Enterprise Strategy Group | Getting to the bigger truth.™

ESG RESEARCH REPORT

Trends in Modern Application Protection

Tool Sprawl and API Proliferation Drive WAAP Interest

By John Grady, Senior Analyst; Bill Lundell, Director of Syndicated Research; and Josh Clark, Senior Research Associate

July 2022

Contents

List of Figures

Executive Summary

Report Conclusions

ESG conducted an in-depth survey of 366 IT, cybersecurity, and application development professionals personally involved with web application protection technology and processes at large midmarket (100 to 999 employees) and enterprise (1,000 or more employees) organizations in North America (US and Canada).

Based upon the data gathered as part of this project, the report illustrates:

- Application environments and processes continue to evolve, creating security complexity. Few organizations support more than 200 public-facing websites and applications, but around half expect to reach this milestone in the next two years. The percentage of organizations running more than 30% of their apps on IaaS is expected to nearly double over the next two years. More than half say securing their organization's web applications has become more difficult over the last two years, most commonly due to an increase in the threat landscape and the increasing usage of cloud services.

- Successful application attacks can impact employees, customers, and the bottom line. Malware-based attacks, credential stuffing/cracking/brute force attacks, and API injection attacks are the most commonly experienced web application and API attacks over the last 12 months. These attacks caused team members to be impacted, application downtime, additional web application protection products or services to be added, and negative impacts to shareholder value and brand standing.

- Protecting web applications is a priority for most, though drivers vary. Most say ensuring secure and available applications is a top three cybersecurity priority. Nearly all organizations anticipate increasing spending on web application and API protection technologies, services, and personnel over the next 12-18 months. The most commonly cited driver of spending on web application protection tools and services is maintaining application uptime/user experience.

- Tool sprawl has become problematic. Most organizations currently use web application firewalls, with the majority of those using multiple WAFs from some combination of cloud service provider, CDNs, security vendors, and open source. Many organizations use multiple web applications tools because they added new tools as they modernized application architectures and cloud providers, and input from application owners/DevOps teams has led to new tool purchases. The top challenges organizations face with the tools they use to protect their web applications are high cost, high alert volume, and difficulty managing the environment.

- APIs are of particular concern and can exacerbate tool sprawl. The biggest challenges organizations face with protecting their APIs are keeping pace with the threats targeting their APIs and data governance or data exposure issues as a result of insecure APIs. Gateways and security tools are rated most effective in discovering and tracking organizations' APIs, while API security tools and intrusion prevention systems are rated most effective in stopping or blocking attacks on APIs.

- There is significant interest in consolidation, with API security as a focus. Three-quarters are actively deploying a WAAP platform or planning to deploy one in the next 12-24 months. The majority have deployed or will deploy WAAP for some of their applications and APIs, and more organizations plan to use WAAP for business-critical applications than secondary applications. API security tops the list of most important tools in a WAAP platform, and the plurality of organizations prefer to deploy their WAAP platform as a cloud-delivered service.

Introduction

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 answer the following questions:

- How many public-facing web applications and websites do organizations support? What percentage run on public cloud infrastructure today, and how is this expected to change over the next 24 months?
- What percentage of organizations' public-facing web applications are based on microservices today, and how is this expected to change over the next 24 months? To what extent do organizations plan to incorporate security processes and controls via DevOps processes?
- How do organizations view web application protection? What challenges do organizations face with protecting their public-facing web applications?
- What kind of web applications and API attacks have organizations experienced in the last year? What impacts do organizations experience from the attacks?
- Is ensuring secure and available applications among the top cybersecurity priorities for organizations? Will organizations increase spending on web application and API protection technologies, services, and personnel? What are the critical drivers of spending?
- Which discrete tools and capabilities do organizations use to protect web applications? Why do organizations use multiple web application protection tools? What challenges do organizations face with the tools they use to protect applications?
- What proportion of organizations' public-facing web applications and websites use APIs today, and how is this expected to change over the next 24 months? What are the biggest challenges with protecting APIs?
- What are organizations' plans regarding WAAP? To what extent have they deployed WAAP? What types of applications and APIs do organizations anticipate would use a WAAP platform? Which tools are the most important in a WAAP platform? How would organizations prefer to deploy a WAAP platform?

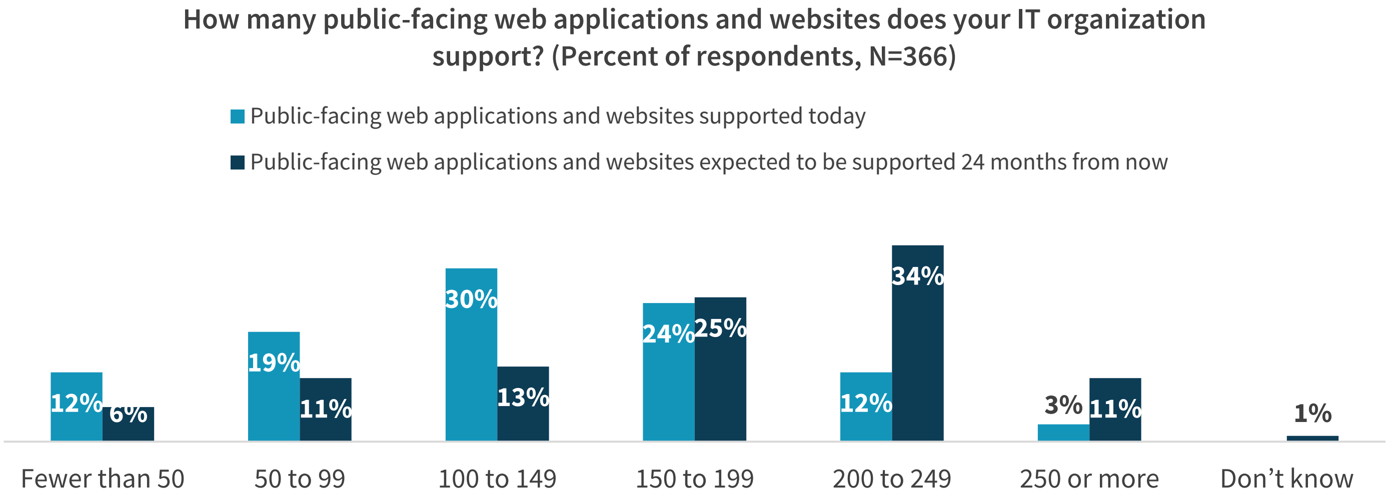
Survey participants represented a wide range of industries including manufacturing, technology, financial services, and retail/wholesale. For more details, please see the *Research Methodology* and *Respondent Demographics* sections of this report.

Research Findings

Application Environments and Processes Continue to Evolve, Creating Security Complexity

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 (see Figure 1).

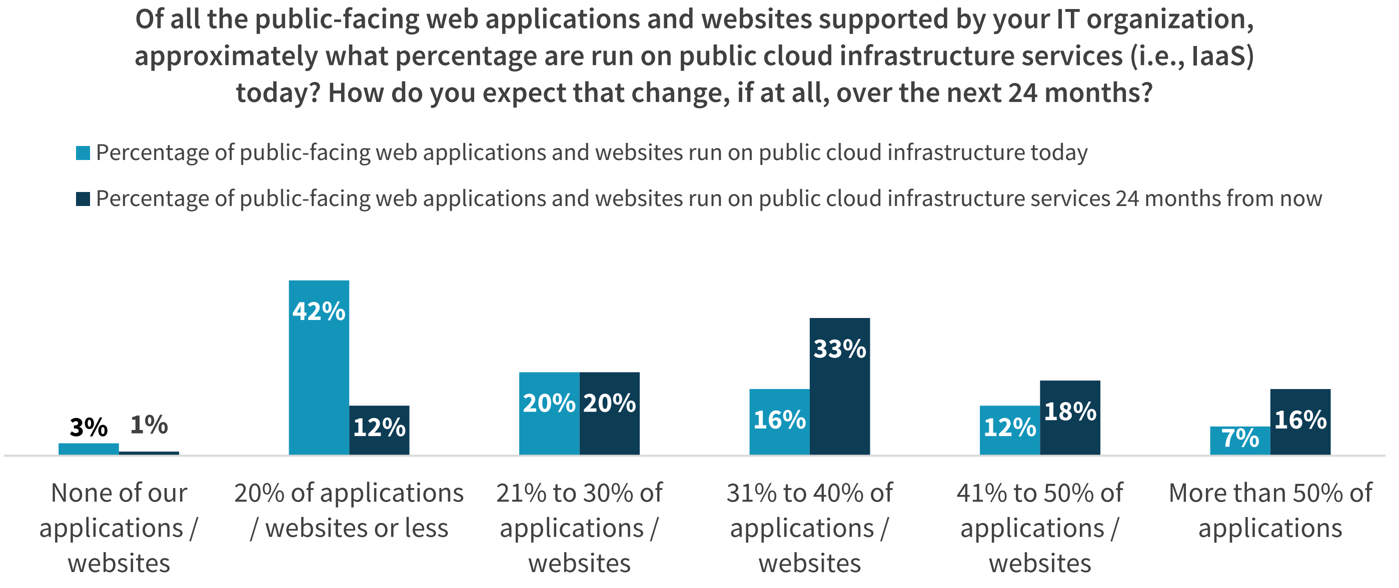
Figure 1. Number of Public-facing Web Applications and Websites Supported by Organization



Source: ESG, a division of TechTarget, Inc.

As the scale of 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 IaaS expected to nearly double over the next two years (see Figure 2).

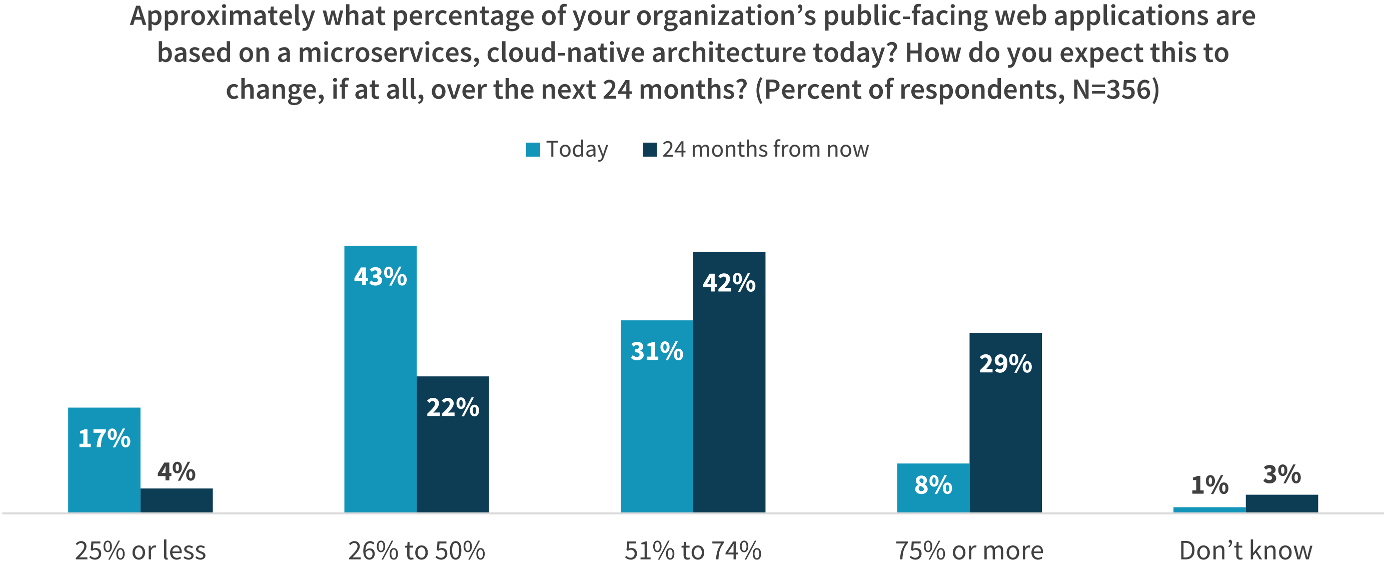
Figure 2. Percentage of Public-facing Web Applications and Websites Run on Public Cloud Infrastructure



Source: ESG, a division of TechTarget, Inc.

Even more telling, 71% expect at least half of their applications to run on microservices (see Figure 3).

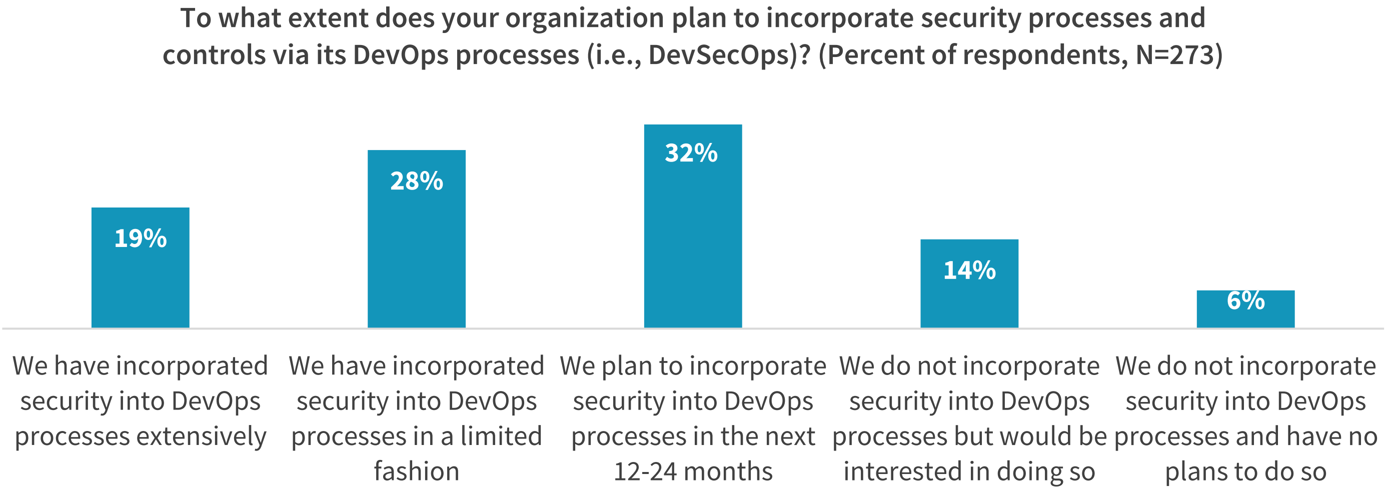
Figure 3. Percentage of Public-facing Web Applications Based on a Microservices, Cloud-native Architecture



Source: ESG, a division of TechTarget, Inc.

To support the shift to IaaS, and more importantly cloud-native, microservices-based architectures, many organizations have turned to agile development methodologies. As shown in Figure 4, 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.

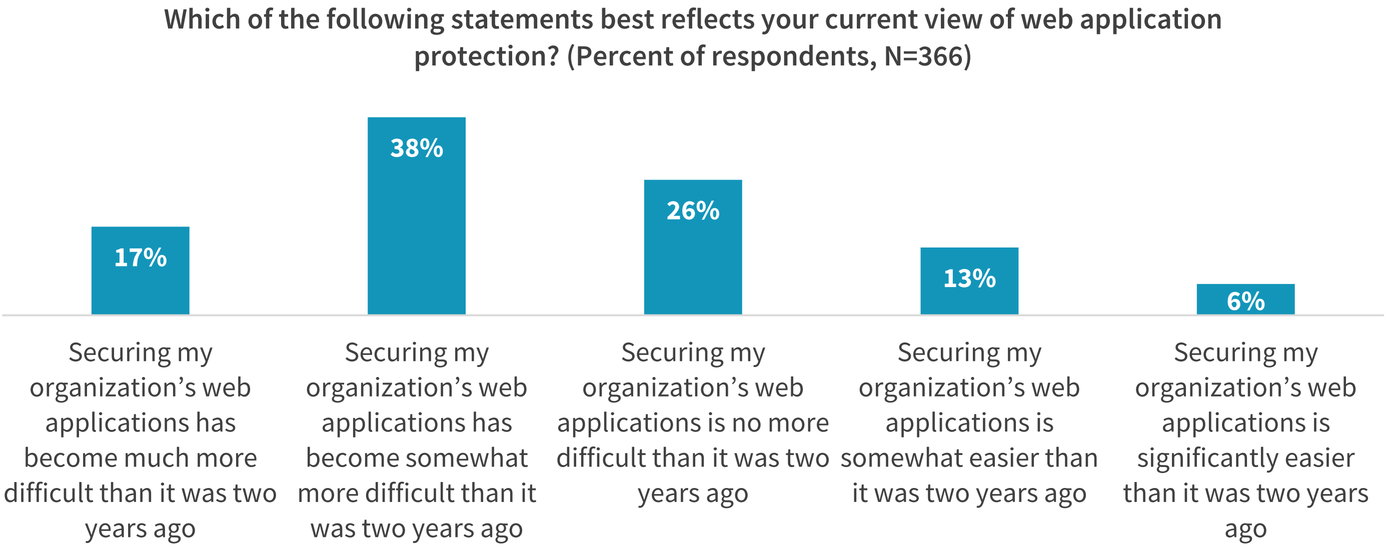
Figure 4. DevOps Has Become Pervasive, but Incorporating Security Remains a Work in Progress



Source: ESG, a division of TechTarget, Inc.

The transitions to cloud, microservices, and DevOps are critical to achieving better agility, scale, and efficiency—but they do create complexity. Overall, according to Figure 5, 55% of organizations say securing their organization's web applications has become more difficult over the last two years. The most common reason was an increase in the threat landscape, cited by 46% of organizations (see Figure 6). 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.

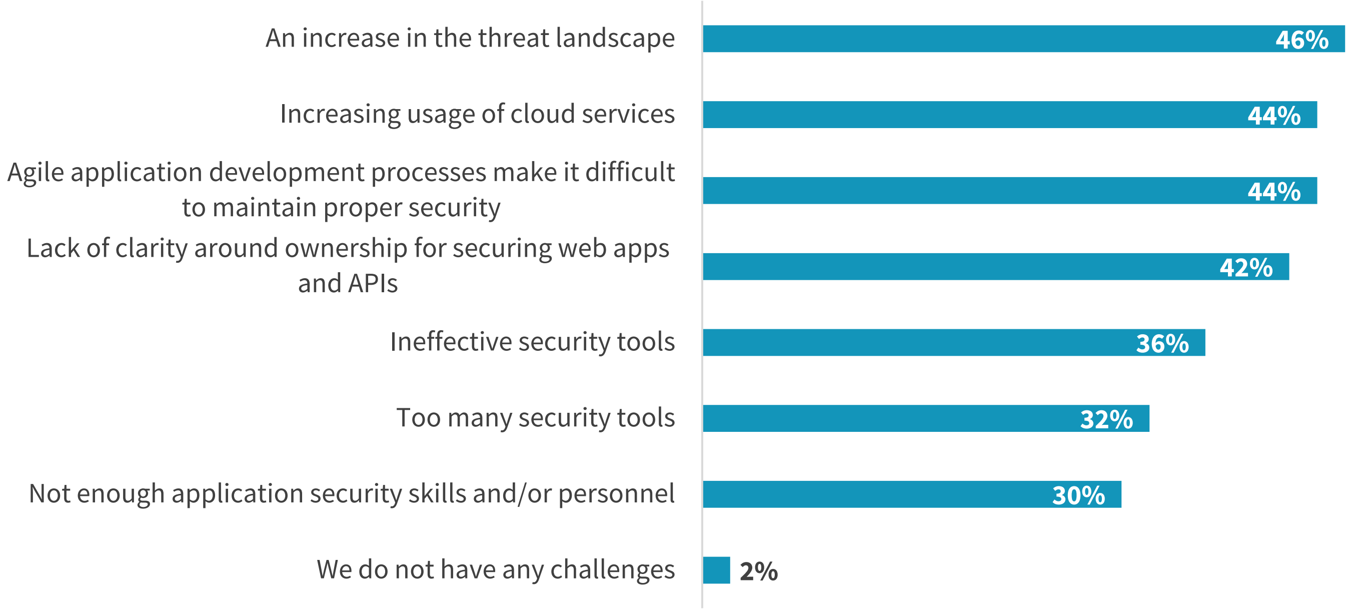
Figure 5. Majority of Organizations Say Securing Web Applications Has Become More Difficult Over the Last Two Years



Source: ESG, a division of TechTarget, Inc.

Figure 6. Threats Are a Commonly Cited Issue, but Only One Among Many

Which of the following challenges does your organization face with protecting its public-facing web applications? (Percent of respondents, N=366, multiple responses accepted)



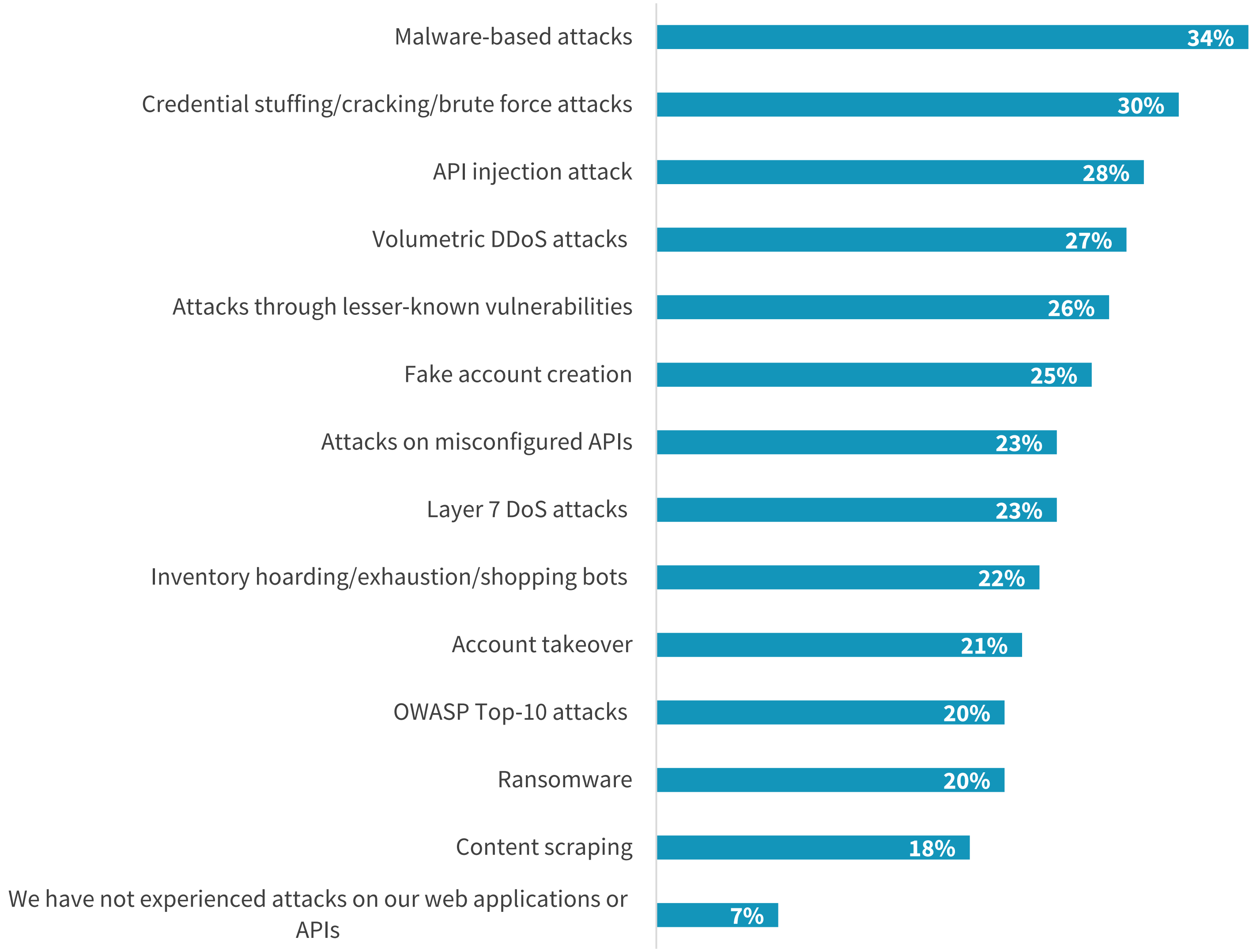
Source: ESG, a division of TechTarget, Inc.

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

Attackers have a wide range of avenues with which to target public-facing applications, as shown in Figure 7. 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 common. Credential stuffing or cracking attacks (30%), fake account creation (25%), and account takeovers (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.

Figure 7. Organizations Have Experiences a Variety of Attacks

Which of the following types of web application and API attacks has your organization experienced over the last 12 months? (Percent of respondents, N=366, multiple responses accepted)

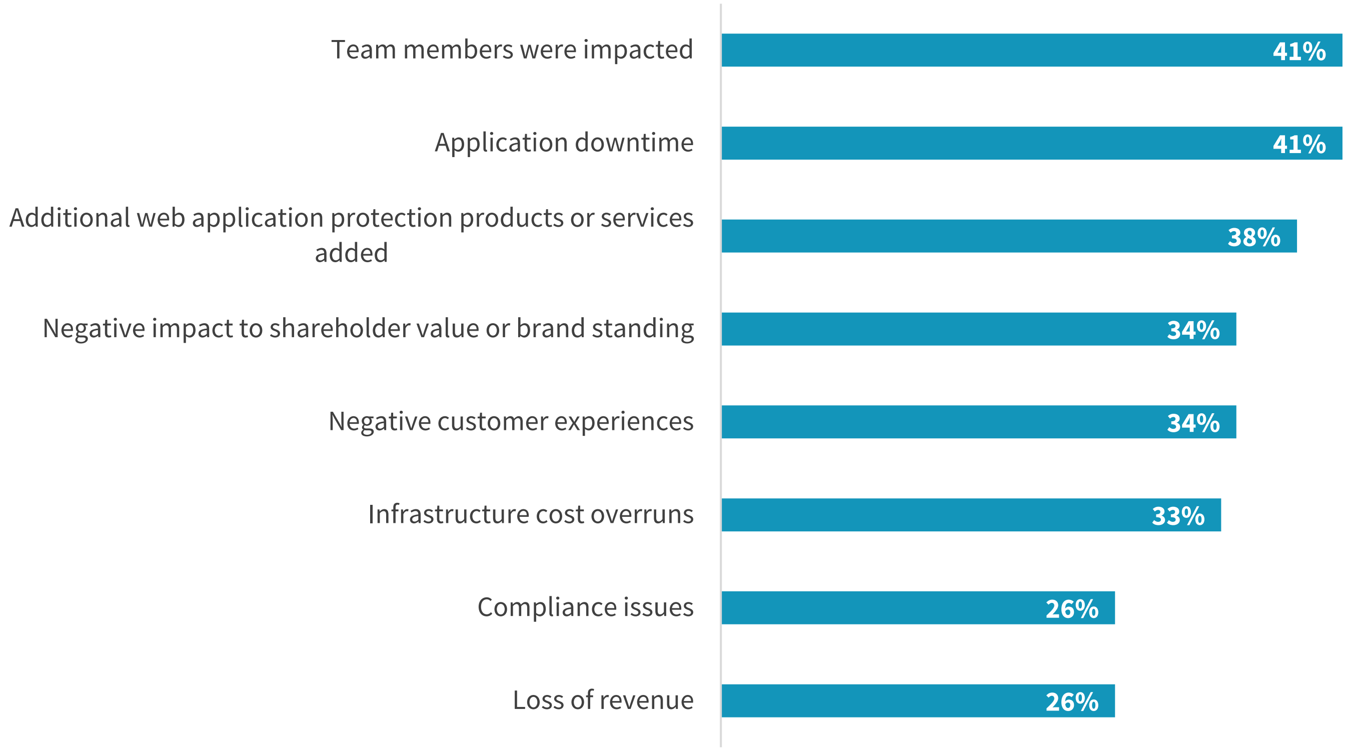


Source: ESG, a division of TechTarget, Inc.

When successful attacks on public-facing applications and APIs do occur, the impacts can be significant, and many are related. As shown in Figure 8, 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 reputation 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.

Figure 8. Application Attacks Can Impact Employees, Customers, and the Bottom Line

What types of impacts did your organization experience from attacks on its web applications and APIs? (Percent of respondents, N=340, multiple responses accepted)

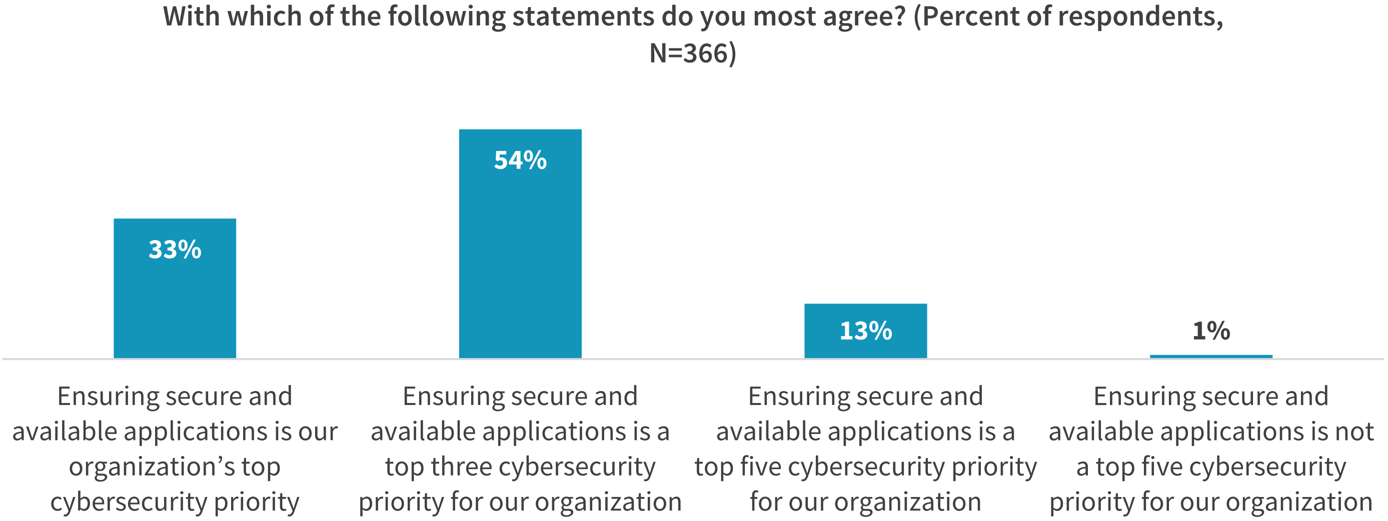


Source: ESG, a division of TechTarget, Inc.

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

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 (see Figure 9).

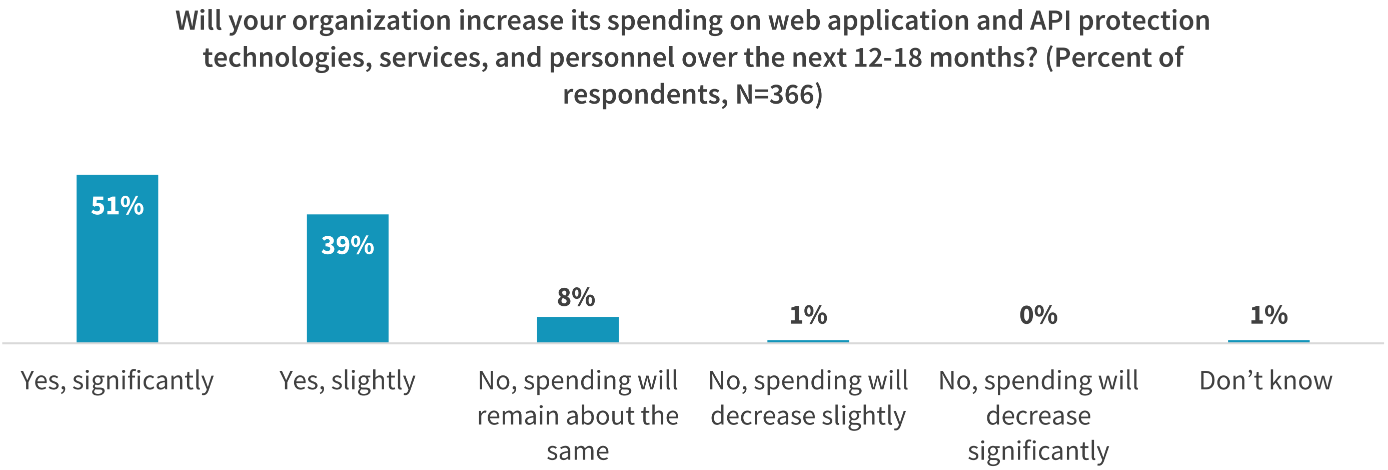
Figure 9. Application Security Is a Cybersecurity Priority for Nearly All



Source: ESG, a division of TechTarget, Inc.

More than just paying lip service to prioritizing application security, organizations are allocating increased budget for protecting their web applications and APIs. According to Figure 10, 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 (see Figure 11). 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.

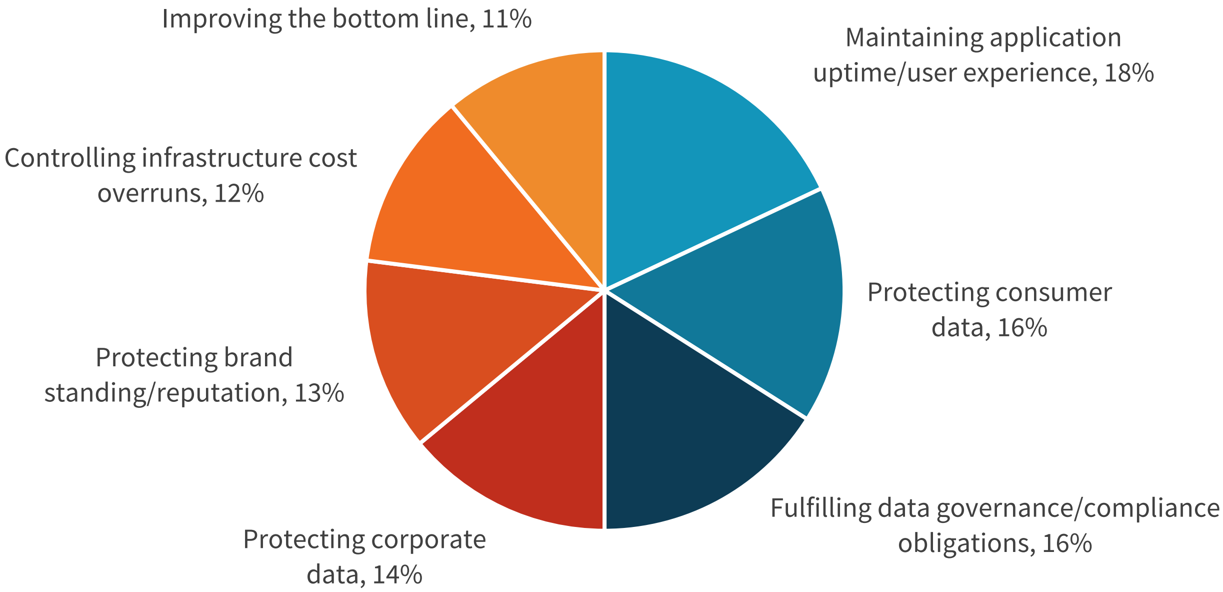
Figure 10. 90% Anticipate Increasing Spending on Web Application and API Protection Technologies, Services, and Personnel Over the Next 12-18 Months



Source: ESG, a division of TechTarget, Inc.

Figure 11. Critical Drivers for Spending on AppSec Vary

Which of the following is the most critical driver of your organization's spending on web application protection tools and services? (Percent of respondents, N=366)



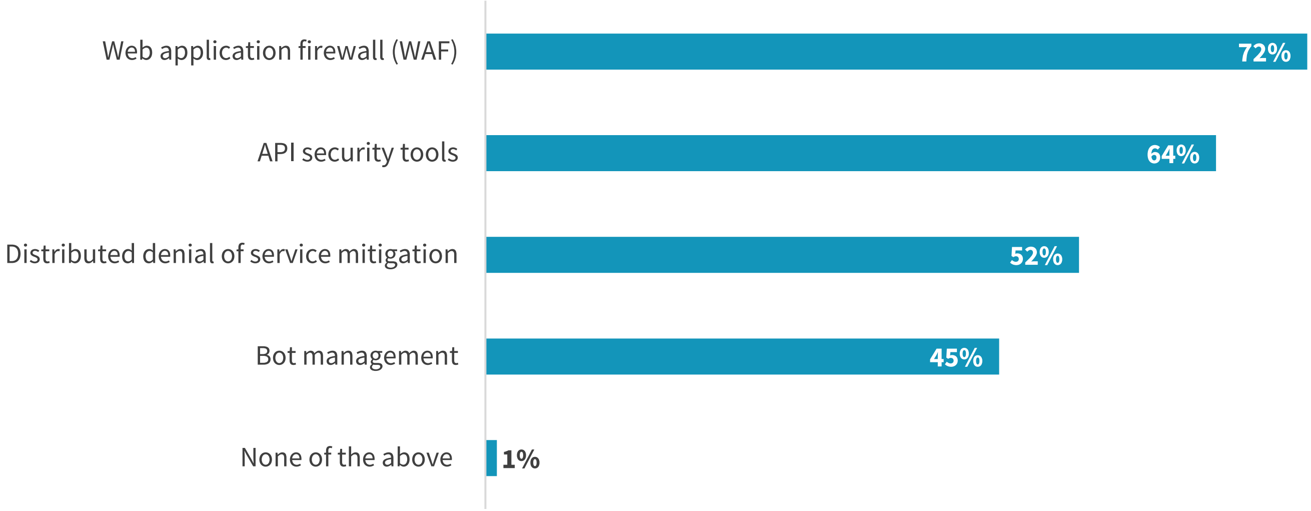
Source: ESG, a division of TechTarget, Inc.

Tool Sprawl Has Become Problematic

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 (see Figure 12).

Figure 12. A Variety of Tools Are Used to Protect Web Apps

Which of the following discrete tools does your organization currently use to protect its web applications? (Percent of respondents, N=366, multiple responses accepted)

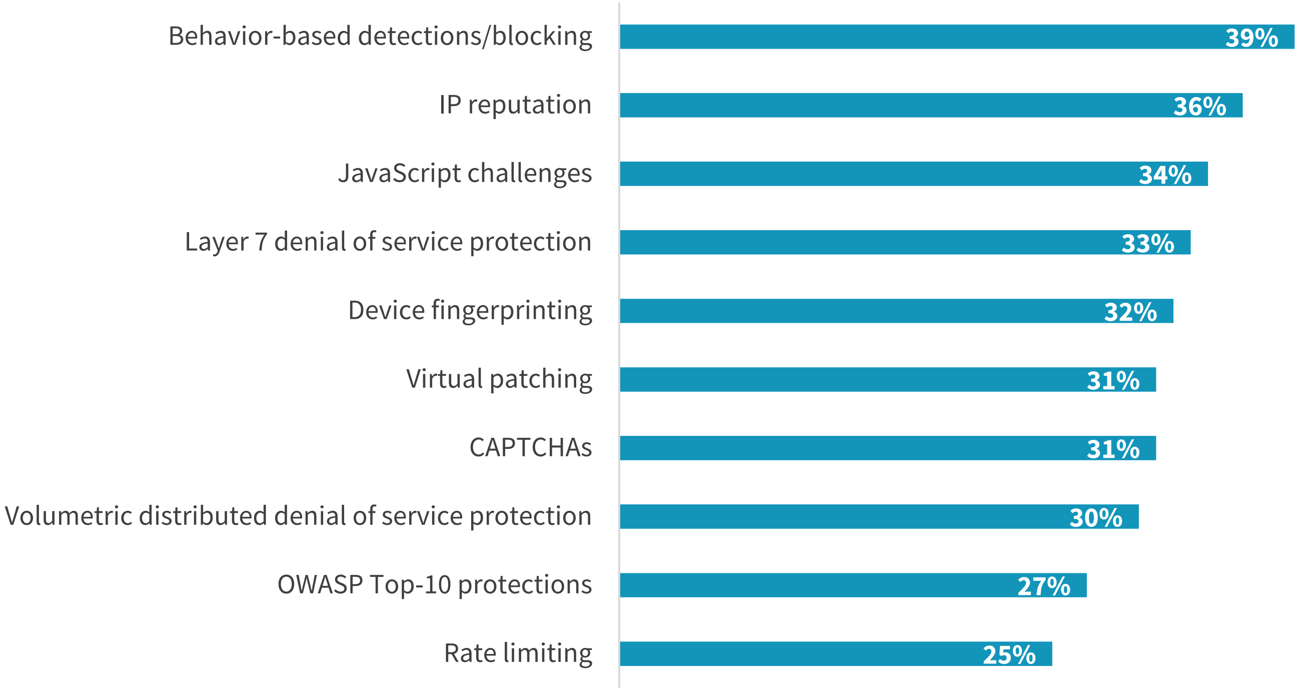


Source: ESG, a division of TechTarget, Inc.

Despite being introduced much more recently, API security tools have become critical for modern, microservices-based environments utilizing APIs. As shown in Figure 13, 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%).

Figure 13. A Variety of Capabilities Are Used to Protect Web Apps

Which of the following capabilities does your organization currently employ to protect its web applications? (Percent of respondents, N=366, multiple responses accepted)

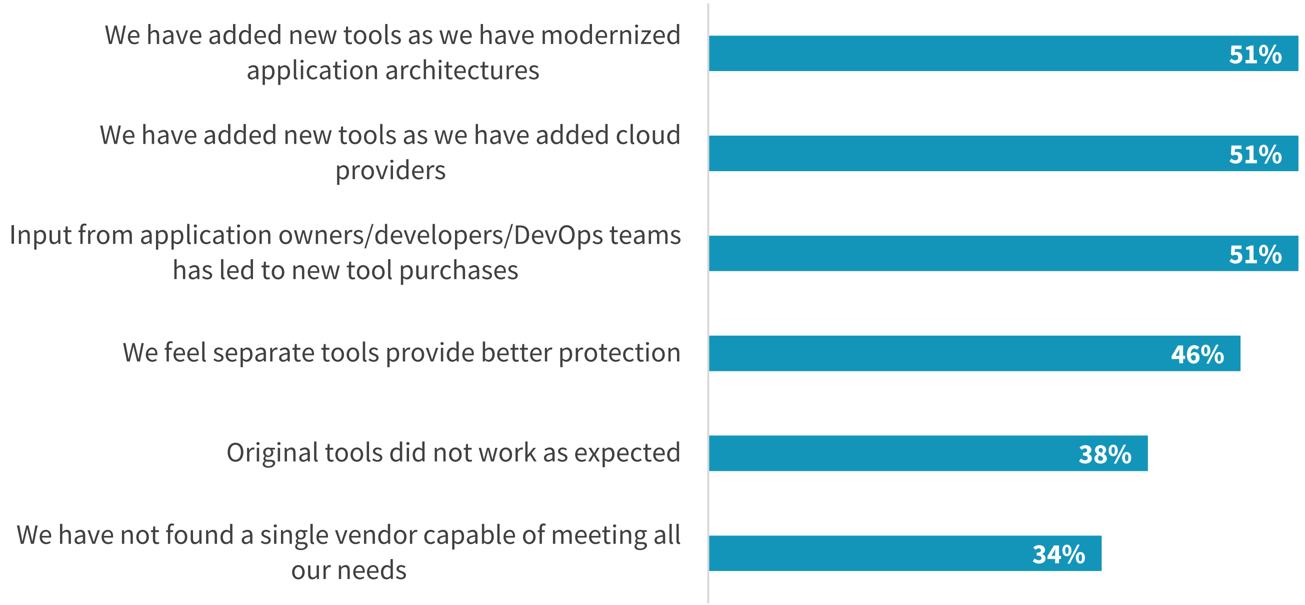


Source: ESG, a division of TechTarget, Inc.

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 (see Figure 14). 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 (see Figure 15).

Figure 14. Reasons to Use Multiple Web Application Protection Tools

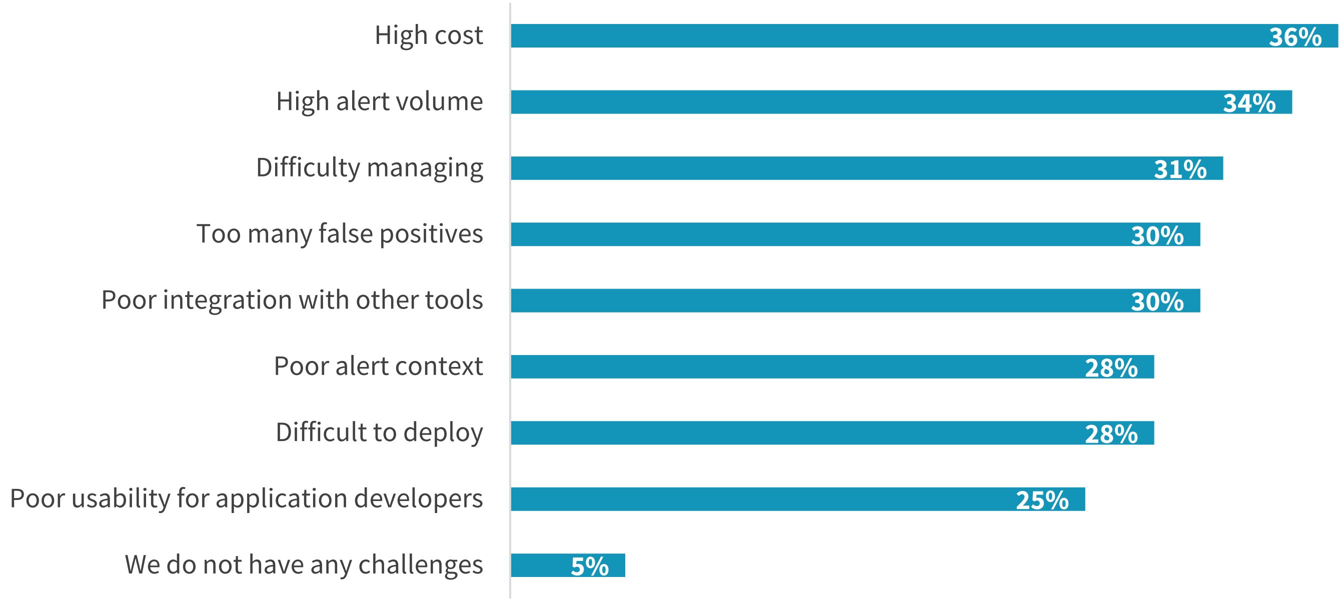
You indicated your organization uses multiple web application protection tools. Which of the following reasons best describes why? (Percent of respondents, N=213, multiple responses accepted)



Source: ESG, a division of TechTarget, Inc.

Figure 15. Web Application Security Tool Challenges

Which of the following challenges does your organization face with the tools it uses to protect its web applications? (Percent of respondents, N=366, multiple responses accepted)

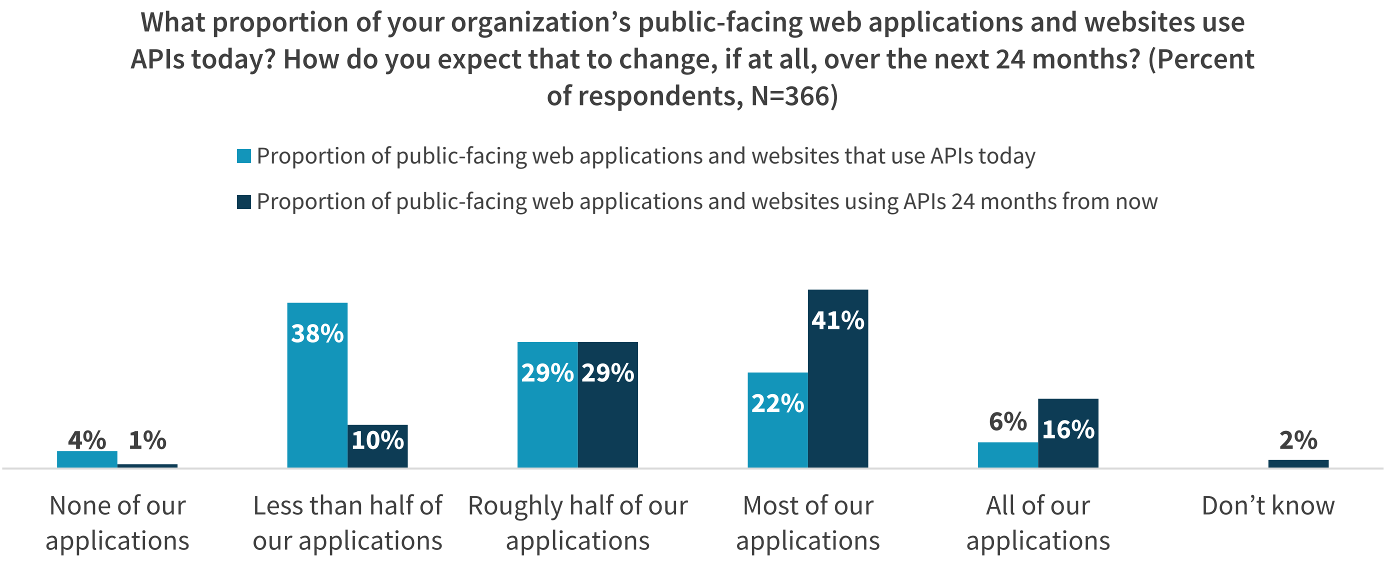


Source: ESG, a division of TechTarget, Inc.

APIs Are of Particular Concern and Can Exacerbate Tool Sprawl

API usage has grown as applications have become increasingly interconnected and the use of microservices-based architectures has expanded. In fact, according to Figure 16, 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.

Figure 16. API Usage Trends

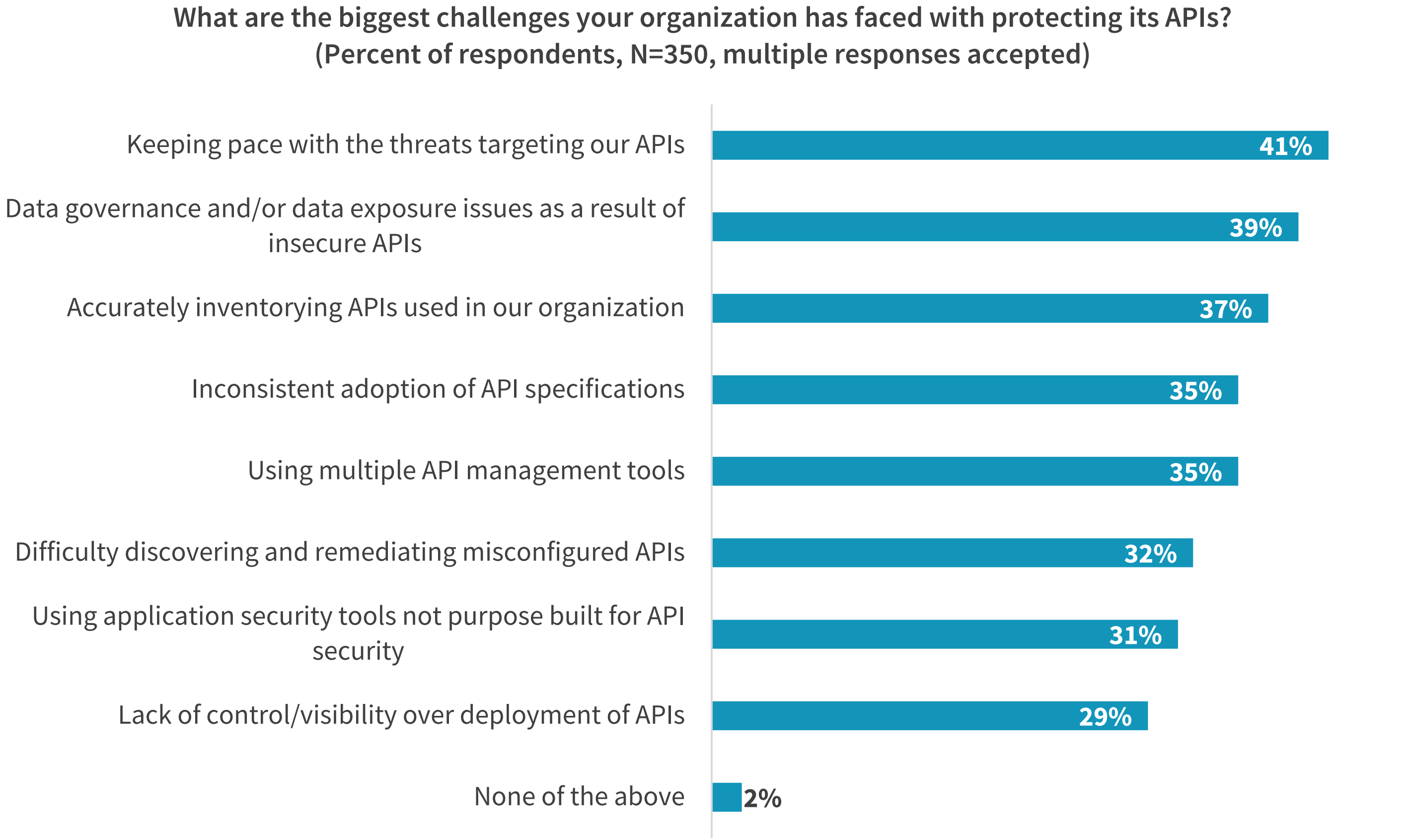


Source: ESG, a division of TechTarget, Inc.

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 (see Figure 17). 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%).

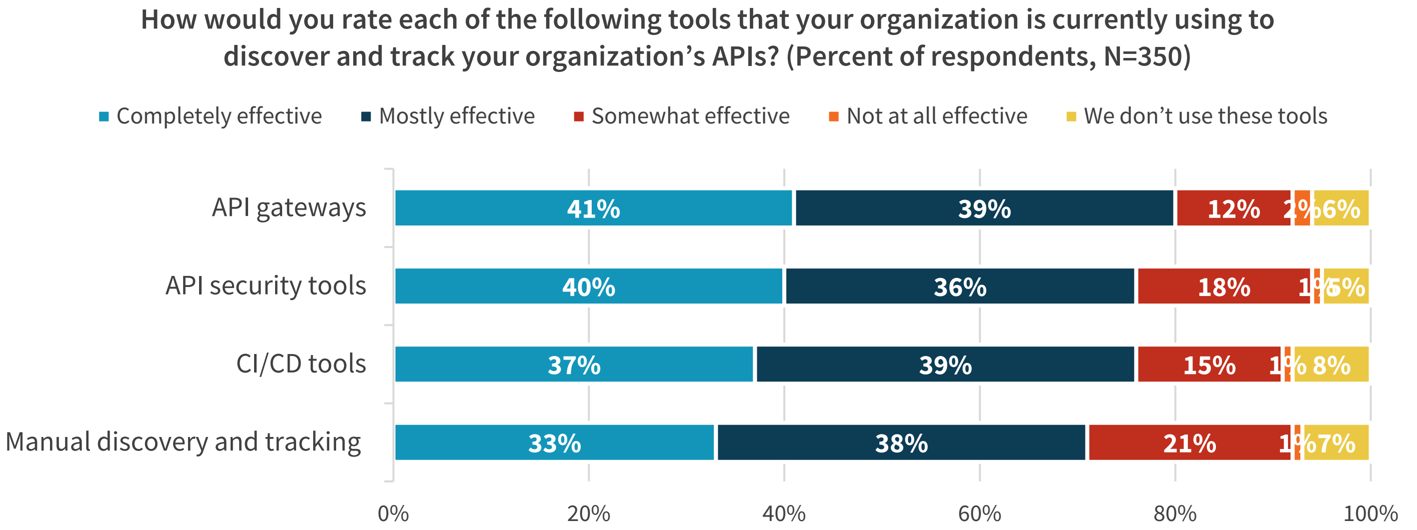
As noted, the range of tools used to discover, manage, configure, and protect APIs is long. Figure 18 reveals that API gateways and API security tools are most commonly identified as being completely effective in terms of discovering and tracking APIs, while 43% cited interactive application security testing (iAST) as completely effective for discovering and remediating API coding errors (see Figure 19). When it comes specifically to protecting APIs, some organizations attempt to apply network security tools 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 at least one-third found IPS, NGFW, bot mitigation, and WAF completely effective indicates that there remains confusion in the market (see Figure 20).

Figure 17. APIs Have Become Ubiquitous, Posing Many Challenges



Source: ESG, a division of TechTarget, Inc.

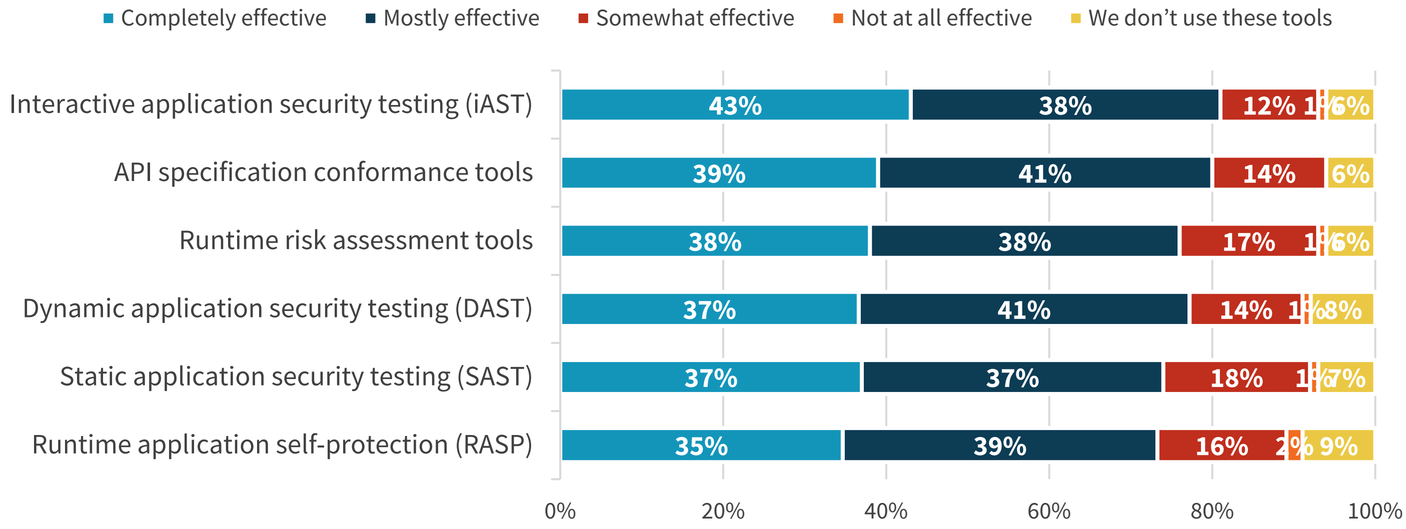
Figure 18. Effectiveness of Tools Used to Discover and Track APIs



Source: ESG, a division of TechTarget, Inc.

Figure 19. Effectiveness of Tools Used to Discover and Remediate API Coding Errors

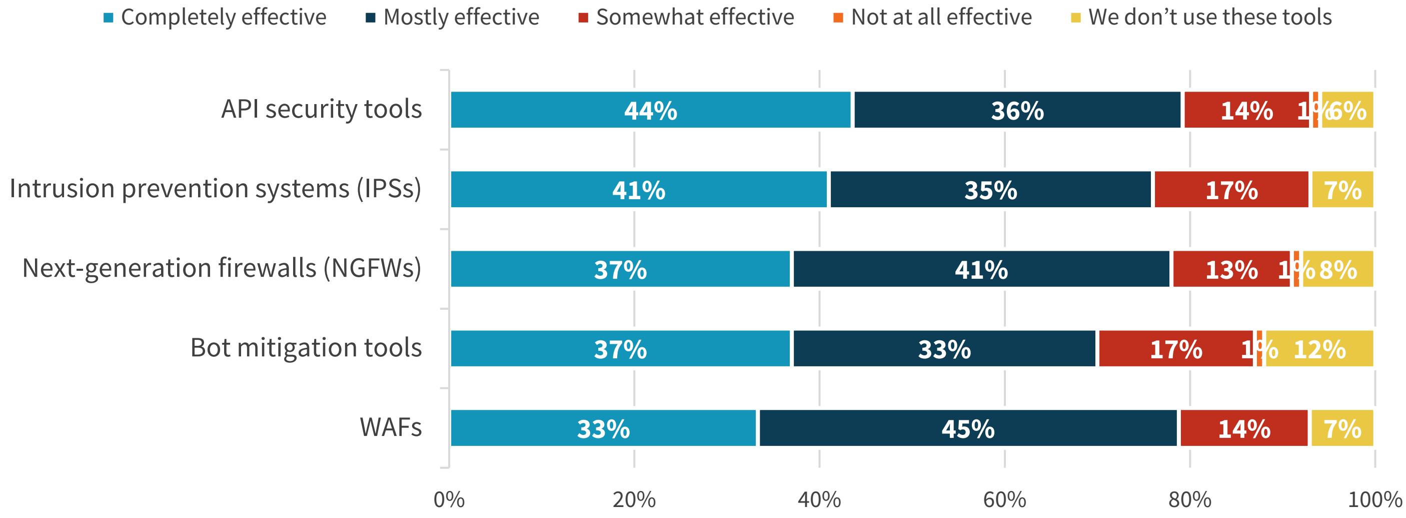
How would you rate each of the following tools that your organization is currently using to discover and remediate API coding errors? (Percent of respondents, N=350)



Source: ESG, a division of TechTarget, Inc.

Figure 20. Effectiveness of Tools Used to Stop or Block API Attacks

How would you rate each of the following tools that your organization is currently using to stop or block attacks on APIs? (Percent of respondents, N=350)

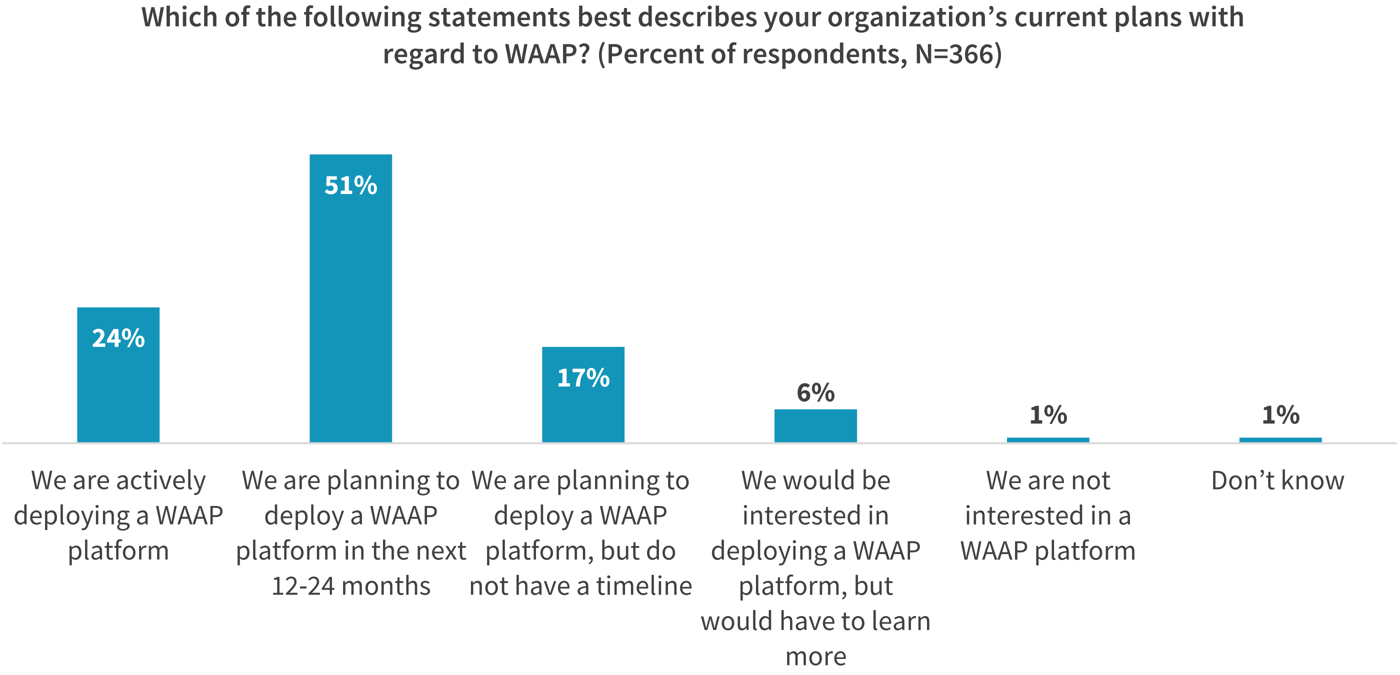


Source: ESG, a division of TechTarget, Inc.

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

Due to the use of many different tools, cross-vector attacks, etc., interest in converged web application and API protection (WAAP) platforms has increased. WAAP solutions are an integrated platform of application protection controls consisting of web application firewall, API security, bot mitigation, and denial of service prevention, which is deployed externally in front of or alongside web applications and can be delivered as a cloud service, an appliance (physical, virtual, or software), or a module embedded in an application delivery controller (ADC). As shown in Figure 21, three-quarters of respondents indicated they are actively deploying a WAAP platform or planning to deploy one in the next 12-24 months.

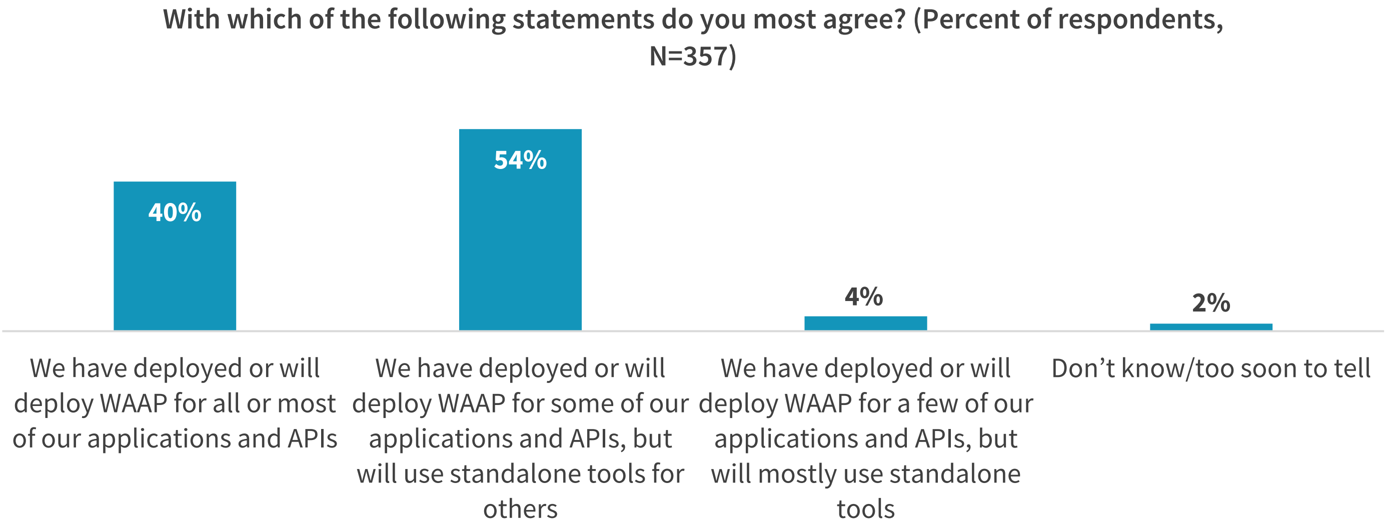
Figure 21. Majority of Organizations Plan to Deploy a WAAP Platform in the Next 12-24 Months



Source: ESG, a division of TechTarget, Inc.

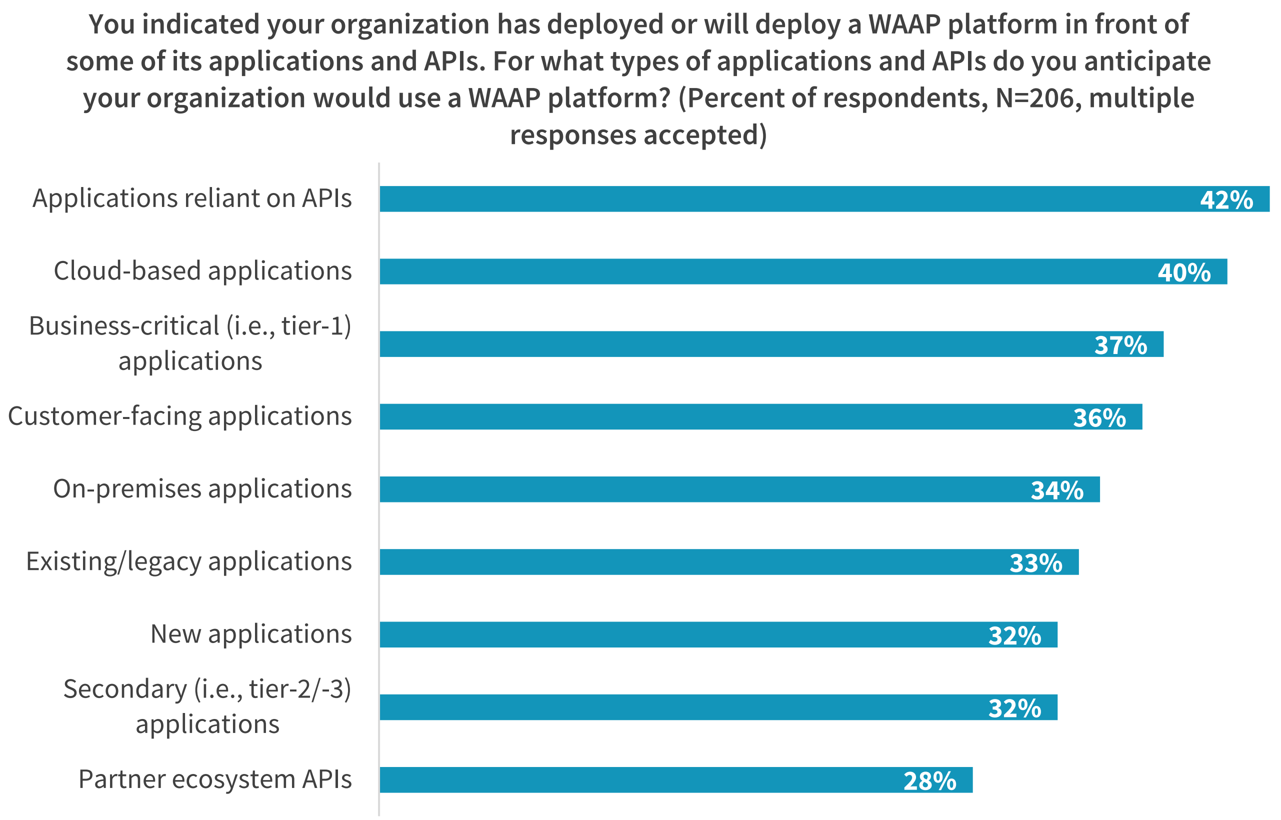
While 40% believe they will deploy WAAP across all their applications, the majority (54%) will continue to use a mix of tools depending on the application in question (see Figure 22). Yet that does not mean WAAP is seen as a secondary control. In fact, according to Figure 23, more organizations plan 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%).

Figure 22. Extent of WAAP Deployment



Source: ESG, a division of TechTarget, Inc.

Figure 23. Types of Applications and APIs Expected to be Protected by a WAAP Platform

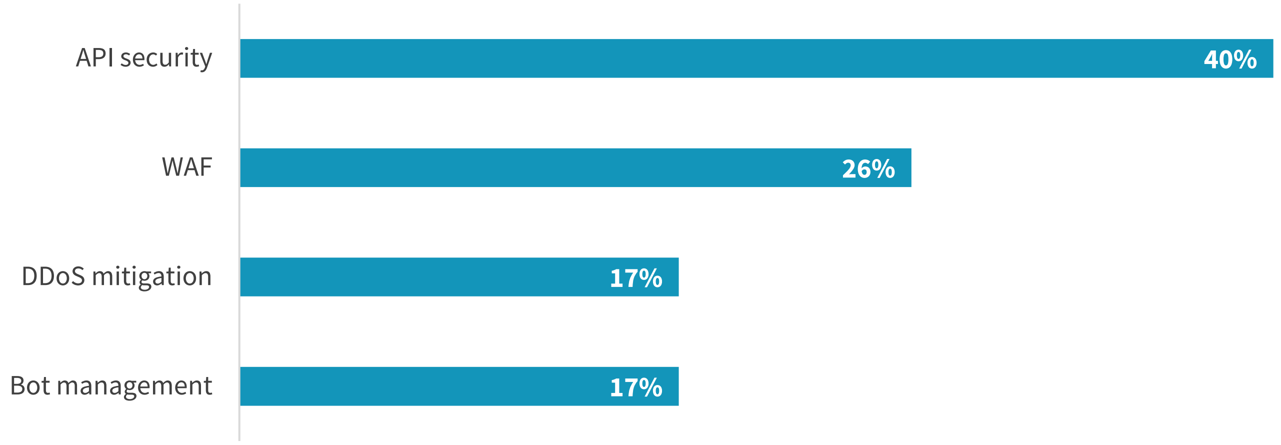


Source: ESG, a division of TechTarget, Inc.

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 (see Figure 24). 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. As shown in Figure 25, 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.

Figure 24. Most Important Tools in a WAAP Platform

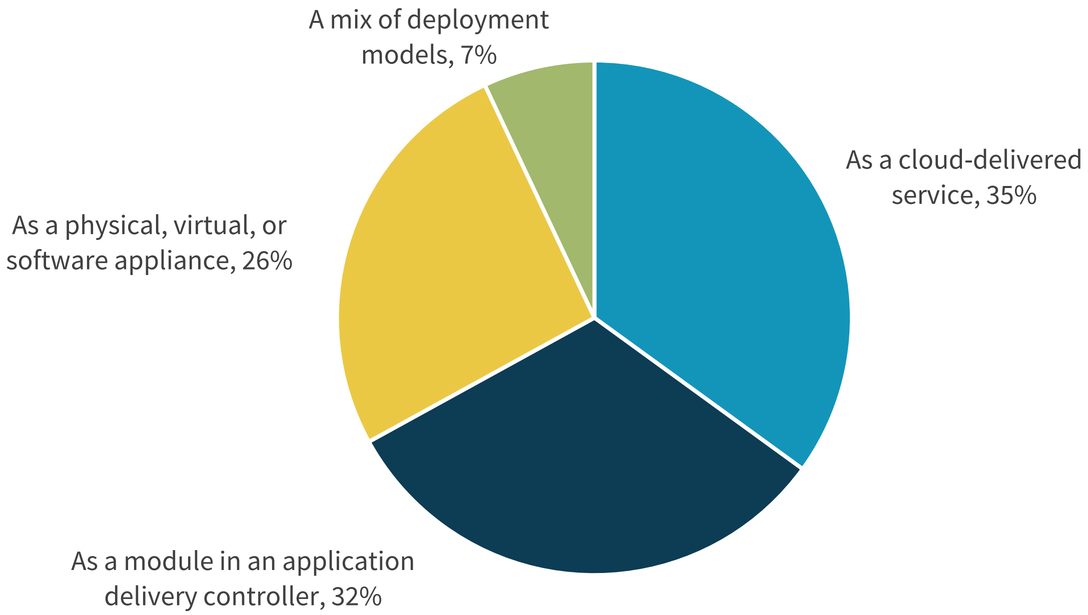
Which of the following tools do you believe are most important in a WAAP platform? (Percent of respondents, N=357, percent ranked #1 displayed)



Source: ESG, a division of TechTarget, Inc.

Figure 25. WAAP Platform Deployment Preference

Which of the following best describes how your organization would prefer to deploy a WAAP platform? (Percent of respondents, N=357)



Source: ESG, a division of TechTarget, Inc.

Conclusion

Application security has reached a tipping point. The speed and scale with which applications are deployed has made it more difficult than ever for security teams to keep pace with their developer counterparts, while the composition of, locations of, and threats targeting applications have pushed traditional tools toward obsolescence. As a result, security teams should prioritize modernizing their application security program to better meet today's challenges and ensure these critical business resources are adequately protected. To successfully do so, ESG proposes the following recommendations:

- Prioritize WAAP tools. Most security teams use multiple application security tools. In addition to the cost and complexity of managing a variety of tools, security can suffer. It can be difficult to correlate alerts across different tools, and with many attacks now being cross-vector (i.e., using bots to target APIs to ultimately compromise a web application), protection should be unified. WAAP offers a consolidated solution to reduce complexity, improve efficiency, and ultimately provide better protection across web applications and APIs from a wide range of attacks.

- Focus on flexibility and broad coverage. While much of the focus on applications has to do with the shift to cloud and new architectures, most organizations will continue to support on-premises and legacy applications well into the future. To help avoid tool sprawl, organizations should consider WAAP tools that provide deployment flexibility and can be applied to a variety of application types. Legacy, on-premises applications may still require hardware appliances, while cloud-resident applications may be better suited for a SaaS-based deployment. The ability to consume security services as a module in an application delivery controller also remains attractive for many organizations. The first steps should be inventorying the applications in use, aligning expectations for cloud expansion or on-premises repatriation, and ensuring tool choices support both current and future goals.

- Prioritize coverage for APIs. The use of APIs will continue to grow exponentially as microservices-based architectures take hold and application ecosystems expand. This creates a critical need for API security to be not just a checkbox attribute of a WAAP solution but rather a key component. This should include automated discovery, profiling, and protection as baseline features of the core solution, as well as support for multiple API specifications.

- Understand application security is a team sport. As application development has become democratized and distributed across different parts of the organization, so too has responsibility for security. While the security team ultimately takes ownership, it is incumbent on them to work with development teams to understand their processes and select tools that enable them to continue to be agile while also ensuring applications pushed into production have the proper safeguards in place. Integrating security into DevOps practices is certainly a significant part of this, but less formalized improvements can help move the needle as well and ensure that security does not become an obstacle to development.

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.

Please see the *Respondent Demographics* section of this report for more information on these respondents.

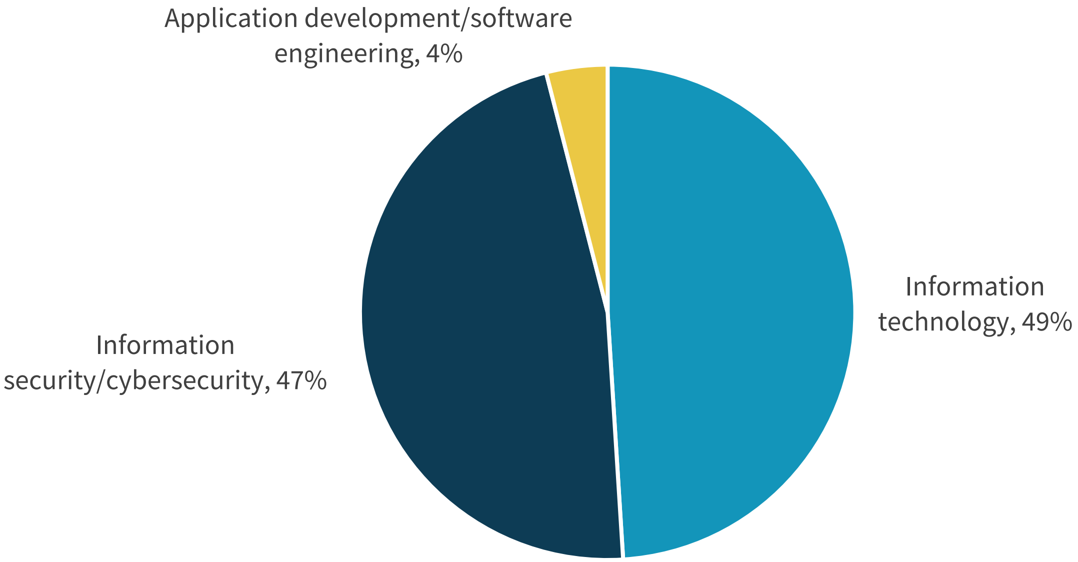
Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

Respondent Demographics

The data presented in this report is based on a survey of 366 qualified respondents. Figure 26 through Figure 29 detail the demographics of the respondent base at an individual and organizational level.

Figure 26. Respondents by Job Function

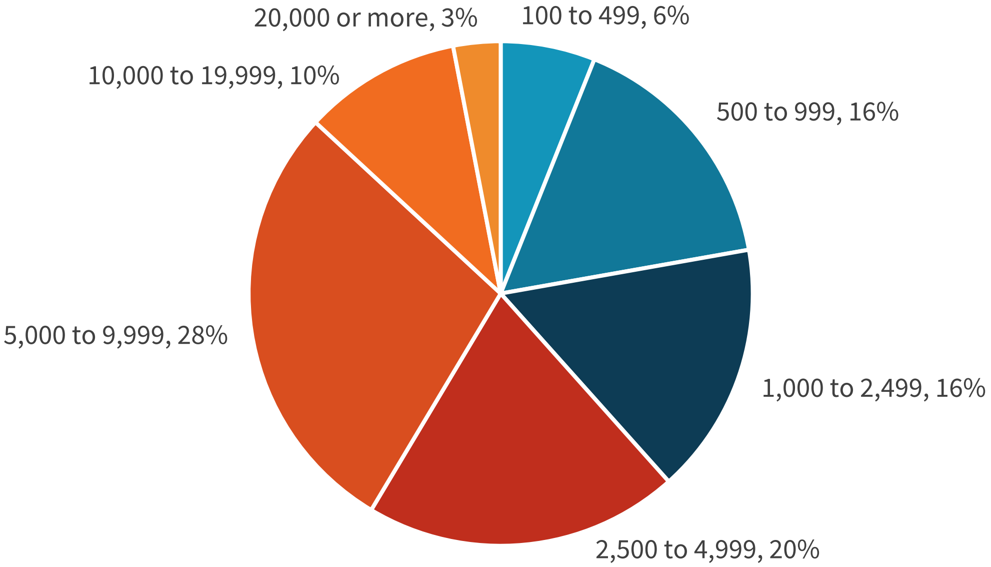
Which of the following best describes your current job function? (Percent of respondents, N=366)



Source: ESG, a division of TechTarget, Inc.

Figure 27. Respondents by Number of Employees

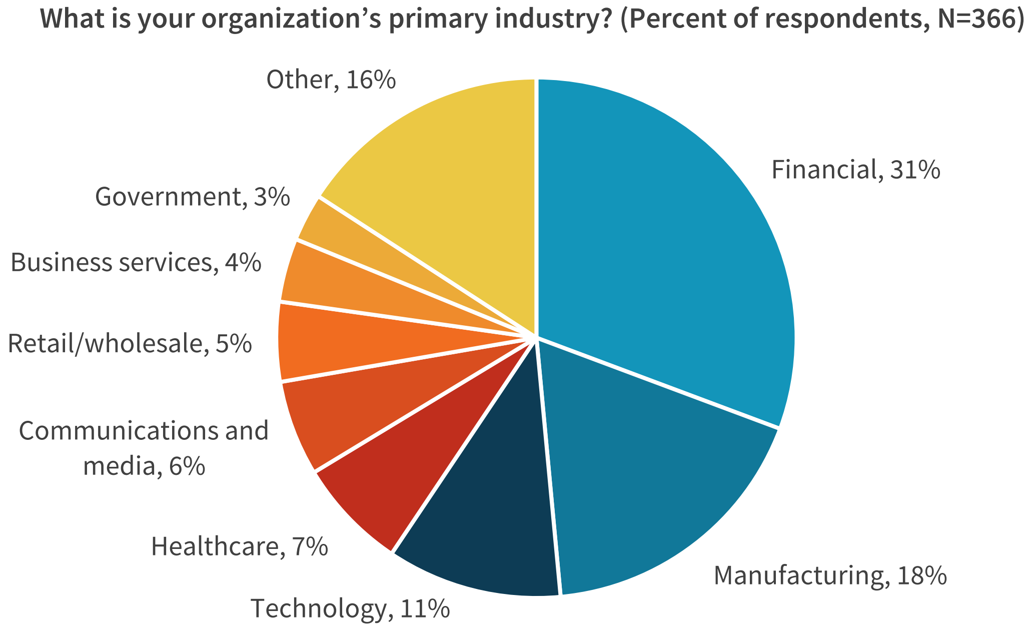
How many total employees does your organization have worldwide? (Percent of respondents, N=366)



Source: ESG, a division of TechTarget, Inc.

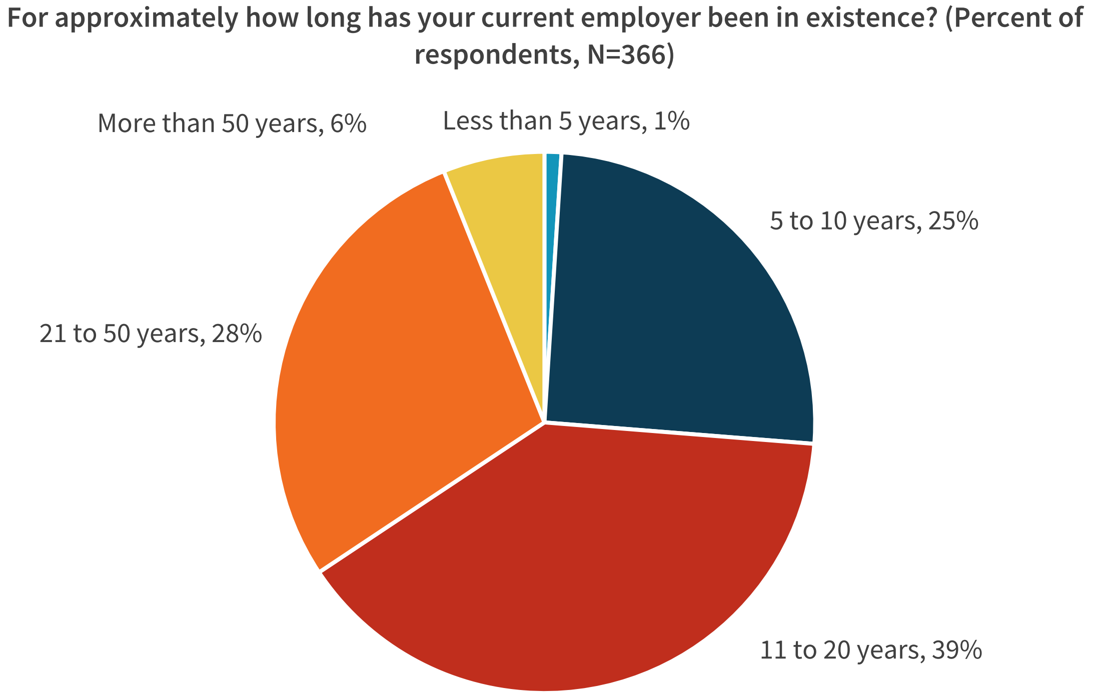
Respondents were asked to identify their organization's primary industry. In total, ESG received completed, qualified responses from individuals in 22 distinct vertical industries, plus an "Other" category. Respondents were then grouped into the broader categories shown in Figure 28.

Figure 28. Respondents by Industry



Source: ESG, a division of TechTarget, Inc.

Figure 29. Respondents by Age of Organization



Source: ESG, a division of TechTarget, Inc.

ESG a division of TechTarget

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

www.esg-global.com contact@esg-global.com 508.482.0188