Enterprise Strategy Group | Getting to the bigger truth.™

Trends in Modern Application Protection

Tool Sprawl and API Proliferation Drive WAAP Interest

John Grady, Senior Analyst

MAY 2022

Research Objectives

Securing applications has become more difficult than ever. Increasingly heterogeneous application environments coupled with distributed responsibility for application security has resulted in security complexity and tool sprawl. Further, attackers understand this challenge and use it to their advantage. While exploits against known application vulnerabilities remain common, advanced campaigns use bots to amplify denial of service and credential attacks that target web applications as well as the APIs they rely upon. Converged application protection platforms have emerged to address many of these issues, but organizations can struggle with prioritizing the capabilities they require, assessing the different types of tools available, and meeting the diverse needs of a broad set of stakeholders.

In order to gain insight into these trends, ESG surveyed 366 IT, cybersecurity, and application development professionals personally involved with web application protection technology and processes at North American organizations.

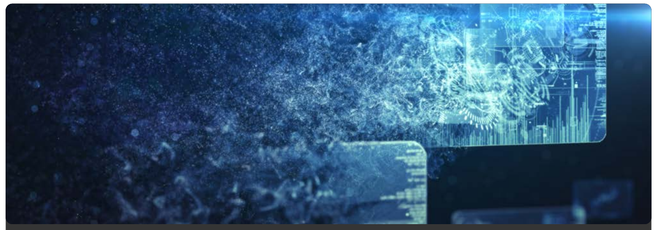
THIS STUDY SOUGHT TO:

- **Gain insights** into how changing application environments and API usage have impacted security strategies and the challenges security teams face in navigating this transition.
- **Understand the inflection point** organizations have reached with traditional web application firewalls.
- **Examine the impact** of attacks on respondent organizations and how the threat landscape is changing tool requirements.
- **Gauge buyer preferences** for converged web application and API protection solutions, and understand considerations and use cases where layered approaches may still be preferred.

Back to Contents

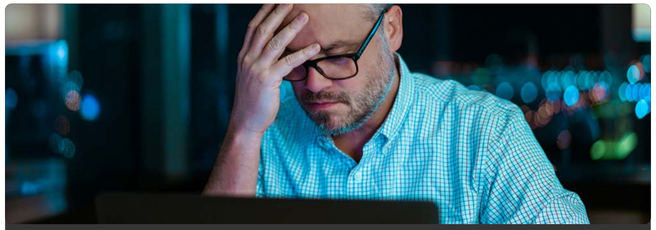
KEY FINDINGS

CLICK TO FOLLOW



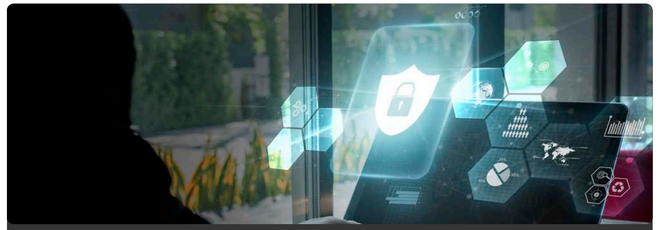
Application Environments and Processes Continue to Evolve, Creating Security Complexity

The shift to cloud and adoption of agile DevOps are among the factors making application security more difficult.



Successful Application Attacks Can Impact Employees, Customers, and the Bottom Line

The broad range of attacks across applications and APIs makes prioritizing defense difficult.



Protecting Web Applications Is a Priority for Most, Though Drivers Vary

Most say ensuring secure and available applications is a top 3 cybersecurity priority.

Tool Sprawl Has Become Problematic

New application architectures, locations, and processes all contribute to sprawl.

APIs Are of Particular Concern and Can Exacerbate Tool Sprawl

Visibility is a critical challenge to securing APIs.

There Is Significant Interest in Consolidation, with API Security as a Focus

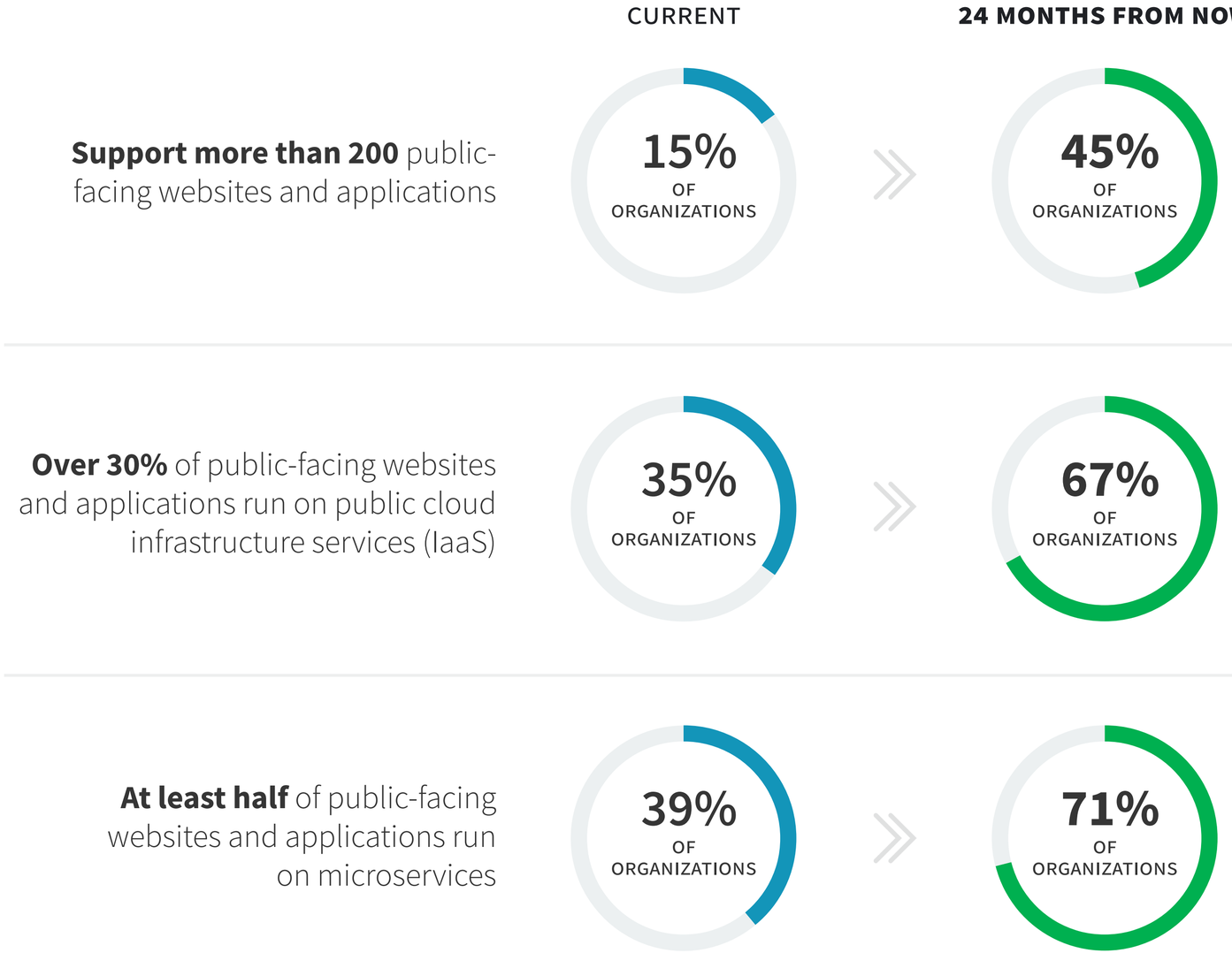
Many anticipate deploying WAAP in front of business-critical applications.

Application Environments and Processes Continue to Evolve, Creating Security Complexity

The Scale and Composition of Application Environments Will Change Significantly Over the Next 24 Months

More than ever, organizations rely on applications to engage with customers, connect with partners, and ultimately drive revenue for the business. While only 15% of organizations support more than 200 public-facing websites and applications today, nearly half (45%) expect to reach this milestone in the next 24 months. Yet as the scale of application deployments continues to accelerate, many organizations find themselves at an inflection point with their application environments. The reliance on the public cloud continues to grow, with the percentage of organizations running more than 30% of their applications on infrastructure-as-a-service (IaaS) expected to nearly double over the next 2 years. Even more telling, 71% expect at least half of their applications to run on microservices.

Public-facing websites and applications landscape.



Back to Contents

DevOps Has Become Pervasive, but Incorporating Security Remains a Work in Progress

To support the shift to IaaS, and more importantly cloud-native, microservices-based architectures, many organizations have turned to agile development methodologies. To better enable these practices, nearly three-quarters (74%) of organizations currently use DevOps to some extent. However, the incorporation of security remains a work in progress. Specifically, only 19% have extensively incorporated security into DevOps processes, with an additional 28% incorporating security in a limited fashion. This gap can result in security teams losing visibility across the environment and ultimately increase the potential for attackers to exploit critical applications.

> “While 74% of organizations currently use DevOps, **only 47% have incorporated security processes and controls.”**

We have incorporated security into DevOps processes:

19%
Extensively

28%
In a limited fashion

32%
Plan to in 12-24 months

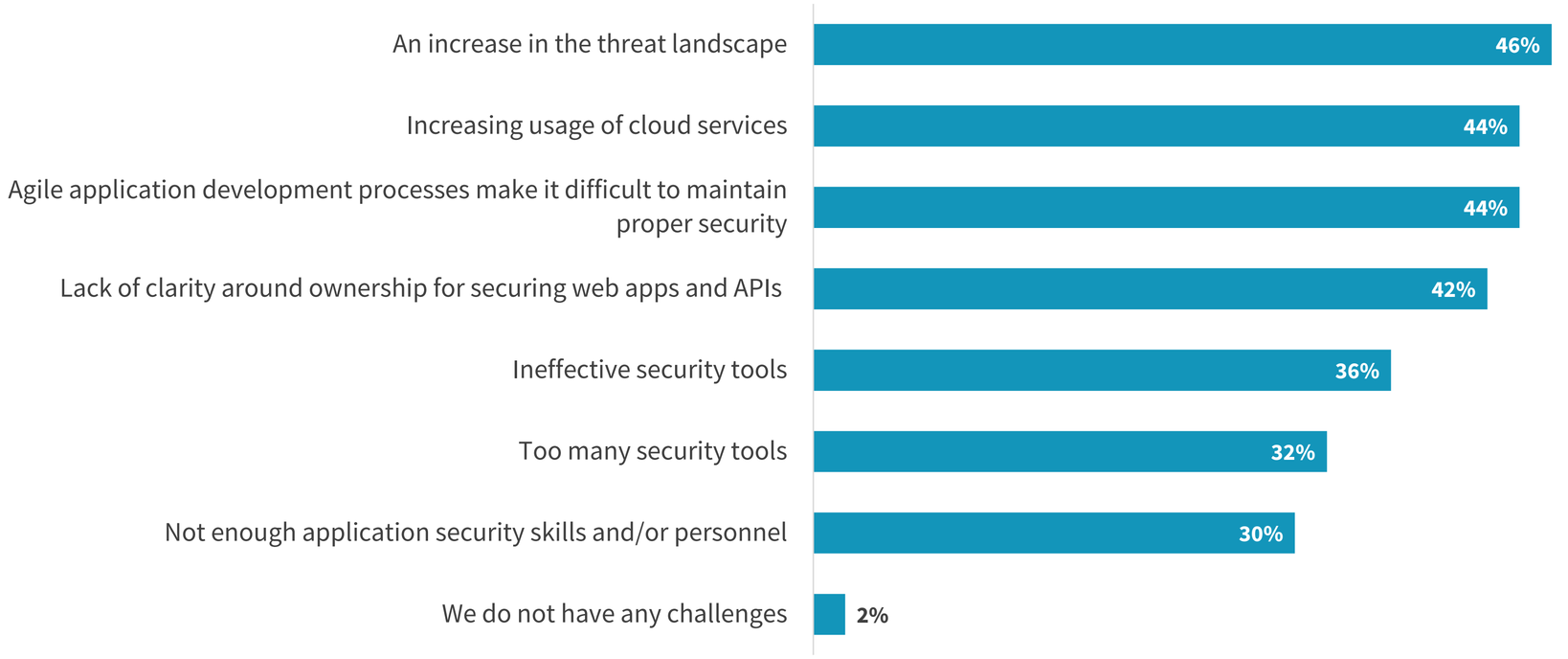
Back to Contents

Threats Are a Commonly Cited Issue, but Only One Among Many

The transitions to cloud, microservices, and DevOps are critical to achieve better agility, scale, and efficiency—but they do create complexity. Overall, 55% of organizations say securing their organization's web applications has become more difficult over the last 2 years. The most common reason was an increase in the threat landscape, cited by 46% of organizations. Yet the increasing use of cloud services (44%), incorporation of agile development processes (44%), and lack of clarity around ownership for security (42%) were close behind. Further, the security tools designed to protect corporate applications can often add complexity. Specifically, 36% say security tools are ineffective, and 32% indicated their organization has too many security tools.

55%
of organizations **say securing their organization's web applications has become more difficult over the last 2 years.**

Challenges faced protecting public-facing web applications.



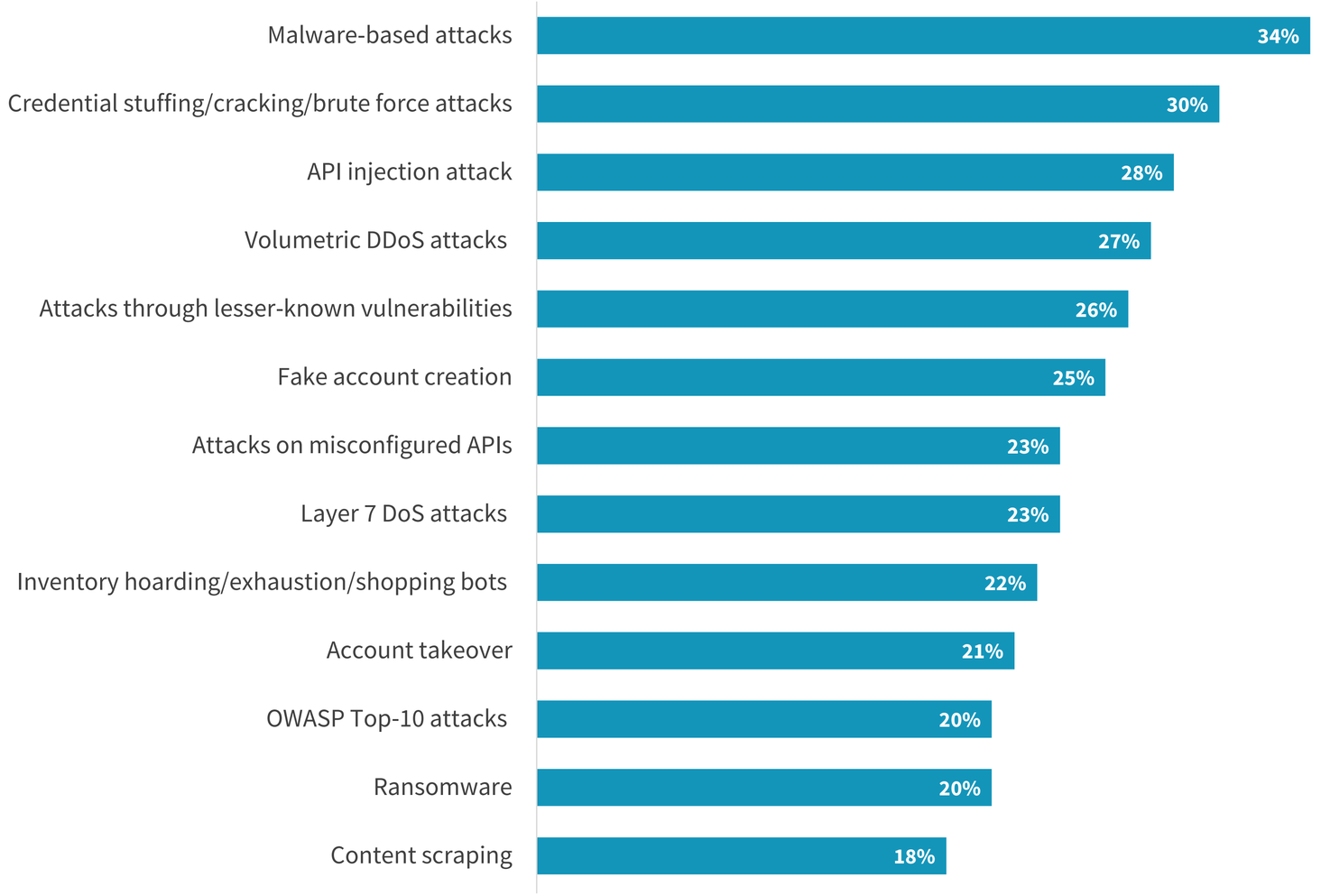
Back to Contents

Successful Application Attacks Can Impact Employees, Customers, and the Bottom Line

Organizations Have Experienced a Variety of Attacks

Attackers have a wide range of avenues with which to target public-facing applications. Traditional application attacks using malware (34%), lesser-known vulnerabilities (26%), and OWASP Top-10 vulnerabilities (20%) were commonly reported. Denial of service attacks also remain a staple for attackers, with 27% reporting volumetric attacks, and 23% seeing Layer 7 attacks. However, credential-based attacks and attacks on APIs are becoming more commonplace. Credential stuffing or cracking attacks (30%), fake account creation (25%), and account takeover (21%) were often reported. On the API side, 28% of organizations reported injection attacks, while 23% reported attacks exploiting misconfigurations. Bots are often the common thread across many of these types of attacks, allowing bad actors to quickly scale denial of service, credential-based, and API attacks and overwhelm defenses.

Types of web application and API attacks experienced in the last 12 months.



Back to Contents

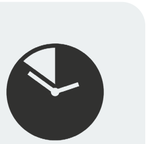
Application Attacks Can Impact Employees, Customers, and the Bottom Line

When successful attacks on public-facing applications and APIs do occur, the impacts can be significant, and many are related. Over 40% of organizations reported application downtime as the result of a web application or API attack. When applications are not available, customers can be impacted. Specifically, 34% reported negative customer experiences and 26% reported lost revenue as the result of application attacks. Further, when data breaches occur as the result of an application attack, brand standing and shareholder value can be affected (34%) and compliance issues can arise (26%). While not ideal or necessarily fair, these results help explain why 41% of respondents indicated that team members were impacted as the result of an application attack. This can include everything from requiring additional training, through reassignment, to termination.

Impacts organizations experienced from attacks on web applications and APIs.

41%

Team members were impacted

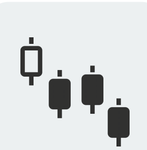


41%

Application downtime

38%

Additional web application protection products or services added



34%

Negative impact to shareholder value or brand standing

34%

Negative customer experiences

33%

Infrastructure cost overruns

26%

Compliance issues

26%

Loss of revenue

Back to Contents

Protecting Web Applications Is a Priority for Most, Though Drivers Vary

Application Security Is a Cybersecurity Priority for Nearly All

Security teams have a variety of initiatives to plan for and support. Implementing zero trust, securing remote and hybrid work, supporting cloud migration, and modernizing threat detection and response are all important in their own right. However, the criticality of applications to the business and long list of negative impacts that can arise when those applications are not available or become compromised have resulted in most organizations elevating application security to one of their top cybersecurity priorities. In fact, one-third say that ensuring secure and available applications is their organization's top cybersecurity priority, with an additional 54% placing it as a top three cybersecurity priority.

> "Implementing zero trust, securing remote and hybrid work, supporting cloud migration, and modernizing threat detection and response **are all important in their own right."**

33%
Ensuring secure and available applications is our organization's **top** cybersecurity priority

54%
Ensuring secure and available applications is a **top three** cybersecurity priority for our organization

Back to Contents

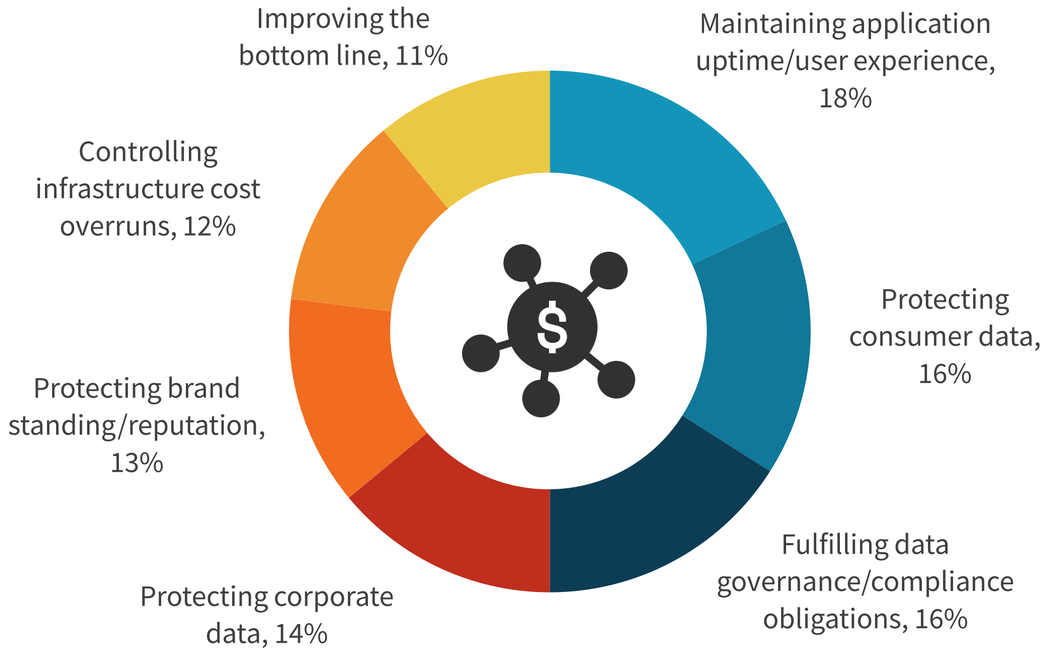
Critical Drivers for Spending on AppSec Vary

More than just paying lip service to prioritizing application security, organizations are allocating increased budget for protecting their web applications and APIs. Nine out of ten organizations anticipate increasing spending on web application and API protection technologies, services, and personnel over the next 12-18 months. While there is consensus on prioritization and increasing spending, there is less agreement on the top driver. Most organizations are focused on traditional security outcomes. The most common response selected was maintaining application uptime and user experience, cited by 18% of respondents. Protecting data, both consumer (16%) and corporate (14%), was also near the top of the list. Spending on application security to fulfill compliance and data governance requirements also continues to be common (16%). Yet some organizations do view application security spending as a business enabler. Controlling infrastructure cost overruns was selected by 12%, while 11% indicated that improving the bottom line was top of mind.

90%

anticipate increasing spending on web application and API protection technologies, services, and personnel over the next 12-18 months.

Most critical driver of spending on web application protection tools and services.



Back to Contents

Tool Sprawl Has Become Problematic

A Variety of Tools and Capabilities Are Used to Protect Web Apps

While it is heartening to see organizations emphasizing application security and increasing spending, these dollars must be spent effectively. Currently, 72% of organizations use web application firewalls, with the vast majority of those using multiple WAFs from some combination of cloud service provider, CDNs, security vendors, and open source. Despite being introduced much more recently, API security tools have become critical for modern, microservices-based environments utilizing APIs. While foundational capabilities such as OWASP Top-10 vulnerability protections (27%) and virtual patching (31%) remain common, many organizations have begun to utilize advanced features such as behavior-based detections (39%), JavaScript challenges (34%), and device fingerprinting (32%).

Discrete tools used to protect web applications.

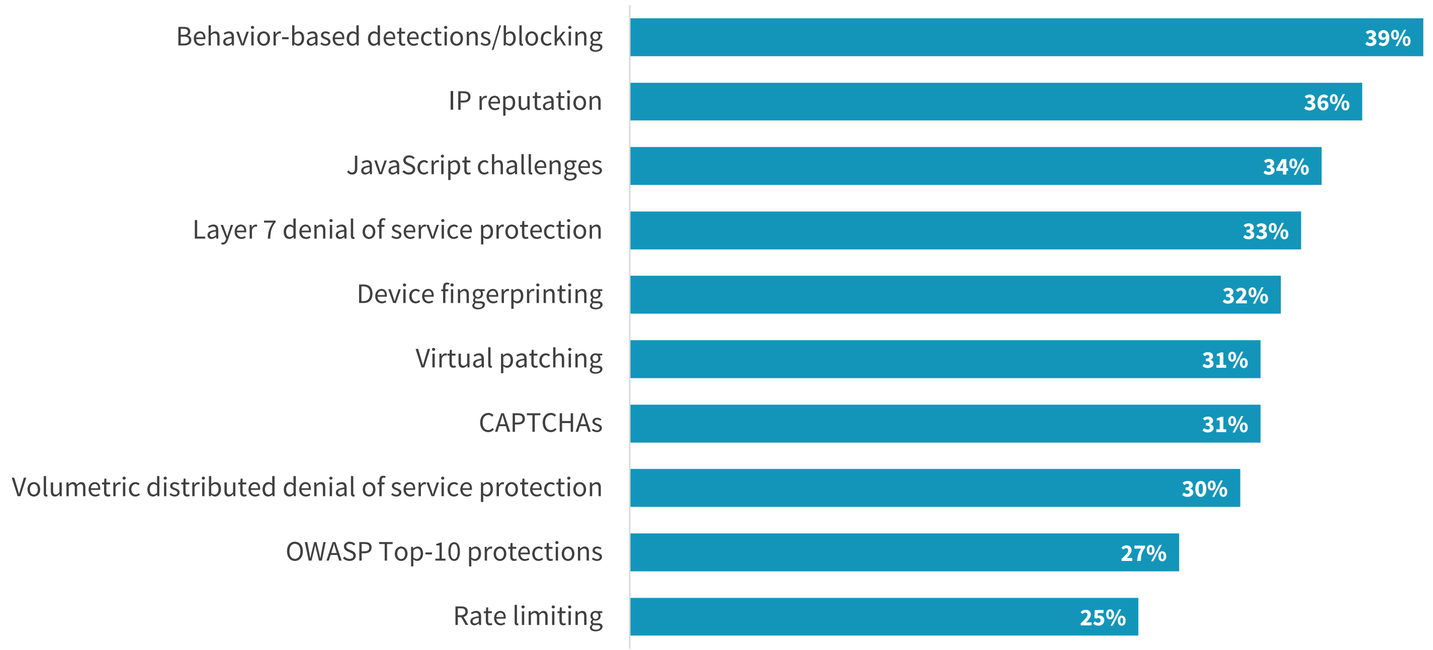
72%
Web application firewall (WAF)

52%
Distributed denial of service mitigation

64%
API security tools

45%
Bot management

Capabilities employed to protect web applications.



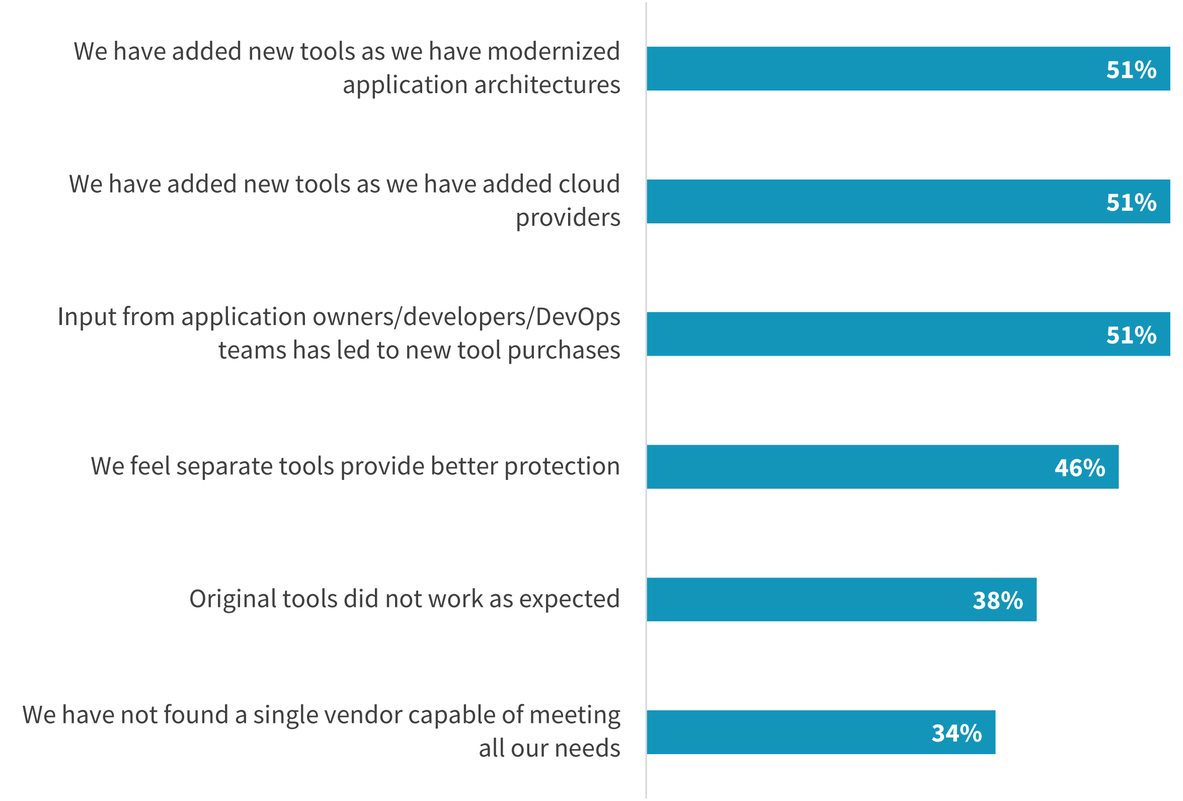
Back to Contents

Tool Sprawl Can Occur Naturally or by Choice

There are a variety of reasons organizations end up with so many application security tools. As applications shift to the cloud and microservices are adopted, it can be natural to incrementally add tools for those specific use cases. Along the same lines, as DevOps has taken hold and security becomes more democratized, it only makes sense for developers to have a voice in tool selection. On the other side of the coin, 46% use multiple tools because they feel it provides better protection. Additionally, 38% added products when their original tools did not work as expected. Yet the challenges tools generally pose can become magnified if sprawl becomes too wide. Cost, alerts and false positives, and management were all mentioned as top challenges and are likely to become worse when multiple tools are deployed.

Web application security tool challenges.

Reasons to use multiple web application protection tools.



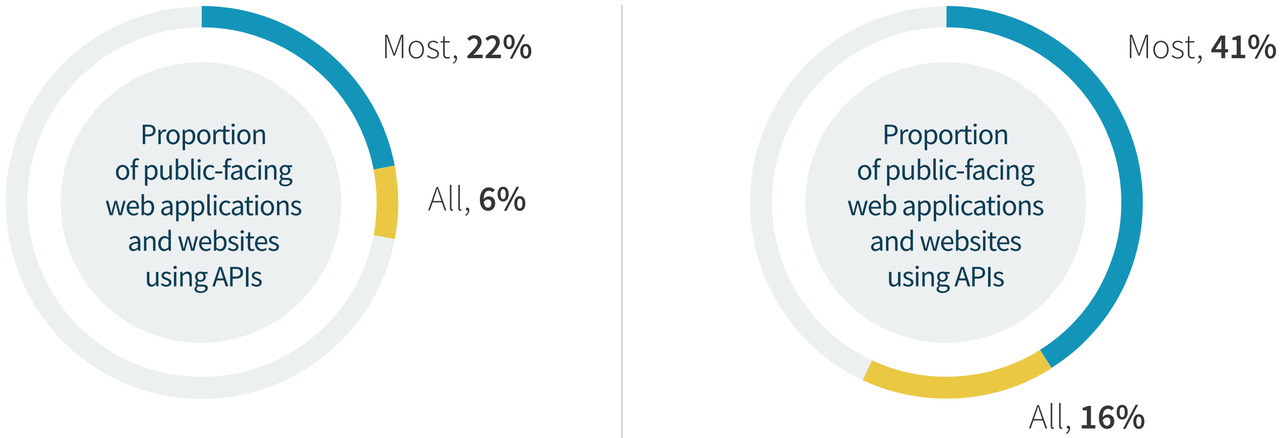
Back to Contents

APIs Are of Particular Concern and Can Exacerbate Tool Sprawl

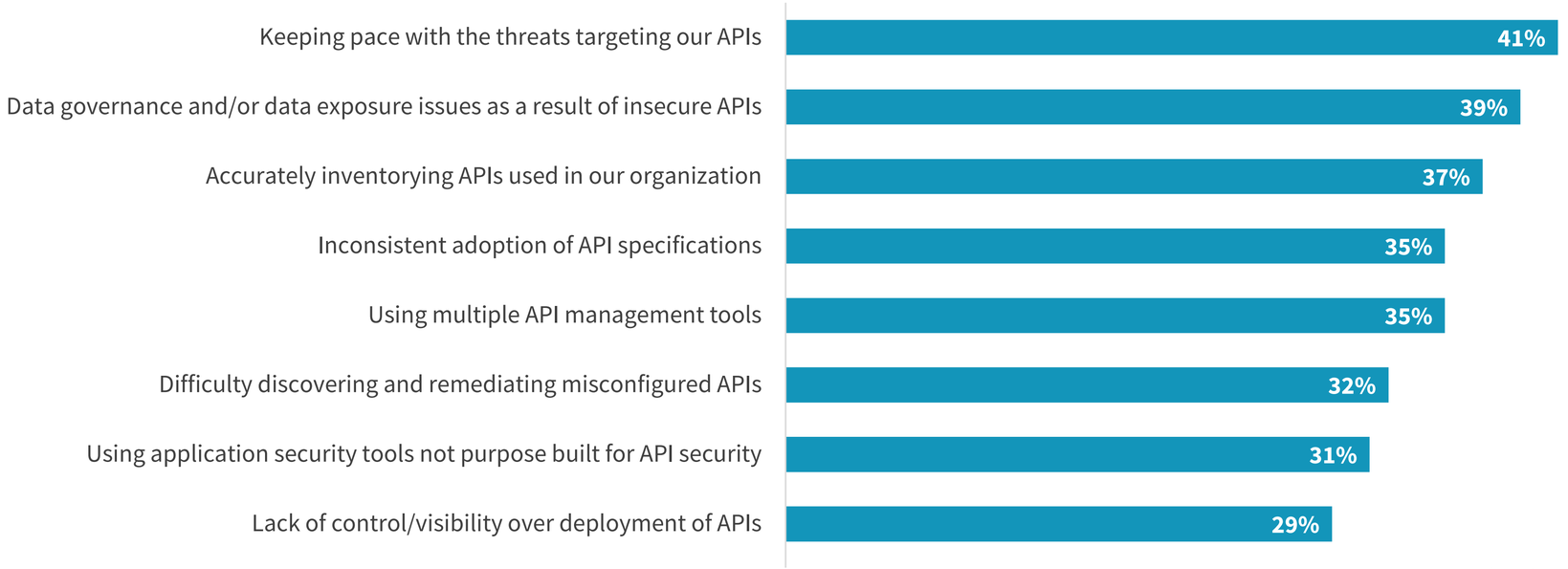
APIs Have Become Ubiquitous, Posing Many Challenges

API usage has grown as applications have become increasingly interconnected and the use of microservices-based architectures has expanded. In fact, only 4% of organizations currently say they have no applications that rely on APIs. However, the scale of applications dependent upon APIs is poised to grow significantly. Within two years, more than half (57%) of organizations believe that most or all of their applications will use APIs. Yet this shift can pose challenges when not properly addressed. Attackers have come to see APIs as attractive, often inadequately defended, targets and focus their attention accordingly. Further, as the scale of APIs in use across an organization increases, visibility can become a problem. More than one-third (37%) cited challenges with inventorying APIs, while 32% cited issues discovering and remediating misconfigurations. Finally, inadequate tooling comes into play again, both due to the use of too many tools (35%) and use of tools not purpose built for API security (31%).

API usage trends.



Biggest challenges protecting APIs.



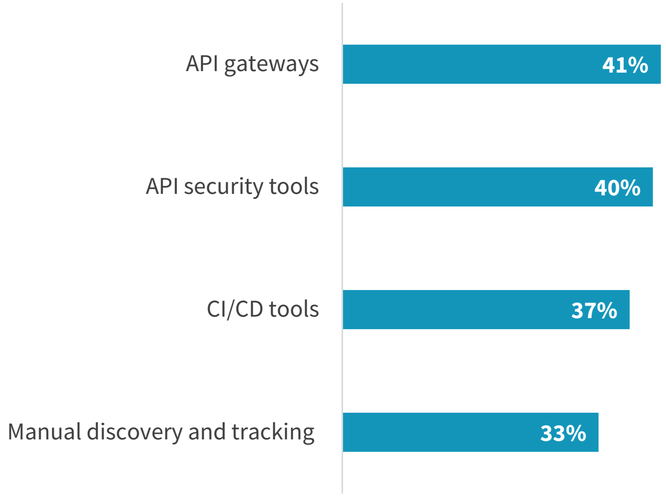
Back to Contents

Key Gaps Remain Across the API Security Lifecycle

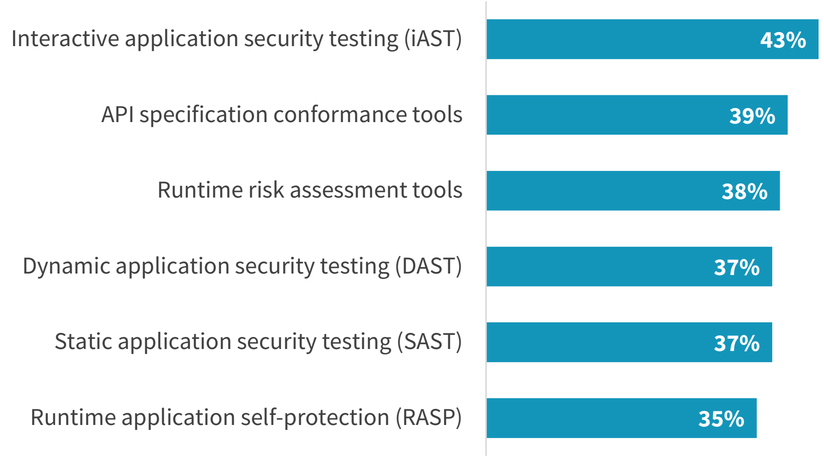
As noted, the range of tools used to discover, manage, configure, and protect APIs is long. When it comes specifically to protecting APIs, some organizations attempt to apply network security tool such as IPS or next-generation firewalls, or general application security tools such as WAF or bot mitigation. While these tools may be successful in preventing some basic types of attacks, they typically lack the visibility necessary to track the APIs in use across an entire environment, assess whether APIs are properly configured, and detect stealthy anomalous activity. While 44% of organizations indicated that API security tools were completely effective for protection, the fact that more than one-third found IPS, NGFW, bot mitigation, and WAF completely effective indicates that there remains confusion in the market.

Percentage of organizations that believe their API protection tools are *completely effective:*

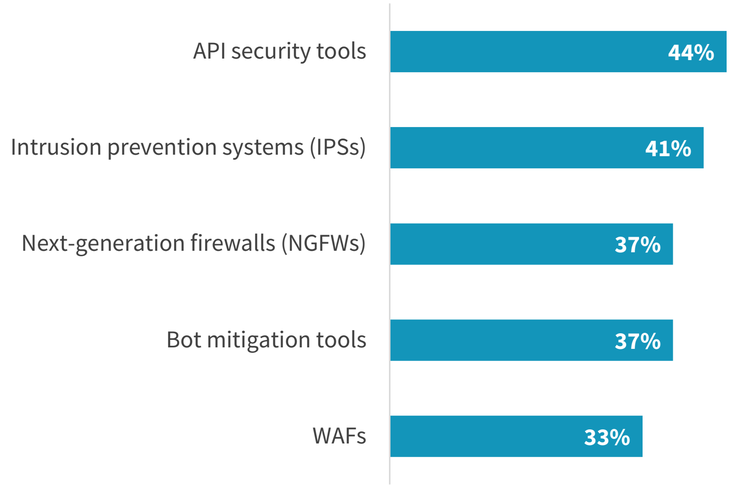
Tools to discover and track APIs.



Tools to discover and remediate API coding errors.



Tools to stop or block API attacks.



Back to Contents

There Is Significant Interest in Consolidation, with API Security as a Focus

Strong Interest in Consolidation, but WAAP Deployment Will Be Phased

Due to the use of many different tools, cross-vector attacks, etc., interest in converged web application and API protection (WAAP) platforms has increased. Three-quarters of respondents indicated they are actively deploying a WAAP platform or planning to deploy one in the next 12-24 months. While 40% believe they will deploy WAAP across all their applications, the majority (54%) will continue to use a mix of tools depending on the application in question. Yet that does not mean WAAP is seen as a secondary control. In fact, more organizations plan to use WAAP for business-critical applications (37%) than secondary applications (32%). The most common usage, at least to start, is expected to be for applications reliant on APIs (42%) and resident in the cloud (40%).

Three-quarters

of respondents indicated they are actively deploying a WAAP platform or planning to deploy one in the next 12-24 months.

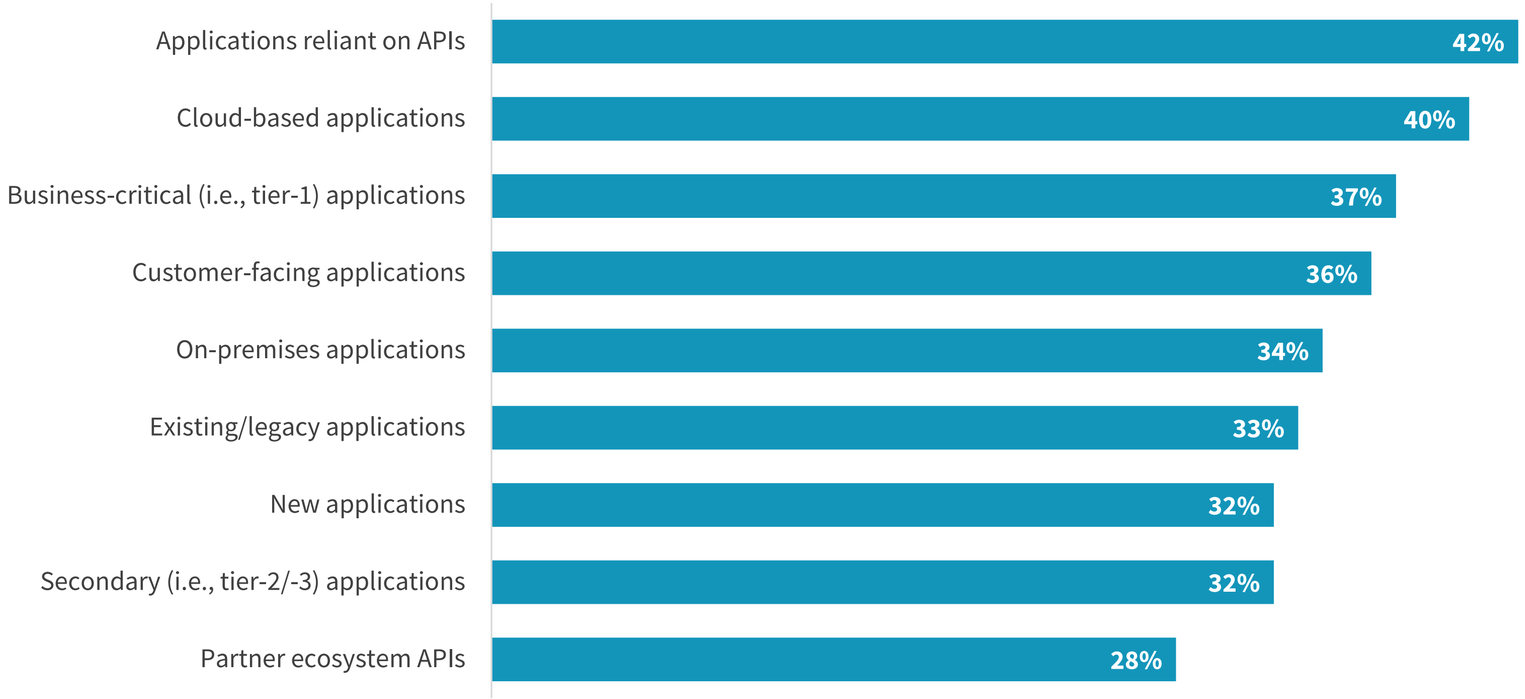
Extent of WAAP deployment.

40%
have deployed/ will deploy for most apps and APIs.

54%
have deployed/will deploy for some apps and APIs; standalone tools for others.

4%
have deployed/will deploy for a few apps and APIs; standalone tools for most.

Types of applications and APIs expected to be protected by a WAAP platform.



Back to Contents

API Security and Deployment Flexibility Are Critical

This brings about the question: What characteristics should WAAP platforms have? As one might expect based on the previous findings, API security tops the list of most important tools in a WAAP platform, cited by 40% of respondents. While WAF, DDoS, and bot management were called out less frequently, these capabilities obviously remain a key component of WAAP. However, the explosion of APIs means discovery and protection capabilities must be purpose built rather than an afterthought. Interestingly, respondents were split on the ideal form factor for WAAP. While 35% prefer WAAP to be delivered as a cloud service, 32% desire a module-based approach, and 26% remain drawn to a traditional appliance model. The need to protect legacy applications will continue for some time, ultimately requiring a flexible approach to WAAP.

Most important tools in a WAAP platform.

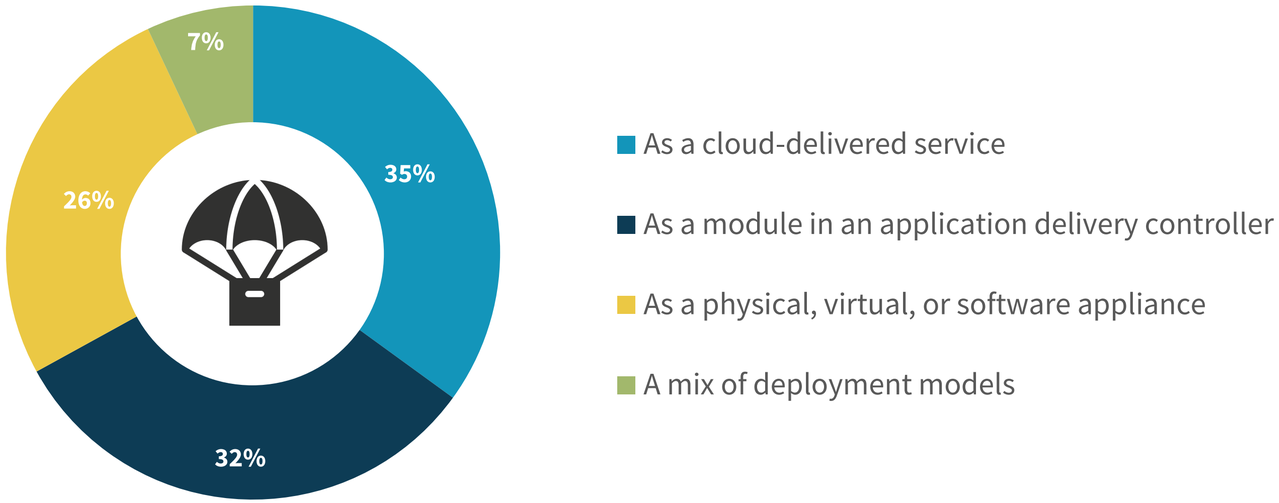
40%
API security

26%
WAF

17%
DDoS mitigation

17%
Bot management

WAAP platform deployment preference.



Back to Contents

Qualys®

Qualys is a Leading Provider of Cloud Cybersecurity, Compliance & IT Solutions

Qualys, Inc. is a pioneer and leading provider of disruptive cloud-based cybersecurity, compliance, and IT solutions. Qualys helps enterprises large and small to streamline and automate their IT security and compliance programs on a single cloud platform for cyber resiliency, better business outcomes, and substantial cost savings. Qualys Web Application Security (WAS) solution gives organizations the ease of use, centralized management, and integration capabilities to keep attackers at bay and their web applications secure.

LEARN MORE

ABOUT ESG

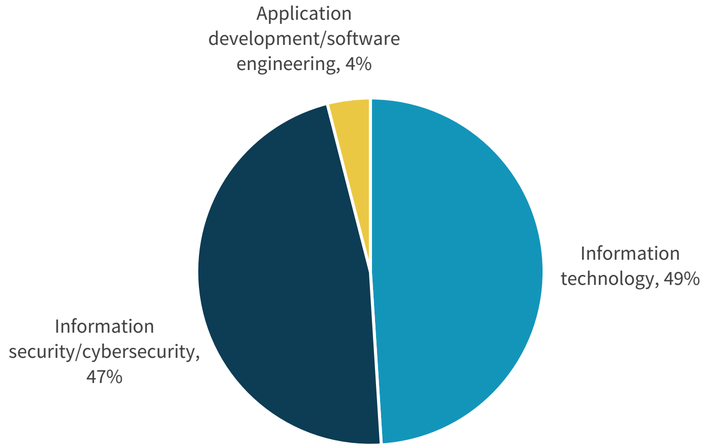
Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

Research Methodology

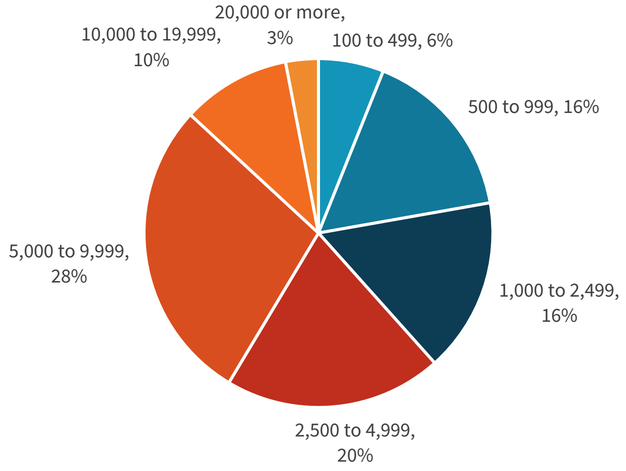
To gather data for this report, ESG conducted a comprehensive online survey of IT, cybersecurity, and application development professionals from private- and public-sector organizations in North America between February 18, 2022 and February 28, 2022. To qualify for this survey, respondents were required to be IT, cybersecurity, and application development professionals familiar with their organization's cybersecurity environment and web application protection tools, processes, and strategies. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 366 cybersecurity and application development professionals.

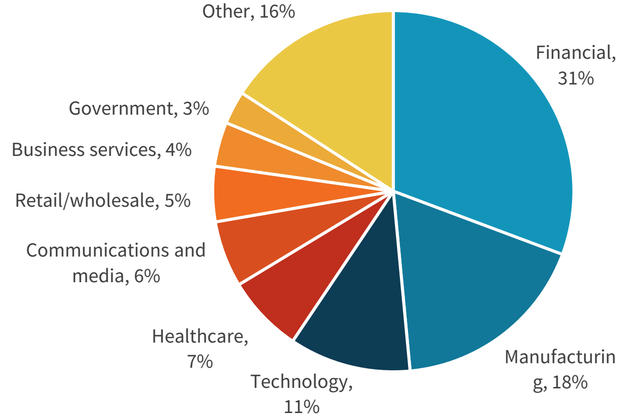
RESPONDENTS BY JOB FUNCTION



RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY INDUSTRY



Back to Contents

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.