A Forrester Consulting
Thought Leadership Paper
Commissioned By Google

January 2021

State Of Online Fraud And Bot Management

Protect Your Organization From Bot Attacks To Future-Proof Your Business

FORRESTER®

Table Of Contents

Project Director:
Ana Brzezinska,
Market Impact Consultant

Contributing Research:
Forrester's Security & Risk research group

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

Executive Summary

As the global economy continues to adjust to the new normal that the COVID-19 pandemic has created, businesses — especially B2C organizations with an online presence — have had to adjust to a surge in web traffic. More and more commerce has migrated to the web in a dramatic increase from pre-pandemic levels, where the growth was constant and steady. This increase in web traffic has translated to an increase in both good and bad automated traffic. Good automated traffic comes from approved partner applications and search engines, while bad traffic comes from malicious bot activity. Bots account for over half of all automated web traffic and nearly a quarter of all internet traffic in 2019, leaving professionals to thread the needle.[1]

As more and more commerce moves to the web, bot attacks are only continuing to increase, and the stakes become higher and higher for businesses. Many businesses believe that their piecemeal approach of denial-of-service (DDoS) protection, web application firewall (WAF), and/or content delivery networks (CDNs) is enough to manage bots. However, this approach leaves them woefully vulnerable to attacks. In fact, 81% of survey participants are not using a full bot management system, meaning that their internal teams are left tying together disparate systems into a cohesive approach. Recognizing these gaps in security, 75% of survey participants plan to increase their investment in bot management over the next 12 months.

Google commissioned Forrester Consulting to evaluate bot management approaches. To explore this topic, Forrester conducted an online survey with 425 respondents across the globe who have responsibility over fraud management, attack detection and response, and/or user data protection at their organization.

61% agree that there is more awareness across the company of the need to manage bot fraud.

KEY FINDINGS

- **Bot fraud is a growing concern throughout organizations.** From the C-suite to the on-the-ground teams, awareness of bot fraud is growing. But at the same time, so too is the recognition that these are not properly prepared to fend off attacks today.
- **Bot management suffers from a siloed approach.** Most organizations leave critical teams out of the bot management decisioning process, resulting in: 1) hundreds of hours of productivity lost to bot attack resolution and 2) losses of 1% or more of revenue per attack vector.
- **Bot attack frequency is expected to continue growing.** In recognizing that the number of bot attacks will increase over the next year, 75% of surveyed decision-makers plan to increase their organization's investment in bot management. Most recognize that reduced customer friction — which will improve customer experience (CX) — will be the top benefit from improved bot management.

Bot Fraud Is A Growing Area Of Concern — And Firms Are Not Prepared

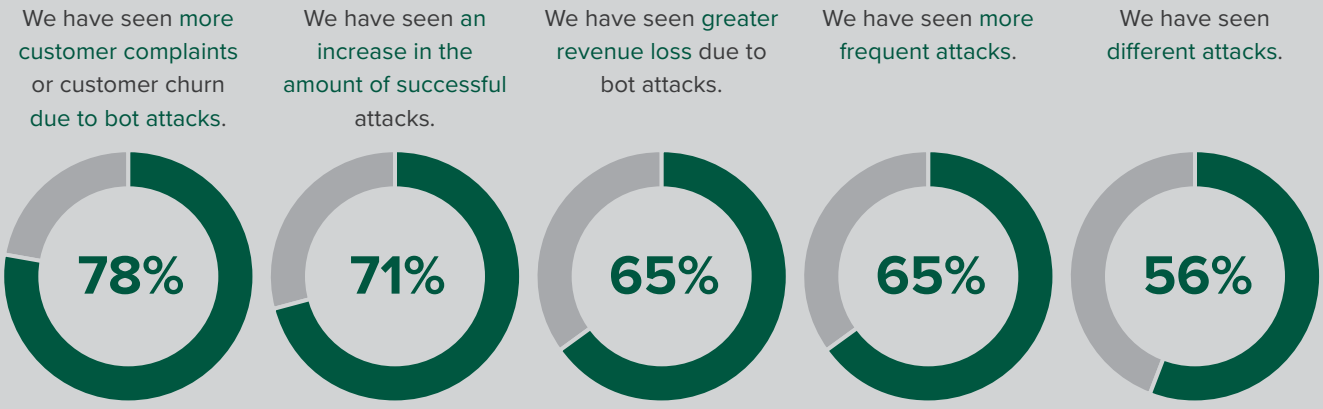
Across organizations, bot fraud is becoming a growing area of concern. Eighty-three percent of respondents agree that their organization believes that bot attacks are a problem, and nearly two-thirds noted that there is more awareness across the company of the need to manage bot fraud. And this awareness extends to the C-level as well: 52% noted that their executive team has asked about bot attacks within the last six months.

83% of respondents recognize that bot attacks are a problem.

- **Bot attacks are increasing in frequency.** Eight-four percent of companies have seen an increase in the number of bot-based attacks over the last year — and COVID-19 has only increased this number of attacks. As more commerce moves to online channels, businesses are seeing a marked increase in bot attacks. Two-thirds of surveyed decision-makers note that they have seen more frequent attacks since the pandemic began; 71% note that they have seen an increase in the amount of successful attacks; and 56% have seen different types of attacks since the beginning of the pandemic (see Figure 1).
- **Most organizations are underprepared to fend off bot attacks.** Seventy-eight percent of organizations are using DDoS protection, WAF, and/or CDNs to manage bots; only 19% are currently using a full bot management system. At the same time, on average, organizations are only protecting themselves against three different types of attacks — most commonly card fraud, ad fraud, and influence fraud attacks. This narrow approach leaves businesses open to a whole range of other bot-based attacks.
- **The majority of organizations are not protecting themselves against the most important and common attacks.** Only 15% of businesses are currently protecting themselves against web scraping attacks, yet 73% face such an attack on a weekly basis. And 63% report losing between 1% and 10% of their revenue to web scraping attacks alone (see Figure 2). Many businesses focus on the types of attacks that are mostly commonly in the news, rather than the attacks that can cause the most damage to their bottom lines.

Figure 1

"Which of the following, if any, impacts have the COVID-19 pandemic had on your organization?"

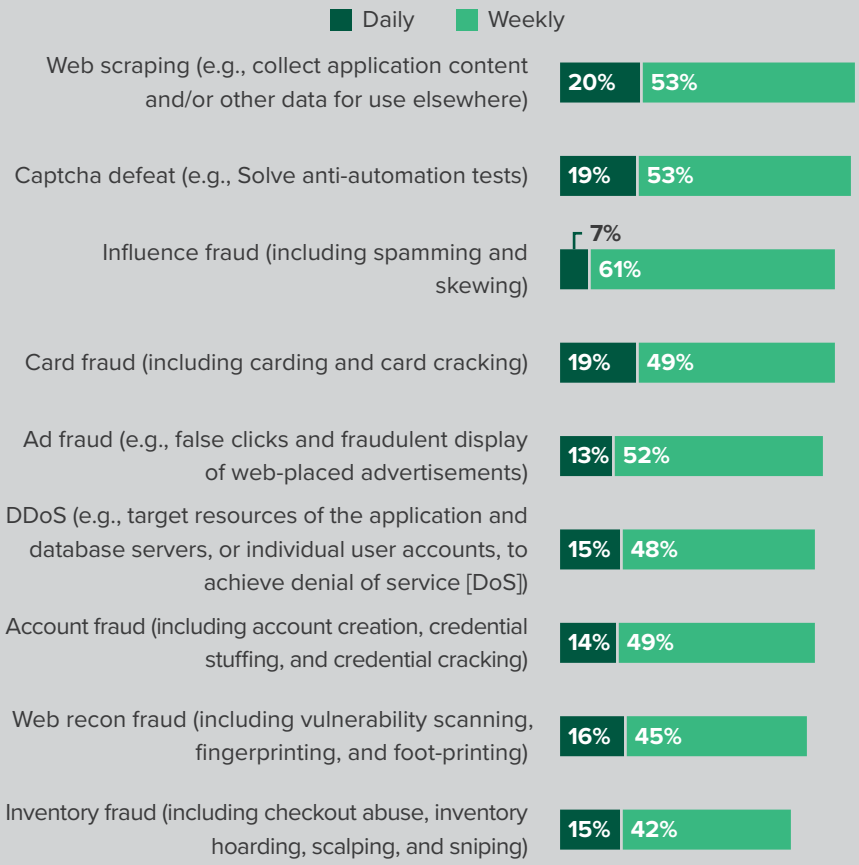


Base: 425 global CIOs/CISOs, product managers, and anyone with ownership for information security related to user data
Source: A commissioned study conducted by Forrester Consulting on behalf of Google, November 2020

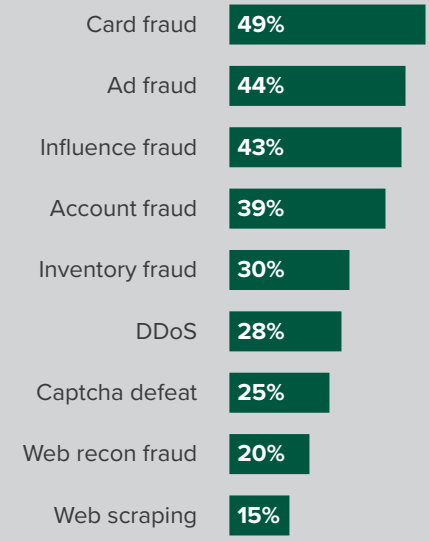
FORRESTER®

Figure 2

Top 5 Most Frequent Attack Types



Percent Currently Protecting Against Those Attacks



Financial Impact Of Those Attacks

Base: 425 global CIOs/CISOs, product managers, and anyone with ownership for information security related to user data
Source: A commissioned study conducted by Forrester Consulting on behalf of Google, November 2020

FORRESTER®

Most Firms Lack The Holistic Approach Needed To Prevent Bot Fraud

Despite the acknowledgement of the prevalence and persistency of bot attacks, many organizations struggle to contain bot attacks. Businesses spend hundreds of hours remediating attacks instead of proactively threat hunting, because often they use a collection of preventative measures, rather than a complete bot management system.

- **Good bot management requires a holistic company approach.** While most agree that their security, CX, e-commerce, and/or marketing teams should be actively involved in bot management decisions, few organizations actually involve all of these teams. In fact, on average, only two teams are involved in the bot management decision-making process (see Figure 3). Most commonly, application security teams and security operations teams lead the charge. However, it's the e-commerce, fraud, and network security professionals that most commonly consume the data from bot management tools. This disconnect means two things: 1) Capabilities desired by the e-commerce or fraud teams are left out of final bot management decisions and 2) oftentimes, work is being duplicated across the teams because of silos.
- **Most organizations do not have a formal policy to manage and respond to attacks.** Only two in five organizations have a formal (i.e., written down and shared widely) policy to manage bots and bot fraud response. The lack of a cohesive approach to manage and respond means that, on average, firms are spending 424 hours — 53 working days — across roles resolving the situation after an attack.

Figure 3

Top 3 Teams Most Likely Involved In Bot Management Tool Decision-Making

48% Application security teams

45% Security operations teams

41% E-commerce teams

Top 3 Teams That Administer Or Consume The Data From Your Bot Management Tool

59% E-commerce pros needing to understand impact of attacks on their revenues

58% Fraud pros needing to understand and respond to fraudulent activities resulting from attacks

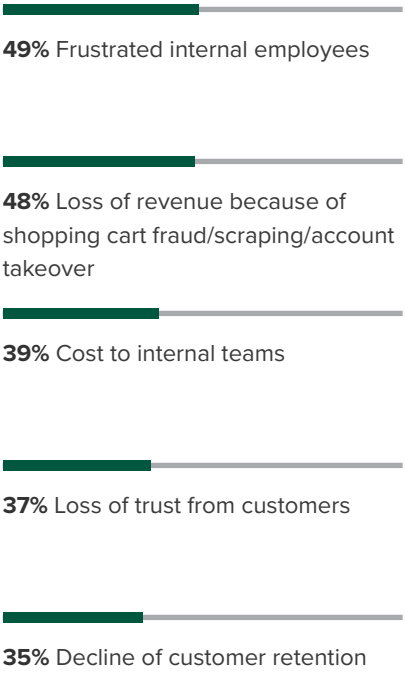
54% Network security pros configuring the product to respond to attacks

Base: 425 global CIOs/CISOs, product managers, and anyone with ownership for information security related to user data
Source: A commissioned study conducted by Forrester Consulting on behalf of Google, November 2020

- **Frustrated internal employees are the top result of bot attacks.** Before even loss of revenue, surveyed decision-makers noted that the top result of bot attacks is frustrated internal employees (see Figure 4). Spending almost two working months to resolve attacks means that employees' time is tied up in the minutia of attack resolution, rather than on more high-level strategic work. At a time when finding and retaining security talent is already challenging, incidents like these, that distract employees from strategic work, are another threat to the security team's goals and continuity. On top of that, many businesses report a loss of revenue because of shopping cart fraud, scrapping, and/or account takeover — in fact, over half of all retail businesses report experiencing a loss of revenue because of bot attacks.
- **Current approaches to bot management leave businesses playing whack-a-mole.** Fifty-six percent of decision-makers note that their fraud management team struggles to keep up with the volume of attacks, and nearly two-thirds of the survey pool noted that they are unable to do proactive threat hunting, since they are tied up in the day-to-day management of bot attacks (see Figure 5).

Figure 4

"To the best of your knowledge, which of the following are you experiencing as a result of these bot attacks?"



Base: 425 global CIOs/CISOs, product managers, and anyone with ownership for information security related to user data
Source: A commissioned study conducted by Forrester Consulting on behalf of Google, November 2020

Figure 5

"Which of the following challenges does your organization face?"

Base: 425 global CIOs/CISOs, product managers, and anyone with ownership for information security related to user data
Source: A commissioned study conducted by Forrester Consulting on behalf of Google, November 2020

FORRESTER®

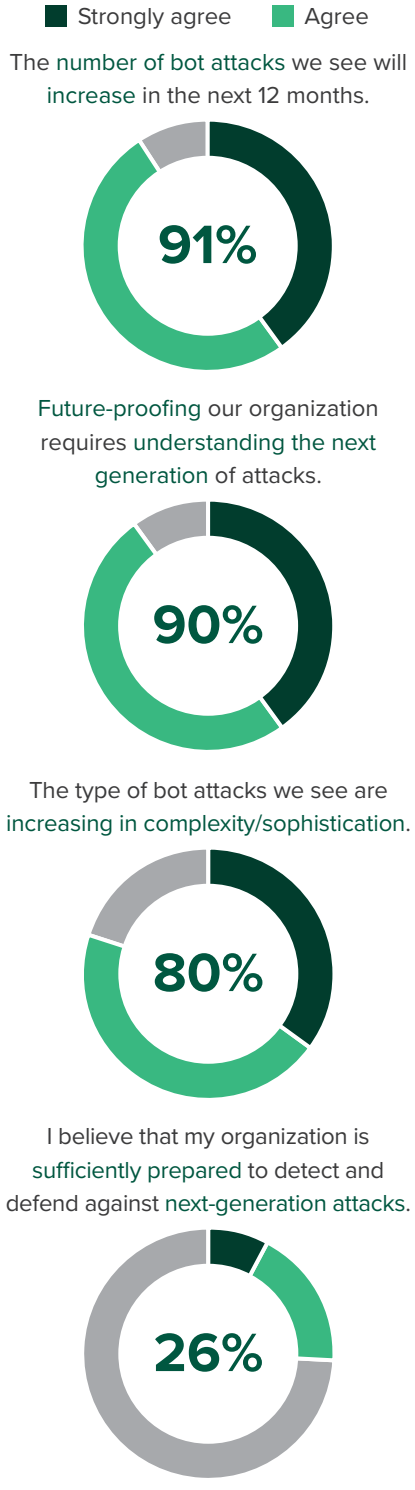
Future-Proofing Your Business Requires A Cohesive Bot Management Approach

As more and more commerce is executed through online channels, bot attacks will only continue to increase in frequency and severity. Ninety percent of decision-makers recognize that understanding the next generation of attacks is critical in the quest to future-proof their organizations. To level up their bot management, businesses must look to a complete bot management solution, rather than piecemeal approaches.

- **The future of successful business relies on understanding and managing bots.** Bot attacks are not going away: 91% of respondents recognize that the number of bot attacks they see will increase in the next months. Eighty percent note that the types of attacks they are seeing are increasing in complexity; and only 26% agree that their organization is sufficiently prepared to detect and defend against next-generation bot attacks (see Figure 6).
- **Businesses are ready to invest in bot management to help bridge the gap.** Recognizing the gulf between today's approaches and tomorrow's attacks, 75% of decision-makers have noted that they expect to invest more in bot management over the next 12 months than they have in the past 12 months. And C-level executives are on board: Only one-third of organizations anticipate an executive team roadblock, meaning that for two-thirds of organizations, the C-level is ready to back these investments.
- **Improving CX is the top anticipated benefit of improving bot management.** At its core, bot fraud is fundamentally an attack on your customer — they are unable to purchase the goods they want, get the groceries they need, or access the information they require. By investing in an improved bot management system, 72% of decision-makers anticipate reduced customer friction, followed by reduced fraud (62%), and improved analytics into sales/ad campaigns (58%).
- **Similarly, decision-makers are looking to invest in a tool that improves CX.** Improving security and detecting threats are naturally the top two capabilities that decision-makers look for in a bot management system. However, improving CX was the third most highly rated priority for business leaders. Improving bot management and improving CX are fundamentally linked: As you improve your organization's ability to detect and respond to bot attacks, your customers have a better experience navigating your site. And critically, Forrester has noted that there is a direct line between improving CX and growing your bottom line — for every 1-point improvement in a retailers' CX score, they can anticipate a $523 million increase in incremental revenue.[2]

Figure 6

"Please state your level of agreement with the following statements."



Base: 425 global CIOs/CISOs, product managers, and anyone with ownership for information security related to user data
Source: A commissioned study conducted by Forrester Consulting on behalf of Google, November 2020

FORRESTER®

Key Recommendations

Organizations are struggling under the weight of evolving bot attacks, and it's good news that firms are ready to invest in better solutions. To drive success in your bot management programs, you must:

Use the bot challenge to break down organizational silos. Bots impact security, fraud, marketing, e-commerce, and executive stakeholders. Align across these different teams to understand your organization's bot risk and enumerate requirements for a bot management solution. Ensure that marketing and e-commerce teams notify their security and fraud teams about upcoming campaigns and sales events that could lead to bot attacks. Send both weekly and ad hoc reports on bot trends and particular bot incidents to all concerned parties.

Make the leap to a holistic bot management solution. WAF and DDoS solutions won't protect against the business logic attacks associated with ad fraud, inventory hoarding, low and slow credential stuffing, and web scraping attacks. Look for a bot management solution that can detect even the most sophisticated bots, keep up with bots as they evolve to evade detections, and employ a range of responses to deflect the attacks. Consider the impact of your chosen solution on your customers' experience, and avoid adding friction to legitimate customer interactions. Also look for solutions that give your internal team quick visibility into bot traffic and enable a rapid response to bot attacks.

Expand bot protections to address a broader set of possible attacks. If firms are only protecting their organization against three types of bot attacks on average, they are still exposed to a range of bot-based threats. Even within a particular attack type, such as inventory hoarding, the types of merchandise considered valuable enough to hoard can change — as the coronavirus-inspired runs on hand sanitizer and toilet paper demonstrated. Make sure your bot management solution can address the full range of bot-based threats. Build bots into your risk assessments and at least quarterly, review the content, products, and services that your applications offer to identify any that could become desirable bot targets.

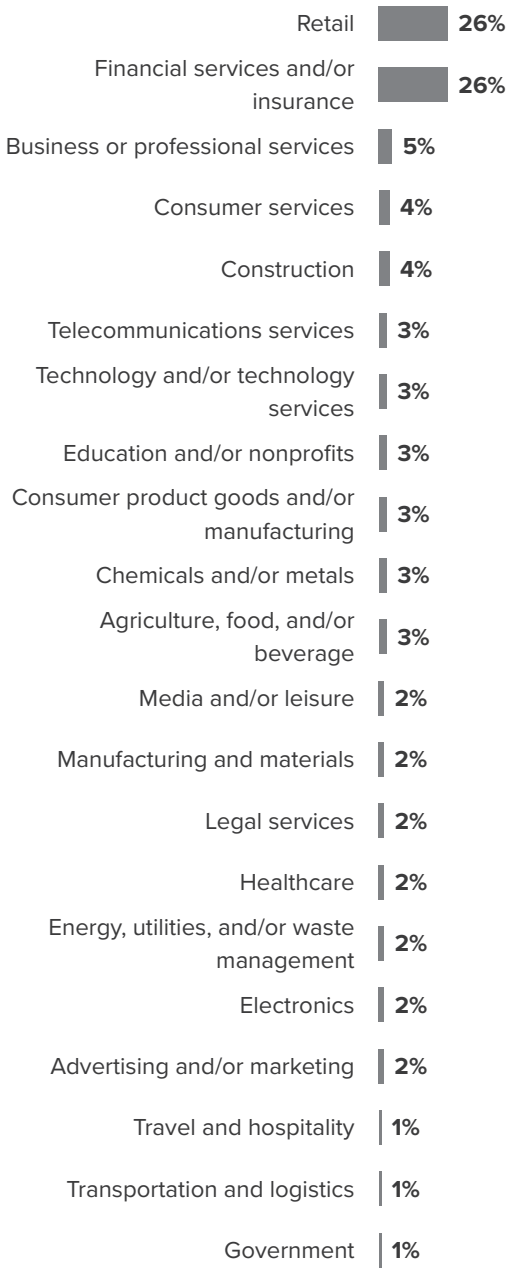
Keep customer experience and employee experience top of mind. Ultimately, a solid bot management response enables customers to effectively do business with your website and access the products and services they need without any friction. Track false positives and customer usage metrics carefully, and review those weekly to make sure that frustrating challenges aren't turning customers away. At the same time, continue to measure the number of bot incidents and internal response costs to track whether your bot management implementation is in fact reducing the number of incidents and the time your team spends in remediation.

Appendix A: Methodology

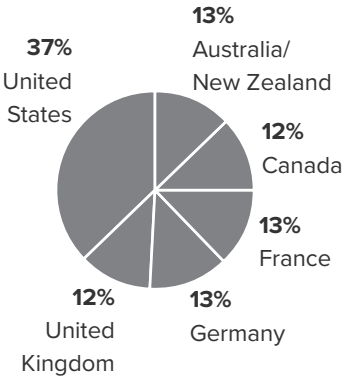
In this study, Forrester conducted an online survey of 425 global CIOs/CISOs, product managers, and professionals with ownership for information security that is related to user data across the globe. Survey participants included decision-makers in fraud management, attack detection and response, and/or user data protection. Respondents were offered a small incentive as a thank you for time spent on the survey. The study began in November 2020 and was completed in December 2020.

Appendix B: Demographics

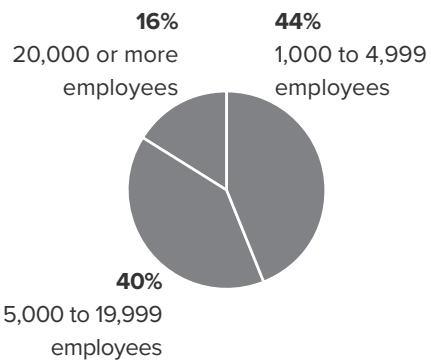
INDUSTRY



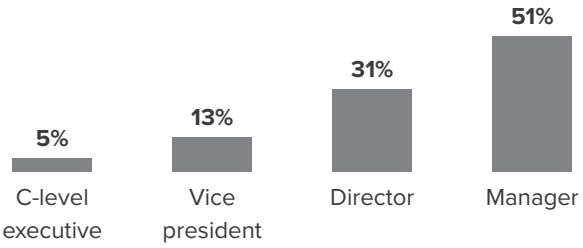
COUNTRY



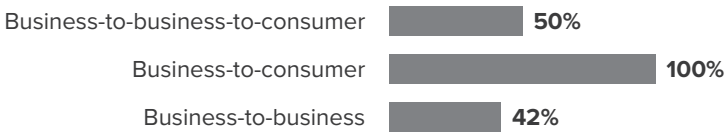
COMPANY SIZE



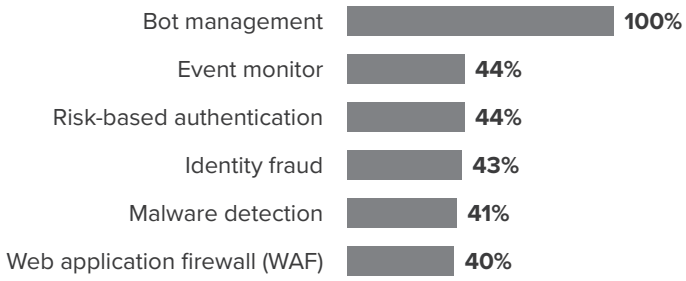
RESPONDENT LEVEL



BUSINESS MODEL



ANTIFRAUD TOOLS USED



Base: 425 global CIOs/CISOs, product managers, and anyone with ownership for information security related to user data
Source: A commissioned study conducted by Forrester Consulting on behalf of Google, November 2020

FORRESTER®

Appendix C: Endnotes

[1] Source: “New Tech: Bot Management, Q4 2019,” Forrester Research, Inc., December 13, 2019 and “The Forrester Tech Tide™: Application Security, Q4 2020,” Forrester Research, Inc., October 8, 2020.

[2] Source: “How Customer Experience Drives Business Growth, 2020,” Forrester Research, Inc., December 3, 2020.