Market Pulse

From Bad Bots to Malicious Scripts: The Effectiveness of Specialized Defenses

Modern digital businesses face an ever-growing array of threats, from bad bots and account takeover attacks to malicious scripts and audience hijacking attempts. A recent global survey from Akamai and Foundry investigated the prevalence and effectiveness of specialized third-party solutions that combat these challenges. Research findings show that not only are these technologies prevalent, but the companies using them have seen significant, quantifiable improvement in their ability to mitigate risk and prevent damage to the business – and to customers.

CSO

SPONSORED BY Akamai

Organizations of all sizes are digitizing their operations and business infrastructure to drive competitive advantage. They depend heavily on digital security measures and controls to prevent fraudulent and abusive behaviors online.

Akamai partnered with Foundry to investigate the effectiveness of specialized security measures against online fraud and abuse tactics, surveying more than 300 IT (47%) and security (53%) decision-makers.

These decision-makers came from a diverse group of companies: 45% had more than 5,000 employees while 97% had more than 1,000; industries included retail (48%), manufacturing, production and distribution of consumer-packaged goods and direct to consumer (39%), and travel and hospitality (13%).

The respondent pool was also globally diverse, with 32% from the US, 36% from Europe and 32% from Asia-Pacific (APAC).

Respondents were asked about the solutions they had in place for four broad categories of fraud and abuse: malicious bots, account takeover (ATO) attacks, script protection, and audience hijacking prevention.

Malicious Bots

Akamai sees tens of billions of bot calls daily, some of which are benign and many of which are malicious.

Three-quarters of survey respondents (75%) experienced malicious bot attacks in the last 12 months. Malicious bots can be used for a myriad of malevolent purposes. They're probably best known for monopolizing limited inventory, especially during high heat events – sneaker bots, for instance, corner the market on limited-edition athletic footwear – but these inventory-hoarding bots also snap up huge quantities of concert tickets and hotel reservations, and anything else perceived as valuable but of limited stock.

Bots can also scrape content from websites or launch credential-stuffing attacks that lead to account takeovers. They can overwhelm applications and websites with distributed denial-of-service (DDoS) attacks that prevent legitimate users from accessing web resources. Malicious bots make up a significant portion of today's internet traffic.

But even benign bots can diminish site performance and skew analytics. While activities such as content or price scraping aren't malicious, strictly speaking, they can slow performance, resulting in a degraded customer experience. It's important to have visibility into and control over all bot traffic. With this information, organizations can make better decisions on the actions they take to reduce friction for genuine customers.

Bot operators are constantly evolving their tactics and techniques to evade detection, so vendors must constantly adjust their countermeasures. Almost nine out of 10 (89%) use third-party or a combination of third-party and in-house solutions to combat malicious bots. These countermeasures were especially common in the US (96%) and Europe (93%). Just over eight in 10 (83%) had had a solution in place for longer than one year, with the US having the most longevity (89%).

54%

of those using third-party solutions to combat malicious bots report their cybersecurity capabilities have **significantly** improved since they began using these solutions.

Essentially all respondents (97%) reported an improvement in their efforts to combat bots, with more than half (54%) those using third-party solutions reporting their cybersecurity capabilities have improved significantly since deployment. Those in the consumer-packaged goods and retail sectors were the most likely to report improved

Figure 1 | **Those in the CPG and retail verticals are the most likely to report significant improvement in their ability to address malicious bots after employing specialized solutions.**

Change in cybersecurity capabilities since using specialized solutions to address malicious bots **(% reporting significant improvement)**

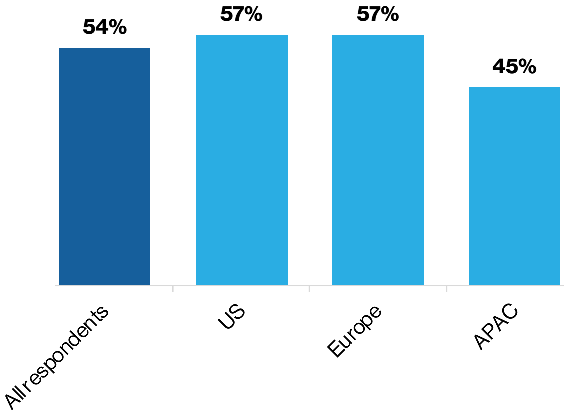


Figure 2 | **Nearly half (47%) indicate their ability to handle traffic surges has improved since they began using specialized bot management solutions.**

Areas improved from leveraging specialized third-party bot management solutions

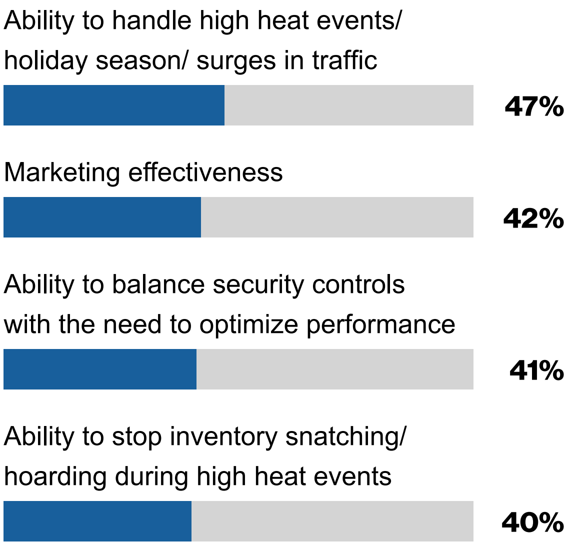
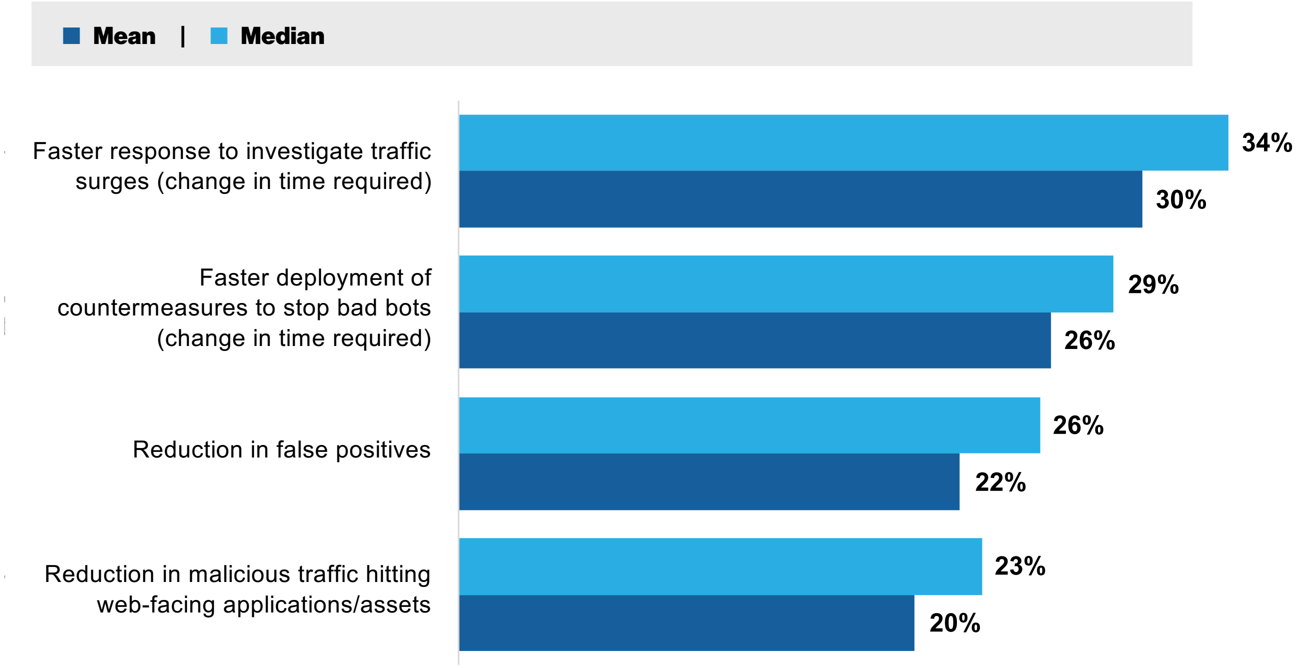


Figure 3 | **Respondents report that their response to investigate traffic surges is 30%-34% faster on average since employing specialized solutions.**

KPI improvement since implementation of specialized third-party bot management solutions



capabilities (60% and 54%, respectively), and companies in the US and Europe saw significant improvement (57%).

Of those who saw significant improvement, the top three capabilities and gains most frequently mentioned were:

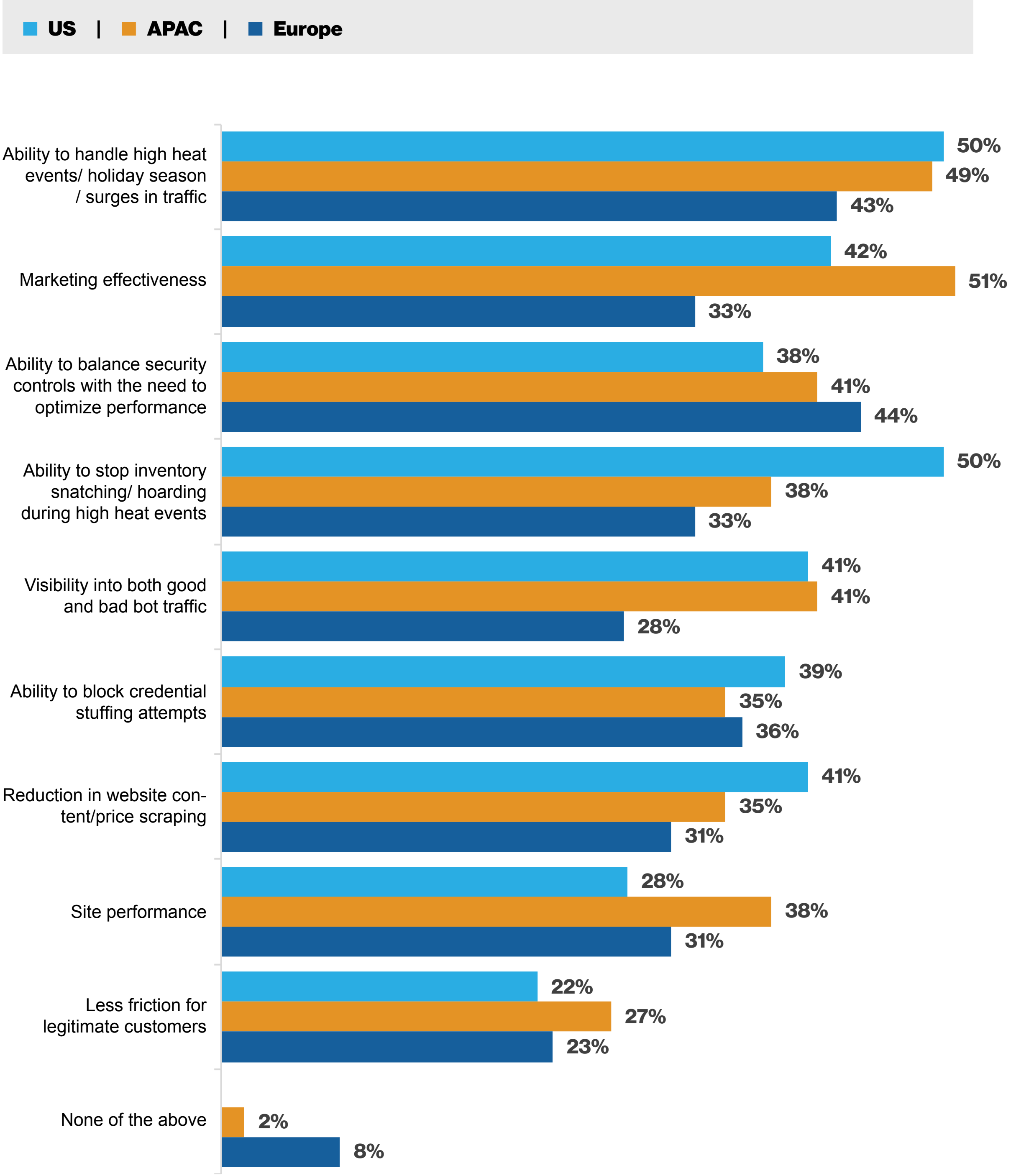
- **The ability to handle high heat events and surges in traffic: 47%**
- **An improvement in marketing effectiveness: 42%**
- **The ability to balance security controls with performance optimization: 41%**

Specialized bot management solutions also conferred significant business benefits. Companies saw, on average:

- **34% faster response to traffic surges**
- **29% faster time to deploy countermeasures to stop bad bots**
- **26% reduction in false positives**

Figure 4 | **Respondents in EMEA are more likely than other to note increased marketing effectiveness from leveraging specialized bot management solutions.**

Areas improved from leveraging specialized third-party bot management solutions



SOURCE: FOUNDRY

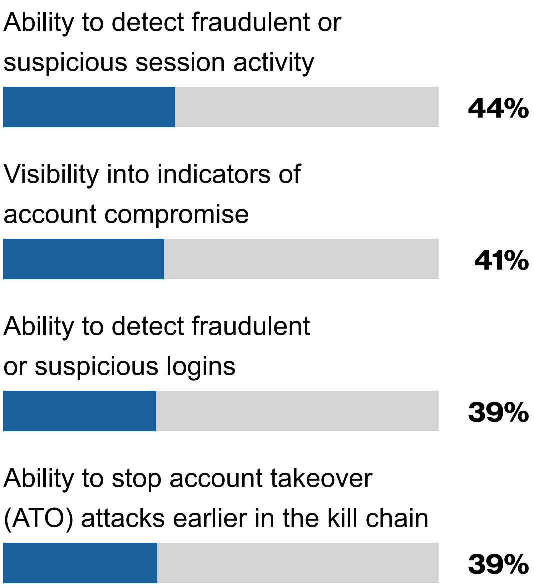
Account Takeover Attacks

ATO attacks are a huge problem for commerce organizations. More than three-quarters (79%) of respondents said their businesses had been targeted by ATO attacks in the last 12 months. The problem was particularly acute in the US, where 90% of respondents said their organizations had been targeted.

Cybercriminals use a variety of techniques to commandeer legitimate accounts. Once they control an account, they can siphon off loyalty points and transfer digital assets, drain gift card balances, and make fraudulent purchases using stored credit card information. They may even sell the entire account to another bad actor.

Figure 5 | **After employing specialized ATO solutions, respondents most frequently report better detection of suspicious activity and improved visibility into indicators of account compromise.**

Areas improved from leveraging specialized third-party ATO prevention solutions



Even unsuccessful ATO attempts are harmful. Credential stuffing involves the automated input of stolen username/password combinations across multiple sites. Hackers will also employ frequently used and/or easily guessed passwords against known accounts. The traffic these attempts generate can significantly reduce resource availability for legitimate users, resulting in slow response times – and unhappy customers.

Successful ATO attacks can destroy customer trust and seriously damage a brand's reputation. They also consume already-strained security resources.

The vast majority of respondents said their companies had countermeasures in place, using a third-party solution (83%) or a combination of in-house and third-party solutions (64%). Europe (95%) and the US (93%) are the two regions with the highest use of specialized solutions.

More than eight out of 10 (81%) of those who use specialized defenses to combat ATO attacks have had them in place for at least one year, with the US (85%) and Europe (87%) the most likely to have had solutions in place for at least that long.

Two-thirds of respondents said that their cybersecurity capabilities had significantly improved since deploying specialized ATO defenses, while 31% said they had somewhat improved. The most frequently reported gains by those who saw significant improvement were:

- **The ability to detect fraudulent or suspicious activity: 44%**
- **Visibility into indicators of account compromise: 41%**
- **The ability to detect fraudulent or suspicious logins: 39%**

Benefits of these account takeover prevention solutions included:

- **34% reduction time to be notified of suspicious activity**
- **33% reduction of online losses and claims**
- **30% reduction in internal staff time spent on fraud investigations**

Business outcomes differed significantly by region. APAC respondents were much more likely to report a reduction in financial losses after leveraging specialized ATO solutions (50%, compared to 33% in the US and 27% in Europe). European respondents were more likely to gain visibility into indicators of account compromise (50%, versus 41% in the US and 24% in APAC).

Figure 6 | Respondents report that the time it takes to be notified of suspicious activity has been cut by 28%-34% since implementing specialized ATO prevention solutions.

KPI improvement since implementation of specialized third-party ATO prevention solutions

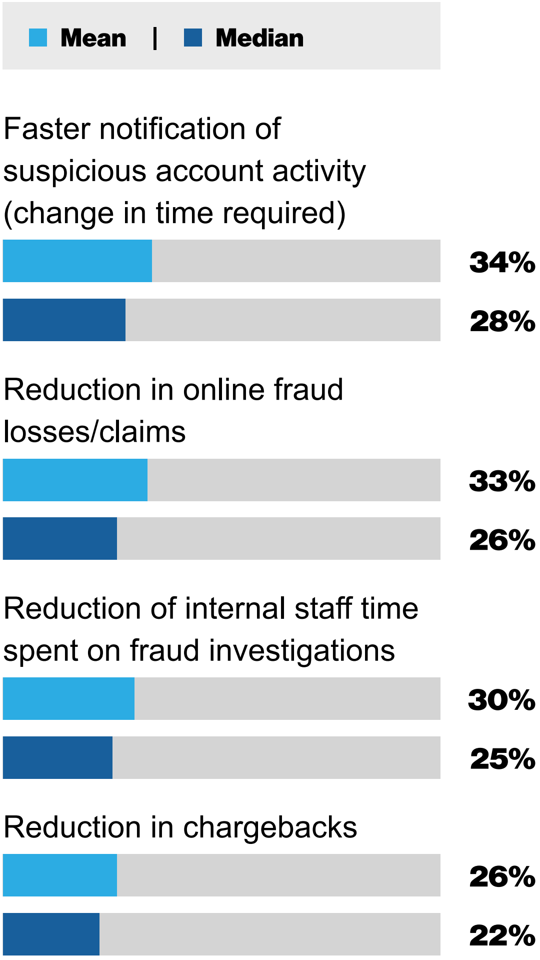
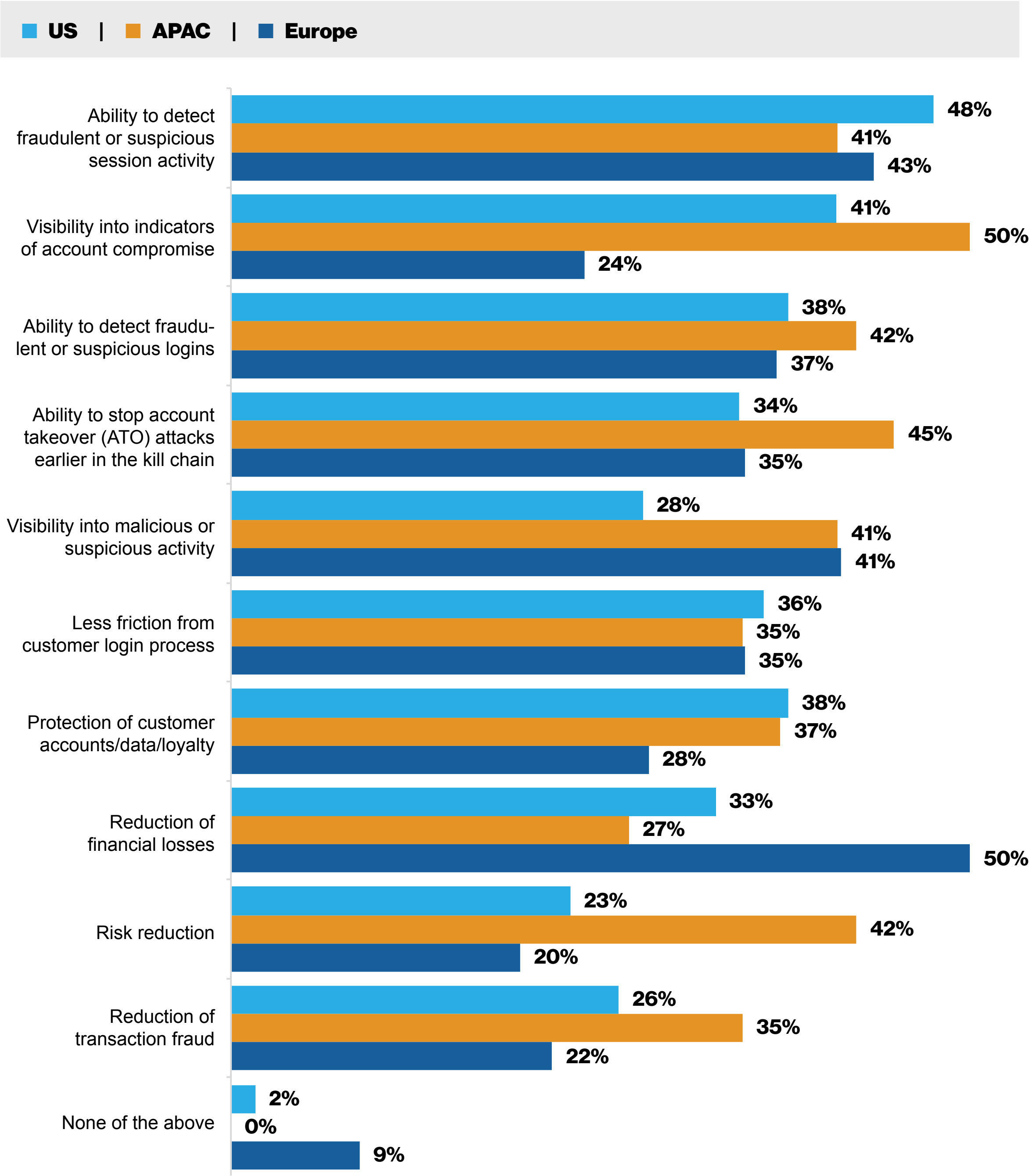


Figure 7 | **Respondents in APAC are more likely than others to report reduction in financial losses from leveraging specialized ATO solutions; those in Europe more often report risk reduction.**

Areas improved from leveraging specialized third-party ATO prevention solutions



Script Protection

The use of third-party scripts has dramatically risen over time, with over 94% of websites leveraging at least one third-party resource, according to the HTTP Archives' Web Almanac for 2021. Third-party scripts enable functionality, marketing tools, and analytics, and generally enhance the overall user experience (UX). They also come with significant security and privacy risks.

While bots and ATO attacks affect servers, malicious scripts represent a client-side threat. Because scripts are numerous and continuously changing, they can be extremely difficult to monitor, which makes the web browser a critical threat surface.

Script attacks can take various forms, such as web-skimming and formjacking. Entire criminal syndicates (most notoriously Magecart) have organized themselves around these kinds of techniques to steal payment card data and personally identifiable information (PII). Script attacks can cause significant financial harm for organizations and diminish trust with customers, partners, and payment processors.

The need for organizations to have client-side security in place is more critical than ever – especially on checkout and payment pages where personal and financial data is being collected. Organizations must have visibility into all scripts running on their site, the ability to detect suspicious behavior, and mitigation measures to defend against attacks.

Client-side security is a key focus of the Payment Card Industry Data Security Standard (PCI DSS v4.0). To comply, any organization processing payment cards online must know what scripts are running on their site, when they change, and when they stop running.

In-house, client-side security solutions like Content Security Policies (CSPs) do have downsides. They can be extremely tedious, and difficult for security teams to keep up with, are often not developer-friendly and can stunt innovation and degrade UX. So, it's important to balance security controls with performance, UX, and digital innovation.

The survey found that suspicious script behavior is common. More than eight in 10 (81%) respondents overall said their organizations have been targeted by suspicious script behavior within the last 12 months, with 94% of US respondents reporting targeting versus 72% in Europe.

Third-party specialized defenses are extremely common, with 85% saying they have such defenses deployed, either alone or in combination with in-house solutions to fight against suspicious script behaviors (57% use a combination). Just over three-quarters (76%) have had a solution in place for more than a year, with APAC seeing the lowest rate of longevity at 67%.

71%

of those using third-party script protection solutions have seen **significant reduction** in abusive script behaviors such as web skimming, form jacking, affiliate fraud, etc.

Essentially all (98%) of those using third-party specialized script protection solutions say their cybersecurity capabilities have improved at least somewhat since their deployment, with 58% saying that they'd seen significant improvement. The US was the region most likely to see improvement (65%).

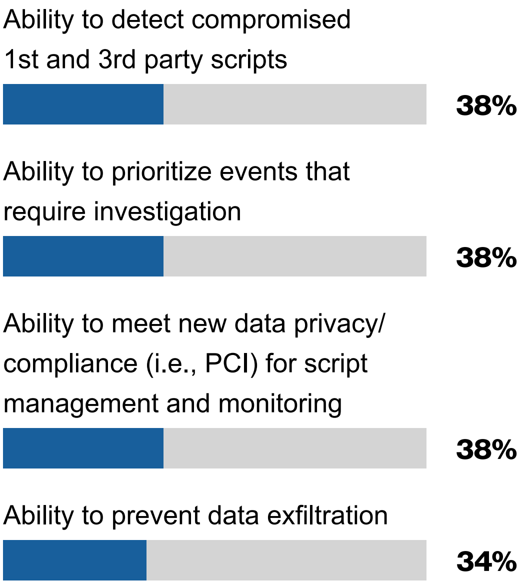
More specifically, 71% of those using third-party solutions saw a significant reduction in abusive script behaviors, with another 24% seeing moderate reduction. Of those who saw significant improvement, the three most frequently reported gains were:

- **The ability to detect compromised first- and third-party scripts: 38%**
- **The ability to prioritize events that require investigation: 38%**
- **The ability to meet compliance requirements: 38%**

Again, there were significant regional differences in benefits. For example, the US was far more likely to say that they were better able to prevent bad actors from executing and injecting malicious code into third-party JavaScript (41%) than Europe (27%) and APAC (24%). The US was also better able to meet new data privacy and compliance standards for script management and monitoring (47%), compared to Europe (35%) and APAC (29%).

Figure 8 | More than one-third (38%) have improved their ability to detect compromised scripts, are better able to prioritize suspicious events, and have a better ability to meet compliance requirements after employing script protection solutions.

Areas improved from leveraging specialized third-party script protection solutions

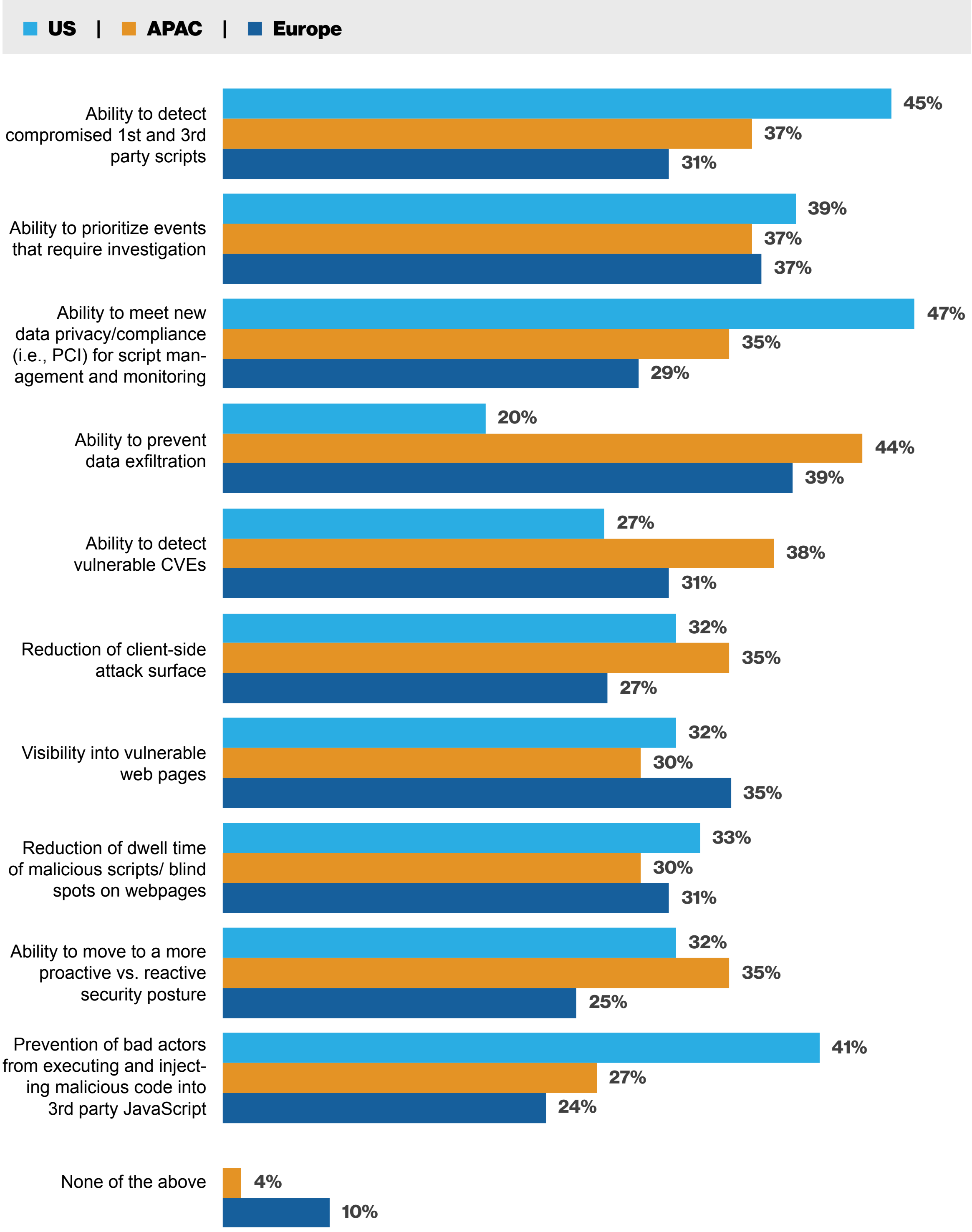


Specialized third-party script protection solutions also provide the following benefits:

- **30% reduction in the number of malicious or unwanted scripts requiring remediation**
- **28% faster time to update privacy controls**
- **26% reduction in script monitoring/ management workload**

Figure 9 | **Respondents in Europe and APJ are more likely than U.S. respondents to note an improved ability to prevent data exfiltration after using script protection solutions.**

Areas improved from leveraging specialized third-party script protection solutions



SOURCE: FOUNDRY

PHOTO BY YOUR

39%

of US companies said they had been affected by audience hijacking tactics – the highest amongst global respondents.

Audience Hijacking

Audience hijacking is an emerging but significant threat, and organizations already see its potential to do harm – 93% of respondents are familiar with the concept. Just over one-quarter (26%) said their organizations have been affected by audience hijacking tactics, with the US the most affected at 39%.

As another in-browser, client-side threat, audience hijacking is a risk that retailers need to keep top-of-mind. It occurs as a result of browser extensions, widgets, or other browser plug-ins that distract or divert a site visitor from a retailer's online buying journey.

Unfortunately, because audience hijacking occurs within browsers, retailers have limited visibility into its effects, including how often it occurs and its effect on key performance indicators. A window to in-browser script behaviors is crucial for retailers to understand how audience hijacking may be affecting their business.

Especially when economic times are tough, every sale counts. Users bring a lot of baggage with them on their local machine, as their browsers could have extensions that they either knowingly or unknowingly install. Retailers need to be able to identify when and how audience hijacking is occurring so they can take countermeasures to help protect their business – and their customers – from unwanted or malicious in-browser behaviors.

Audience hijacking has both customer conversion and security implications. While some extensions enhance the browser experience, others are

Figure 10 | **Most respondents (93%) report being aware of audience hijacking.**

Are you aware of a new cybersecurity challenge known as "audience hijacking"? **(% "YES")**

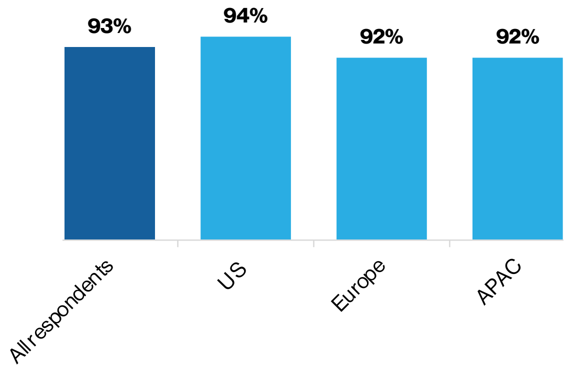
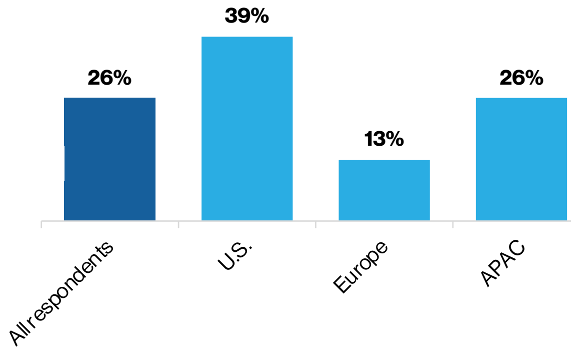


Figure 11 | **One-quarter (26%) of all respondents indicate their organizations have been impacted by audience hijacking in the past 12 months.**

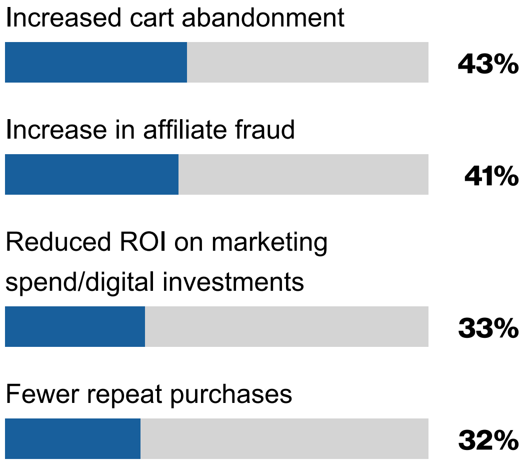
As far as you are aware, has your organization been impacted by audience hijacking within the past 12 months? **(% "YES")**



purpose-built to execute harmful activities. For example, a malicious actor can use a benign browser extension to push their own ads and move users out of competitors' conversion funnels, manipulate payment schema affiliates, or even steal PII.

Figure 12 | **The top impacts of audience hijacking include increased cart abandonment (43%) and increased affiliate fraud (41%).**

How has audience hijacking impacted your organization? (Among those impacted by audience hijacking)



In the survey, those who had experienced audience hijacking said the top two effects on their businesses were increased cart abandonment (43%) and increased affiliate fraud (41%).

Best Practices to Prevent and Combat Fraud

Detection is just the first step in combating online fraud and abuse. These attacks are often progressive in nature. Bot credential stuffing attacks, for instance, eventually lead to ATO if not nipped in the bud. Security must adapt to keep up with the latest threats and stop attackers earlier in the kill chain.

Adaptive security is the key to preventing more damage to revenue, brand, and customer loyalty. Security and antifraud teams need deeper, richer information, backed by threat research so they can take appropriate action. Legacy static approaches are not sufficient to meet the challenges of today's threat landscape.

Take "good" bots, for example: organizations need to define which ones they want to allow and which they want to slow down or block. Some bots may scrape information to, say, inform competitors of product pricing and availability. Companies may decide to deceive these bots into thinking they're getting the information that they want, but instead serve up data that's no longer relevant. Another strategy is to punish bots by increasing their compute burden, which makes them less efficient and more expensive for those running them.

There's a large opportunity to better understand these threats while improving business outcomes, but teams need visibility to make informed decisions. Getting that visibility almost always requires outside expertise.

Companies can't hire their way out of today's threat landscape. They must have the right specialized defenses and a partner with relevant – and recognized – expertise to optimize internal resources, and free them up to focus on driving growth, digital innovation, customer retention and profitability.

Malicious bots, scripts, and ATO attacks are pervasive and will continue to pose ever greater challenges for commerce organizations as digital innovation and investment drives competitive advantage and customer loyalty. Third-party specialized defenses that address unique challenges show exceptional effectiveness at mitigating and reducing the risk from online threats. It's critical for protecting both the brand and online revenue.

Akamai provides comprehensive bot, ATO, and script protection solutions on a platform that's designed for performance and scale. With Akamai as a partner, commerce organizations can focus on driving their business forward, confident that specialized solutions will protect revenue and brand loyalty while removing unnecessary friction from the path to purchase. ◆

To learn more about Akamai's bot, ATO, and script management solutions or to request a demo, **visit Akamai.**

The United States

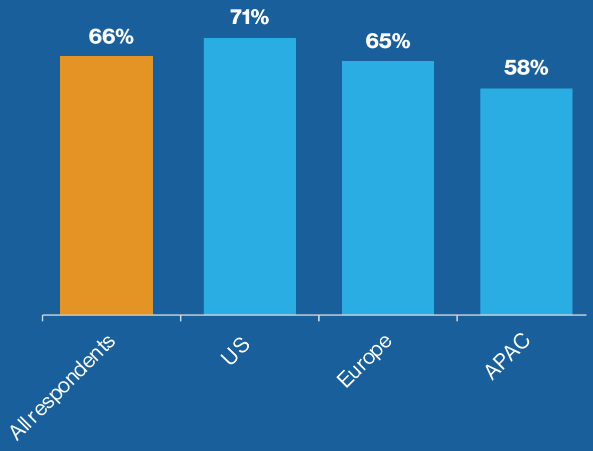
Generally speaking, the US faces the greatest threat level and has responded accordingly by deploying the highest rate of specialized defenses. Not surprising, the US is the most likely to see significant benefits from these solutions.

ATO

Nine in 10 organizations said they'd been targeted by ATO attacks within the last year, the highest rate of all three regions and well above the overall 78% response. More than 9 in 10 (93%) have deployed a specialized ATO solution – higher than the overall response rate (83%). More than 7 in 10 (71%) saw significant improvement in their ability to respond to ATO attacks (as opposed to 66% overall).

Figure 13 | Seven in ten respondents at US organizations (71%) report significant improvement in their ability to address ATO attacks since employing specialized solutions.

Change in cybersecurity capabilities since using specialized solutions to address ATO attacks
(% reporting significant improvement)



BOTS

The US faces the highest rate of bot attacks, with 88% having experienced an attack in the last year (well above the 75% overall response), and nearly all US organizations (96%) have a specialized solution in place, again the highest rate among the regions. It's also the most likely to have had a specialized solution in place for at least a year (83%).

Over half (57%) of US respondents saw significant improvement in their ability to address malicious bots after deploying a solution, tied with Europe and higher than the overall rate of 54%. Additionally, 42% saw improvement in their marketing effectiveness and 64% saw significant improvement in their website availability – the highest rate and well above the 55% rate overall.

SCRIPT PROTECTION

Almost every respondent (94%) was affected by suspicious script behavior over the prior 12 months, the highest rate and above the overall rate of 81%. The same percentage (94%) use specialized script protection solutions, tied with Europe and above the 85% overall rate.

Correspondingly, US companies have seen significant benefits: 65% say they've improved their cybersecurity capabilities (versus 59% overall) and 73% have seen a reduction in abusive script behaviors (versus 71% overall).

AUDIENCE HIJACKING

The majority of US respondents (94%) are aware of audience hijacking and nearly 4 in 10 (39%) have been affected by it (well above overall rate of 26%).

Europe

The threat level is high in Europe (though not quite as high as the US). European organizations have a high rate of deployment for specialized security solutions as well, and are seeing significant benefits as a result.

ATO

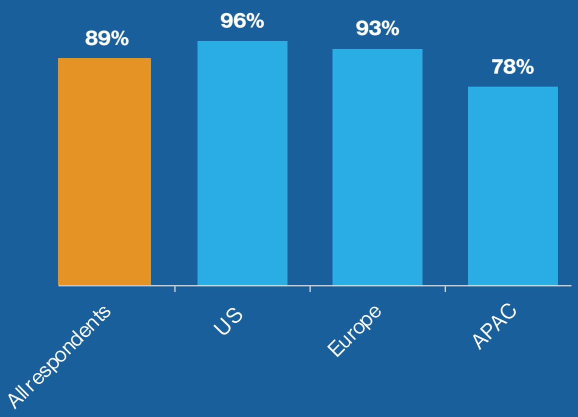
Just under three-quarters (73%) of organizations said they'd been targeted by ATO attacks within the last year, slightly less than the overall response (78%), and Europe is tied with the US for its rate of deployment of specialized ATO solutions. Most (65%) saw significant improvement in their ability to respond to ATO attacks – on par with the 66% overall response rate – and 42% saw significant risk reduction, well above the 30% overall rate.

BOTS

Nearly three-quarters (73%) of European respondents experienced bot attacks, a significant figure though slightly less than the 75% overall rate. European organizations are also very likely to have a specialized solution to deal with malicious bots (93%), compared to 89% overall.

Figure 14 | Use of specialized solutions to combat malicious bots is more widespread in the US and Europe when compared with APAC.

Use of specialized solutions to combat malicious bots **(% using third-party or a combination of third-party/in-house solutions)**



Europe was tied with the US in having 57% of respondents experiencing significant improvement in their ability to address malicious bots after deploying a solution (higher than the overall rate of 54%). Additionally, 51% saw improvement in their marketing effectiveness, the highest among the regions, and 60% saw significant improvement in their website availability, above the 55% overall rate.

SCRIPT PROTECTION

Though Europe had the lowest rate (72%) of organizations targeted by suspicious script behavior that figure represents a dangerous threat environment. As in the US, nearly all European organizations (94%) use specialized script protection solutions, higher the 85% overall rate.

Correspondingly, European companies have seen significant benefits: 56% say they've improved their cybersecurity capabilities (versus 59% overall) and 76% have seen a reduction in abusive script behaviors, the highest rate and above the 71% overall response.

AUDIENCE HIJACKING

Nearly all European respondents (92%) are aware of audience hijacking, but only 13% said they've been affected, the lowest rate and below the 26% overall rate.

Asia-Pacific

APAC's threat level is significant, but lower than Europe and the US. Accordingly, APAC has a lower rate of deployment for specialized solutions and has not seen the same level of benefit.

ATO

The ATO threat environment is high, with 73% saying they've been attacked in the previous 12 months (lower than the overall rate of 78%). APAC has the lowest rate of deployment for ATO solutions at 60% (much lower than the 83% overall rate).

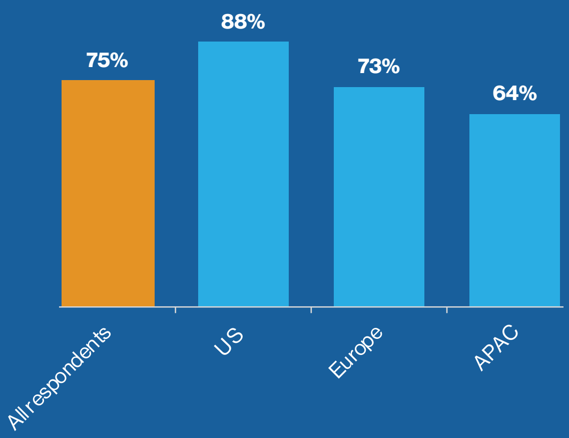
The region has also realized the lowest rate of benefits, with 58% saying they've seen significant ability to address ATO attacks (compared to 66% overall), and the lowest rate of risk reduction (20%), below the 30% overall rate.

BOTS

Only 64% of APAC respondents experienced bot attacks in the previous 12 months (compared to 75% overall). And while the rate of deployment for specialized solutions to combat malicious bots is high (78%), it's still the lowest rate and below the 89% overall rate.

Figure 15 | Three-quarters (75%) indicate their organizations have been targeted by malicious bots in the past 12 months.

In the past 12 months has your company been the target of any of the following cybersecurity challenges? **% "YES" to Malicious Bots**



Benefit rates for APAC were low as well, with 45% seeing significant improvement in their ability to address malicious bots, 33% seeing significant improvement in their marketing effectiveness, and 41% seeing significant improvement in website availability.

SCRIPT PROTECTION

Malicious scripts are a serious problem in APAC, with 78% saying they've been targeted, which is just a bit less than the overall rate of 81%. But only 67% use specialized script protection solutions, the lowest rate and well below the 85% overall rate. The region has also seen the lowest rate of benefit, with 54% seeing significant improvement in cybersecurity capabilities and 59% seeing a reduction in abusive script behaviors.

AUDIENCE HIJACKING

Essentially all (92%) APAC organizations are aware of audience hijacking, while 26% have been affected by it.