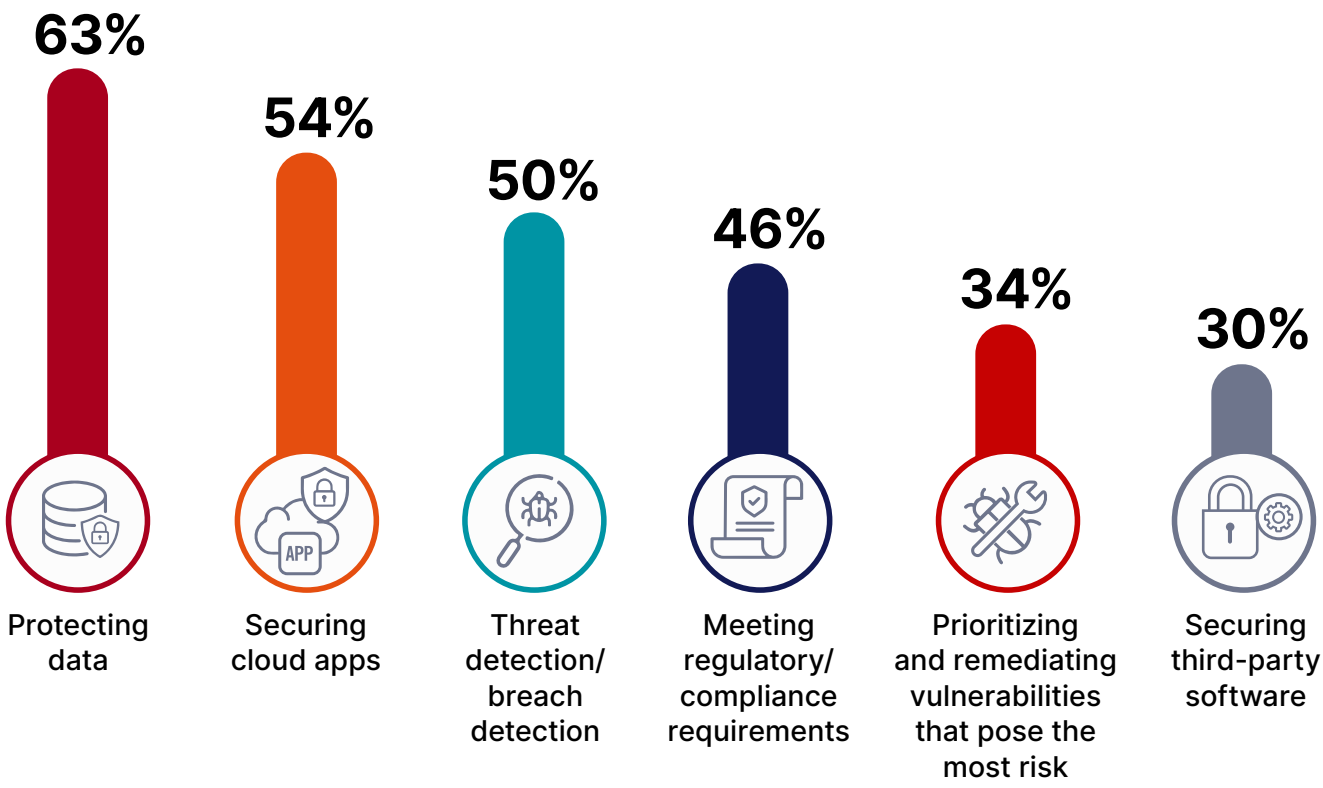
Organizations that integrate advanced security tools and DevSecOps practices tend to report higher confidence, while those struggling with legacy systems and staffing shortages remain vulnerable. This variation in confidence underscores the disparity in maturity levels across organizations.

Shifting Concerns in Application Security

Protecting applications and the data they handle is critical as organizations increasingly rely on digital ecosystems to deliver value to customers while safeguarding sensitive assets.

Protecting data remains a top concern for 63% of respondents, a significant rise from 43% last year, highlighting growing awareness of data security amidst a surge in breaches and regulatory mandates. Securing cloud applications, now at 54%, has also gained prominence compared to last year's 40%, reflecting the increasing reliance on cloud infrastructure and the growing sophistication of cloud-native threats. Threat and breach detection, consistently critical, is cited by 50%, holding steady as organizations prioritize rapid threat identification and response capabilities. Notably, while regulatory and compliance concerns remain significant at 46%, effective vulnerability management at 34% underscores ongoing struggles with prioritizing risks as application environments grow more complex.

What are your biggest application security concerns?



The rising focus on cloud applications illustrates a broader shift toward securing cloud-native architectures. For instance, an organization migrating legacy workloads to the cloud might grapple with challenges like securing APIs and monitoring dynamic environments. This trend underscores the importance of advanced threat detection and the ability to adapt to increasingly decentralized and cloud-driven infrastructures.

Additional responses include:
Securing mobile apps 27% | Meeting customers' security needs and requirements 24% | Effective threat modeling 21% | Securing commercial off-the-shelf software 8% | Don't know/unsure 6%

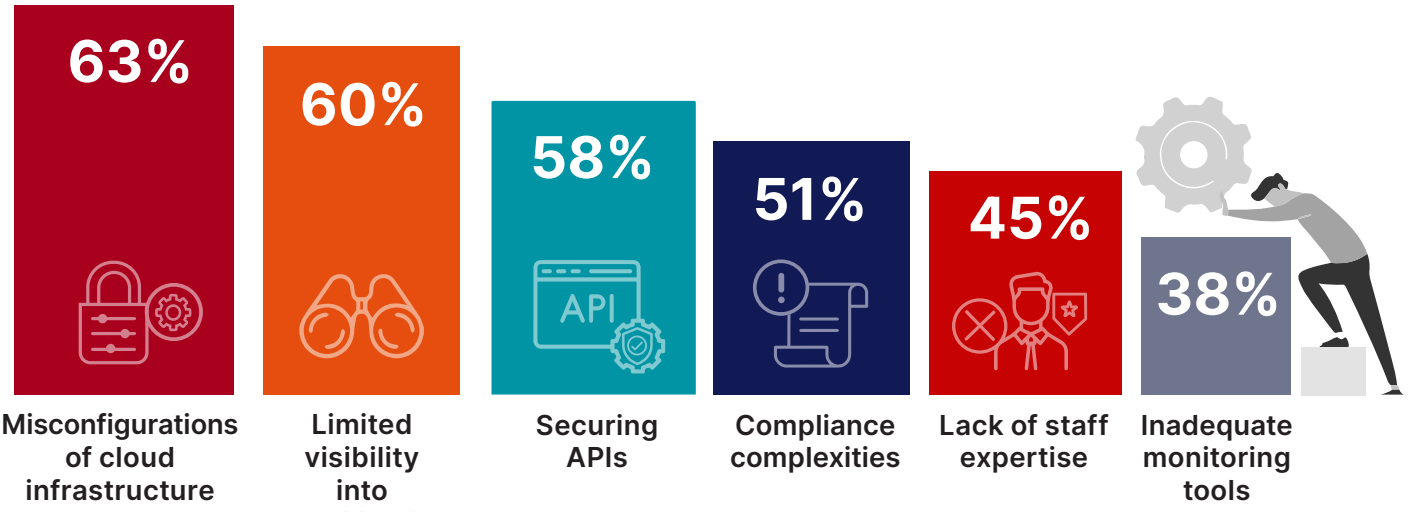
Overcoming Challenges in Securing Cloud Applications

As organizations span their applications across hybrid and multi-cloud environments, they encounter a range of security challenges that must be addressed to protect sensitive data and maintain operational integrity.

The survey reveals that misconfigurations of cloud infrastructure are the most significant application security challenge, cited by 63% of respondents. This aligns with findings from last year's report, emphasizing the critical nature of proper configuration management in preventing security breaches. Limited visibility into workloads follows closely, with 60% of participants highlighting this issue, underscoring the necessity for comprehensive monitoring tools to oversee dynamic cloud environments. Securing APIs concerns 58% of respondents, reflecting the growing reliance on interconnected services and the need to safeguard these communication channels.

Compliance complexities (51%) and lack of staff expertise (45%) further illustrate the multifaceted difficulties organizations face in maintaining robust cloud security postures.

Which challenges do you face in securing cloud applications?



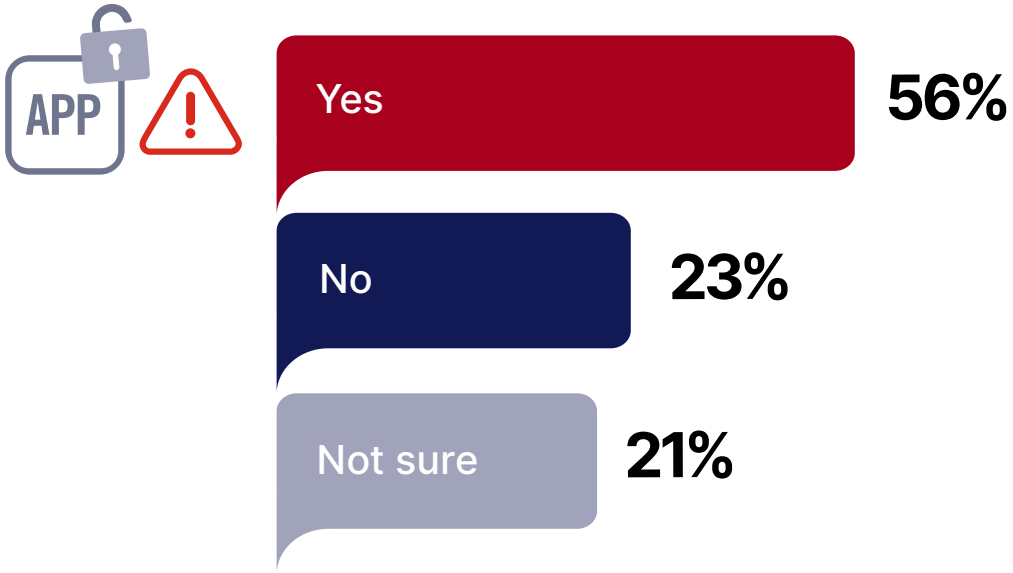
These challenges manifest in various ways. For instance, a company might experience a data breach due to a misconfigured Microsoft Azure storage bucket, exposing sensitive customer information. Similarly, limited visibility into cloud workloads can hinder the rapid detection and mitigation of malicious activities, allowing threats to persist undetected.

Application Breaches on the Rise

Understanding the frequency and anatomy of web-application attacks and security breaches provides critical insight into the effectiveness of current security measures and the evolving threat landscape organizations face.

The survey data reveals that a majority, 56% of respondents, have experienced a breach or compromise in the last 12 months, up from 50% in last year's survey, highlighting the persistent and widespread nature of application security risks. In contrast, 23% reported no breaches, suggesting that nearly a quarter of organizations may have more effective defenses in place or have been fortunate in avoiding attacks. Notably, 21% were unsure if their organization experienced a breach, reflecting potential gaps in visibility and incident detection capabilities—a critical weakness given the stealthy nature of many modern attacks.

Has your organization experienced an application breach or compromise in the last 12 months?



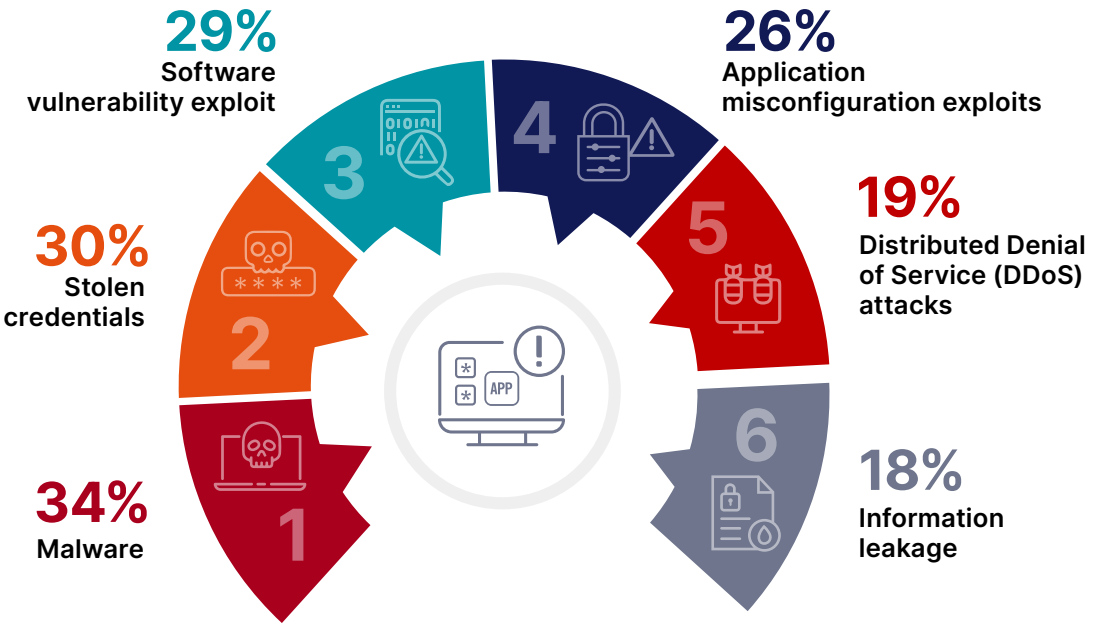
In 2023, MGM Resorts faced a significant breach after attackers exploited vulnerabilities in their applications, resulting in widespread operational disruptions and the exposure of sensitive customer data. The incident, reportedly involving a social engineering attack that led to unauthorized access, highlighted weaknesses in securing applications and integrated systems. This breach underscores the critical need for robust application security focusing on a proactive security posture by implementing continuous application monitoring and advanced threat detection capabilities.

Understanding Application Attack Vectors

The types of attacks organizations face against their applications offer a clear window into adversary tactics and the areas where defenses either hold strong or fall short.

Malware injection remains the most reported attack vector at 34%, an increase from 29% last year, underscoring its ongoing prominence and the necessity for robust malware defenses. Stolen credentials, usually carried out by sophisticated bots, at 30%, continue to represent a significant challenge, rising from 21% last year. This increase reflects the growing prevalence of credential stuffing and brute force attacks against identity systems as adversaries exploit weak or reused passwords. Software vulnerability exploits, reported by 29% this year (up slightly from 26%), and application misconfiguration exploits at 26% (similar to prior years), highlight the persistent challenges of vulnerability management and secure configuration practices. Other notable attack vectors include DDoS (19%) and information leakage (18%), both of which align with prior data, emphasizing the dual threats of service disruption and data exfiltration. Some attack vectors, such as injection attacks (15%) and cross-site scripting (9%), have declined slightly from last year, possibly due to improved developer awareness and the adoption of solutions like Web Application Firewalls (WAFs).

Which of the following security attacks against applications has your organization experienced over the past 12 months?



This data underscores the real-world impact of application security gaps. For example, in 2024, a significant breach occurred when hackers infiltrated Snowflake Inc.'s cloud servers, compromising data from over 100 customers, including sensitive personal information and corporate records. This incident highlights how vulnerabilities in cloud applications can lead to substantial data exposures, affecting numerous organizations and individuals.

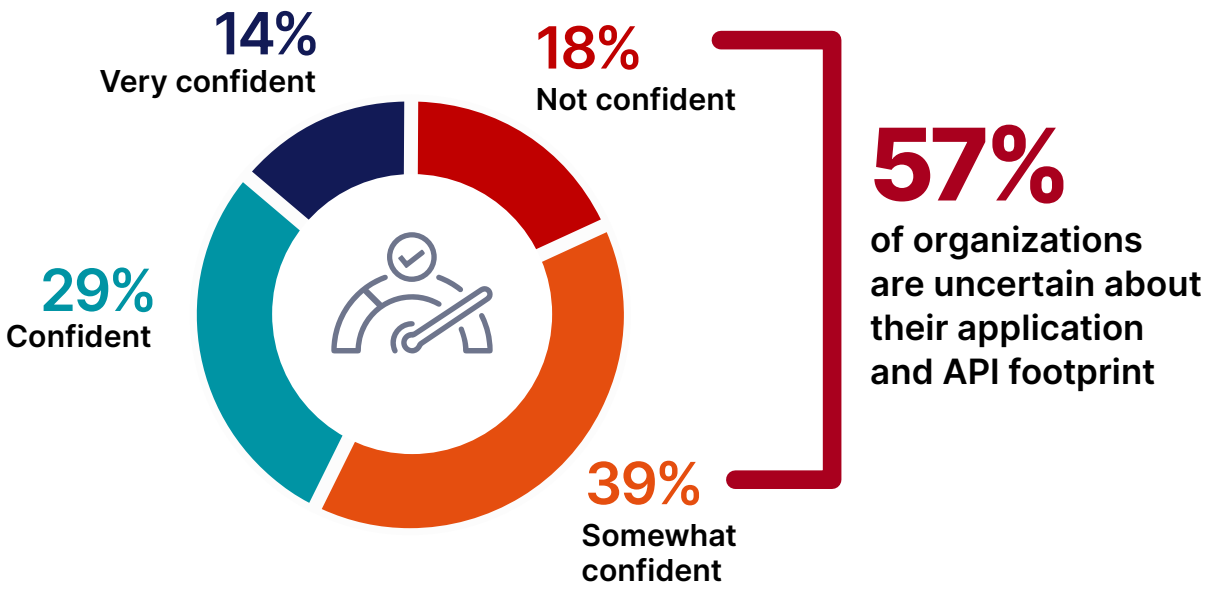
Additional responses include:
Injection attacks (e.g., SQL injection) 15% | Brute force attacks 13% | Web fraud 12% | Unpatched libraries (Using components with known vulnerabilities) 10% | Cross-Site Scripting (XSS) 9% | Man-in-the-Middle (MitM) attacks 7% | Content spoofing 5% | Cross-Site Request Forgery (CSRF) 4% | Clickjacking 3% | Other 5%

Blind Spots in API Security

Awareness of all applications and their APIs used within an organization is vital for maintaining a secure and compliant IT environment and is a key factor in addressing risks such as shadow IT and undocumented APIs.

The survey shows that only 14% of respondents are very confident they know all applications and APIs in use, a notable decline from last year's 21%. While 29% report being confident (down from 34% last year), 39% are only somewhat confident (up from 31%), and 18% admit they are not confident (up from 14%), resulting in a significant majority (57%) of organizations expressing varying degrees of uncertainty about their application and API footprint. This trend suggests increasing challenges in maintaining visibility over expanding and dynamic application environments, which could be driven by factors like the surge of non-human entities like bots and IoT devices, growing reliance on cloud-native services, remote work, and third-party integrations.

How confident are you that you know all applications and APIs used in your organization today?



These findings have real-world implications, exemplified by breaches such as the 2022 Optus API vulnerability incident. In this case, attackers exploited an unmonitored API endpoint, gaining access to sensitive customer data, and exposing the organization's lack of visibility over its application ecosystem. Such incidents highlight the risks posed by shadow IT and poorly monitored APIs, which can serve as entry points for attackers.

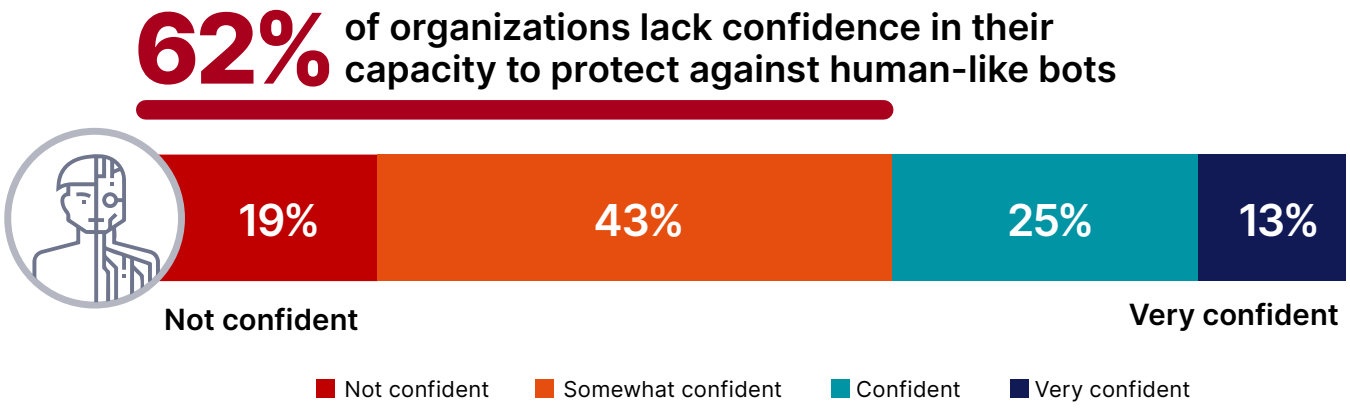
Defending Against the Rise of Human-Like Bots

The ability to protect against human-like bots—sophisticated automated scripts mimicking legitimate users—has become a critical component of application security. These bots are increasingly used for attacks such as credential stuffing, scraping sensitive data, and other malicious activities, making preparedness a key measure of an organization's defense capabilities.

Only a small fraction of respondents (13%) reported being very confident in their preparedness, with an additional 25% feeling confident. However, the majority—62%—are only somewhat or not at all confident, indicating significant gaps in defenses against this advanced bot activity.

This lack of confidence mirrors broader concerns identified in the survey, such as low visibility into APIs and applications (57% expressing uncertainty), which are prime targets for bots. The data suggests a recurring theme: organizations struggle to maintain control and visibility over their environments, leaving them vulnerable to automated, human-like adversaries.

How confident are you in being prepared to protect against human-like bots?



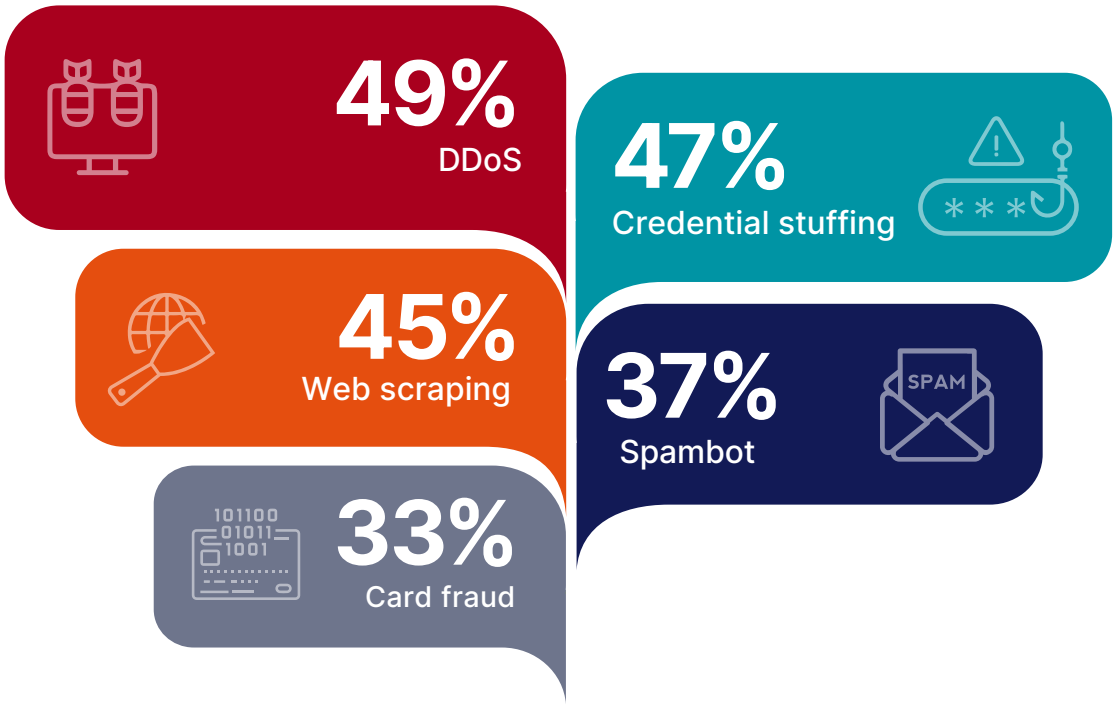
In June 2024, for example, Levi Strauss & Co. experienced a credential stuffing attack where cybercriminals used bots to exploit login credentials obtained from third-party breaches, compromising over 72,000 customer accounts. The attackers gained access to personal information, including order history, names, email addresses, home addresses, and partial credit card details. Such attacks underscore the importance of advanced detection tools capable of distinguishing between legitimate users and bots.

Denial-of-Service – The Most Common Bot Attack

As organizations prepare for increasingly sophisticated and human-like bots, understanding the most concerning attack types provides a strategic foundation for targeted defenses.

DDoS attacks (49%) rose to the top of the list of bot attacks organizations are most concerned with, up from 47% a year ago. Credential stuffing, last year's top concern, has shifted to second place this year at 47%. This reordering suggests that operational disruption caused by DDoS attacks is gaining prominence as a critical risk. Web scraping and card fraud remain significant at 45% and 33%, respectively, signaling consistent worry about data theft and financial harm. Spambots, cited by 37%, reflect heightened awareness of reputational risks from bot-generated spam and fake traffic. These results show that while credential stuffing remains a core concern, the focus is broadening as organizations recognize bot-driven threats' versatility and growing impact.

Which types of bot attacks are you most concerned with?



To illustrate the growing threat: In October 2023, Google mitigated the largest DDoS attack to date, which peaked at 398 million requests per second, exploiting a vulnerability in the HTTP/2 protocol. Similarly, in January 2025, Cloudflare reported a record-breaking DDoS attack that reached 5.6 terabits per second, originating from a Mirai-based botnet comprising 13,000 compromised devices.

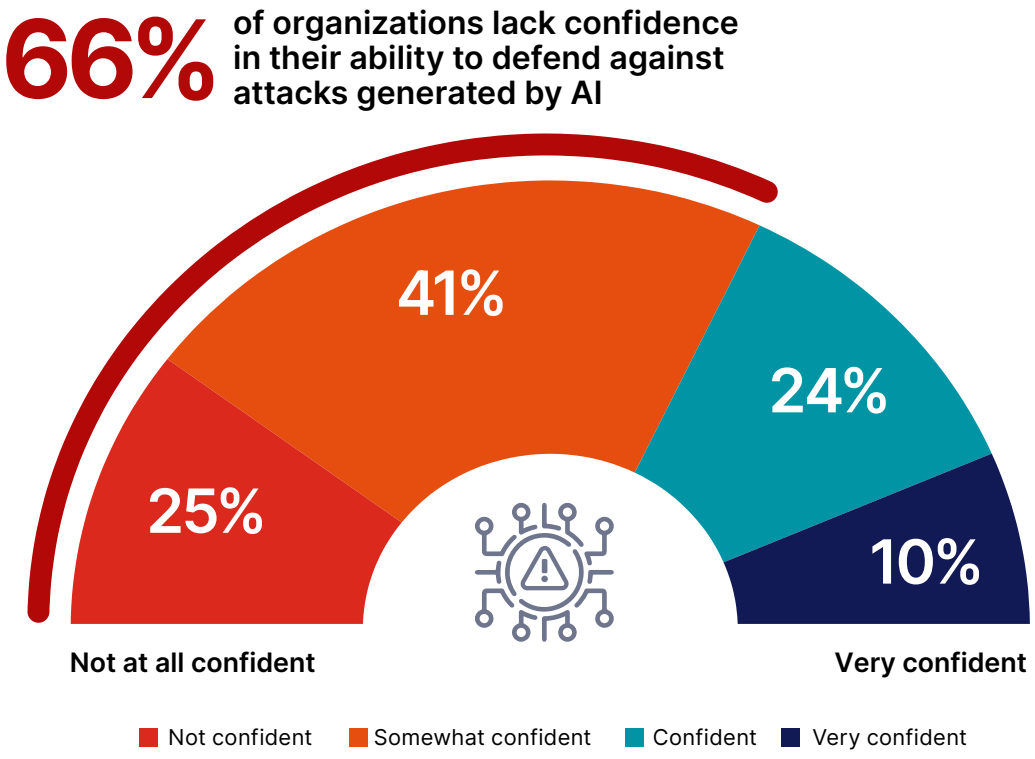
Rising Concerns About AI-Driven Attacks

As artificial intelligence becomes a tool for attackers to generate more sophisticated threats that evade traditional protections, finding zero-day vulnerabilities and quickly creating exploits, organizations must adapt their defenses to counter AI-generated attacks effectively.

The data indicates that only 10% of respondents are very confident in their ability to defend against AI-driven attacks, while 24% feel confident. However, most organizations—66%—lack full confidence in their ability to defend against AI attacks.

This low confidence highlights the rapid evolution of AI as a tool for adversaries, outpacing many organizations' capabilities to recognize, adapt to, and mitigate its impact. Combined with previously discussed findings, such as a lack of visibility into applications and APIs (57% expressing uncertainty) and limited confidence in defending against human-like bots (62% reporting lack of confidence), this data underscores a recurring theme: organizations struggle to keep pace with the sophistication of emerging threats, particularly those powered by advanced technologies like AI.

How confident are you in your ability to defend against attacks generated by AI?



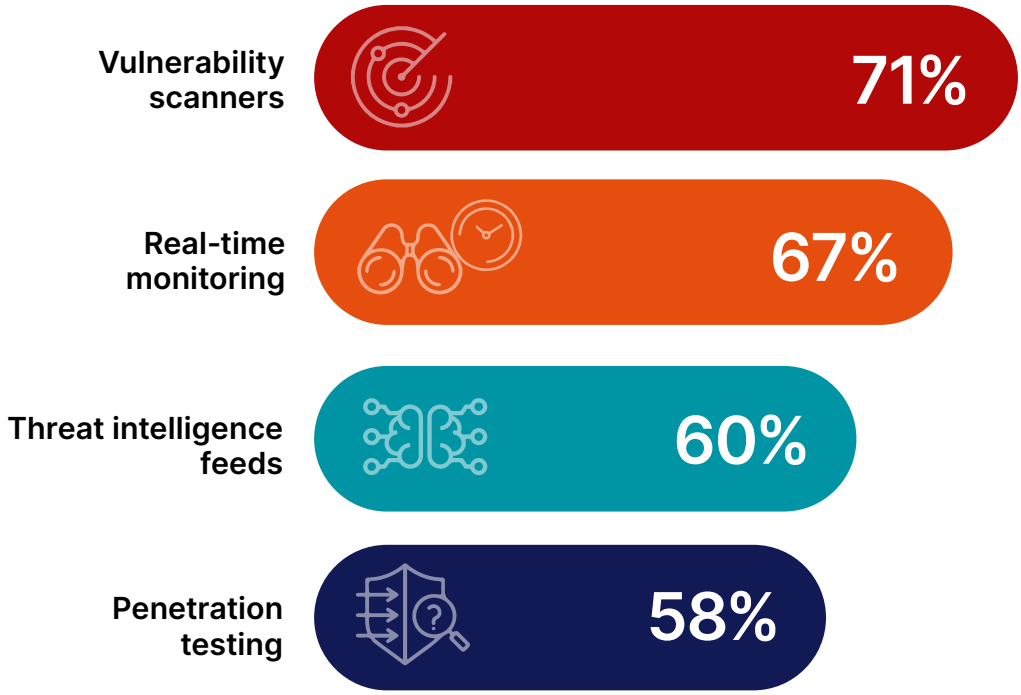
For example, cybercriminals increasingly employ AI to craft convincing phishing emails, utilizing information mined from social media to create personalized messages that are difficult to distinguish from genuine correspondence. Deepfake technology has also been used to impersonate executives, leading to fraudulent communications that deceive employees into transferring funds or sharing sensitive information.

Strategies for Detecting Emerging Threats

Detecting emerging application threats early on requires a combination of tools and processes that provide visibility, intelligence, and actionable insights.

The data reveals that vulnerability scanners are the most frequently utilized tool to detect application threats, with 71% of respondents relying on them to identify application weaknesses. Real-time monitoring follows closely at 67%, reflecting the importance of continuous observation to detect active threats as they unfold. Threat intelligence feeds, employed by 60%, provide crucial context on the latest attack trends. This context is important for making the proper prioritization and supporting business decisions. In contrast, penetration testing, used by 58%, serves as a proactive measure to uncover vulnerabilities before adversaries can exploit them. The consistent reliance on these tools underscores the need for layered and integrated approaches to application threat detection.

What tools or processes does your organization use to detect emerging application threats?



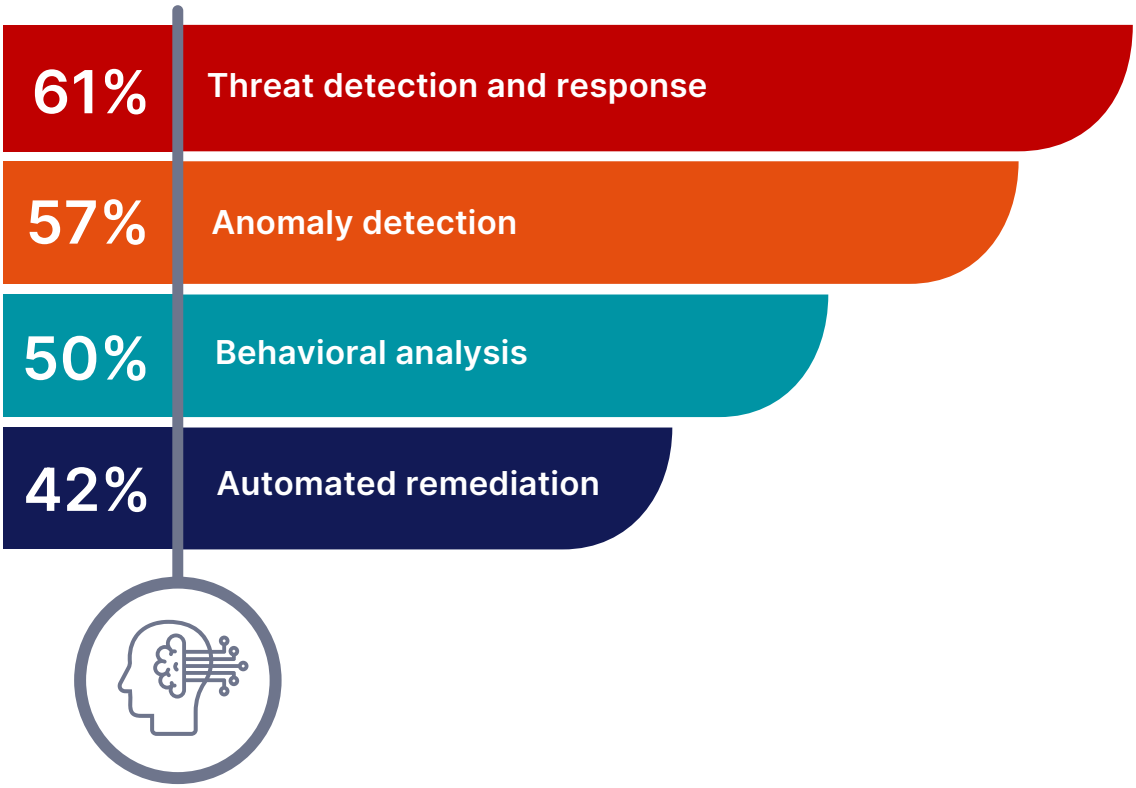
These findings align with practices where multiple tools are successfully employed in tandem. For example, in the 2023 MOVEit Transfer breach, attackers exploited a zero-day vulnerability in the widely used file transfer software. Organizations leveraging real-time monitoring and updated threat intelligence feeds could detect unusual activity early and patch the vulnerability quickly, minimizing the impact. This incident underscores the necessity of combining proactive scanning with reactive monitoring to address evolving threats effectively.

Applying AI and Machine Learning in Security

Given the increasing reliance on real-time monitoring, vulnerability scanning, and threat intelligence feeds discussed earlier, integrating AI models into these functions is a natural progression to enhance detection, analysis, and response capabilities, and ideally to provide business context and recommendations for the near future.

The survey reveals that 61% of respondents apply AI to threat detection and response, making it the most common use case. This reflects the growing need for advanced solutions to identify complex attack patterns in real time. Anomaly detection follows closely at 57%, emphasizing the importance of pinpointing irregular user and machine behaviors that may signal potential threats. Behavioral analysis, used by 50%, further illustrates the focus on understanding user and entity behaviors to identify deviations that could indicate malicious activity. Automated remediation, employed by 42%, rounds out the list, showcasing an increasing trend toward using AI to take immediate action against detected threats, minimizing human intervention and response time.

In which areas are you applying AI or machine learning?

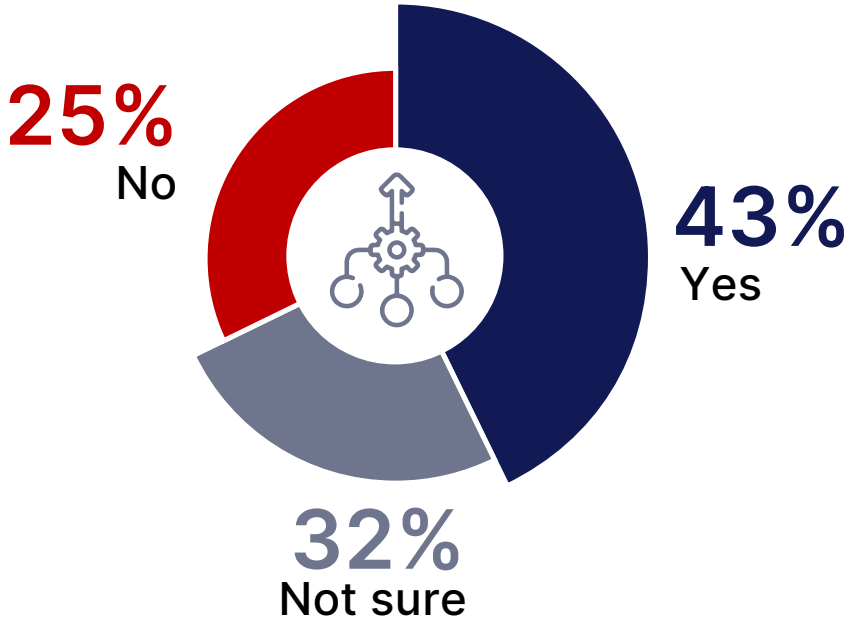


Consolidating Application Security Tools

As organizations adopt increasingly sophisticated technologies to secure their applications, the proliferation of disparate tools often creates inefficiencies, rising expenses, and unnecessary complexity.

The data reveals that 43% of respondents are considering consolidating their application security tools this year—building on a broader trend where most organizations have already made the choice to streamline their toolsets to improve integration, reduce costs, and eliminate redundancies. However, 25% indicate no plans to consolidate, suggesting some organizations may be satisfied with their current setups or lack the resources to undergo such a transformation. The remaining 32% are uncertain, possibly highlighting hesitancy in the face of competing priorities or the challenges of selecting unified solutions that meet all security needs.

Is your organization looking to consolidate application security tools in 2025?



This trend aligns with broader discussions about the reliance on multiple tools for application threat detection, such as separate vulnerability scanners, real-time monitoring, and penetration testing, as mentioned previously. Tool sprawl often creates silos, delayed response, and operational inefficiencies, making consolidation an appealing strategy to streamline processes and improve collaboration across security teams.

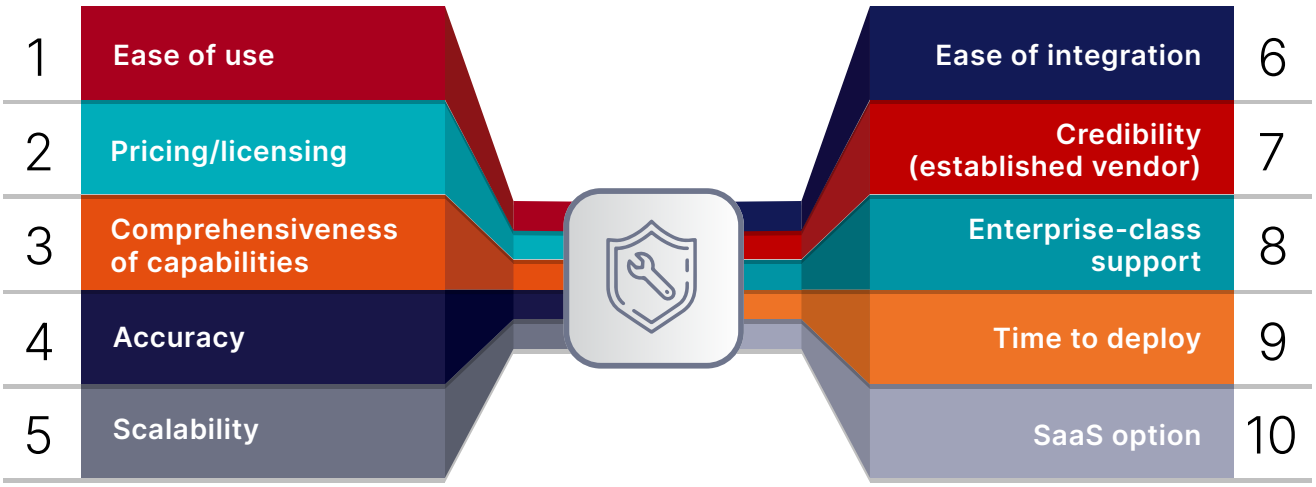
How to Select Application Security Solutions

As organizations refine their security strategies, selecting application security tools or services can be challenging and must be guided by clear criteria that balance functionality, cost, and operational needs.

When asked to rank the most important factors, ease of use emerges as the top selection criterion, underscoring that in an increasingly complex application security landscape, organizations prioritize intuitive security tools that reduce operational burdens—even ahead of more robust security features—and help teams overcome the ongoing skills shortage. Pricing and licensing are ranked second, highlighting budget constraints and the demand for flexible, cost-effective solutions. The comprehensiveness of capabilities comes in third, signaling that organizations value tools capable of addressing various security challenges. Accuracy ranks fourth, emphasizing the need for reliable detection and prevention to minimize false positives and negatives, while scalability and ease of integration round out the middle of the rankings, pointing to the operational practicality of solutions.

This prioritization aligns with broader trends discussed earlier, such as the push toward consolidating security tools (43% plan to consolidate in 2025), where ease of integration and comprehensive capabilities play essential roles. Additionally, the reliance on real-time monitoring and advanced technologies like AI for threat detection highlights the critical importance of accuracy and scalability, as organizations must respond to increasingly sophisticated threats at scale.

What are your most important criteria for selecting an application security tool or service?

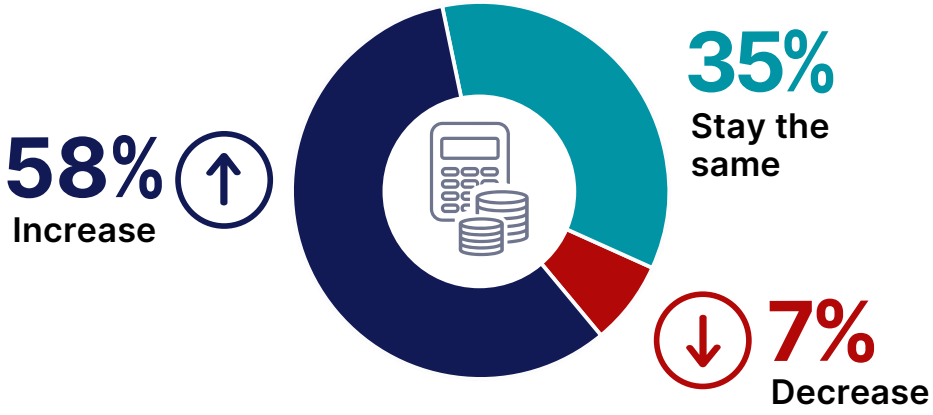


Increasing Budget for Application Security

As threats against applications' complexity grows, organizations adjust their resource allocation to prioritize evolving security needs.

Most respondents (58%) report that their budgets for securing applications will increase in the next 12 months, reflecting the growing recognition of application security as a critical component of organizational risk management. Meanwhile, 35% expect budgets to remain the same—meaning about one in three organizations will not increase their cybersecurity investments—suggesting they believe current allocations are sufficient to maintain existing security postures. Only 7% anticipate a decrease in their application security budgets, showing that reductions are relatively rare and likely constrained to organizations with limited resources or shifting priorities.

How is the budget for securing your applications changing over the next 12 months?



These findings align with previously discussed trends, such as the push for consolidating application security tools and the growing reliance on advanced technologies like AI for threat detection and response. The increased investment in security is a logical response to concerns over sophisticated threats, like AI-generated attacks and human-like bots, and the need for comprehensive visibility across applications and APIs.

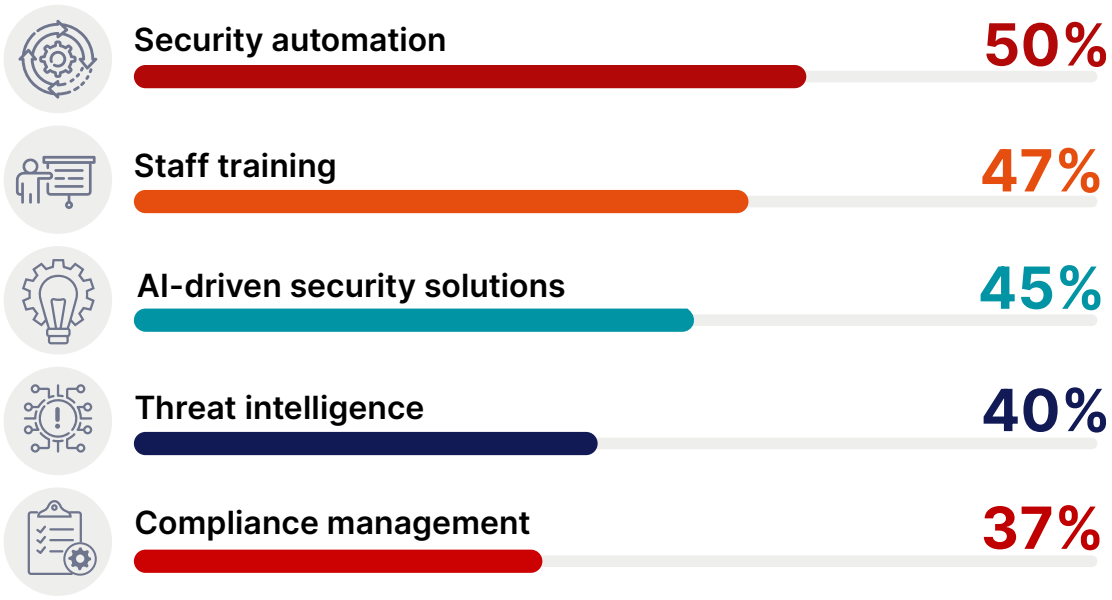
Investment Priorities for Application Security

As organizations face increasingly complex threats in cloud environments, their investment priorities and resource allocation reveal the strategies they are adopting to enhance application security.

Security automation leads the list, cited by 50% of respondents, reflecting the growing emphasis on streamlining processes to address security gaps efficiently and at scale. Staff training follows at 47%, underscoring the recognition that human expertise is as critical as technology in mitigating risks. AI-driven security solutions, prioritized by 45%, illustrate the demand for advanced tools to detect and respond to emerging threats proactively. Investments in threat intelligence (40%) and compliance management (37%) highlight the need to stay ahead of adversaries while navigating the increasingly stringent regulatory landscape.

These investment priorities align with broader survey findings, such as increased budgets for application security (58% planning budget increases) and the focus on leveraging AI and machine learning for threat detection and anomaly analysis. The emphasis on automation and AI solutions also complements previously discussed trends in tool consolidation, where integrated, scalable platforms can deliver the efficiency organizations are seeking.

In which areas does your organization plan to invest to enhance cloud application security?



Essential Best Practices for Robust Web Application Security

With evolving threats targeting web applications, fortifying application security is critical for reducing risks and ensuring business resilience. The following best practices, backed by industry data, provide a structured approach to strengthening application defenses.

1

EXPAND VISIBILITY ACROSS HYBRID AND MULTI-CLOUD ENVIRONMENTS

Seventy-eight percent of organizations run applications in multi-cloud or hybrid ecosystems, and many struggle with limited visibility across disparate platforms. Adopting a single interface consolidating security and delivery services helps unify policy management, monitor real-time activity, and spot anomalies before they escalate. By centralizing oversight and reducing manual coordination, teams gain the observability to proactively defend against misconfigurations, human error, and stealthy exploits lurking in siloed environments.

2

LEVERAGE AI FOR PROACTIVE THREAT DETECTION

With 61% of organizations adopting AI for threat detection, it is crucial to utilize AI-driven risk scoring, automated threat intelligence, and behavioral analytics to prioritize threats based on their exploitability and business impact. Adaptive security models dynamically adjust defenses, automatically mitigating high-risk threats and minimizing false positives. Real-time, AI-driven threat analytics enhance response times to zero-day threats with maximum accuracy, alleviating alert fatigue and allowing security teams to concentrate on the most critical vulnerabilities.

3

SECURE APIS TO PREVENT DATA LOSS

Fifty-eight percent of respondents cite API security as a primary concern, reflecting how interconnected services can become gateways for threats. Poorly secured APIs have led to breaches like the 2022 Optus API incident, where an unprotected endpoint exposed sensitive customer data. To mitigate these risks, organizations should implement an integrated approach that discovers and catalogs API endpoints, enforces schemas and protocols, and detects anomalous behaviors in HTTP traffic and API calls in real time.

4

IMPLEMENT ADVANCED BOT PROTECTION TO STOP AUTOMATED THREATS

Sophisticated bots are increasingly used for credential stuffing, web scraping, and API abuse, often bypassing traditional security defenses. To combat these threats, organizations must deploy AI-powered bot management solutions that leverage behavioral analysis, machine learning, and deception techniques to neutralize automated attacks. Proactive bot mitigation combined with real-time behavioral analytics ensures organizations protect cloud-hosted assets, user accounts, intellectual property, and online revenue from sophisticated, human-like bot threats.

5

ENSURE CONSISTENT COMPLIANCE AND OBSERVABILITY

Regulatory pressures remain high, with 51% of respondents facing compliance complexities in cloud environments. Web application security that provides both broad coverage and deep observability helps maintain regulatory obligations while detecting and mitigating threats. Teams can proactively audit configurations, enact automated policy updates, and leverage real-time analytics to address evolving compliance requirements and avoid costly violations.

6

UNIFY AND CONSOLIDATE APPLICATION SECURITY TOOLS TO SIMPLIFY OPERATIONS

Fragmented security tools create visibility gaps, inefficiencies, and operational silos. 43% of organizations plan to consolidate their security tools to streamline operations and mitigate blind spots. Adopting a comprehensive, cloud-delivered solution that unifies web application and API security, advanced bot protection, threat analytics, content delivery network (CDN), and distributed denial-of-service (DDoS) capabilities lowers operational overhead and ensures consistent policy enforcement. This approach helps security teams address blind spots by centralizing policies and simplifying management across hybrid and multi-cloud environments.

By adopting these strategies, organizations can strengthen their security defenses, minimize risks, and build a more resilient application security posture.

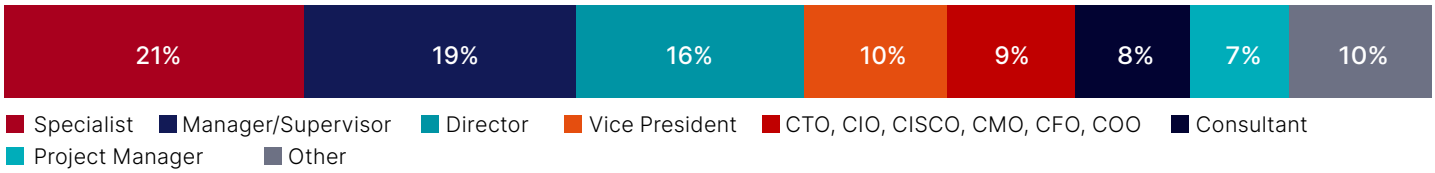
Methodology and Demographics

The 2025 Web Application Security Report is based on a comprehensive survey conducted in early 2025, which gathered insights from 651 IT and cybersecurity professionals in a wide range of industries, including technology, financial services, healthcare, and government. Respondents represent organizations of varying sizes, from small businesses to large enterprises, and include professionals in roles ranging from cybersecurity specialists to C-level executives.

The online survey explored key trends, challenges, and priorities in web application security. The findings provide a well-rounded view of how organizations are navigating the complexities of protecting web applications and adopting security technologies to address emerging threats.

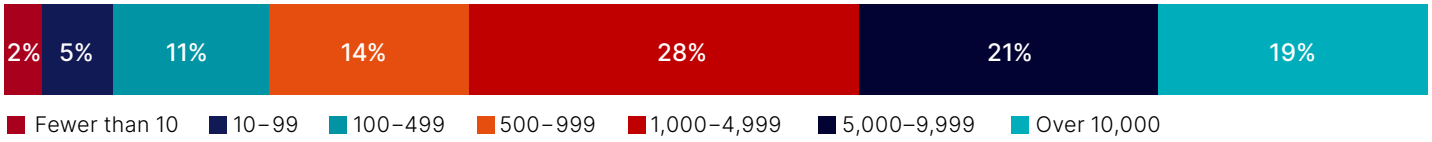
For questions that allow respondents to select multiple answers, the percentages may total more than 100%, as participants could choose more than one option.

CAREER LEVEL

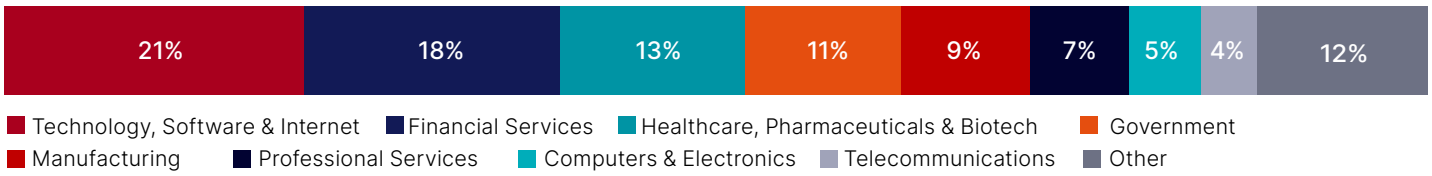


DEPARTMENT

COMPANY SIZE



INDUSTRY



Fortinet (NASDAQ: FTNT) secures the largest enterprises, services providers, and government organizations around the world. Fortinet empowers our customers with complete visibility and control across the expanding attack surface and the power to take on ever-increasing performance requirements today and into the future. Only the Fortinet Security Fabric platform can address the most critical security challenges and protect data across the entire digital infrastructure, whether in networks, application, multi-cloud, or edge environments. Fortinet ranks #1 as a security company, with more than 800,000 clients who trust their solutions and services to protect their businesses.

www.fortinet.com

Cybersecurity
INSIDERS

Cybersecurity Insiders brings together 600,000+ IT security professionals and world-class technology vendors to facilitate smart problem-solving and collaboration in tackling today's most critical cybersecurity challenges.

Our approach focuses on creating and curating unique content that educates and informs cybersecurity professionals about the latest cybersecurity trends, solutions, and best practices. From comprehensive research studies and unbiased product reviews to practical e-guides, engaging webinars, and educational articles - we are committed to providing resources that provide evidence-based answers to today's complex cybersecurity challenges.

Contact us today to learn how Cybersecurity Insiders can help you stand out in a crowded market and boost demand, brand visibility, and thought leadership presence.

Email us at info@cybersecurity-insiders.com or visit cybersecurity-insiders.com