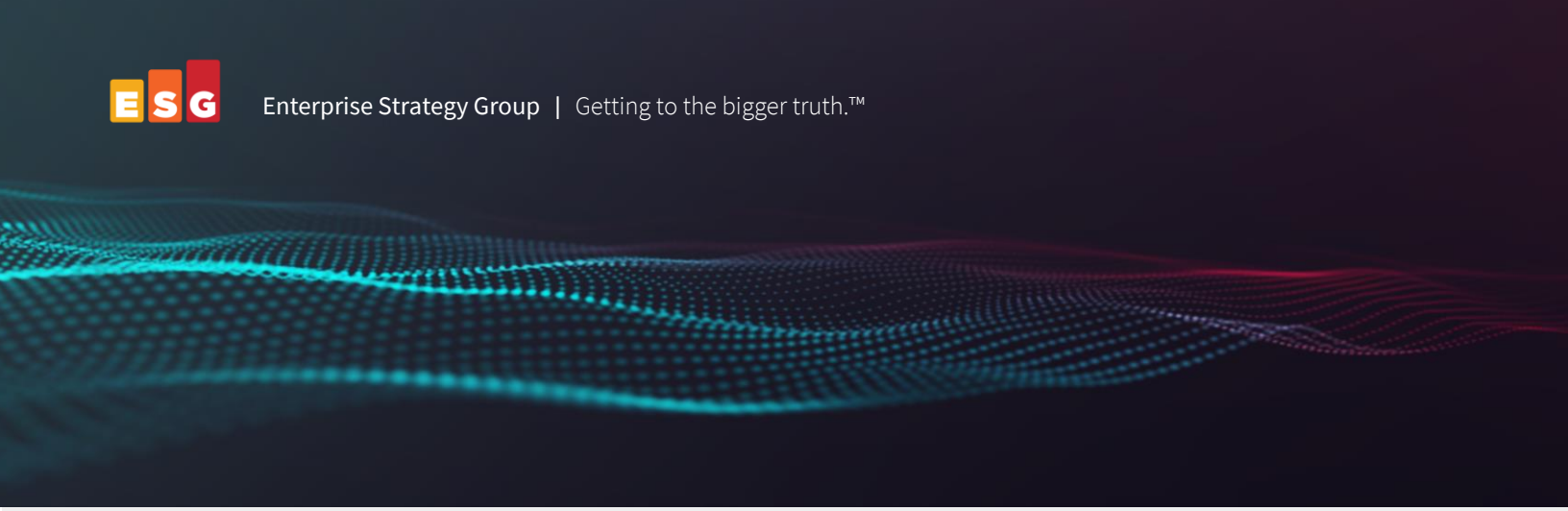


ESG RESEARCH INSIGHTS PAPER

Reaching the Tipping Point of Web Application and API Security

Why yesterday's tools no longer meet the needs of today's dev and sec professionals.

By John Grady, ESG Senior Analyst
Adam DeMattia, Director of Research

July 2021

This ESG Research Insights Paper was commissioned by Fastly and is distributed under license from ESG.

Contents

Executive Summary

Web applications are critical to the success of most businesses today. Their use can help an enterprise engage with its customers; ensure its employees, partners, and affiliates are productive; and ultimately drive revenue for the business. As a result, massive changes in application development processes and supporting technologies have occurred. Specifically, the adoption of agile development methodologies and increasing use of microservices-based architectures have helped increase speed, agility, and flexibility with regards to application development and deployment. Yet for as much innovation that has occurred in these areas, many organizations continue to use traditional web application and API security controls to protect their resources.

To gain deeper insights into modern application trends and the challenges organizations are facing from a web application and API security perspective, Fastly commissioned the Enterprise Strategy Group (ESG) to conduct a global research survey representing 500 organizations located in North America, Europe, and Asia-Pacific and Japan. Based upon the research conducted in this study, ESG concludes:

- Organizations are struggling to maintain adequate security across new application architectures. Half of organizations say web application and API security is more difficult than two years ago, and the shift to public cloud services and API-centric applications are key reasons why. 64% of organizations expect most or all of their applications to use APIs within the next two years and worry about vulnerabilities, malware, and data exfiltration targeting these endpoints.
- Traditional tools were not built with the modern, decentralized enterprise in mind. On average, organizations use 11 web application and API security tools and spend $2.6 million annually. Much of this sprawl is attributable to supporting new architectures and new cloud environments, meaning that as organizations innovate from an application perspective, security becomes more complex and costly.
- These tools often create more problems than they solve. The false positives generated by these tools are as big an issue as successful application attacks. Respondents say false positives cause equivalent application downtime as successful attacks, and 75% indicated their organization spends an equal amount or more time on false positives as actual attacks.
- There is a pressing need for a modern, unified approach to web application and API security. Organizations are often forced to run tools in log or monitor mode or shut them off entirely due to ineffectiveness or overblocking that impedes the business. Yet nine in ten respondents would prefer to run in blocking mode if false positives could be addressed. As a result, 93% are interested in or planning to deploy a consolidated web application and API security solution to improve security efficacy, provide consistent protection across disparate application architectures and environments, and reduce costs.

As Application Architectures Evolve, Complexity Grows

One of the main themes of cybersecurity over the last few years has been that of complexity. Enterprise environments have become a sprawling, interconnected tangle of locations, devices, users, and corporate resources. Applications specifically have seen arguably the greatest level of innovation, allowing developers to code and deploy applications more quickly than ever before. ESG's research found that the average number of internally developed applications respondents support has risen from 139 two years ago to 195 today, with an expectation that this number will reach 263 in two years' time.

This level of agility is fueled in large part by the increasing adoption of public cloud infrastructure and microservices-based architectures. Specifically, respondents indicate that 51% of internally developed applications will reside on IaaS platforms two years from now, and 46% will be built on microservices architectures, a 31% increase for each compared to where things stand today. However, even with these strong adoption trends, the long trail of legacy applications most enterprises must manage will result in traditional monolithic architectures and on-premises data centers remaining a reality for most organizations.

With this as the backdrop, it should come as no surprise that fully half of the respondents surveyed by ESG believe web application and API security is more difficult today than it was two years ago. And while the threat landscape is certainly a core driver of this, the rise in the number of internally developed applications supported, the increasing number of cloud platforms used, and the decentralization of application security responsibilities all contribute to application security complexity.

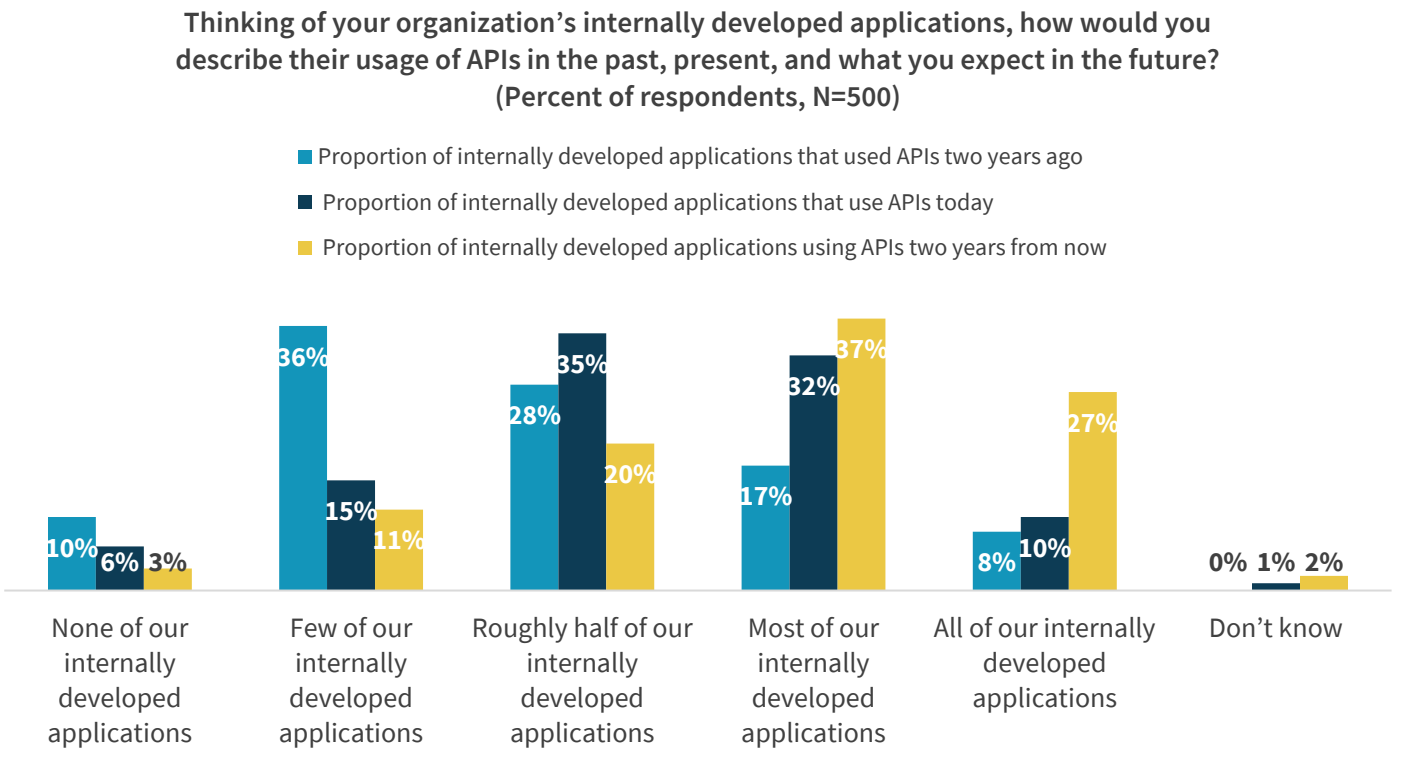
API-driven Architectures Open New Doors for Attacks

A significant part of the application modernization trend is driven by the usage of APIs. Web APIs support the use of microservices, mobile applications, and the development of application ecosystems by connecting internal and external applications together. The industry has seen an explosion of web API usage over the last few years, as exhibited by our research respondents (see Figure 1). Specifically, while 42% of organizations report that most or all of their internal applications rely on APIs today, this number is expected to rise to 64% two years from now.

Regional Insight:

Two years from now, 69% of North American organizations and 66% of European organizations expect most or all of their applications to rely on APIs, compared to 54% of their APJ counterparts.

Figure 1. Past, Current, and Future API Usage

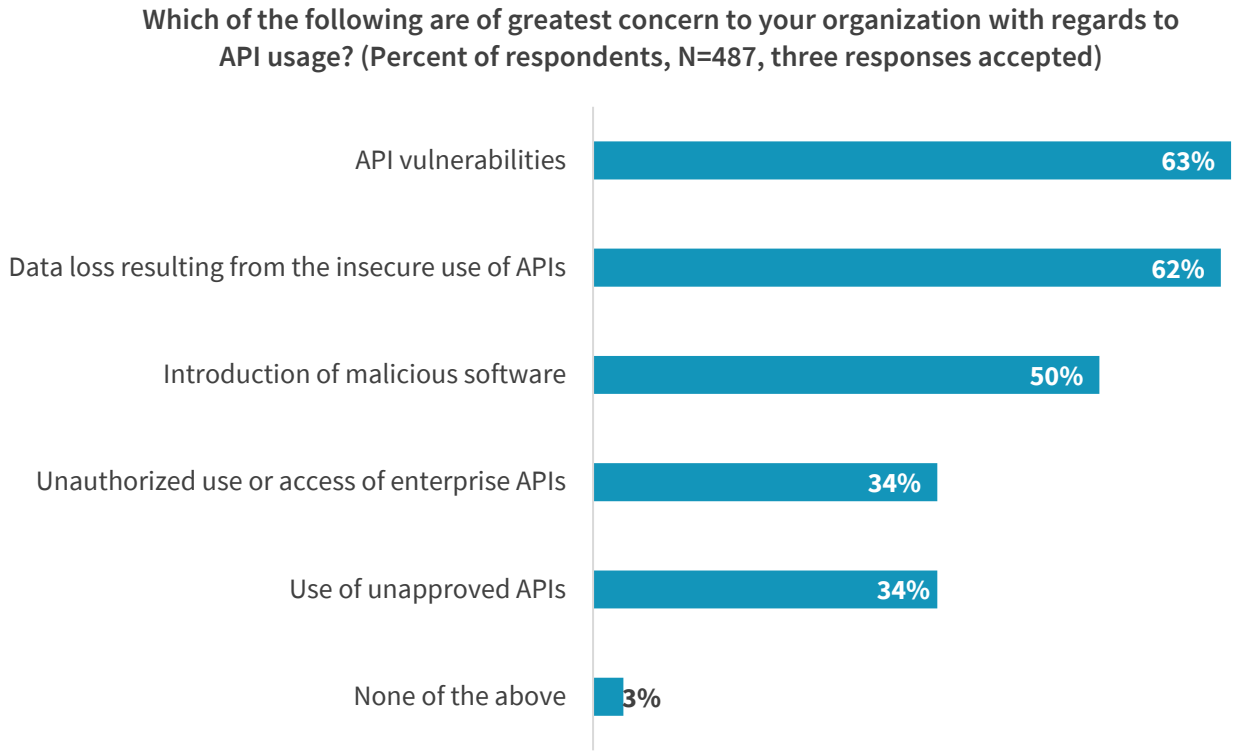


Source: Enterprise Strategy Group

Understanding how prevalent APIs have become provides critical context when assessing the security concerns associated with their usage. These endpoints offer attackers an additional threat vector to exploit by leveraging vulnerabilities, introducing malware, and ultimately exfiltrating data (see Figure 2). The most common API concern for European organizations is vulnerabilities, cited by 70% of respondents, while APJ respondents most commonly cited data loss resulting from the insecure use of APIs.

These concerns are well founded due to the massive API footprint many organizations support and the limited visibility they have over those endpoints, often resulting in undocumented APIs. Increasingly, attackers use bots to scale account takeover, credential scraping, credential stuffing, and fake account creation attacks. Further, the dynamic nature of the API landscape can make it difficult for security teams to keep up. The increasing use of GraphQL as a replacement for REST APIs is one example of this.

Figure 2. Concerns Related to API Usage



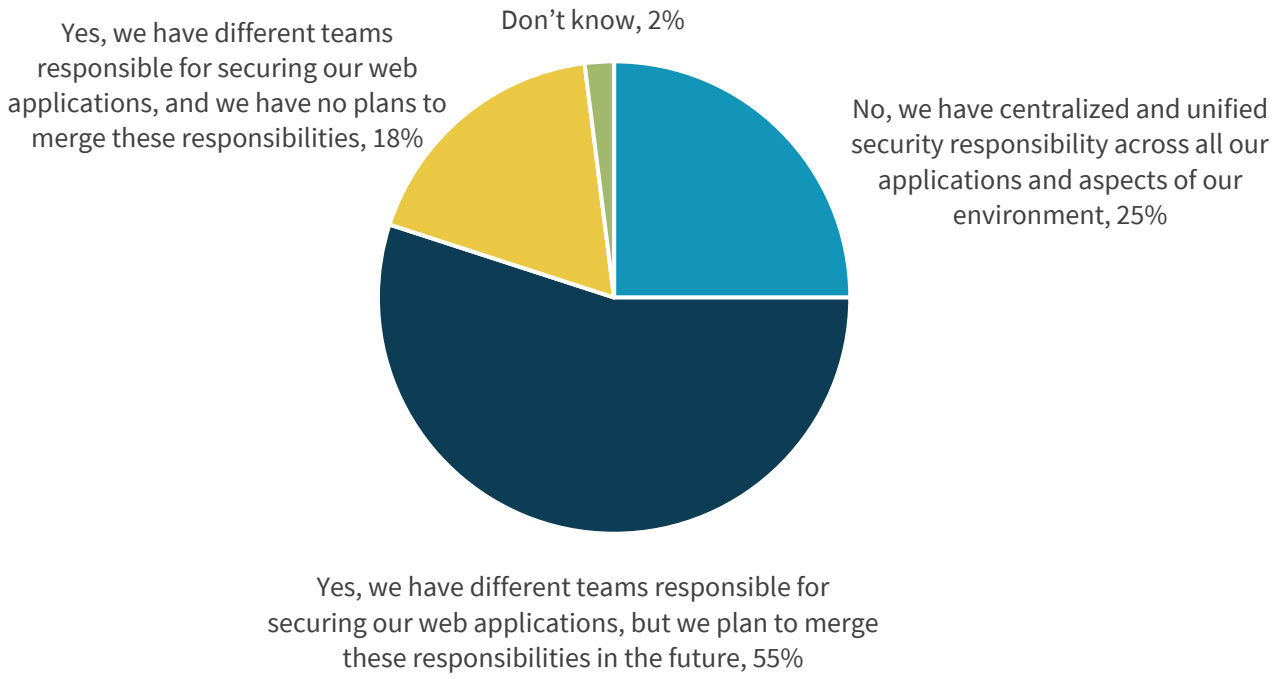
Source: Enterprise Strategy Group

Uncertainty Around Security Ownership Makes for More Complications

Exacerbating these changes in application location and composition is the fact that security responsibility is often distributed across a variety of teams and individuals, limiting centralized oversight. Specifically, 32% of our research respondents indicated that IT operations held primary responsibility for securing web applications, while 21% selected DevOps or application developers, 18% identified security, and 11% pointed to cloud engineering as the primary security owners. While responsibility may vary from one enterprise to another depending on organizational structure, skills, or other considerations, the reality is that application security is a team sport requiring input and cross-functional collaboration to be successful. Yet without some centralization to ensure consistency across tools, policies, and processes, these programs become much more difficult to manage. As shown in Figure 3, only one-quarter of our respondents indicate that their organization has centralized security responsibility across all applications and aspects of their environment.

Figure 3. Ownership of Application Security

Are different groups/individuals in your organization responsible for the security processes, policies, and technology associated with protecting your organization's web applications? (Percent of respondents, N=500)



Source: Enterprise Strategy Group

Traditional Application Security Tools Do Not Solve Today's Problems

To address many of these issues, including new application architectures and locations, API usage, and bot-driven attacks, a wide variety of tools are available for organizations to consider. Traditional web application firewall usage is nearly ubiquitous to protect against OWASP Top 10 and other threats, as well as satisfy compliance requirements. API protection tools can help close the visibility gap previously discussed and prevent attackers from exploiting vulnerable endpoints. Bot management solutions help confirm that application and API traffic is generated by humans and ensure fraudulent activity is blocked. DDoS mitigation products maintain application availability by identifying and blocking low and slow layer 7 attacks, which are often more difficult to detect than volumetric-based layer 3 and 4 attacks.

Respondents reported spending an average of $2.6M annually on 11 different tools for web application and API security.

Our research found that three-quarters of respondents use at least 5 different web application and API tools—yet many use significantly more than that. In fact, respondents reported spending an average of $2.6 million annually on 11 different tools for web application and API security. Based on this significant level of spending across key application attack vectors, one may expect that respondents reported a positive return on investment in the form of strong detection efficacy, a limited number of attacks, and better operational efficiency. However, this assumption would be incorrect.

Defense in Depth Has Led to a Patchwork of Incompatible Tools

Tool sprawl can occur for many reasons, both intentional and unintentional (see Figure 4). Half of the respondents surveyed indicated their organizations use multiple tools because they feel separate tools provide better protection. The desire for best-of-breed is certainly understandable. However, as we will explore shortly, the operational inefficiencies and lack of integration between these different tools often negate any potential capability benefits.

On the other hand, 54% of those surveyed said their organization has added tools as additional cloud providers have been introduced. Some of the benefits of using native security tools from cloud service providers (CSP) are the ease of deployment, management, and billing that come from integrated security capabilities. However, in a hybrid, multi-cloud world where most enterprises have applications spread across their on-premises data center and multiple CSPs, the lack of consistency and common management can create more problems than are solved by this approach. Additionally, 53% reported adding tools based on input from application owners, and 53% said tools were added as application architectures were modernized.

Regional Insight:

62% of North American respondents indicated tool sprawl arose due to new cloud providers being introduced, compared to 46% of European respondents and 50% of APJ respondents.

Figure 4. Factors Driving Application Security Tool Sprawl

Source: Enterprise Strategy Group

Traditional Tools Create More Problems Than They Solve

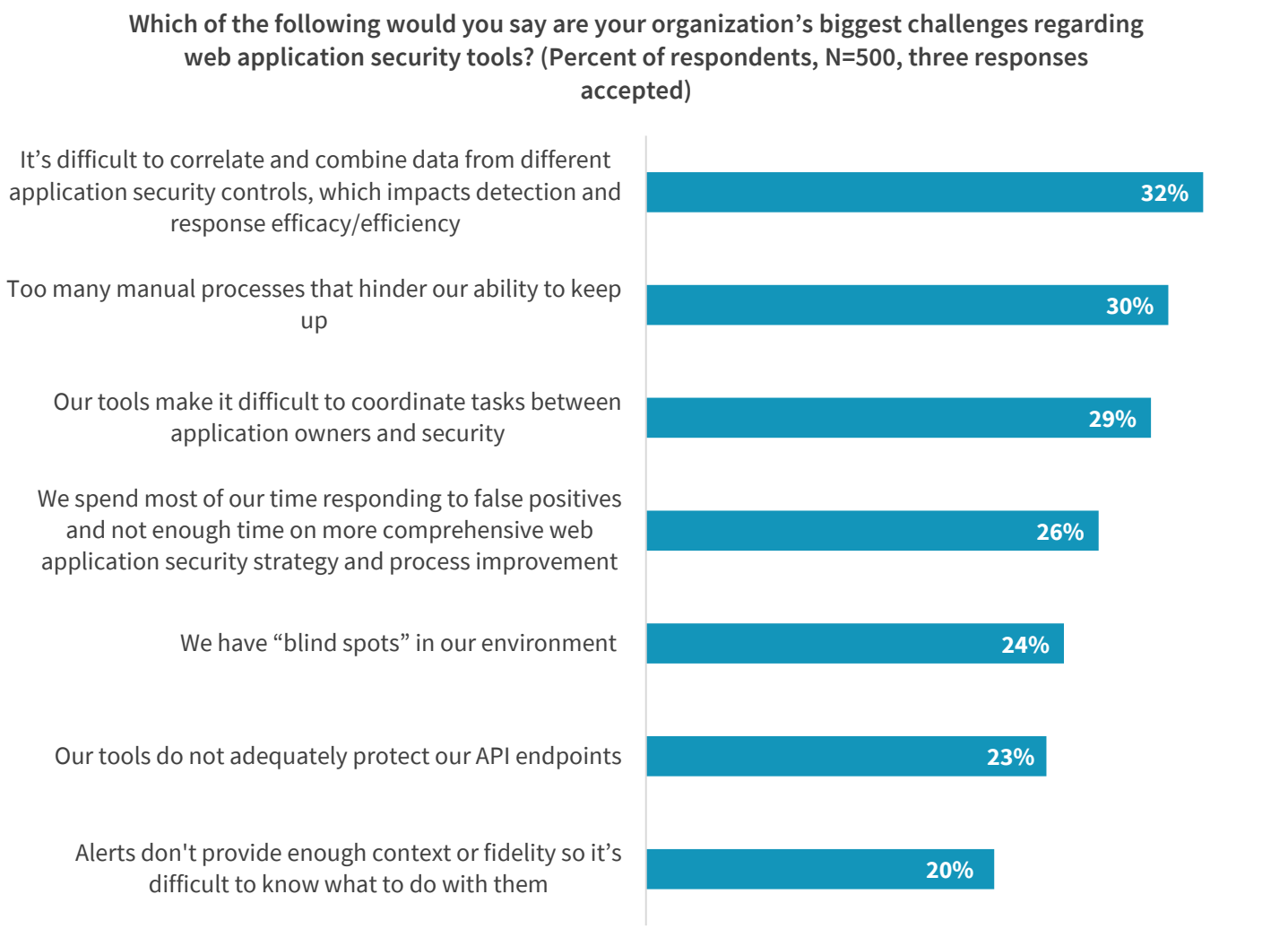
The list of challenges cited by respondents with regard to their organization's web application and API tools is long and varied. Coordinating tasks between application and security owners, a lack of API protection, and poor visibility were all reported (see Figure 5). However, the most common challenge was the difficulty in correlating data across multiple tools,

which was cited by 32% of respondents. When juxtaposed with our previous finding that organizations deploy an average of 11 different tools to improve protection, this is a stunning admission that the strategy is simply not working.

68% of respondents said their organization developed new rules for deployed controls at least monthly, with efficacy testing typically lasting at least a week.

Additionally, 30% of respondents indicated that manual processes hindered their ability to keep up. A significant cause of this is the ruleset customization and testing that web application and API security tools often require. In fact, 68% of respondents said their organization developed new rules for deployed controls at least monthly, with efficacy testing typically lasting at least a week.

Figure 5. Top Application Security Tool Challenges



Source: Enterprise Strategy Group

False Positives Are All Too Common and Overwhelming—They're Also as Time Consuming as Actual Attacks

If the different web application and API security tools deployed by organizations worked effectively, perhaps the inefficiency of the approach could be tolerated. Unfortunately, the data indicates that the efficacy of these tools is lacking. Specifically, respondents reported an average of 53 alerts per day from their web application and API security tools, with 45% of these ultimately determined to be false positives. Given that volume, it is not surprising that nine in ten respondents

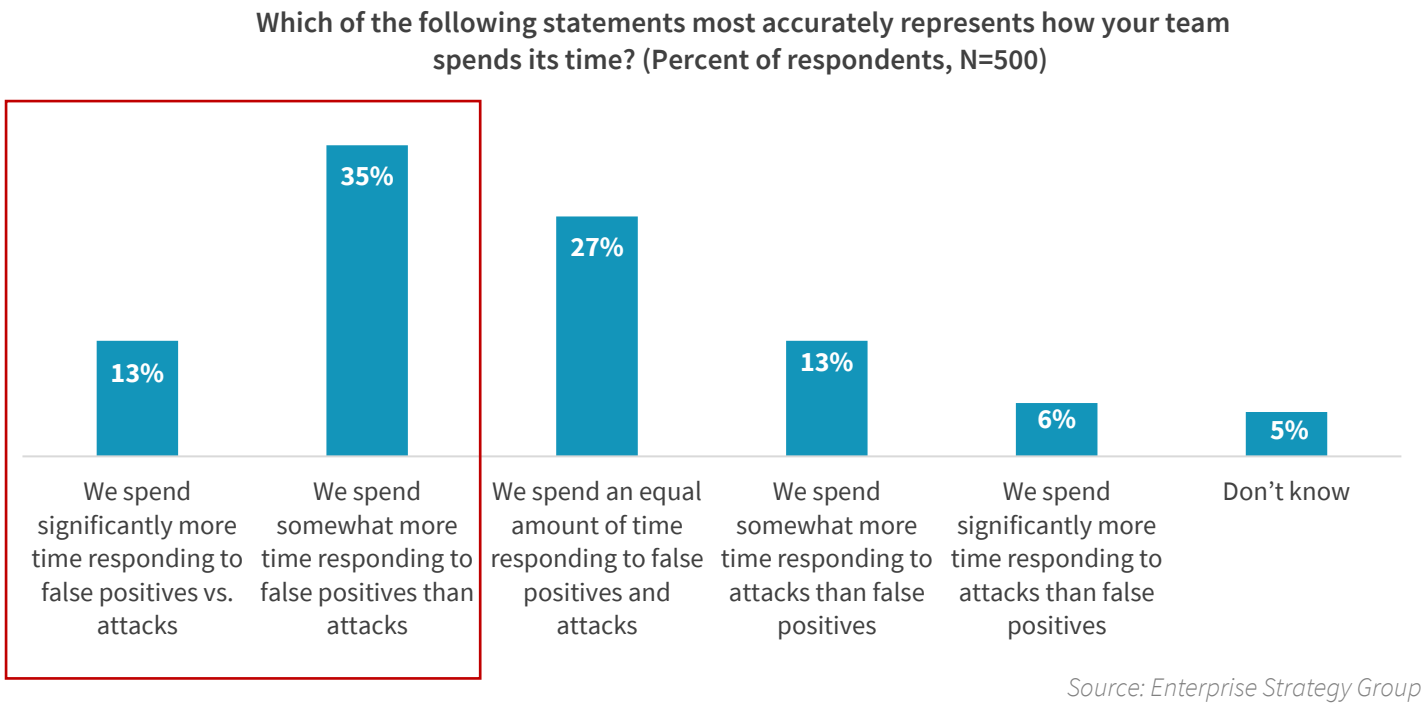
said that false positives were an issue for their organization. But how does this compare to the rate and impact of actual attacks?

In total, 82% of our respondents indicated their organization had suffered a successful attack on their web applications and APIs in the past 12 months. Yet most are seeing not only multiple, but tens of successful attacks annually, with an estimated average of 60 per year. There are many impacts that can result from a successful attack including poor customer experience, compliance issues, loss of brand and shareholder value impacts, and application downtime (which can lead to lost revenue).

46% reported application downtime of a few days or more due to false positives, meaning the average downtime impact of false positives is often the same as actual attacks.

With regard to application downtime, 46% of our respondents indicated systems were offline for an average of at least a few days due to successful attacks. More discouraging though, is the fact that 46% reported application downtime of a few days or more due to false positives, meaning the average downtime impact of false positives is often the same as actual attacks. The ultimate result is that 75% of respondents indicated their organization spends equal or more time on false positives as actual attacks (see Figure 6). This is a disappointing finding as every minute spent on false positives is one not spent on comprehensive application security strategy and process improvement. With many security organizations under-staffed and under-skilled, they are fighting an uphill battle to protect their applications on a daily basis.

Figure 6. Time Spent on False Positives Versus Attacks



Source: Enterprise Strategy Group

Many No Longer Trust Their Traditional Tools—and Simply Turn Them Off

In the face of false positives, organizations have two main options short of doing nothing: run tools out of band in log or monitor mode or turn tools off entirely. Our research found that while the majority (53%) chose to shift to log or monitor mode, 12% report turning their tools off and 26% report doing both (see Figure 7). In other words, more than a third of respondents felt that completely shutting down their security tools was a less-disruptive course of action than continuing

to manage false positives. Of additional note is the fact that these tools are turned off very shortly after they are deployed. Specifically, 82% of respondents indicated their organization turned off web application and API protection tools less than one month after deploying.

Figure 7. Actions Taken as a Result of False Positives

Source: Enterprise Strategy Group

The Time Is Right for an Evolved Solution

Vendors able to deliver tools that free up personnel to focus on these proactive tasks should be viewed as a competitive differentiator and business enabler.

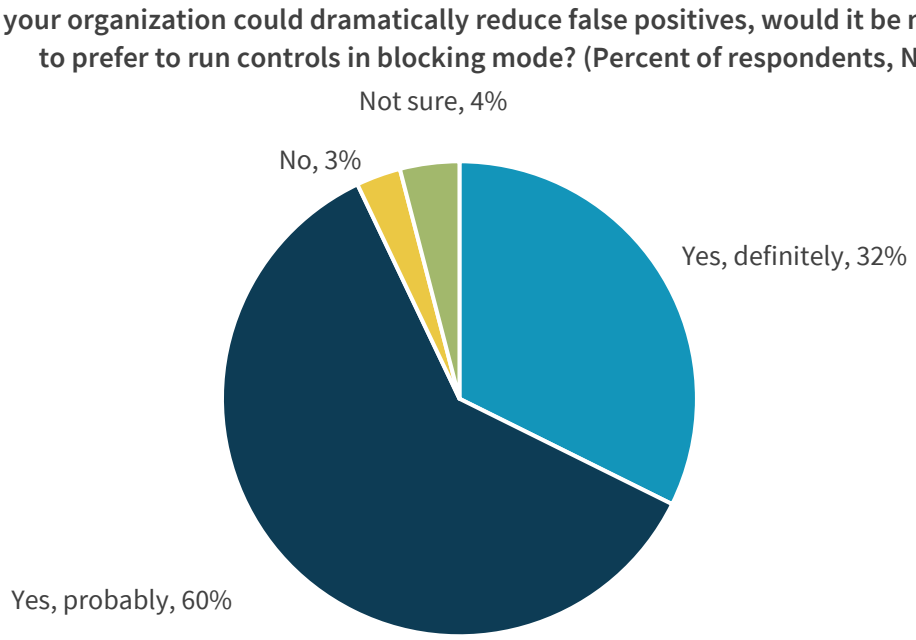
As a result of the fundamental changes to application deployment models and the inefficiency and ineffectiveness of traditional, multi-tool security strategies, the time is right to consider a new approach. Only 4% of our research respondents considered their web application and API security vendor a competitive differentiator. Frankly, this should be much higher. For most businesses today, applications are a critical part of daily operations, if not a direct conduit for generating revenue. The time wasted on manual management tasks and investigating false positives is time that could be spent refining existing applications, coding new ones, or otherwise materially helping the business. Vendors able to deliver tools that free up personnel to focus on these proactive tasks should be viewed as a competitive differentiator and business enabler.

Organizations Want Security Without Compromise—Full Blocking Mode Without False Positives

Based on the data, our respondents are not turning web application and API security tools off or running out of band because they prefer to, but rather because they do not have a choice. False positives can negatively impact the customer experience, result in application downtime, and allow legitimate attacks to sneak in among the noise. With these

undesirable outcomes in mind, it is understandable, if not advisable, that organizations would choose to run tools in log or monitor mode. However, if false positives were not an issue and could be dramatically reduced, more than 9 in 10 respondents (92%) would prefer to run controls in blocking mode (see Figure 8).

Figure 8. Impact of Reducing False Positives on the Preference for Blocking Mode



Source: Enterprise Strategy Group

A Unified Solution is Preferred

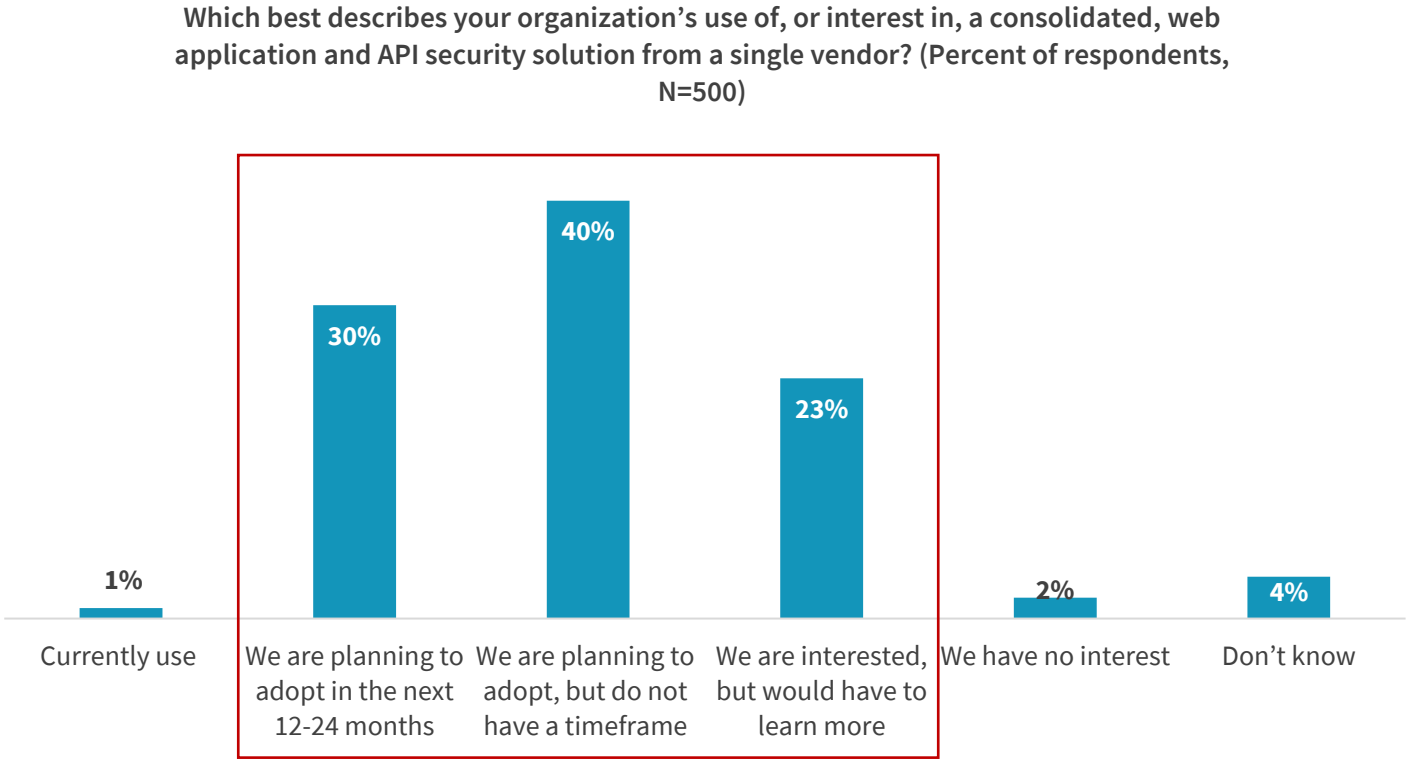
Today, only 1% of our research respondents report using a consolidated web application and API security solution from a single vendor (see Figure 9). Given the emerging nature of these types of offerings, this low penetration is not surprising. However, 93% plan to adopt or are interested in a consolidated approach, portending a massive shift in market preferences over the next few years.

Regional Insight:

37% of North American respondents are planning to adopt a converged solution in the next 12-24 months, compared to 32% of European respondents and 17% of APJ respondents.

Organizations have a variety of motivations behind their interest in unified solutions. First and foremost, many expect better efficacy by ensuring that protections for different threat vectors are integrated. The hope is that this will help reduce blind spots, promote better visibility into attacker campaigns across all parts of the environment, and ultimately reduce false positives. Additionally, many anticipate more simplicity by using a single solution with consistent coverage across application architectures and locations. Finally, there is an expectation of cost savings, both from a solution and an operational perspective. Reducing the number of tools and having a more strategic relationship with a single vendor can yield product and subscription cost savings. Limiting the number of tools personnel must be trained on and improving the effectiveness of those products can create savings on the operational side.

Figure 9. Interest in a Consolidated Web Application and API Security Solution



Source: Enterprise Strategy Group

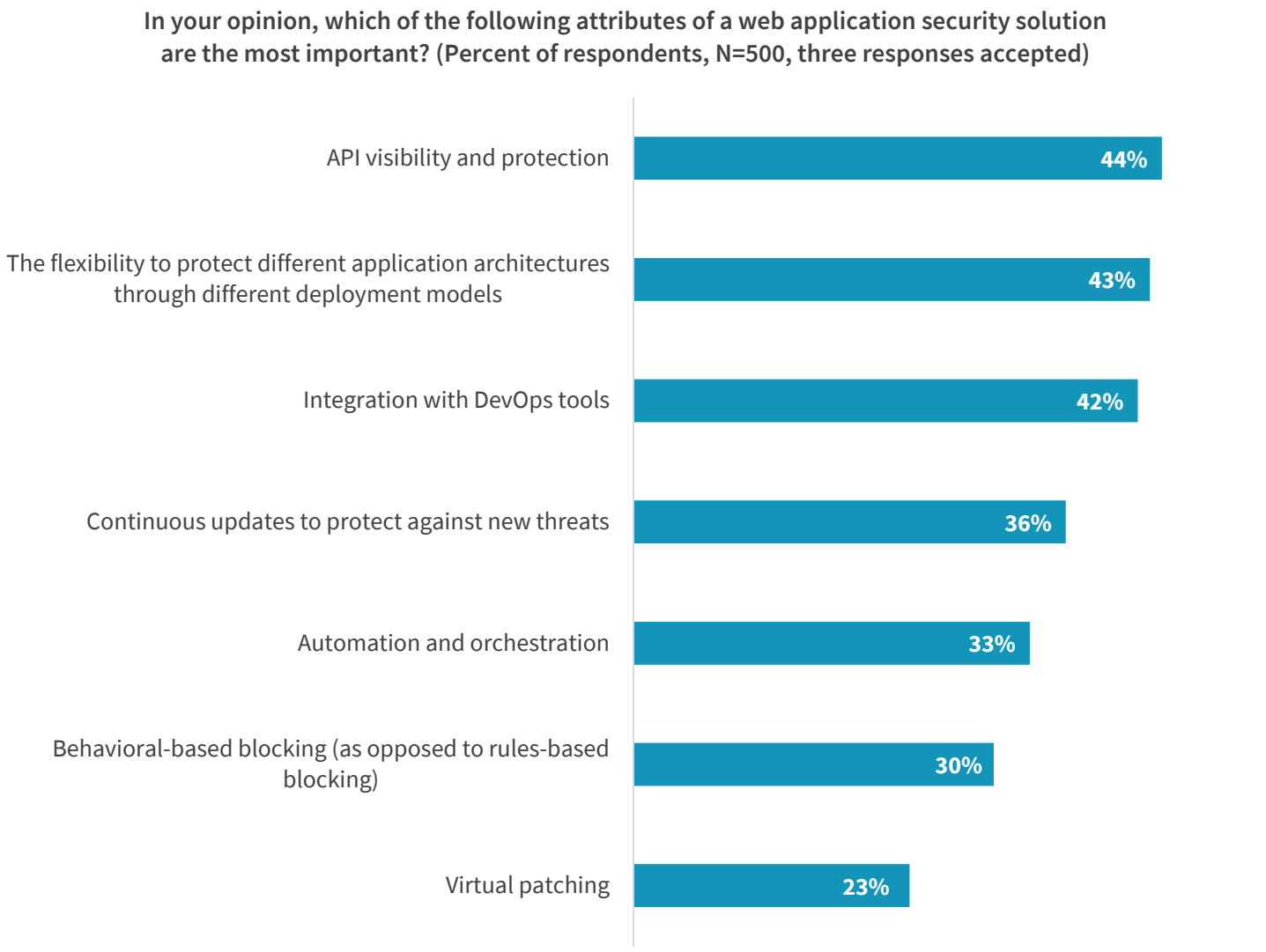
Modern Applications Need Modern Security: Flexible Deployment, DevOps Support, and Strong API Protection

To deliver on these outcomes, modern web application and API security solutions must deliver a broad range of features and capabilities (see Figure 10). The most important of these include:

- API visibility and protection. As the market has moved from web application firewall to web application and API protection, it should be obvious that APIs are increasingly the focus of security strategies. As a result, visibility into the APIs being used, traffic flowing to them, and the associated response of these endpoints are all critical for unified solutions. This includes support for new API technologies such as GraphQL.
- Coverage for different architectures. To protect legacy, container-based, and serverless applications across both on-premises and cloud infrastructure, modern solutions must provide deployment flexibility. The ability to integrate with load balancer and API gateways when possible, run as reverse proxy, deploy in Kubernetes, or as software-as-a-service (SaaS) delivers choice and consistency regardless of the type of application being protected.
- Integration with DevOps tools. No matter how flexible the deployment options are, solutions that don't plug directly into the CI/CD process to ensure deployment as applications are pushed to production cannot scale to meet the needs of modern environments. Given the important role application teams play with regards to security, it is critical that web application and API security tools fit their processes and integrate with tools such as Slack, PagerDuty, Jira, and others.

- Automation and orchestration. In addition to integrating with DevOps tools, web application and API security solutions must provide automation and allow for orchestration across the entire application infrastructure. Manual creation of rules and configurations and rewriting of policy when applications are deployed is not scalable for most enterprises.
- Continuous updates. The dynamic threat landscape makes manually updating, testing, and deploying rulesets a Sisyphean task. Tools that remove this requirement by automating updates can help deliver the operational benefits users expect when moving to a unified solution.
- Behavioral-based blocking. Relatedly, signature-based detection is less effective when attackers are constantly changing tactics and contributes to the false positive issue we have discussed. Identifying the intent behind the request as opposed to waiting for the request itself to be recognized as malicious is important but must be done without generating false positives or increasing false negatives.

Figure 10. Top Attributes in a Web Application and API Security Solution



Source: Enterprise Strategy Group

The Bigger Truth

The best-of-breed versus platform pendulum has swung back and forth in the security space for years. As new threat vectors and security concerns arise, new tools are introduced until the market reaches a tipping point and begins to look to consolidation for operational improvements. In some ways, the application security space is no different. As applications have moved to the cloud, begun to leverage APIs, and become targets of malicious bot attacks, tools have been added, bringing us to the inflection point at which we are currently.

However, rather than making the choice between strong, effective security and a consolidated approach, the criticality of applications to the modern enterprises requires solutions fulfilling both requirements. Application security ownership has become democratized, with application development teams playing a larger role than ever. Web application and API security solutions must be easy for these groups to deploy, without causing friction to their workflows and processes. Separately, the fact that traditional approaches have become so ineffective at preventing attacks and generate false positives that pull critical applications offline should set off alarm bells for any application-centric business.

To address these issues, unified solutions must offer strong API protection, coverage for different architectures, integration with DevOps tools and processes, and strong security efficacy through advanced detection methods including behavioral-based blocking. The adoption of these solutions should be seen not only as an avenue towards improved security, but as a competitive differentiator as well. By adopting more effective and efficient web application and API security solutions, application teams can spend more time on their core competencies—creating and optimizing applications for the business—while security teams focus on preventing legitimate attacks rather than responding to false-positive noise. In this sense, web application and API security modernization should be seen not just as a security priority, but a business imperative.

Appendix: Research Methodology and Demographics

To gather data for this report, ESG conducted a comprehensive online survey of information security and IT professionals knowledgeable about their organization's application development practices and involved in security purchase processes (61%). The survey also included developers, engineering, and DevOps leaders who build and deliver applications for their organization (39%). Respondents were distributed across North America (41%), Europe (30%), and Asia Pacific and Japan (29%). Respondents were employed at organizations with 10 or more employees. Specifically, 10% were employed at small organizations (i.e., those with 10 to 499 employees), 15% at midmarket organizations (i.e., those with 500 to 999 employees), and 75% at enterprises (i.e., organizations with 1,000 or more employees). Respondents represented numerous industry and government segments, with the largest participation coming from manufacturing (23%), financial services (14%), retail/wholesale (14%), technology (11%), healthcare (8%), and communications (8%).

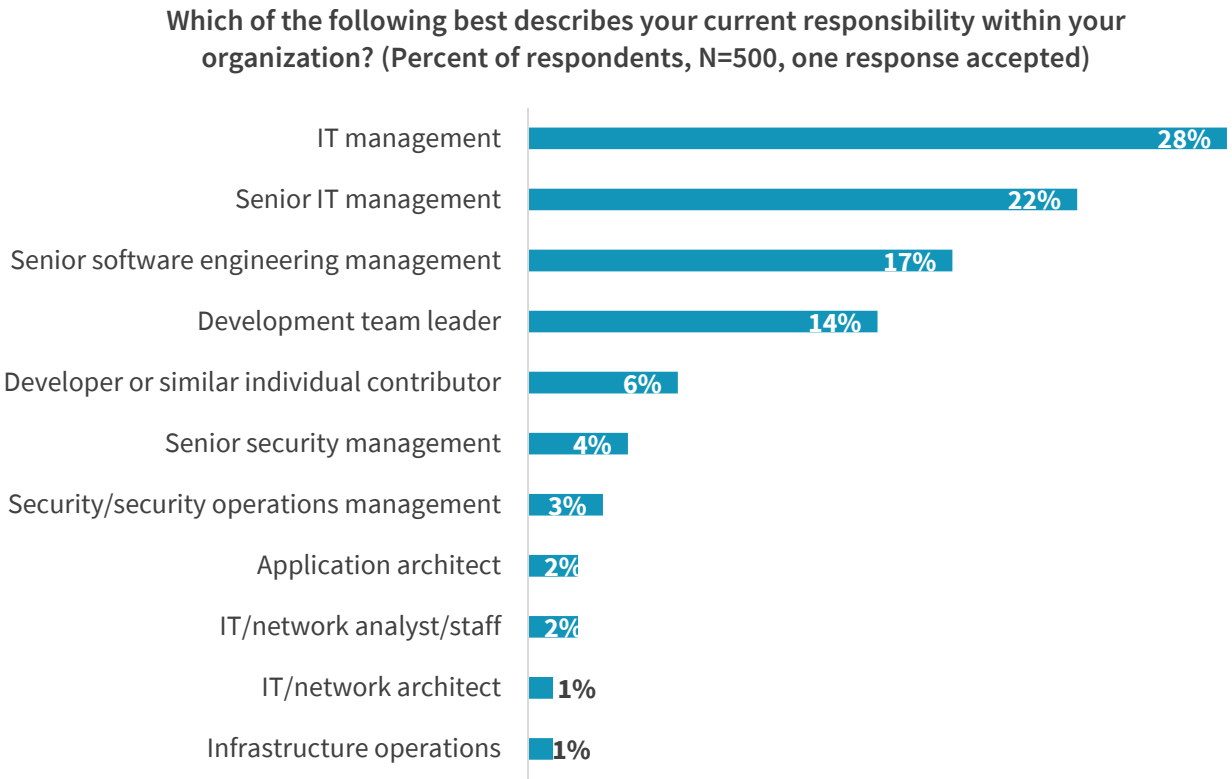
The survey was fielded between March 17, 2021 and March 31, 2021.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on several criteria) for data integrity, a final sample of 500 respondents remained.

All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents. Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

Figures 11 - 14 detail the demographics of the respondent base: individual respondents' roles, as well as respondent organizations' total number of employees, annual revenue, and primary industry.

Figure 11. Survey Respondents, by Current Responsibility

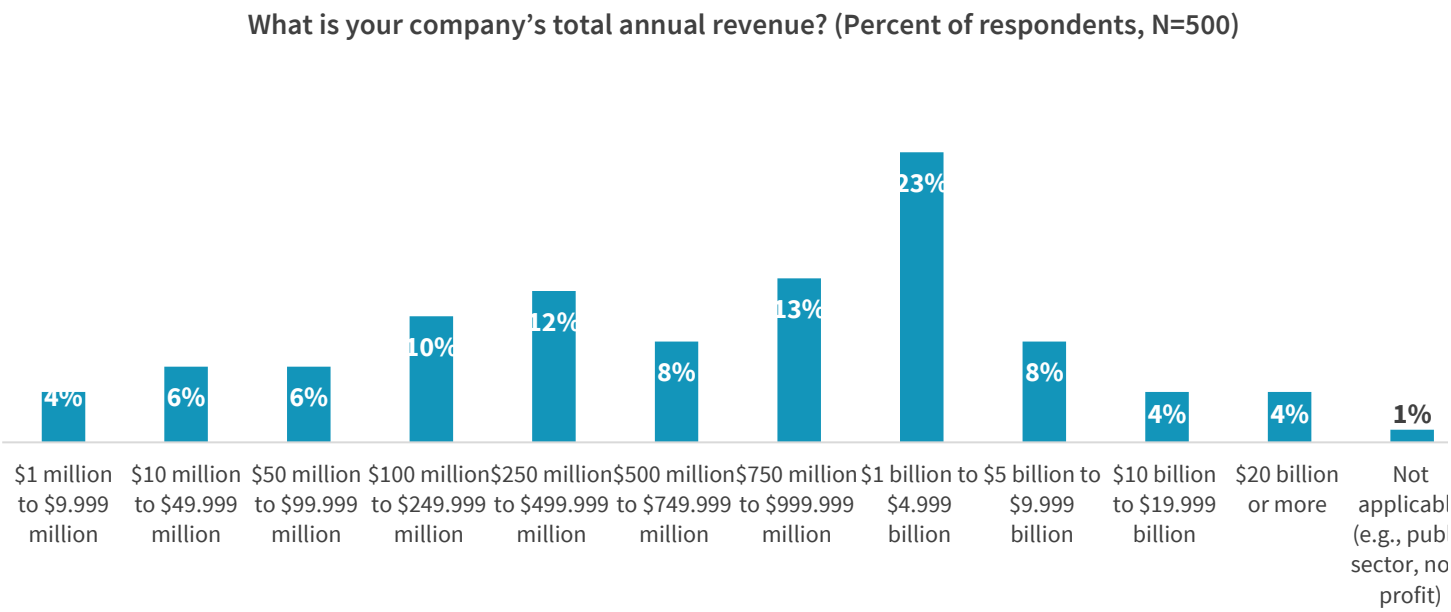


Source: Enterprise Strategy Group

Figure 12. Survey Respondents, by Company Size (Number of Employees)

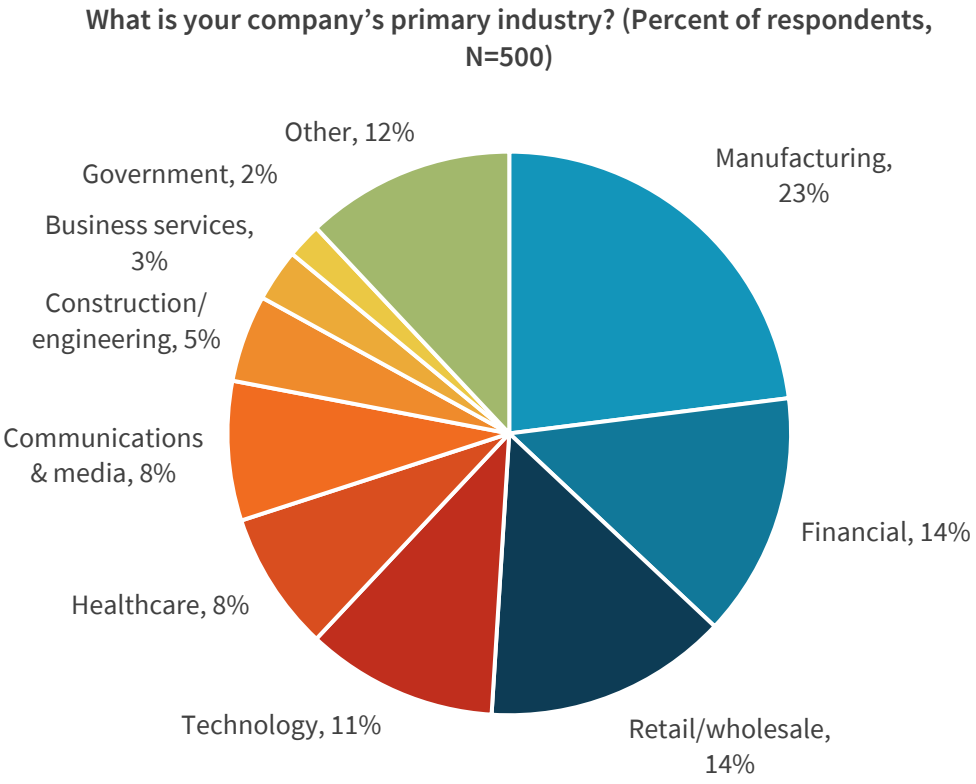
Source: Enterprise Strategy Group

Figure 13. Survey Respondents, by Company Size (Annual Revenue)



Source: Enterprise Strategy Group

Figure 14. Survey Respondents by Industry



Source: Enterprise Strategy Group

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.


www.esg-global.com


contact@esg-global.com


508.482.0188