

WHITE PAPER

Protecting Against Sophisticated Bot Attacks

Preventing Fraud and Abuse with F5 Bot Defense, Built on Google Cloud

By John Grady, Enterprise Strategy Group Senior Analyst

November 2022

This Enterprise Strategy Group White Paper was commissioned by F5 and Google and is distributed under license from TechTarget, Inc.

Contents

Executive Summary	3
Bots Have Become a Critical Threat Vector, but Many Struggle with Defense.....	3
The Impacts of Account Takeover	5
Balancing Security and User Experience	6
Intelligent Protection Against Sophisticated Bots Is Required	7
F5 Distributed Cloud Bot Defense, Built on Google Cloud	8
F5 and Google – Better Together	8
The Bigger Truth	9
Appendix: Research Methodology and Respondent Demographics	10

Executive Summary

Bot-generated attacks have risen in visibility, and defending against these attacks is now a priority for most organizations. Yet challenges persist in accurately identifying bot traffic; protecting a distributed, heterogeneous application environment from these attacks; and minimizing the impact to legitimate users while doing so. To address these issues, intelligent protection against sophisticated bots is a necessity. This should include strong analytics coupled with human expertise, a frictionless user experience, and consistent coverage across different architectures and platforms. F5 Distributed Cloud Bot Defense, built on Google Cloud, supports these requirements and can help prevent fraud and abuse against public-facing web applications.

Intelligent protection against sophisticated bots should include strong analytics coupled with human expertise, a frictionless user experience, and consistent coverage across different architectures and platforms.

To gain deeper insights into modern application trends and the associated security challenges organizations are facing, particularly around bots, F5 and Google commissioned TechTarget's Enterprise Strategy Group (ESG) to survey 150 North American information security decision makers knowledgeable about their organizations' cloud-hosted web applications and security strategies. Further details of the research methodology and survey demographics are presented in the *Appendix* of this report.

Bots Have Become a Critical Threat Vector, but Many Struggle with Defense

As the digital economy continues to expand, the role of web and mobile applications in connecting with prospects, engaging with customers, and driving revenue for the business has become critical. To enable the scale required in today's market, most organizations are turning to the cloud and working to modernize their application architectures. At the same time, attackers clearly understand the importance of these applications and the wealth of valuable information they hold and have continued to refine their methods to exploit gaps in security defenses.

Just as IT and security teams leverage automation to improve efficiency and effectiveness, attackers view bots as an avenue to scale attacks beyond the level they could reach manually.

While attackers use a variety of tactics to target web applications, one of the most common scenarios is the use of bots. Just as IT and security teams leverage automation to improve efficiency and effectiveness, attackers view bots as an avenue to scale attacks beyond the level they could reach manually. This has become a significant challenge for security

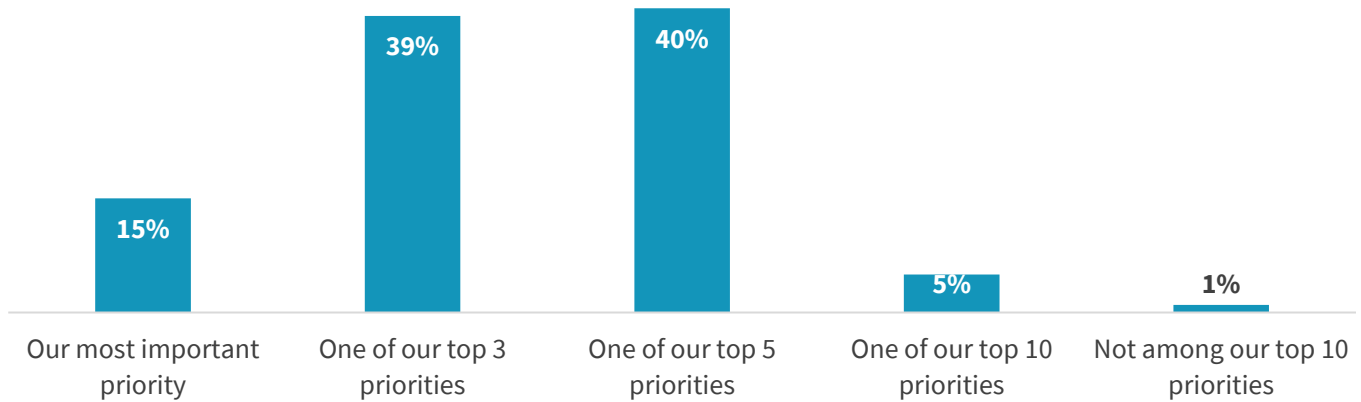
94% say defending public-facing websites and applications from bot-driven attacks is a top 5 priority.

teams. In fact, our research found that protecting public-facing websites and applications from bot-driven attacks has become a top cybersecurity priority for nearly all organizations (see Figure 1). Specifically, 15% of survey respondents say it is their most important security priority, 39% indicate it is a top-three priority,

and 40% report it is a top-five priority. With the range of issues and initiatives information security teams must address, including modernizing security access, implementing zero trust, and securing digital transformation initiatives, this is a telling finding.

Figure 1. Prioritization of Bot Defense

Relative to all of your organization's other security initiatives for the next 12 months, how much of a priority is it to protect its public-facing websites and applications from bot-driven attacks? (Percent of respondents, N=150)



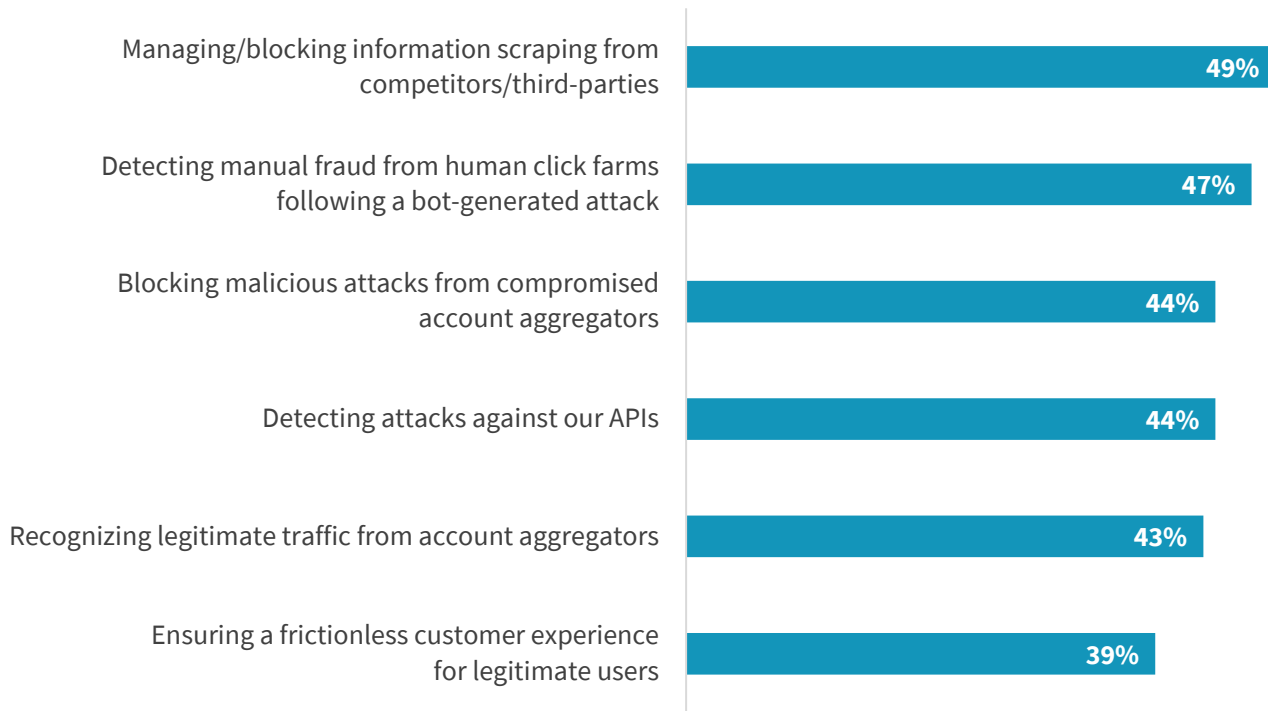
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The versatility of bots creates a variety of problems organizations must address (see Figure 2). Some of the specific challenges include:

- **Managing information scraping.** Nearly half (49%) cite managing or blocking information scraping as a challenge. While bots are typically highlighted for their use in overtly malicious attacks, they are often used to collect pricing or product information that can reduce a company's competitive advantage.
- **Correctly identifying account aggregators.** Account aggregators have become popular in the financial services industry to help customers centrally view and analyze their portfolio across a variety of providers. This can become an issue in the event of a compromise due to the broad access aggregators are often granted across accounts. Accurately detecting this type of fraudulent activity can be incredibly difficult, as highlighted by the fact that 44% of respondents said blocking attacks from compromised account aggregators was an issue, while 43% indicated that correctly identifying legitimate account aggregator traffic was a problem.
- **Protecting APIs.** APIs have become increasingly important as application ecosystems have grown and microservices have become prevalent. While bots continue to directly target applications, they are increasingly used against APIs. These can include denial-of-service attacks, scraping attacks, credential-based attacks, and attacks resulting in data loss. Overall, 44% of respondents reported that detecting bot attacks against APIs was a top challenge.
- **Maintaining a strong user experience.** A number of tools do exist to detect and prevent bot-generated attacks. Unfortunately, many can impact the user experience. Conversely, while more non-intrusive detection methods may be transparent to users, if they are not accurate and they result in false positives, legitimate user interactions may be blocked. This can create the same result, with a frustrated customer taking their business elsewhere.

Figure 2. Prioritization of Bot Defense

When thinking about bot-generated attacks, which of the following issues are most challenging for your organization? (Percent of respondents, N=150, up to three responses accepted per respondent)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The Impacts of Account Takeover

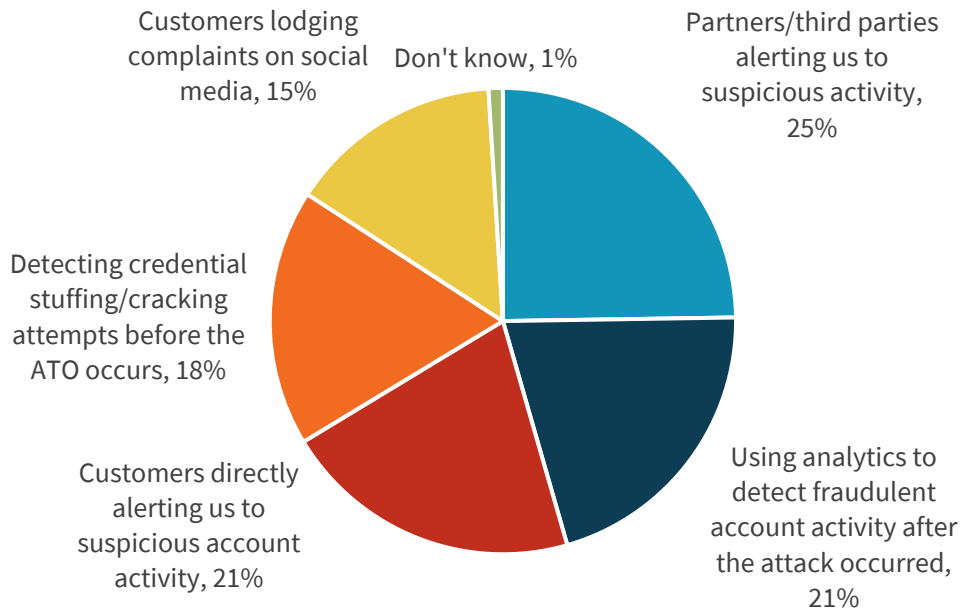
Account takeover (ATO) attacks have become one of the highest priority concerns among organizations managing both customer and employee logins. A variety of elements coming together have made these login applications an attractive and exceedingly exploitable target. The availability of stolen credentials on the dark web has steadily increased while password recycling and the use of weak passwords is widespread. Bots can be used to exploit these issues, allowing attackers to apply stolen credentials and variants to a variety of sites quickly with easily purchased credential stuffing tools in the hopes of finding a match and to do so at a scale that is impossible to achieve manually.

Importantly, these attacks can lead to a variety of downstream impacts. First and foremost, customer trust may be lost in the aftermath of an ATO. Additionally, if personal data is stolen, there may be legal or compliance issues as a result. Further, both direct and indirect financial impacts can result, ranging from the victim company having to cover the cost of fraudulent activity, to remediation costs, to lost revenue.

Unfortunately, many organizations are unprepared to detect these attacks early in the cycle, with more than half of the organizations surveyed (61%) indicating that they had detected, or would expect to detect, an ATO attack via external sources (see Figure 3). Specifically, 25% indicated they have or would expect to find out via partners, 21% from customers directly, and 15% from customers voicing complaints on social media. An additional 21% detect, or would expect to detect, attacks after they occur from analyzing fraudulent activity, at which point the damage has already occurred. Only 18% most often have, or expect, to detect attempted attacks before the ATO occurs.

Figure 3. How ATOs Are Detected

What has been, or would you expect to be, the typical way your organization learned about an account takeover (ATO) attack on its customer login application(s)? (Percent of respondents, N=150)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Balancing Security and User Experience

As noted, many organizations cite maintaining user experience as a challenge with bots. False positives are certainly an issue across cybersecurity. However, in many areas, they are a matter of inconvenience. Security teams can see efficiency impacted when they are forced to track down an inaccurate alert, and customers may be temporarily blocked from

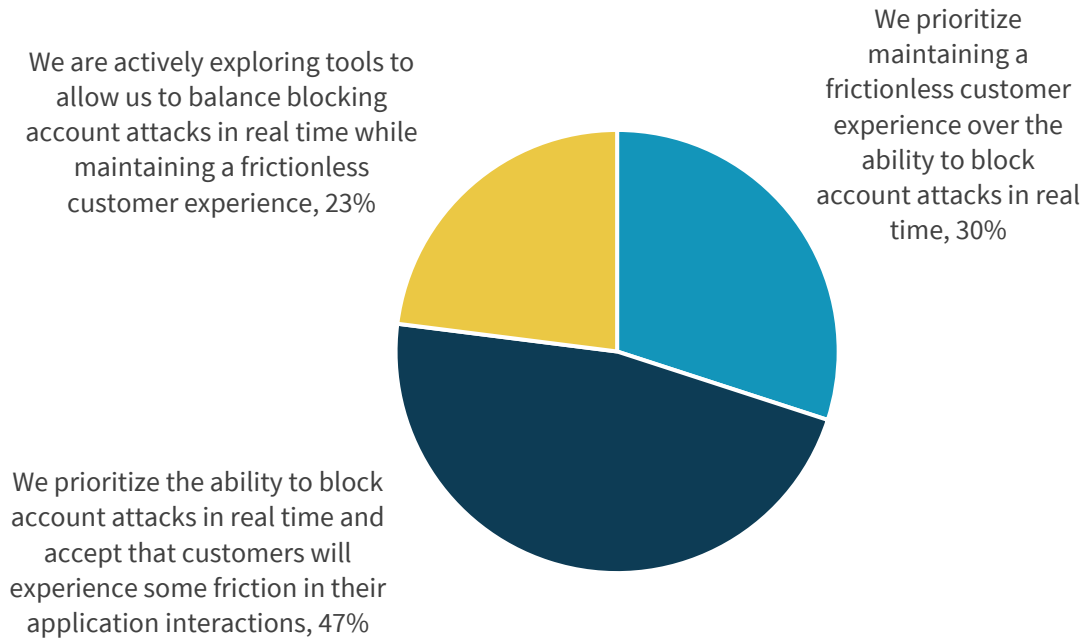
When legitimate users are blocked, the company reputation can suffer, customer loyalty can be impacted, and revenue can be lost.

accessing a resource. Yet, when dealing with public-facing websites, the equation changes significantly. When legitimate users are blocked, the company’s reputation can suffer, customer loyalty can be impacted, and revenue can be lost. So, it is unsurprising that 73% of our research respondents say false positives from application security tools are a critical or significant issue.

However, when asked about user friction with regard to detecting account attacks specifically, respondents were much more willing to err on the side of caution (see Figure 4). Nearly half of organizations (47%) prioritize the ability to block account attacks, even if that comes at the expense of additional customer friction. Conversely, 30% say they would prioritize a frictionless customer experience over the ability to block attacks in real time. Somewhat surprisingly, only 23% say they are exploring tools that will balance blocking ability with customer experience. This implies an expectation that achieving such a balance is hard to attain, and security teams will always have to decide between efficacy and experience.

Figure 4. Balancing Security and User Experience Can Be Difficult

With which of the following statements do you most agree? (Percent of respondents, N=150)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Intelligent Protection Against Sophisticated Bots Is Required

Consolidation and convergence are top of mind across much of the security space, and the application security segment is no different, with the shift toward web application and API protection platforms (WAAP). Yet, while consolidated solutions may help improve efficiency and simplify operations, increased efficacy is not always a given. This is especially true with regard to accurately detecting bot-generated traffic. As a result, bot protection requires purpose-built capabilities, informed by strong analytics.

This is not to say that bot protection cannot be part of a broader application security platform or should be siloed from WAF or API security tools. However, given their criticality in preventing attacks and fraudulent activity by bots, these capabilities cannot be a secondary consideration. With this in mind, security teams should prioritize the following attributes when evaluating bot protection tools:

Security teams should prioritize strong analytics, human expertise, frictionless user experience, and coverage across different architectures and platforms when evaluating bot protection tools.

- Strong analytics.** Bot detection has historically focused on analyzing the requesting device and browser. Unfortunately, attackers have evolved, and current generation bots often use legitimate browsers that can pass JavaScript challenges and other signature-based methods. Strong behavioral analytics supported by AI/ML, which can tie together a variety of telemetry sources, coupled with intelligence on how fraudsters operate, the tactics they use, and the targets they have interest in, have become table stakes in bot defense and help lead to better efficacy.

- **Human expertise.** While analytics are important, fraudsters are continually evolving, and human intervention is often required to understand broad changes in strategies, as well as specific tactical adjustments during prolonged and targeted attacks. Ideally, this human intervention is coupled with managed services support to help SOC teams more efficiently respond to attacks and overcome the skills shortage that many organizations face. Sophisticated retooling that adapts as criminals adjust their tactics can result in prevention rather than detection after the fact.
- **Frictionless user experience.** The goal of any bot prevention solution should be to ensure as few users as possible are impacted. Relying solely on tools that negatively impact the user experience will lead to frustrated users and may have difficulty detecting sophisticated bots. Ideally, AI/ML would be used as an initial detection mechanism to prevent bot attacks, with more intrusive methods applied suspicious traffic to reduce the impact to legitimate users.
- **Coverage across different architectures and platforms.** As important as efficacy is, organizations must be able to deploy tools where applications reside. With organizations increasingly adopting hybrid, multi-cloud infrastructure and microservices-based architectures, a bot protection solution must provide flexible deployment and licensing models to address a variety of application scenarios, as well as provide ease-of-use for better adoption.

F5 Distributed Cloud Bot Defense, Built on Google Cloud

F5, with the help of Google Cloud's robust offerings, enables organizations to mitigate the bot activity that leads to fraud and abuse with resilient, cloud-powered protection that adapts as attackers retool. F5's Distributed Cloud Bot Defense (formerly Shape Security) has a strong track record of delivering effective bot protection to some of the largest organizations in the world, including 48 of the Fortune 50. At its core, Distributed Cloud Bot Defense is an analytics platform that ingests billions of requests each week. This scope of visibility helps ensure accurate detections.

F5's Distributed Cloud Bot Defense (formerly Shape Security) has a strong track record of delivering effective bot protection to some of the largest organizations in the world, including 48 of the Fortune 50.

However, many attackers are extremely motivated and will retool an attack to attempt to compromise a specific target. F5's Distributed Cloud Bot Defense couples human domain experts with its AI/ML capabilities to detect these changes and continually block attacks, even as attacker tactics evolve. The solution can be enabled as part of F5's broader WAAP offering; integrated with its BIG-IP platform; and deployed to protect on-premises, hybrid, or multi-cloud environments.

F5 and Google – Better Together

F5 leverages a variety of Google Cloud services to power its AI-based, real-time fraud prevention capabilities. These include Google Cloud's BigQuery data analytics platform, TensorFlow machine learning platform, Google Cloud Dataflow and Pub/Sub data processing pipelines, along with the Google Cloud Kubernetes platform, compute, Cloud Storage, and networking capabilities.

Distributed Cloud Bot defense is available through a variety of channels for Google Cloud customers. The solution can be purchased via the Google Cloud Marketplace on a pay-as-you-go basis or on a custom basis for 1-, 2-, or 3-year terms. Additionally, customers can purchase software licensing directly from F5 and deploy software on the Google Cloud or leverage F5 enterprise license agreements for both VM- and SaaS-based deployments.

The Bigger Truth

Detecting and managing bot-generated traffic has become a complex, yet incredibly important IT issue. Identifying bot traffic is more difficult than ever. The impacts from malicious activity can be catastrophic, and more teams have a stake in ensuring it does not occur, including not only security, but also customer experience, web, marketing, and fraud and risk teams as well. The good news is that most organizations are putting a priority on protecting their web applications from bot attacks.

Yet, there is an important distinction between simply prioritizing defending against bots and putting effective protections in place that can not only address the broad range of bot attacks, but also do so accurately and without adversely affecting legitimate customers' experiences. F5's Distributed Cloud Bot Defense accomplishes this through the use of strong analytics, supported by human expertise, a frictionless user experience, and consistent coverage for heterogenous, multi-cloud environments. By coupling these capabilities with the resiliency, scalability, and procurement flexibility offered by Google Cloud, F5 offers a solution that should be considered by any organization seeking to modernize its protection against bot-driven attacks.

Appendix: Research Methodology and Respondent Demographics

To gather data for this report, Enterprise Strategy Group (ESG) conducted a comprehensive online survey of security decision makers knowledgeable about their organization’s cloud-hosted web applications and security requirements. Nearly two-thirds of respondents held senior IT or security titles (i.e., CIO, CISO, VP of IT/IS, or equivalent) while the remainder held middle management and staff titles. All respondents were based in North America and employed at organizations with 500 or more employees. Specifically, 26% were employed at midmarket organizations (i.e., those with 500 to 999 employees) and 74% 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 (25%), financial services (19%), healthcare/life sciences (12%), and technology (11%).

The survey was fielded between March 2, 2022 and March 8, 2022.

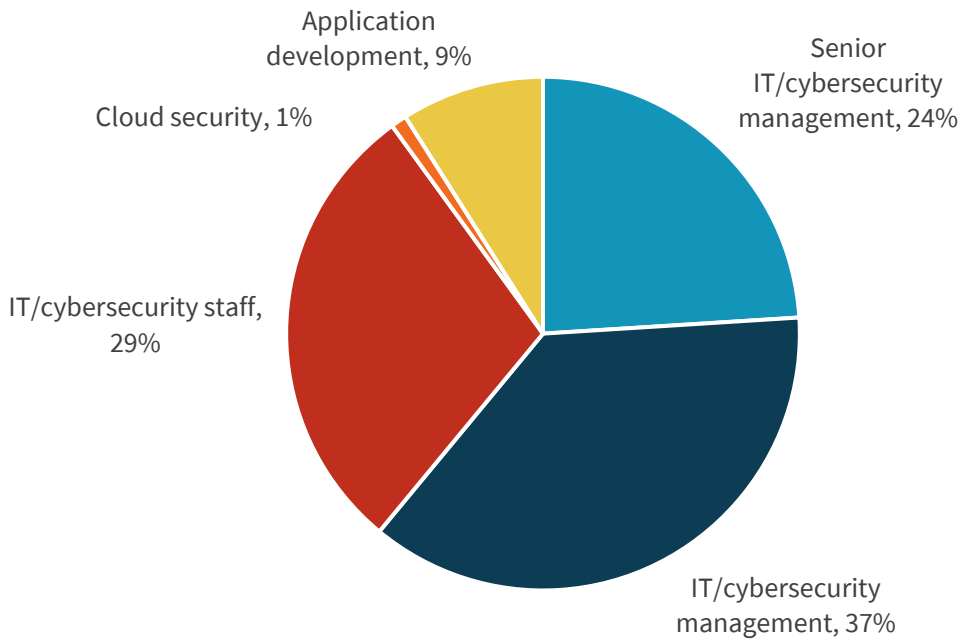
After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on several criteria) for data integrity, a final sample of 150 respondents remained.

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 5-7 detail the full demographics of the respondent base: individual respondents’ roles, as well as respondent organizations’ total number of employees, annual revenue, and primary industry.

Figure 5. Survey Respondents, by Current Responsibility

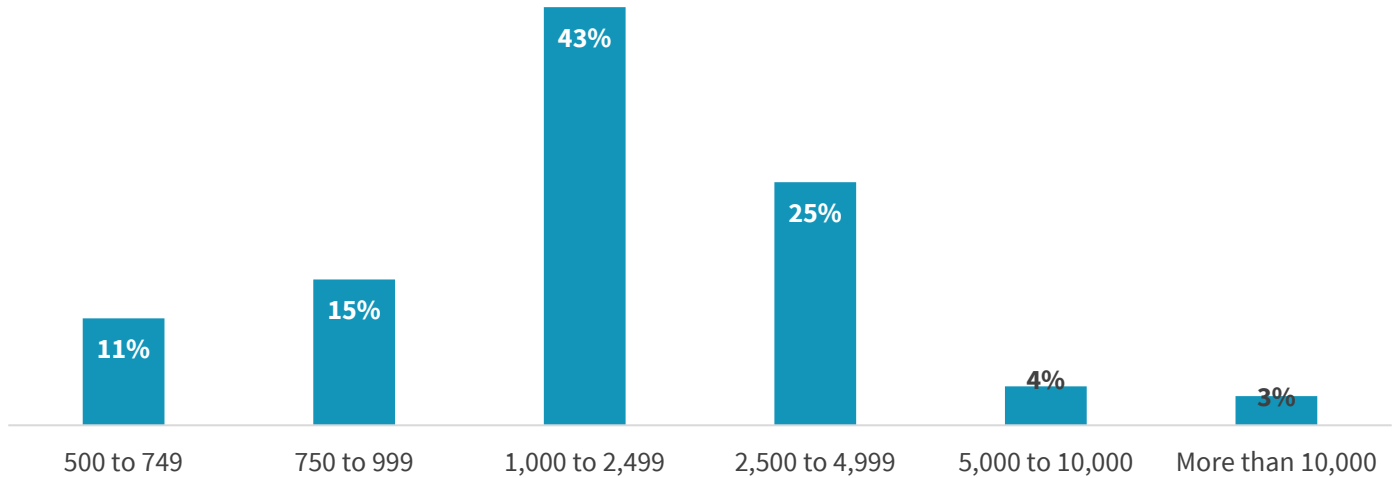
Which of the following best describes your current responsibility within your organization?
(Percent of respondents, N=150)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 6. Survey Respondents, by Company Size (Number of Employees)

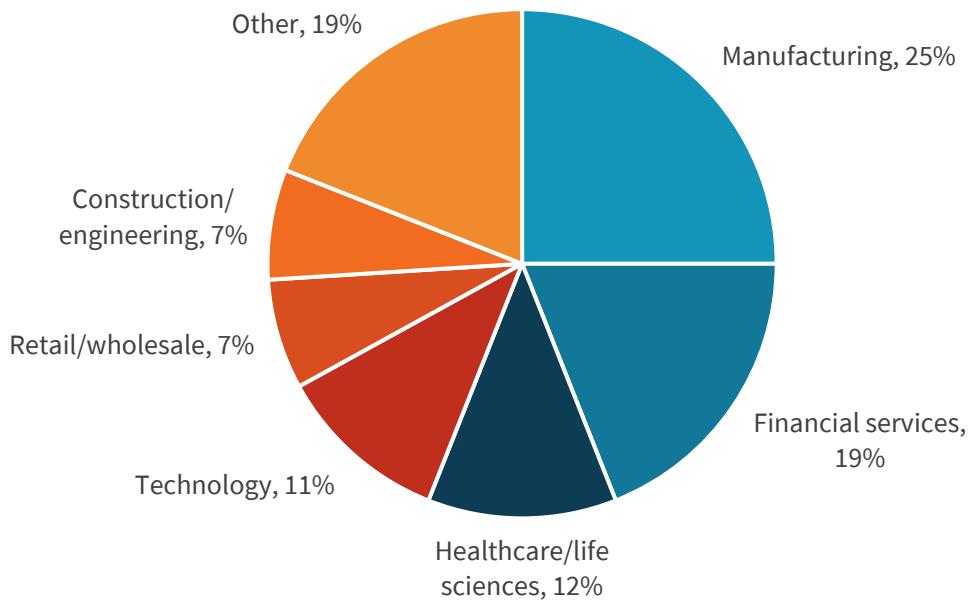
How many total employees does your organization have worldwide? (Percent of respondents, N=150)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 7. Survey Respondents, by Industry

What is your company's primary industry? (Percent of respondents, N=150)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.


This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.



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