Cybersecurity
INSIDERS

2024

Application Security Report

FORTINET®

Introduction

In today's digital ecosystem, the expansion of application and API landscapes offers both opportunities and challenges for organizations. Advancements in application development and integration foster unparalleled business agility and innovation but also enlarge the attack surface, creating numerous opportunities for threat actors to exploit. This complexity presents a formidable challenge for IT security teams to maintain visibility and control, ensuring comprehensive protection against increasingly sophisticated adversaries.

The 2024 Application Security Report, based on a detailed survey of over 500 cybersecurity professionals, is aimed at uncovering current trends, challenges, and practices in application security.

Key findings include:

- **Application Vulnerability:** Half of the respondents report that their applications were compromised in the past year, highlighting the prevalent risk and the critical need for more robust security measures.
- **Expertise Gap:** Only 19% of security professionals identify as experts in application security, highlighting a significant need for further development of skills among the remaining 81% to effectively counteract cyber threats.
- **Visibility Challenges:** 45% of participants are not confident in their awareness of all applications used within their organizations, underlining the difficulties in achieving comprehensive application visibility.
- **Bot Attack Concerns:** 45% raised concerns over their preparedness to defend against sophisticated bots, emphasizing the evolving nature of threats that organizations face.
- **Patch Management Hurdles:** 40% of respondents acknowledge that they are unable to patch vulnerabilities in a timely manner, leaving organizations vulnerable to attacks.

We sincerely thank Fortinet for their essential contribution to this survey. The insights and best practices derived from this survey highlight the critical areas for organizations to focus their efforts in order to minimize and reduce their attack surface. 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

Cybersecurity INSIDERS

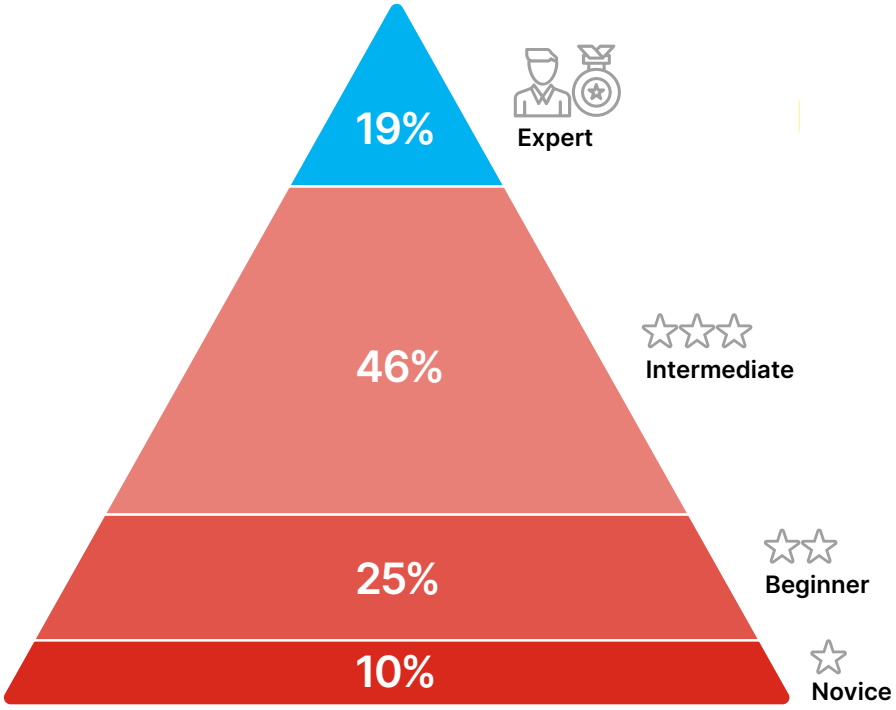
Application Security Expertise

Application security is a critical part of cybersecurity that demands nuanced expertise to effectively navigate its complexities. Applications are becoming increasingly vulnerable due to the rapid pace of digital transformation and the complexity of modern, cloud-first software development. This environment, rich with APIs and third-party services, opens numerous attack vectors. Furthermore, threat actors' evolving tactics, such as AI-automated attacks, often outpace organizational security measures and elevate risk.

Only 19% of the survey respondents identify as experts, possessing extensive experience and a profound grasp of application security, including leadership in security projects. 46% of participants have intermediate proficiency in application security, reflecting an understanding and practical engagement with application security measures. This majority indicates a workforce capable of implementing essential security practices, yet possibly lacking in advanced skills or experience. However, the 35% at the beginner and novice stages highlights a substantial segment that might not yet effectively contribute to safeguarding applications, underscoring a need for targeted upskilling.

To bridge this expertise gap, organizations should prioritize comprehensive training and development for those at the beginner and novice levels. Tailored programs that enhance practical skills and theoretical knowledge in application security will be critical. Furthermore, fostering an environment that encourages collaboration and knowledge exchange among all expertise levels can accelerate the collective advancement towards a more secure application ecosystem.

How would you describe your level of experience with application security?



Confidence in Application Security Posture

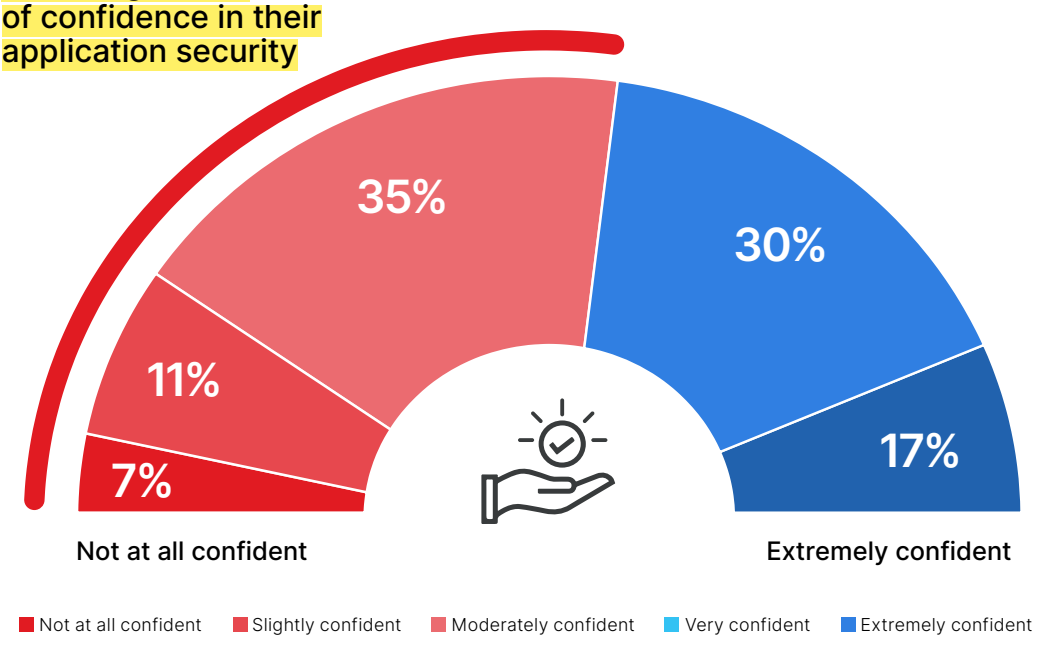
Reflecting on the varied levels of application security expertise, it's also beneficial to examine the confidence levels among cybersecurity professionals regarding their organization's application security posture. This confidence speaks to both the strength of security measures in place and how well these measures are understood and implemented by the cybersecurity team.

More than half of the survey respondents (53%) report a concerning lack of confidence in their organization's application security posture, with 35% being only moderately confident and 18% slightly or not at all confident. This suggests a high degree of doubt in the existing application security strategies.

By focusing on state-of-the-art security practices and tools, as well as cybersecurity training, organizations can not only strengthen their application security posture but also enhance the confidence of their cybersecurity professionals in the organization's overall security strategy.

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

53%
of organizations lack a high level of confidence in their application security



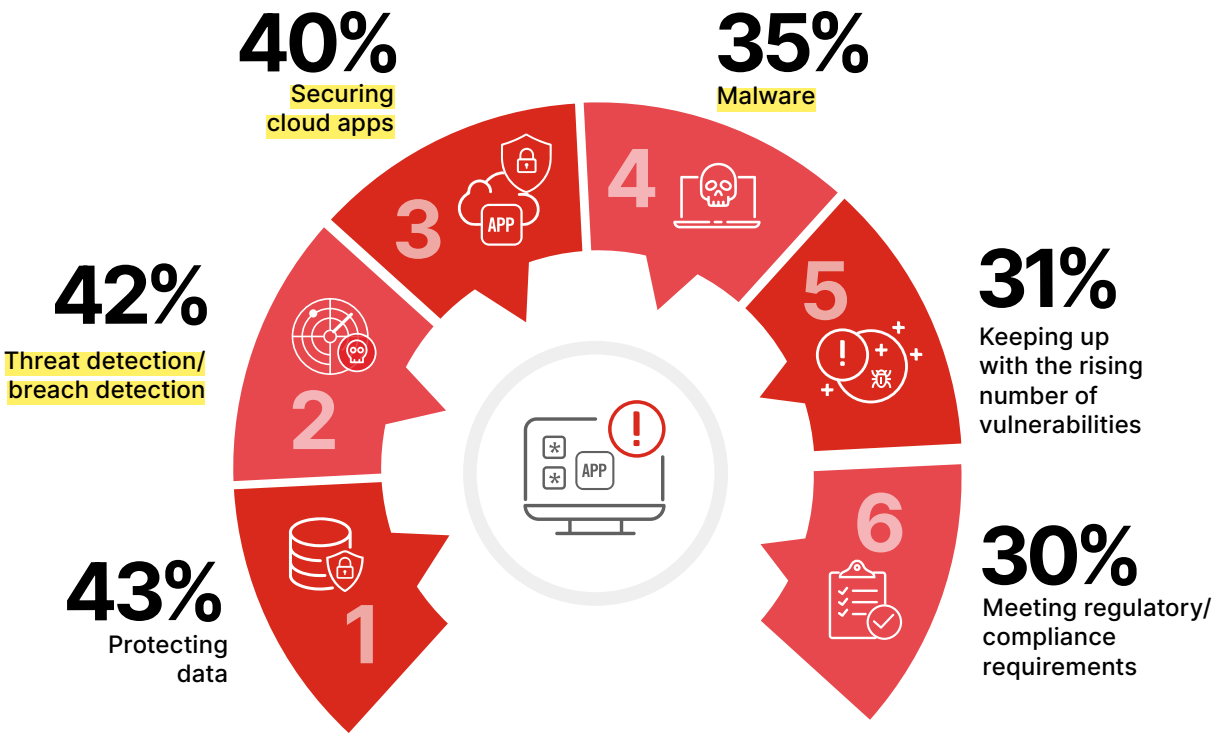
Prioritizing Application Security Concerns

Cybersecurity professionals' wide-ranging concerns about application security reflect the complex nature of this challenge and the need for a comprehensive approach to protect applications at all development stages and across different environments.

The top concern is data protection, noted by 43% of respondents (and in the same spot as in our 2021 survey), underlining the continued importance of shielding sensitive information from unauthorized access and breaches. Close behind, 42% emphasize the need for effective threat and breach detection (up from the #4 spot in 2021), highlighting the necessity for advanced monitoring to quickly spot and address threats. Securing cloud applications, a concern for 40%, points to the shift towards cloud environments and their specific security challenges (rising from the #5 spot in 2021). Additional worries include malware defense, mentioned by 35%, and the task of managing an increasing number of vulnerabilities, identified by 31% of participants. This underscores the evolving threat landscape and the need for vigilant vulnerability management.

Organizations should adopt a comprehensive security strategy, integrating advanced technologies like encryption, modern Web Application Firewalls (WAFs), and Cloud Workload Protection Platforms (CWPP) to enhance data and cloud application security. Embracing DevSecOps principles ensures security is an integral part of the development lifecycle, addressing vulnerabilities in in-house applications. This approach helps tackle key security concerns, fostering a robust and adaptable security posture.

What are your biggest application security concerns?



Additional responses include:
Securing applications we develop 28% | Effectively prioritizing and remediating vulnerabilities that pose the most risk 27% | Effective threat modeling 26% | Meeting customers' security needs and requirements 25% | Securing business apps (ERP, etc.) 24% | Securing open source software 21% | Securing mobile apps 21% | Securing embedded/IoT/hardware 19% | Securing blockchain 13% | Securing commercial off-the-shelf software 11% | Don't know/unsure 7%

Recent Application Breaches

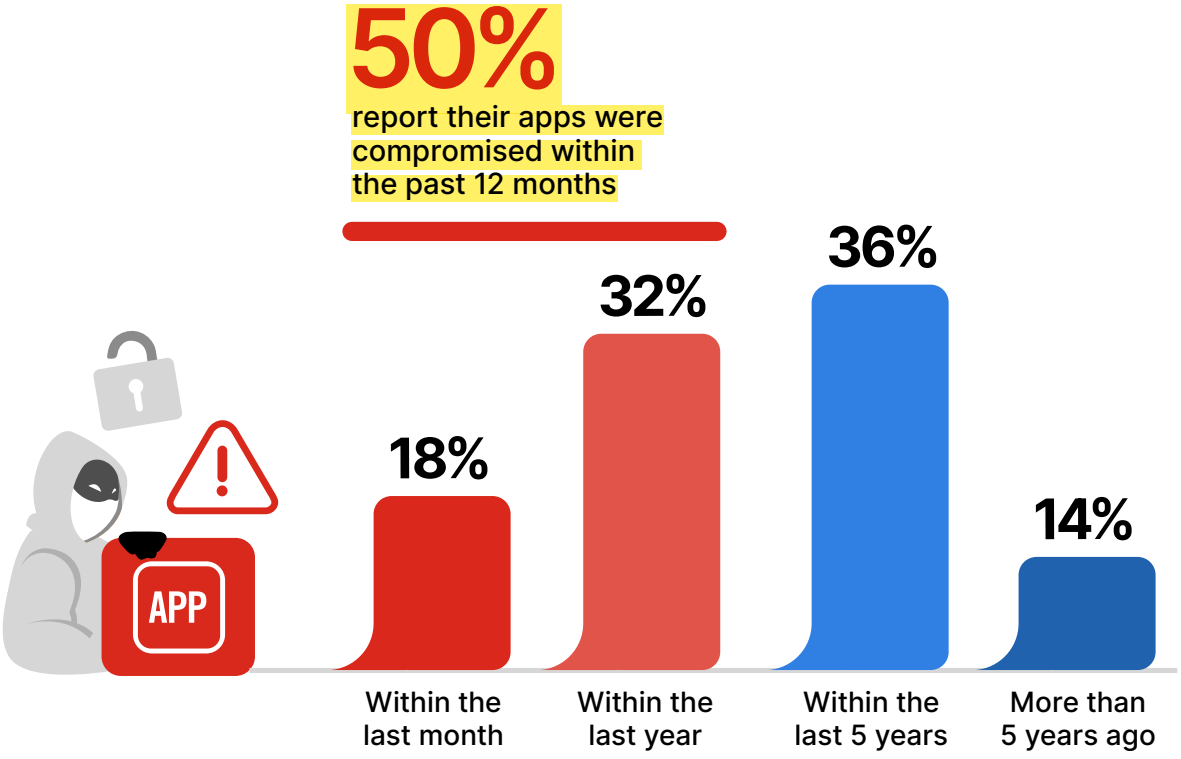
The frequency and recency of application related security incidents within organizations offer crucial insights into the current cybersecurity landscape and the effectiveness of prevailing security measures.

Notably, 50% of respondents reported an application breach within the last year. This statistic highlights the continuous threat activity and the essential need for effective detection and rapid response. Collectively, It indicates that half of the surveyed organizations have encountered recent security incidents, emphasizing the critical need for improved security measures.

On the other side, 36% experienced breaches between 1-5 years ago, pointing out that while many have avoided recent incidents, the threat of breach remains. The 14% with breaches occurring more than 5 years ago suggests either ongoing security success or potential gaps in detecting newer incidents.

Organizations should thus focus on implementing robust, real-time monitoring and response solutions, including next-generation firewalls, web app and API solutions, and automated security orchestration. Embracing continuous security assessment and a Zero Trust model—verifying every access request—can significantly reduce incident risks.

When was the last time that one of your company's applications was breached/ compromised?



Common Application Attack Vectors

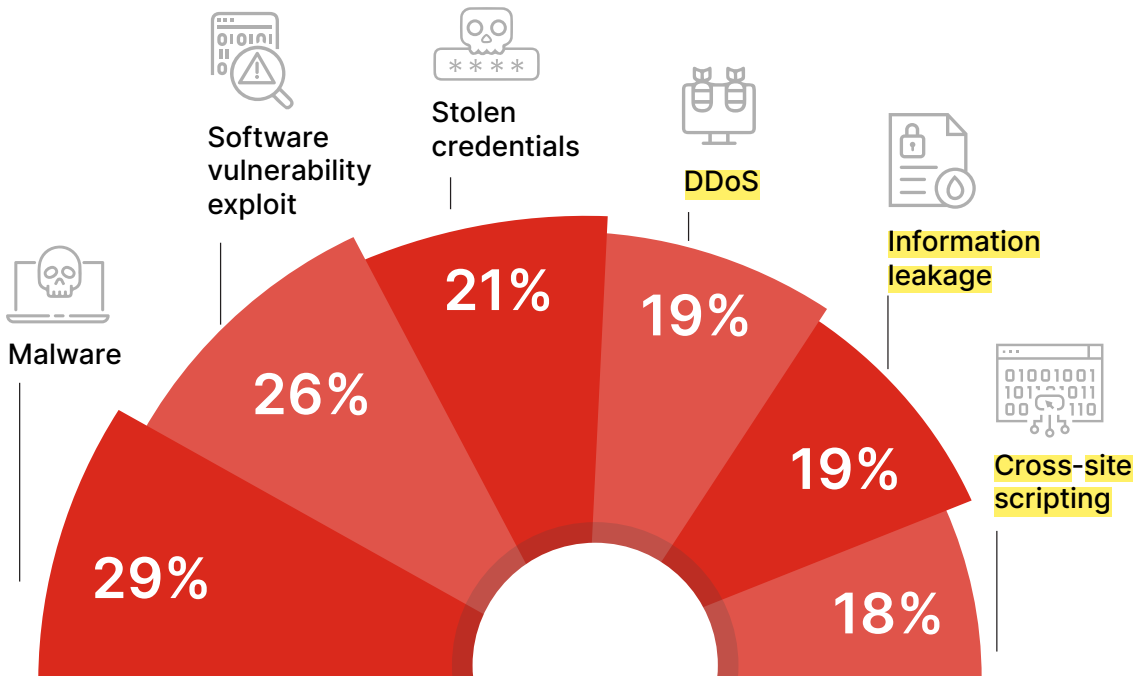
In the context of recent incidents, understanding the types of attacks against applications sheds light on adversary tactics and informs the creation of targeted defense strategies. The array of attack vectors over the past year reflects the complexity of the threat landscape and the need for a comprehensive security approach.

Malware leads the reported attack vectors at 29%, underscoring the need for robust endpoint protection and up-to-date defenses against malicious software. Following closely, 26% of organizations encountered exploits of software vulnerabilities, highlighting the critical need for continuous vulnerability management and timely patching to mitigate the risk of exploitation.

Stolen credentials, reported by 21% of respondents, underscores the importance of robust authentication mechanisms, including multi-factor authentication (MFA), to prevent unauthorized access. DDoS attacks and information leakage, both at 19%, further illustrate the diverse methods attackers employ to disrupt services and exfiltrate sensitive data, calling for advanced threat detection and data protection solutions.

Cross-site scripting and brute force attacks, each cited by 18% and 17% of participants respectively, alongside application misconfiguration and content spoofing, stress the importance of secure coding practices, comprehensive security assessments, and the deployment of solutions such as Web Application Firewalls (WAFs) to defend against these prevalent threats. These common attack vectors underscore the urgent need for organizations to bolster their security posture through a combination of proactive, AI-driven threat intelligence, real-time monitoring, and the adoption of Zero Trust principles.

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



Additional responses include:
Brute force 17% | Application misconfiguration 17% | Content spoofing 13% | Web fraud 13% | SQL injection 12% | Unpatched library 12%
Clickjacking 10% | Cross-site registry 9% | MitM/MitB 4%

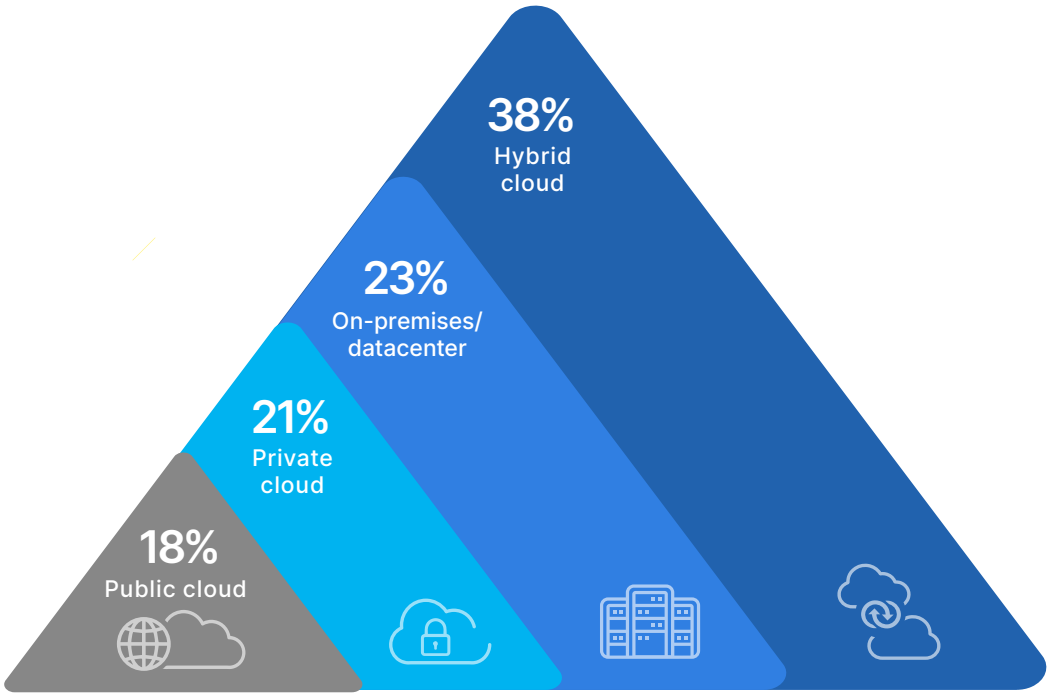
Application Hosting Strategies

The choice of hosting environment for applications significantly influences an organization's operational flexibility, scalability, and security posture. This decision reflects not only technological preferences but also strategic priorities regarding data sovereignty, access control, and threat mitigation.

The largest group of respondents, 38%, reveals a preference for hybrid cloud environments, suggesting a strategic balance between the scalability and innovation offered by cloud services and the control and security associated with on-premises resources. This approach likely reflects an understanding of the nuanced security needs across different hosting environments, as well as a desire to leverage the benefits of both without fully committing to the security and compliance complexities of a cloud-only approach. The on-premises/datacenter model, favored by 23% of organizations, underscores a continued reliance on traditional hosting methods, possibly due to regulatory requirements, data sensitivity concerns, or specific performance needs. While offering greater control over security configurations, this choice requires robust internal security measures and infrastructure maintenance.

Private cloud solutions, selected by 21%, highlight the importance of exclusive resource utilization within a controlled environment, offering a compromise between the scalability of cloud services and the security and control of on-premises hosting. Public cloud adoption, at 18%, while the least common response, still represents a significant portion of organizations moving towards fully cloud-based solutions, attracted by their cost-effectiveness, scalability, and the evolving security features offered by cloud providers. In light of the varied attack vectors mentioned earlier, it's crucial for organizations to tailor their security strategies to their chosen hosting environments. Hybrid and multi-cloud architectures demand sophisticated security orchestration and policy management to ensure consistent security postures across different platforms. For on-premises and private cloud environments, dedicated security controls and vigilant monitoring are paramount. Public cloud users must navigate shared responsibility models, ensuring that their configurations and usage adhere to best security practices. Emphasizing advanced threat protection, data encryption, and identity and access management across all environments can help mitigate the specific risks associated with each hosting model.

Where are the majority of your applications hosted?



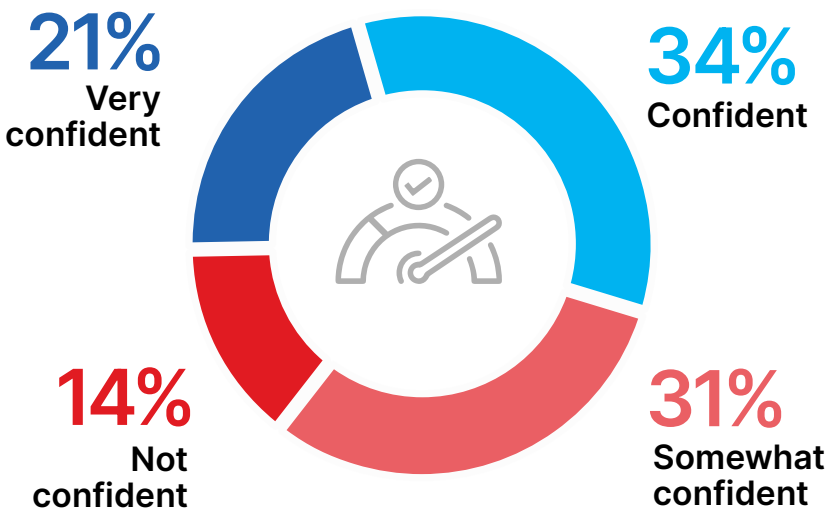
Navigating Application Awareness

Ensuring comprehensive awareness of all applications within an organization is crucial for mitigating security risks, especially in the context of shadow IT, where unauthorized applications can introduce vulnerabilities. Only 21% of survey respondents feel very confident in their knowledge of applications used, highlighting either effective control measures or a possible underestimation of their organization's true application landscape.

Conversely, the 45% indicating varying degrees of uncertainty (somewhat confident to not confident) underscores the challenges shadow IT presents, from bypassing security protocols to complicating compliance. This finding emphasizes the need for strong governance strategies and technologies like application discovery tools to reveal hidden applications.

To curb the risks of shadow IT and enhance organizational security posture, fostering an environment of security consciousness and clear policies for technology adoption is crucial. Initiatives should focus on bridging IT governance with organizational innovation, ensuring a secure and adaptable application environment.

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



API Inventory Confidence

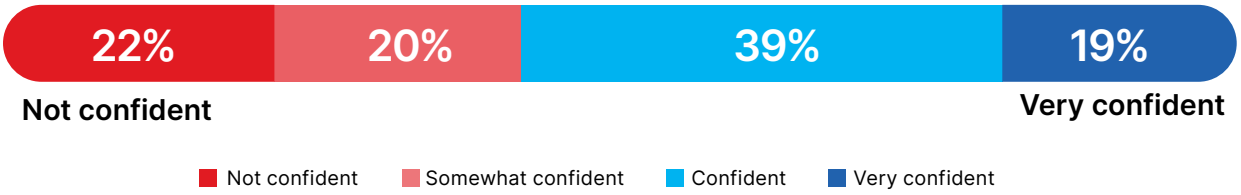
APIs play a critical role in application integration and communication, yet they introduce unique security challenges and shadow IT risks without careful management and documentation.

A majority (58%) feel confident or very confident in their knowledge of all APIs in their organization, suggesting effective governance and discovery practices in place for these crucial components. This level of assurance suggests robust API management strategies, including the use of API gateways and management platforms to catalog and secure API landscapes. However, this level of assurance could also suggest a degree of overconfidence among cybersecurity professionals, potentially overlooking gaps in their API inventory management.

On the other hand, 42% expressing some doubt or outright lack of confidence underscores the complexities and challenges in achieving complete visibility over their API footprint. This group highlights the potential for shadow APIs—unauthorized or undocumented APIs that can expose organizations to severe security threats due to inadequate oversight.

To tackle these issues, a balanced approach of technology and policy is essential. Organizations should adopt advanced API tools that include discovery for enhanced visibility and security across all APIs. It's also crucial to foster a culture that emphasizes clear governance around API creation and use, encouraging developers to maintain up-to-date API documentation and reviews. This strategy not only reduces the risks associated with shadow APIs but also bolsters the security infrastructure, ensuring APIs are consistently managed according to security best practices.

How confident are you that you know all of your APIs in your organization today?



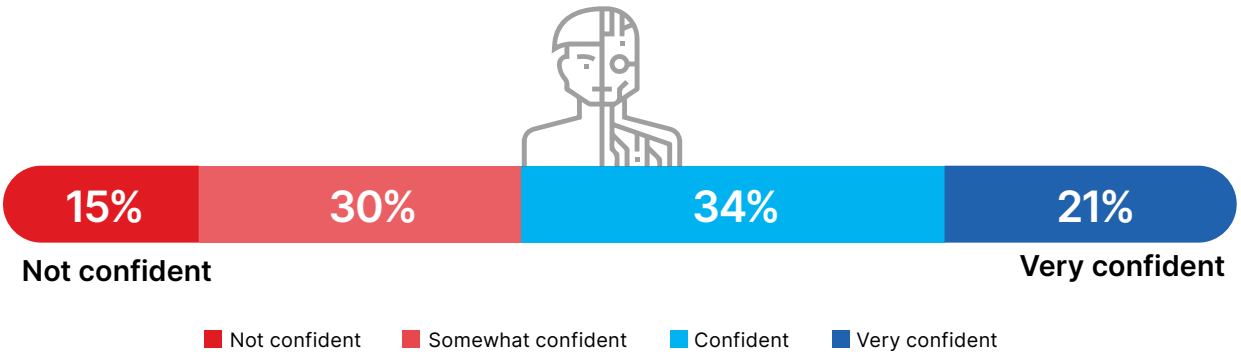
Defending Against Sophisticated Bots

The rise of sophisticated, human-like bots marks a significant cybersecurity challenge, where distinguishing between legitimate user interactions and automated, often AI-powered, attacks becomes increasingly difficult. These bots can mimic human behavior, making them particularly effective at evading detection and exploiting vulnerabilities in applications and APIs.

A majority (55%) feel confident or very confident in their ability to defend against such advanced bots. This suggests a high level of optimism or trust in current security measures and strategies to identify and mitigate these threats. However, the 45% who are only somewhat confident or not confident at all reflect the complexities involved in defending against bots that closely emulate human behavior. This concern suggests a recognition of the inadequacy of traditional security measures and a call for more advanced, innovative solutions to adapt to the advancing tactics of automated threats.

To better prepare for human-like bots, leading organizations invest in next-generation security solutions that incorporate advanced machine learning and behavioral analytics. These technologies can analyze patterns of activity to distinguish between genuine users and sophisticated bots. Additionally, fostering a culture of continuous learning and adaptation is crucial, encouraging teams to stay informed about the latest threat vectors and defense mechanisms.

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



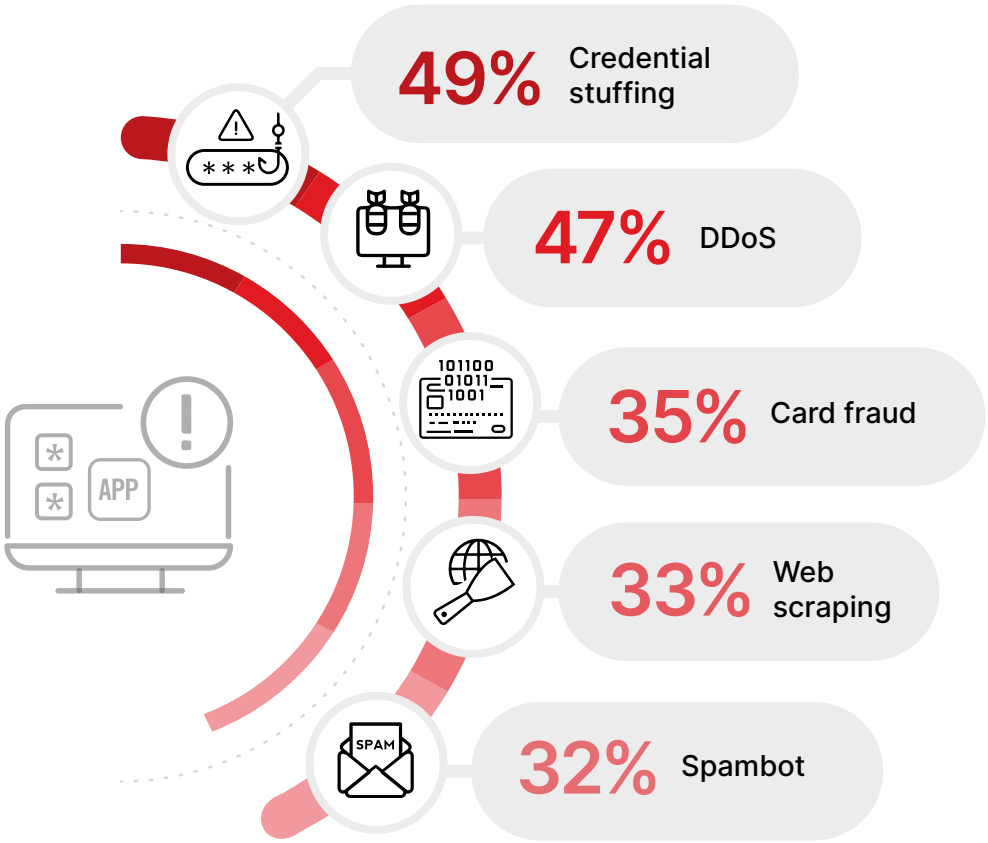
Bot Attack Concerns

In the context of preparing for sophisticated bots, understanding the most concerning bot attacks provides important insight into the threat landscape and guides defense strategies.

Credential stuffing, identified by 49% of respondents, emerges as the tope concern, underscoring the acute awareness of the risks associated with unauthorized access to user accounts. This type of attack leverages stolen username-password pairs (often from a data breach) to gain access to accounts across different services through large-scale automated login requests. Closely following at 47% are DDoS (Distributed Denial of Service) attacks. These attacks disrupt service availability, directly impacting business operations and damaging reputations. Card fraud and web scraping attacks, with 35% and 33% respectively, also rank high. Card fraud represents a direct financial threat to organizations and their customers, while web scraping can lead to the loss of intellectual property and competitive advantages, underscoring the broad implications of bot attacks beyond just security breaches.

To mitigate these bot threats, organizations should employ a layered security approach that includes advanced features such as browser fingerprinting, biometric detection, real-time threat intelligence, and comprehensive analytics. Educating users on the importance of secure password practices and implementing multi-factor authentication can further reduce the risk of credential stuffing and other bot-related attacks.

Which types of bot attacks are you most concerned with?



Resources for Vulnerability Management

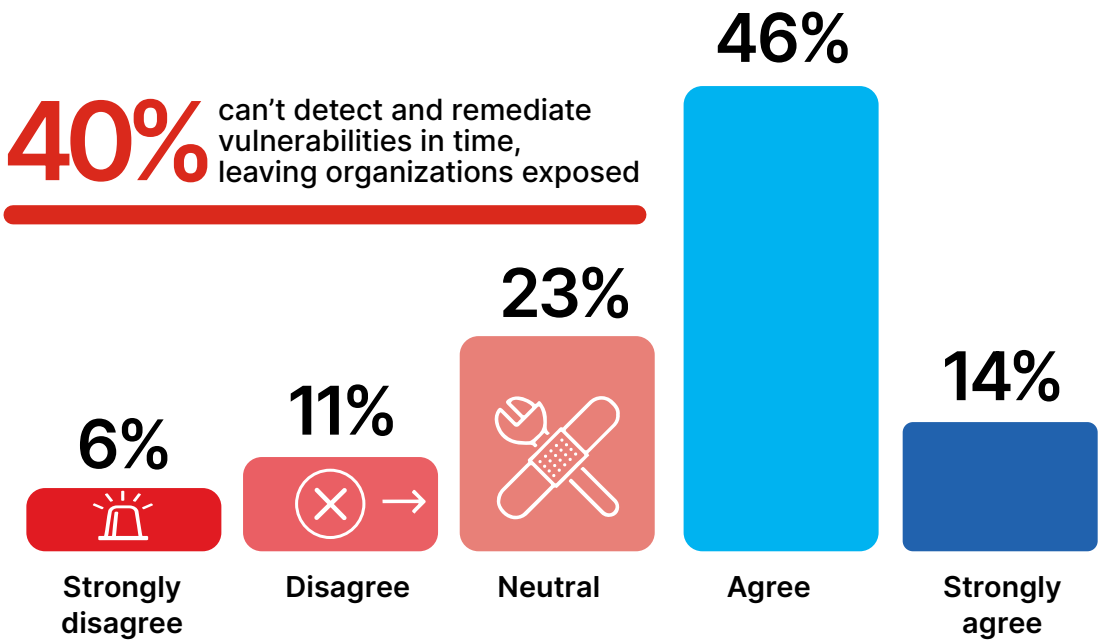
Swift detection and remediation of application vulnerabilities are key to a secure application landscape, particularly against the backdrop of complex threats, from sophisticated bots to credential stuffing attacks.

Sixty percent of survey respondents, including those agreeing or strongly agreeing, reflect confidence in their organization's vulnerability management resources. This confidence suggests trust in the effectiveness of their tools, processes, and teams to preemptively address security vulnerabilities.

However, an alarming 40% of organizations say they can't detect and remediate vulnerabilities in time, leaving organizations exposed. This group reports gaps in their vulnerability management practices, possibly due to constraints in budget, expertise, or technology.

Improving vulnerability management requires strategic investments in both advanced technology and skill development. Organizations should consider leveraging automated security scanning tools, continuous integration/continuous deployment (CI/CD) pipelines with integrated security checks, and threat intelligence platforms to gain insights into emerging threats. Equally important is fostering a culture of security within development teams, ensuring that security is a priority throughout the application lifecycle, from design to deployment.

Does your organization have ample resources to detect and remediate application vulnerabilities in a timely manner?

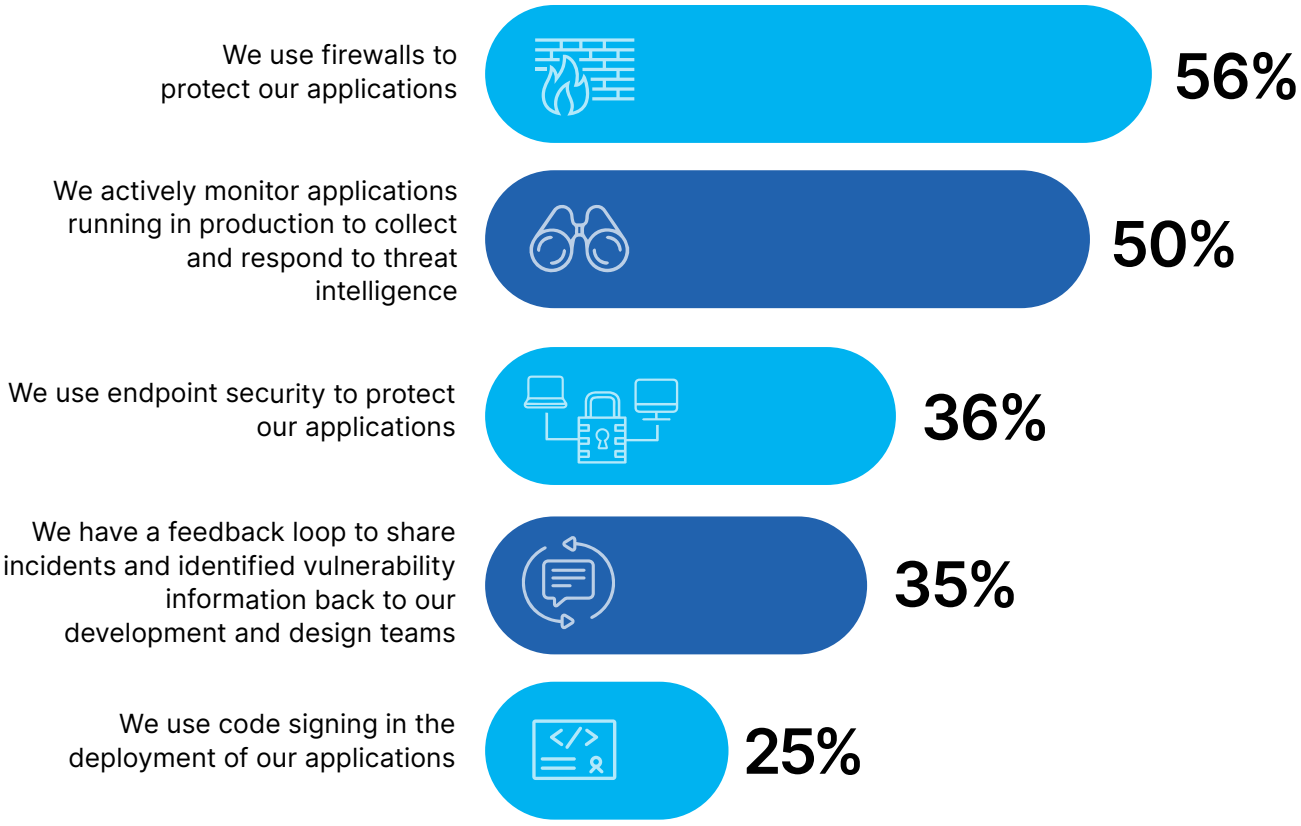


Strategies for Application Monitoring

Organizations employ a variety of monitoring techniques to ensure their applications remain resilient against cyber threats. The reliance on firewalls, as indicated by 56% of participants (up from 43% in our 2021 survey), showcases the continued importance of this foundational security measure in protecting applications from unauthorized access and attacks. Meanwhile, 50% of organizations actively monitor applications in production (unchanged since 2021), utilizing threat intelligence to identify and respond to potential security issues in real-time. Endpoint security, mentioned by 36%, highlights the recognition of protecting not just the application environment but also the devices accessing these applications that could serve as entry points for attackers.

To further enhance application security monitoring, organizations should consider integrating security solutions like Web Application Firewalls (WAFs) and automated vulnerability scanning tools. These technologies, coupled with a robust security culture that emphasizes the importance of security at every stage of the application lifecycle, can provide a comprehensive defense mechanism against potential threats.

How are you currently monitoring applications for security issues?



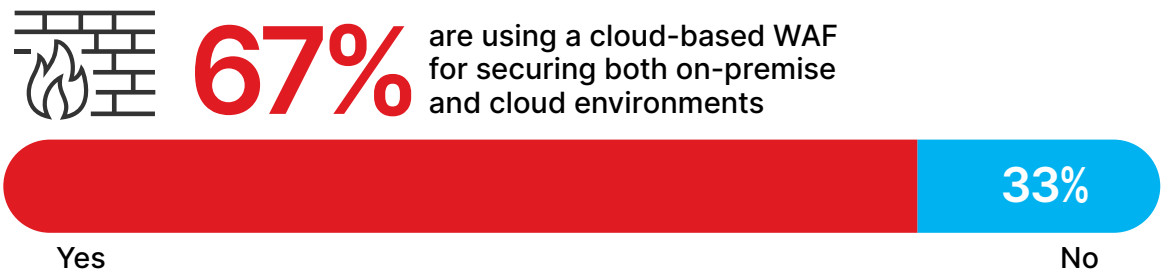
Adopting WAF Protection

The deployment of Web Application Firewalls (WAFs) across both on-premise and cloud environments is a vital part of modern cybersecurity strategies. A majority of organizations, 67%, use WAFs (up from 46% in 2021), which underscores their effectiveness in safeguarding applications from a wide range of threats, including SQL injection, cross-site scripting (XSS), and other sophisticated attacks that target the application layer.

This high WAF adoption rate reflects a strategic approach to application security and the necessity to protect assets regardless of their deployment environment. This security posture is essential, especially with the rise of hybrid cloud models, ensuring consistent protection across diverse infrastructures.

For the 33% not currently utilizing WAFs, adopting this technology presents an opportunity to strengthen their security framework. Integrating a WAF into security architectures provides an additional layer of defense, offering real-time threat analysis and mitigation capabilities.

Are you using a Web Application Firewall (WAF) for securing both on-premise and cloud environments?



A staggering 90% of survey respondents highlight the importance of Web Application Firewalls (WAFs) in securing API workloads, an increase from 79% in 2021, signaling a shift in application security priorities. This consensus reflects a recognition of WAFs' role in countering modern cyber threats. With APIs serving as vital channels for data exchange and application functionality, they increasingly attract cyber attacks due to their widespread use, potential vulnerabilities, and access to sensitive data.

Ensuring that WAFs can effectively interpret and protect API traffic has become essential to address these security challenges head-on.

Is it important to you that a WAF understand API workloads and be able to protect them?

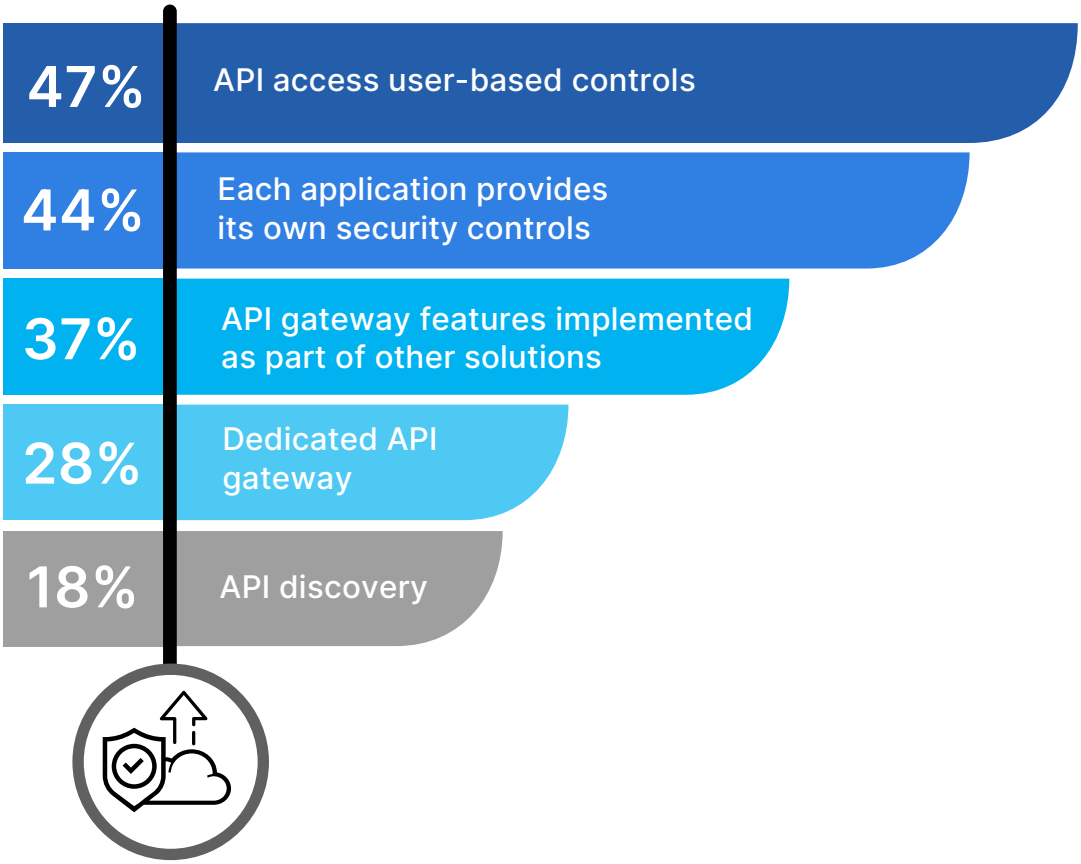
API Security Strategies

The survey responses reveal varied approaches to API security, emphasizing the importance of tailored solutions to protect these critical interfaces. API access controls like OAuth, used by 47% of respondents, underscores the importance of robust authentication to restrict API interactions to authorized entities.

Additionally, 44% of organizations rely on application-native security measures, such as API keys and rate limiting, indicating a decentralized approach to safeguarding against abuse. Meanwhile, 37% incorporate API gateway features into their security infrastructure, such as WAFs, to strengthen API protection through network-level controls. The adoption of dedicated API gateways by 28% and API discovery tools by 18% reflects strategies aimed at managing API interactions and uncovering APIs across the digital ecosystem, respectively.

This array of API security measures illustrates the comprehensive and layered defense mechanisms organizations deploy to navigate the complexities of API security more effectively.

To secure your application APIs, which solutions have you deployed?



Application Security Best Practices

In the face of evolving cyber threats, fortifying application security has never been more important. Below are essential best practices derived from industry insights and survey findings, designed to empower cybersecurity professionals with actionable strategies for enhancing their organization's defense mechanisms against sophisticated attacks.

IMPLEMENT ROBUST AUTHENTICATION & ACCESS CONTROLS:
Deploy mechanisms like OAuth and multi-factor authentication to ensure application access is restricted to authorized users and systems.

DEPLOY WEB APPLICATION FIREWALLS (WAFS):
Utilize WAFs to protect both on-premise and cloud-hosted applications from a range of threats, aligning with our findings that 67% of organizations use WAFs for comprehensive protection.

SECURE APIS VIGOROUSLY:
Choose a WAF that discovers and protects your APIs as well as your web applications. The significant concern for protecting API workloads is confirmed by 90% of organizations.

MONITOR APPLICATIONS & UTILIZE THREAT INTELLIGENCE ACTIVELY:
Keep a vigilant eye on application performance and potential security threats in real time, a practice adopted by 49% of organizations.

ENCRYPT SENSITIVE DATA DILIGENTLY:
Protect sensitive data through encryption both in transit and at rest. Prioritizing the protection of data, as 43% of respondents did, is crucial in safeguarding against breaches and ensuring privacy.

ASSESS VULNERABILITIES & APPLY PATCHES REGULARLY:
Conduct continuous vulnerability assessments and apply patches promptly to address security flaws.

IMPLEMENT RATE LIMITING & API KEYS:
Utilize rate limiting and API keys for each application to prevent abuse and ensure secure API usage, as indicated by the 44% of organizations that rely on application-centric security controls.

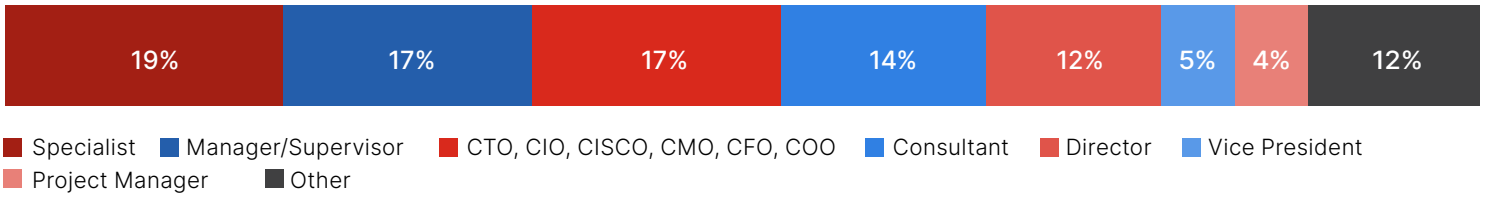
DEVELOP A SECURITY-FOCUSED CULTURE:
Foster a security-aware culture within the organization, emphasizing the importance of security best practices across all roles involved in application development, deployment, and use.

By adhering to these best practices, cybersecurity professionals can significantly enhance the security posture of their application footprint, effectively mitigating risks and ensuring a resilient defense against the evolving threat landscape.

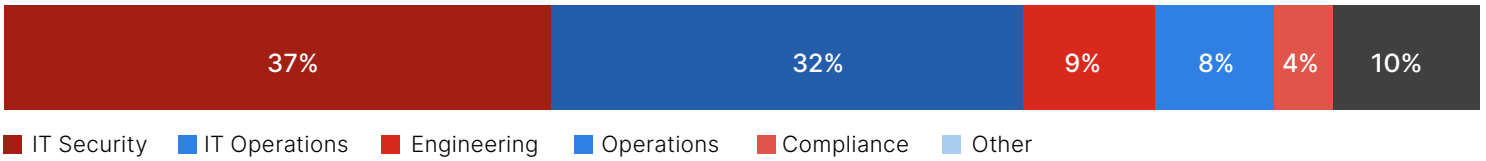
Methodology and Demographics

The 2024 Application Security Report is based on a comprehensive global survey of 507 cybersecurity professionals conducted in February 2024, to uncover how cloud user organizations are adopting the cloud, how they see cloud security evolving, and what best practices IT cybersecurity leaders are prioritizing in their move to the cloud. The respondents range from technical executives to IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

CAREER LEVEL

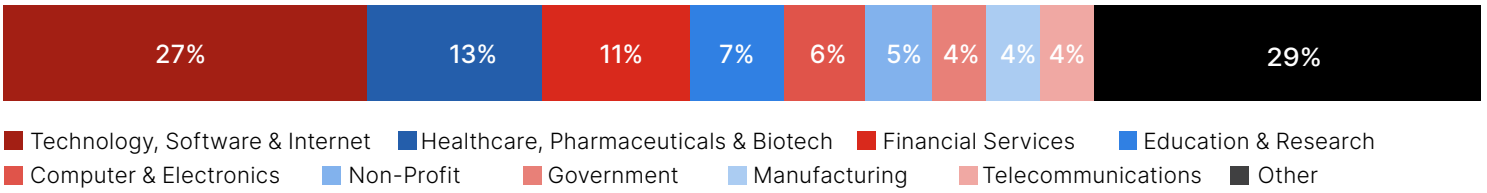


DEPARTMENT



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 the company with the most security appliances shipped worldwide and more than 730,000 customers trust Fortinet 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