Independent market research and competitive analysis of next-generation business and technology solutions for service providers and vendors

HEAVY READING
CUSTOM REPORTS

DDoS Mitigation Strategies:
The Automation Factor

A custom Heavy Reading survey report produced for NETSCOUT

NETSCOUT®

AUTHOR: JIM HODGES, CHIEF ANALYST, HEAVY READING

TABLE OF CONTENTS

1. INTRODUCTION AND KEY FINDINGS 4

1.1 Key Findings 4

2. SURVEY DEMOGRAPHICS SUMMARY 7

Figure 1: Survey Respondents by Geography 7
Figure 2: Survey Respondents by Communications Service Provider Type 8
Figure 3: Survey Respondents by Company Annual Revenue 8
Figure 4: Survey Respondents by Job Function 9

3. STAFFING SECURITY NETWORKS 10

Figure 5: Security Team Hiring 10
Figure 6: Operational Security Development Team Challenges 11
Figure 7: Hiring Qualified Security Team Resources 11

4. SECURING THE NETWORK 12

Figure 8: DDoS Protection Concerns 12
Figure 9: DDoS Attack Blocking Confidence 13
Figure 10: DDoS Blocking – Customer Perspective 13
Figure 11: DDoS 12-Month Attack Trends 14
Figure 12: Implementing Automated DDoS Response 15
Figure 13: DDoS Enforcement Strategy Factors 16
Figure 14: Security Capability Support Confidence Levels 17
Figure 15: Automated Attack Blocking Preferences 17
Figure 16: Ranking Automated Security Response Attributes 18
Figure 17: Automated Blocking Implementation Challenges 19
Figure 18: Advanced Security Support Capability Confidence 20
Figure 19: Authentication Capabilities 21
Figure 20: Information Sources 21
Figure 21: Automated Data Integration Methods 22
Figure 22: Automated Data Export 23
Figure 23: DDoS and the Public Cloud 24
Figure 24: DDoS Impact on Mobile Networks 24
Figure 25: Implementing Automated Security Policy 25

5. APPENDIX A: FILTER GROUP DATA 26

Figure 26: Security Team Hiring: U.S. vs. RoW 26
Figure 27: OPSEC Development Team Challenges: U.S. vs. RoW 26
Figure 28: Hiring Qualified Security Team Resources: U.S. vs. RoW 27
Figure 29: DDoS Protection Concern: U.S. vs. RoW 28
Figure 30: DDoS Attack Blocking Confidence: U.S. vs. RoW 28
Figure 31: DDoS Blocking – Customer Perspective: U.S. vs. RoW 29

Figure 32: DDoS 12-Month Attack Trends: U.S. vs. RoW 30
Figure 33: Implementing Automated DDoS Response: U.S. vs. RoW..... 31
Figure 34: DDoS Strategy Enforcement Strategy Factors: U.S. vs. RoW 31
Figure 35: Security Capability Support Confidence Levels: U.S. vs. RoW 32
Figure 36: Automated Attack Blocking Preferences: U.S. vs. RoW 33
Figure 37: Ranking Automated Security Response Attributes: U.S. vs. RoW... 33
Figure 38: Automated Blocking Implementation Challenges: U.S. vs. RoW 35
Figure 39: Advanced Security Support Capability Confidence: U.S. vs. RoW .. 36
Figure 40: Authentication Capabilities: U.S. vs. RoW 37
Figure 41: Information Sources: U.S. vs. RoW 38
Figure 42: Automated Data Integration Methods: U.S. vs. RoW 39
Figure 43: Automated Data Export: U.S. vs. RoW..... 40
Figure 44: DDoS and the Public Cloud: U.S. vs. RoW 41
Figure 45: DDoS Impact on Mobile Networks: U.S. vs. RoW 42
Figure 46: Implementing Automated Security Policy: U.S. vs. RoW 43

TERMS OF USE 45

1. INTRODUCTION AND KEY FINDINGS

While communications service providers (CSPs) continue to make progress in transforming themselves into cloud service providers, the journey represents a complex undertaking on many levels. This includes coming to terms with the additional security requirements that the cloud imposes. The reality that CSPs now face is that security demands an even greater level of vigilance. As a result, CSPs must reassess their security strategies and factor in the role that new automation-based technologies will play in helping them fortify their networks.

This report presents in detail the key findings of a recently completed market research survey designed to document CSPs' technology preferences and challenges associated with implementing artificial intelligence (AI)-based security technologies to manage distributed denial-of-service (DDoS) attacks.

1.1 Key Findings

Staffing Security Networks

Despite an escalation in the number and complexity of security threats, **only 43% of CSP survey respondents indicated they planned to grow their security team**. Another 43% plan to retain current staffing levels.

Lack of skilled resources is the leading factor why they are not growing security resources. Almost half of the survey respondents (49%) cited hiring the right team members as a challenge; 66% of these respondents were Rest of World (RoW) respondents versus only 31% of U.S. respondents.

Inability to hire skilled resources is having a negative impact. When asked about the challenges inherent in building and maintaining an effective operational security (OPSEC) team, **lack of headcount (50%)** ranked higher than other factors, such as limited capex to buy security equipment (46%) and limited opex to administer security networks (43%).

Securing the Network

While many CSPs are facing significant challenges in ramping up their security teams, they are still experiencing growth in network attacks, including DDoS attacks. For example, 55% to 56% of the respondents are still seeing "measured growth" for DDoS volume, application, and protocol layer attacks, while 16% to 20% are experiencing "strong growth" for the same attack types. In aggregate form, this equates to 71% to 76% of respondents encountering a significant level of DDoS growth.

Given a need to manage more DDoS attacks with the same staff resources, not surprisingly, **three-quarters of the respondents (73%) are either "extremely concerned" (24%) or "concerned" (49%)** about their ability to protect infrastructure and applications or services from DDoS attacks.

Despite these concerns, **45% of CSPs are "confident" and 20% are "very confident" that their security teams are up to the task of managing DDoS attacks**. In looking at these numbers, however, it is important to note that while 81% of U.S. respondents are either "very confident" (29%) or "confident" (52%), only 53% of RoW respondents have similar views (13% and 40%, respectively). Greater difficulty in hiring staff by RoW respondents is likely a major factor in their lower confidence level.

Since DDoS attacks can have devastating impacts on customer experience, it makes sense that **87% of CSPs believe that their customers consider DDoS blocking a strategic imperative**. This belief is confirmed by the 40% "extremely important" and 47% "important" response rates.

One approach to managing DDoS security threats with an undersized security team is to automate certain security functions. And this process has already started. In fact, **33% of the respondents indicated they have already implemented some form of automated DDoS support**. In addition, 19% of the respondents indicated they plan to implement some automated DDoS capabilities within 12 months, while another 25% see the implementation window taking place within 12 to 18 months. **This equates to 44% implementing within 18 months, arriving at a total implementation rate of 77% by period close**. Although Heavy Reading believes that this aggressive compressed implementation curve will likely slip, it does confirm that a majority of CSPs believe that automation has already become a vital component of their DDoS mitigation strategy.

CSPs will rely on a number of automation-based capabilities to block DDoS attacks. While the ability to auto-detect DDoS attacks garnered the highest "extremely important" response level (45%), the tight range of response scoring (39% to 45%) confirms that it is only one of several important capabilities.

This makes sense because **currently, more than 4 out of 10 CSPs have either limited confidence or no confidence in their ability to manage critical functions**, such as not blocking traffic or reporting what is being blocked.

While CSPs will use automation in a number of ways to thwart various DDoS attack variants, their **primary focus is to leverage automation to block both volumetric and protocol-level attacks (54%)**.

Although CSPs understand the value of automation, **79% believe it is also very important (40% "extremely important" and 39% "important") that they are able to override automated decisions** to maintain system control.

The problem is that **a sizable number of CSPs (29%) have either limited or no confidence that they will be able to support this vital capability**.

Even more concerning is that **typically, more than 60% of CSPs are concerned that automation will make it difficult to prevent blocking legitimate traffic**. Some of the concerns are visibility related due to limited insight of the applications/services running in the network (67% "major challenge" and "challenge") or even the ability to correctly authenticate legitimate users and block attackers (70% "major challenge" and "challenge").

An additional challenge that CSPs must confront is **deciding which information sources they will rely upon to make traffic blocking decisions**. Based on "primary source" inputs, the **two preferred sources by a slight margin are abnormal increase in traffic from a specific application/protocol and abnormal increase in traffic from a specific Internet Protocol (IP) domain (both 54%)**. Rounding out the top three is behavioral traffic analysis (49%).

A related consideration of managing the data generated by automated DDoS systems is what data should be exported to other security systems. In this case, **the leading data source based on "extremely important" response levels is the reason for the traffic being blocked (51%)**.

In the survey, **57% of the CSPs indicated they believe that if they run their services in public clouds, their public cloud vendor will provide adequate DDoS protection** despite the lack of history that this is the case.

Despite the challenges and uncertainty, **almost half of the survey respondents (49%) indicated their preferred automation implementation option is to allow automated systems to take over DDoS security enforcement**. In contrast, a second group (30%) will take a more measured approach and continue to rely on manually created human processes, with AI and machine learning (ML) systems running in the background for comparative purposes only.

2. SURVEY DEMOGRAPHICS SUMMARY

This research report is based on a comprehensive online survey launched in 3Q 2019. The survey created by Heavy Reading in collaboration with NETSCOUT was distributed by email to Light Reading's global list of service provider employees.

These respondents were invited to take the survey on the understanding of anonymity (i.e., that their names, job titles, and employers would not be made available to the study's sponsors or eventual readers) and that the results will only be presented in aggregate form. Respondents were not told which suppliers sponsored the study.

The survey included 26 questions and was promoted to attract a large base of high-value respondents. As shown in **Figure 1**, a global mix of 80 qualified CSP respondents took the survey. Non-qualified, non-CSP responses were deleted. The largest employee sample was from the U.S. (49%), followed by Asia Pacific (18%), Central/Eastern Europe (10%), Canada (6%), Western Europe (6%), Central/South America (5%), and the Middle East (5%).

To provide additional market-level insight on security strategy execution, the survey responses were filtered using two equal-sized geographic sample groups: the U.S. and the RoW. While only notable variances in response trends between these the groups are documented in the main body of this report, granular response data for each question is provided in table format in **Appendix A**.

Figure 1: Survey Respondents by Geography

	Percent
U.S.	49%
Asia Pacific	18%
Central/Eastern Europe	10%
Canada	6%
Western Europe	6%
Central/South America	5%
Middle East	5%
Other (Please specify)	1%

Question: Where is your company located? (N=80)
Source: Heavy Reading

The survey attracted a broad range of CSP types and sizes. Of these, as shown in **Figure 2** below, the three largest groups represented were converged operators (44%), mobile operators (30%), and fixed-line/cable operators (16%). This is a desirable split given that these operators are on the front line of security enforcement and often face unique security implementation challenges.

Figure 2: Survey Respondents by Communications Service Provider Type

	Percent
Converged operator (fixed and mobile assets)	44%
Mobile operator	30%
Fixed-line/cable operator	16%
MVNO, MVNE with infrastructure	4%
Hosting/cloud provider	4%
IPX/wholesale/roaming or signaling hub provider	1%
Other (please specify)	1%

Question: What type of communications service provider (CSP) do you work for? (N=80)
Source: Heavy Reading

As shown in **Figure 3**, 60% of the respondents worked for CSPs that generated more than $1 billion of revenue on an annual basis (26% + 34%), while 40% (10% + 14% + 10% + 6%) generated revenue of less than $1 billion per year.

Figure 3: Survey Respondents by Company Annual Revenue

	Percent
Less than $50 million	6%
$50 million to $199 million	10%
$200 million to $499 million	14%
$500 million to $999 million	10%
$1 billion to $5 billion	26%
More than $5 billion	34%

Question: What is your company's annual revenue? (N=80)
Source: Heavy Reading

As illustrated in **Figure 4** below, 80% of survey respondents performed what Heavy Reading considers technical roles, which is a desirable figure given that this survey had a strong technical focus. For example, 39% performed network planning and engineering roles, while 18% performed R&D or technical strategy roles.

Figure 4: Survey Respondents by Job Function

	Percent
Network planning & engineering	39%
R&D or technical strategy	18%
Corporate management	14%
Network operations	10%
IT, data center, & cloud domain	9%
Sales & marketing	5%
Security architect	3%
Security operations	1%
Product management	1%
Other (please specify)	1%

Question: What is your primary job function? (N=80)
Source: Heavy Reading

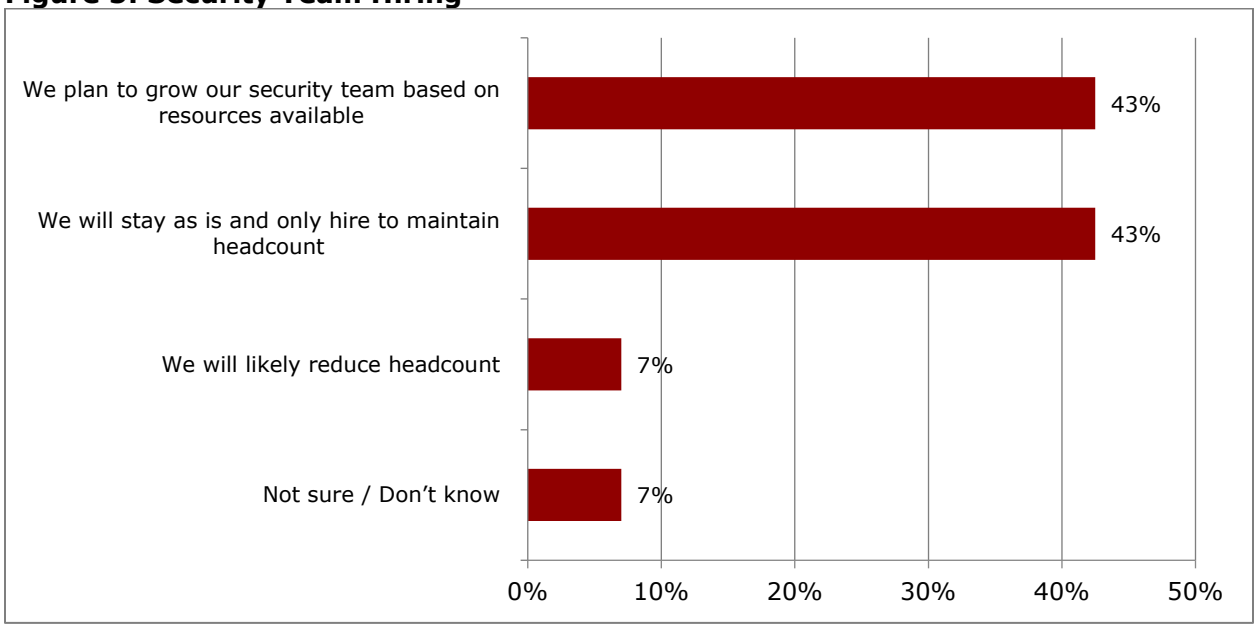
Additionally, 10% performed network operation functions. In order to achieve a higher technical response level, certain groups, such as hardware and software developers, were excluded from taking the survey. The remaining 20% of the respondents typically performed corporate management roles (14%), which Heavy Reading also considers desirable. Most respondents who perform these roles are involved in making strategic resource hiring and investment decisions.

3. STAFFING SECURITY NETWORKS

One of the realities that CSPs face in securing their networks is the need to hire and retain adequate staff resources to stay ahead of the threat curve. Aligned with this philosophy, as shown in **Figure 5**, 43% of respondents indicated they planned to grow their security team subject to response availability. However, within this group, 51% of U.S. respondents expect to grow team resources compared to only 34% of their RoW counterparts (see **Figure 26**).

In contrast, an identically sized group indicated they plan to remain in "status quo" mode and only hire to maintain headcount. While this is somewhat disappointing given the security challenges CSPs face, Heavy Reading believes several factors must be considered, including the finite pool of security resources for hire (see **Figure 7**).

Figure 5: Security Team Hiring



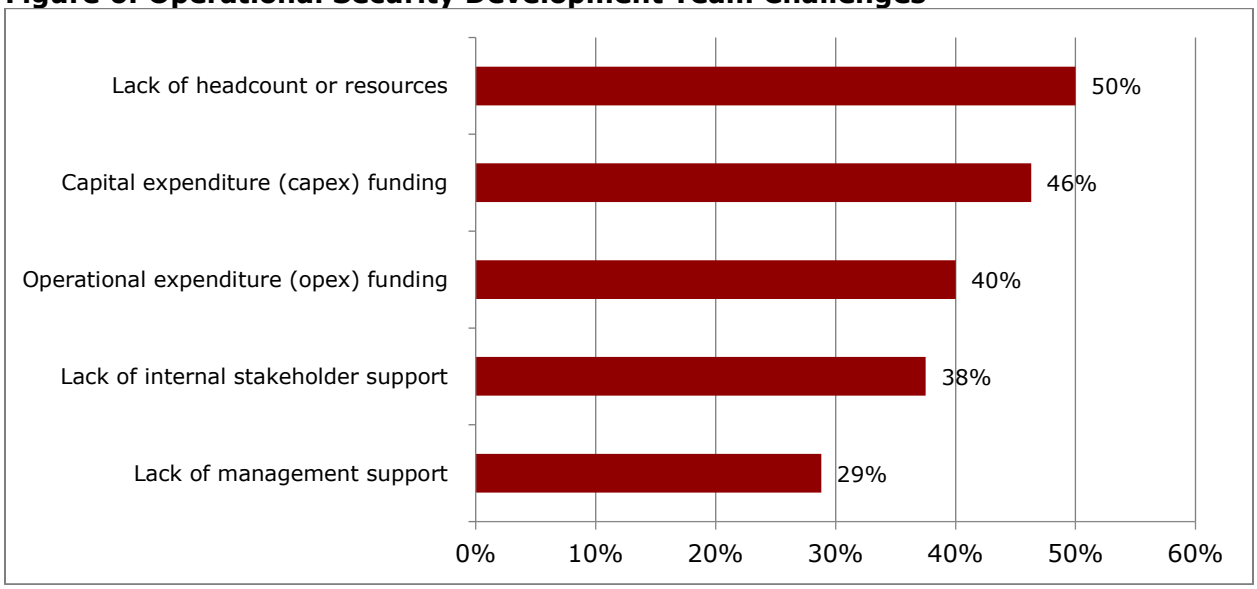
Question: Which statement best reflects the hiring status of your security team resources over the next 12 months? (N=80)
Source: Heavy Reading

Even though roughly half of the survey respondents plan to only maintain headcount, that does not mean they feel they have the necessary resources to meet their security obligations.

As illustrated in **Figure 6** below, when asked about the challenges inherent in building and maintaining an effective OPSEC team, the respondents focused on a number of factors, including lack of headcount (50%), limited capex to buy security equipment (46%), and limited opex to administer security networks (40%).

It is worth noting that while RoW and U.S. respondents are generally aligned on the impact of capex and opex funding challenges, a much larger percentage of RoW respondents cited lack of headcount resources (63% vs. 36% U.S.) and lack of management support (39% vs. 18% U.S.) as two key challenge areas (see **Figure 27**).

Figure 6: Operational Security Development Team Challenges

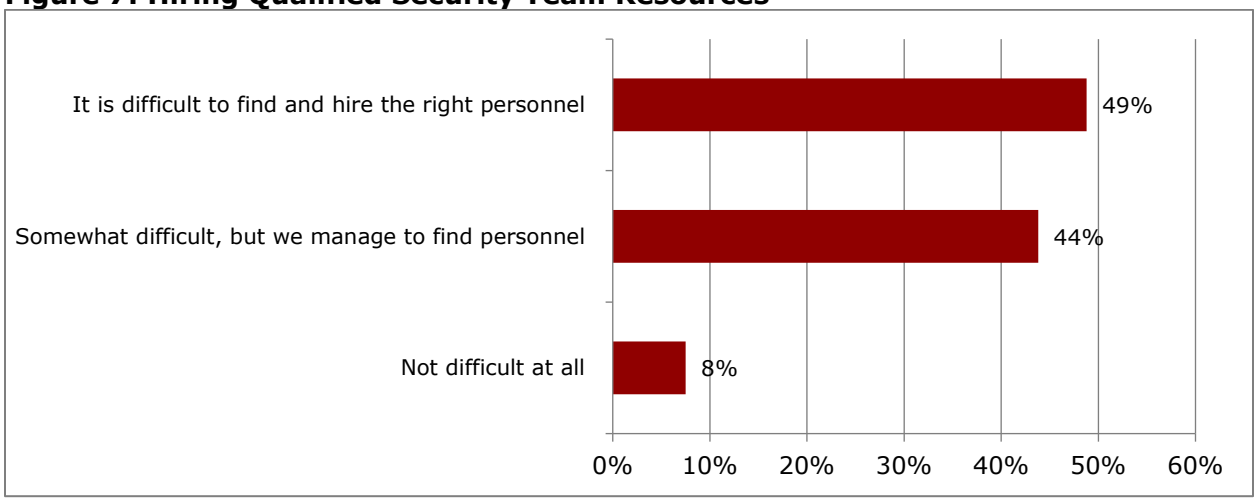


Question: What challenges do you face in building and maintaining an effective operational security (OPSEC) team? (Select all that apply) (N=80)
Source: Heavy Reading

If there were any lingering doubts that the lack of skilled security resources continues to be an issue, **Figure 7** definitively closes the feedback loop. As shown in the figure, almost half of the respondents (49%) cited hiring the right team members as a challenge.

Of these, consistent with previous input, a larger group of RoW respondents are feeling the strain in securing the team resources they vitally require (RoW 66% vs. U.S. 31% – see **Figure 28**).

Figure 7: Hiring Qualified Security Team Resources



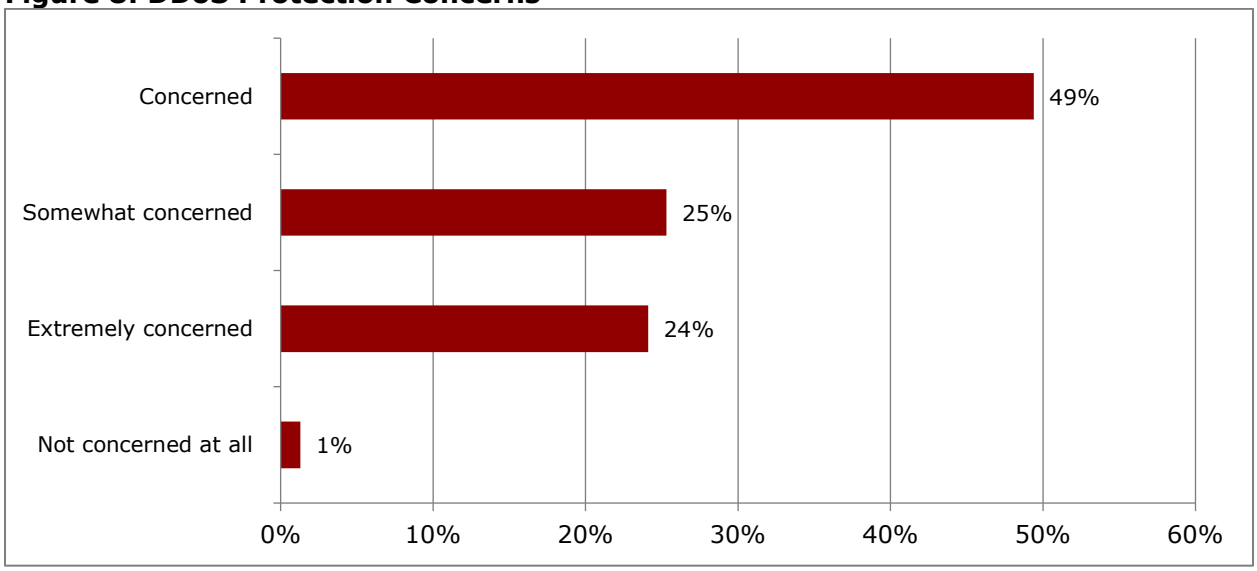
Question: How difficult is it to hire qualified security team resources for your organization? (N=80)
Source: Heavy Reading

4. SECURING THE NETWORK

As documented in the previous section, CSPs are facing significant challenges in ramping up their security teams to meet current threat types, including DDoS attacks, the focus of the research project.

Given this limitation, it is not surprising, as shown in **Figure 8**, that almost three-quarters of the respondents (73%) are either "extremely concerned" (24%) or "concerned" (49%) about their ability to protect infrastructure and applications or services from DDoS attacks.

Figure 8: DDoS Protection Concerns

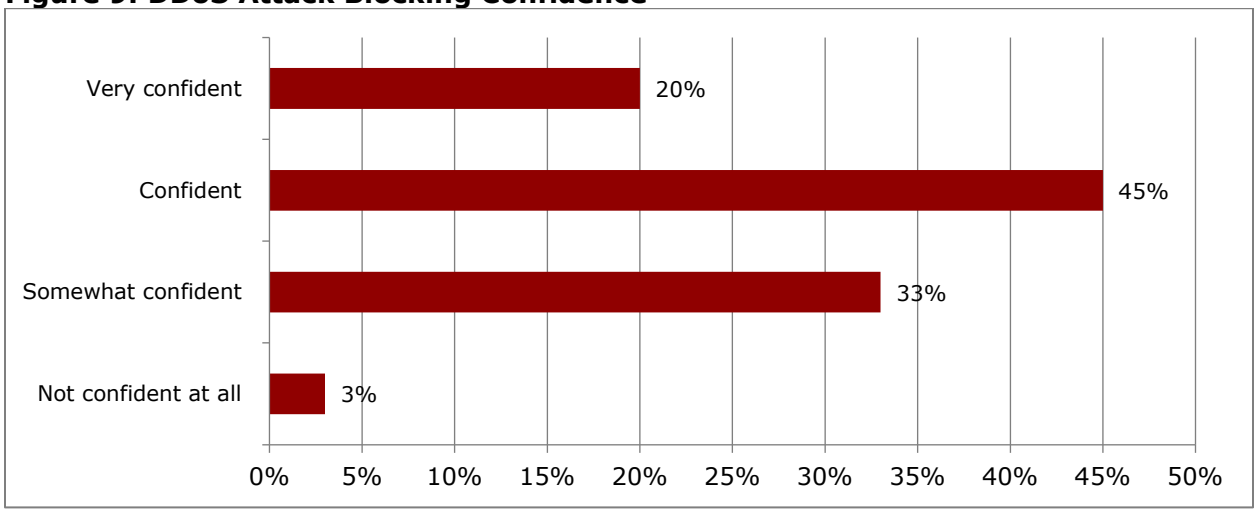


Question: How concerned is your team/organization about protecting your infrastructure and application/services from DDoS attack? (N=79)
Source: Heavy Reading

Despite DDoS protection concerns, many CSPs remain confident that, for now, they are still ahead of the curve in DDoS attack mitigation. For example, as shown in **Figure 9** below, 45% are "confident," while 20% are "very confident" that their security teams are up to the task.

In looking at these numbers, however, it is important to document the deviation between the two filter groups. While 81% of U.S. respondents are either "very confident" (29%) or "confident" (52%) in their ability to block DDoS attacks, only 53% of RoW respondents have similar views (13% and 40%, respectively). Instead, a much greater percentage of RoW respondents (48%) assess their abilities as only "somewhat confident" versus 18% of U.S. respondents, which indicates that RoW respondents believe they are in a much less secure position (see **Figure 30**).

Figure 9: DDoS Attack Blocking Confidence

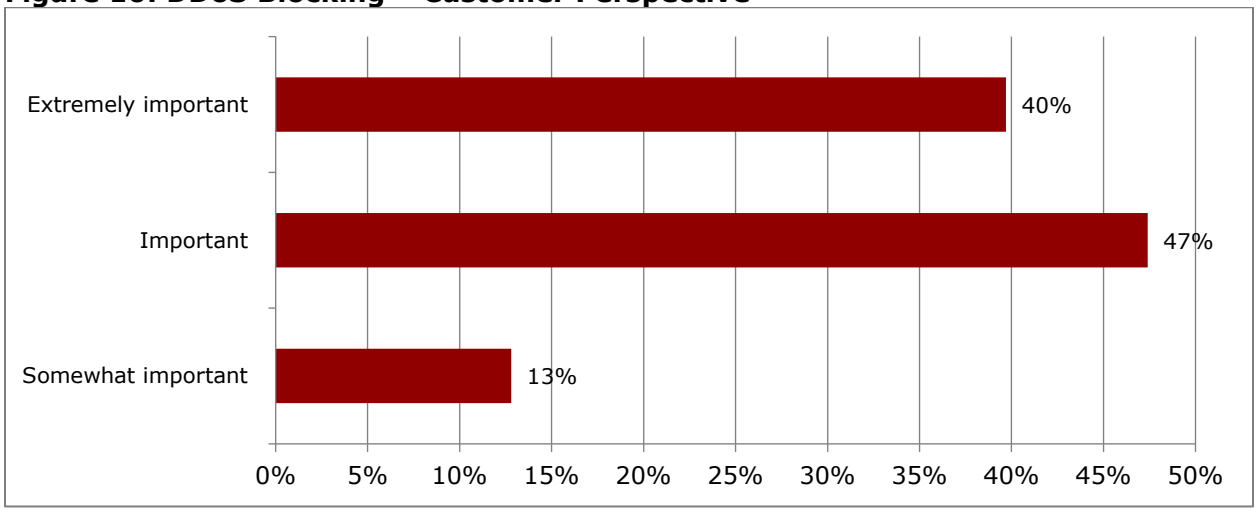


Question: To what extent are you confident in your ability to block DDoS attacks? (N=80)
Source: Heavy Reading

Because DDoS attacks can have devastating impacts on customer experience, it makes sense that CSPs would believe that their customers consider DDoS blocking a strategic imperative. This belief is confirmed in **Figure 10**, with 40% "extremely important" and 47% "important" response rates. This equates to 87% of the survey respondents identifying the relative importance of not affecting customer access.

Within the two filter groups, U.S. and RoW respondents had identical 40% "extremely important" response levels. However, RoW respondents displayed a much higher level of "somewhat important" response rates (23% vs. 3% for U.S. respondents). This indicates that in certain RoW markets, CSPs perceive that their customers are less concerned about protection from DDoS attacks (see **Figure 31**).

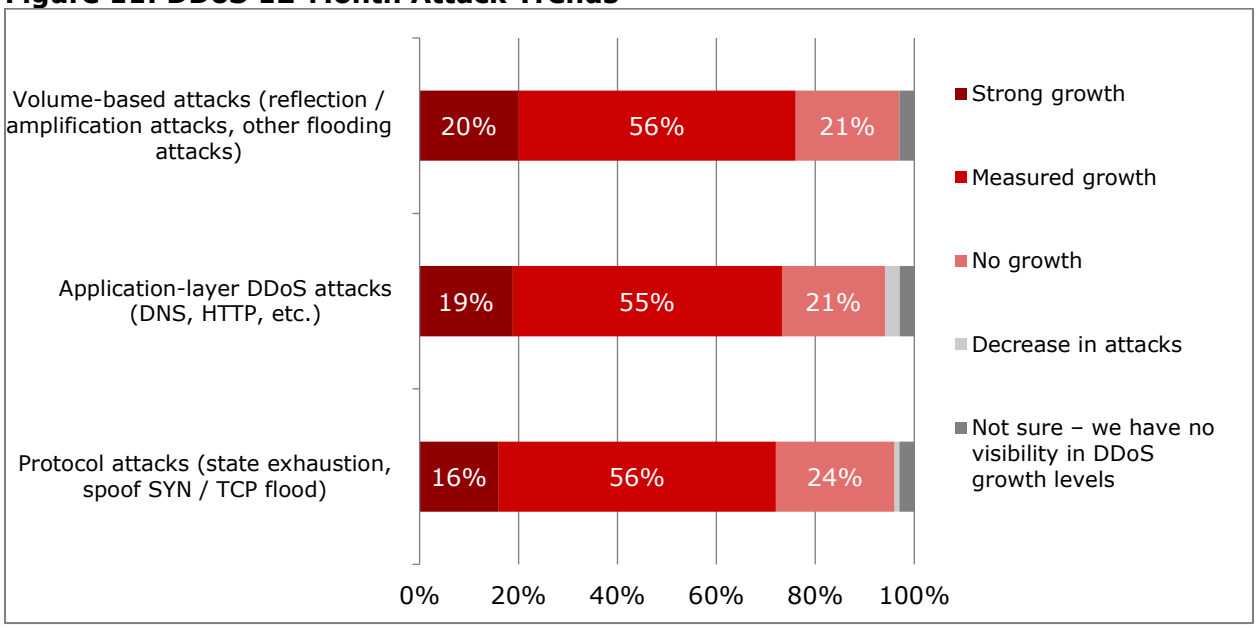
Figure 10: DDoS Blocking – Customer Perspective



Question: How important to your customers is your ability to block DDoS attacks? (N=78)
Source: Heavy Reading

Another DDoS concern that CSPs must address is the ongoing growth of DDoS attacks. As shown **Figure 11**, 55% to 56% of the respondents are still seeing "measured growth" for DDoS volume, application, and protocol layer attacks, while 16% to 20% are experiencing "strong growth" for the same attack types. In aggregate form, this equates to 71% to 76% of respondents encountering a significant level of DDoS growth.

Figure 11: DDoS 12-Month Attack Trends



Question: What has been the trend for the following types of DDoS attacks in your environment over the last 12 months? (N=80)
Source: Heavy Reading

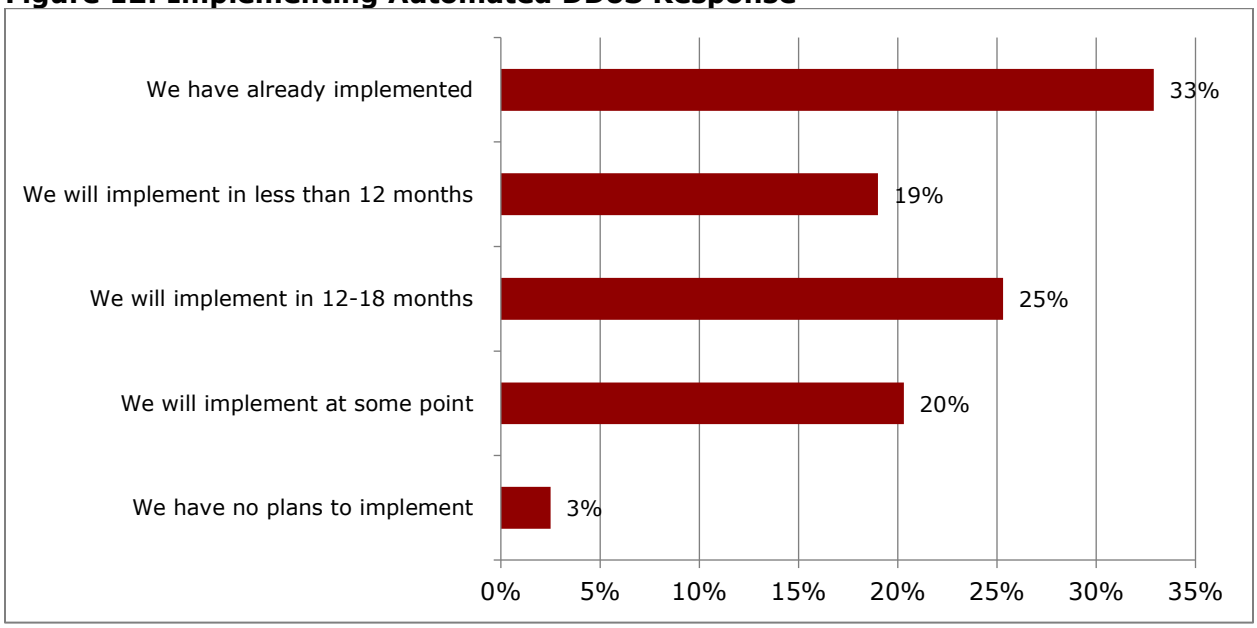
One of the key objectives of this project was to factor in the role that automation would play in minimizing the impact of DDoS attacks. As a starting point, because automation can be used in a number of ways to combat DDoS, the first question simply asked respondents if they had implemented any form of automated DDoS protection technology. As **Figure 12** below illustrates, 33% of the respondents indicated they have already implemented some form of automated DDoS support.

In addition, 19% of the respondents indicated they plan to implement some automated DDoS capabilities within 12 months, while another 25% see the implementation window taking place within 12 to 18 months. This equates to 44% implementing within 18 months, arriving at a total implementation rate of 77% by period close.

Although Heavy Reading believes that this aggressive compressed implementation curve will likely slip, it does confirm that a majority of CSPs believe that automation has already become a vital component of their DDoS mitigation strategy.

In looking at the two filter groups, while U.S. respondents were ahead in terms of actual implementation progress, within the 12- to 18-month implementation window, the inputs were similar (see **Figure 33**).

Figure 12: Implementing Automated DDoS Response



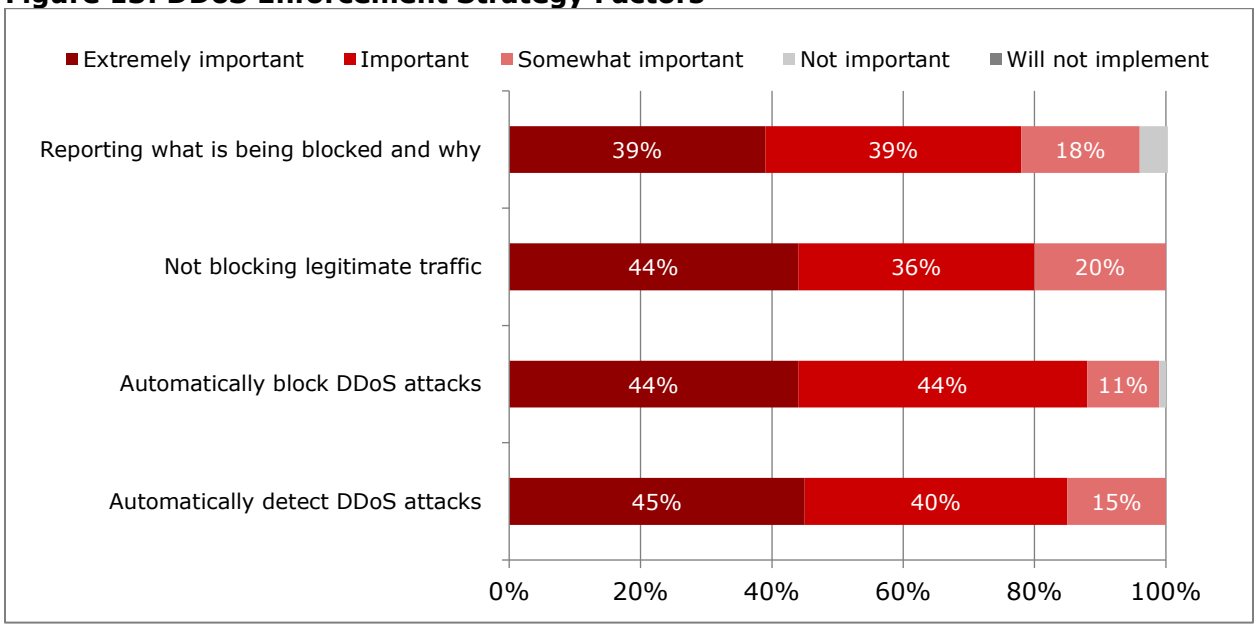
Question: When do you plan to implement automated technologies to respond to DDoS attacks without human intervention? (N=80)
Source: Heavy Reading

Managing DDoS attacks is a complex undertaking because an effective strategy must be able to strike a balance between blocking threat vectors without blocking legitimate users. To do this, CSPs must be able to capture and document why traffic is being blocked, the applications affected, and what steps and capabilities were deployed to support the auto-detection process.

Consequently, as shown in **Figure 13** below, CSPs will rely on a number of automation-based capabilities to meet their requirements. In examining the "extremely important" response levels, while the ability to auto-detect DDoS attacks garnered the highest response level (45%), the tight range of these responses (39% to 45%) confirms that it is only one of the important capabilities.

In Heavy Reading's view, this confirms that automation will need to be deployed using a range of functions, including reporting what is being blocked and why (39%). Stated differently, there is no single technology or capability that can be deployed to mitigate all DDoS attacks. What is required is a powerful amalgam of technology capabilities that can be deployed holistically.

Figure 13: DDoS Enforcement Strategy Factors



Question: How important are the following to your DDoS security enforcement strategy? (N=78-80)
Source: Heavy Reading

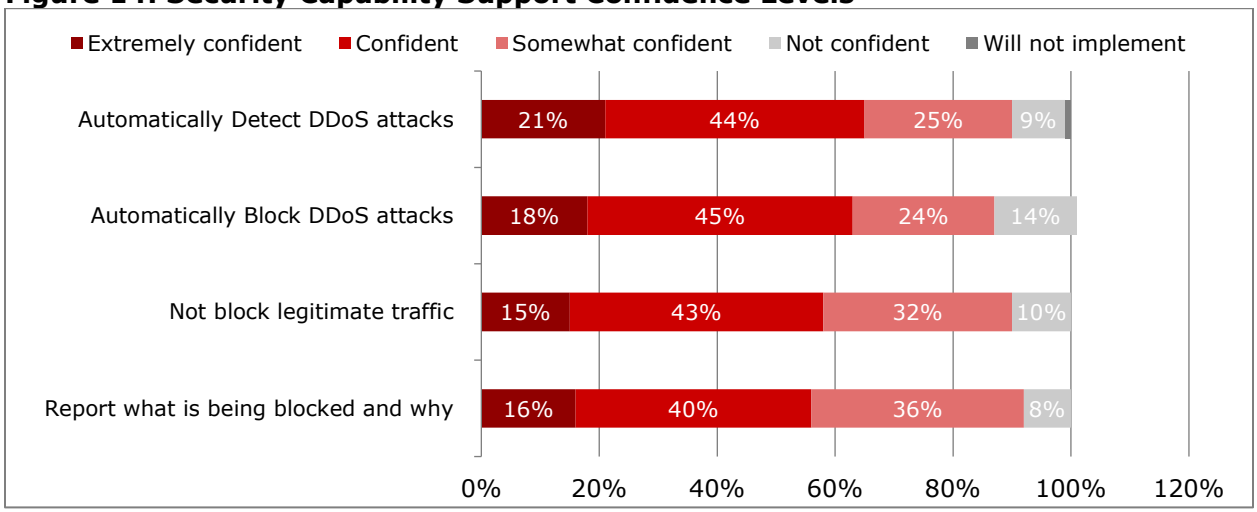
Given the complexity of DDoS attacks and the need to deploy to a number of capabilities, in the next question, Heavy Reading asked the survey respondents to what extent they were confident in being able to detect, block, and report DDoS incidents. As shown in **Figure 14** below, 55% to 66% of CSPs are either "extremely confident" (15% to 21%) or "confident" (40% to 45%) in their abilities here. These numbers are consistent with the general confidence level numbers documented in **Figure 9.**

However, the relatively high response levels of "somewhat confident" (24% to 36%) and "not confident" (8% to 14%) are also a concern. This is especially true for capabilities such as not blocking traffic and reporting what is being blocked. The combined total of these limited or no confidence responses translate into 42% and 44% of the population, respectively.

Because both capabilities are considered critical capabilities, a greater than 4 out of 10 score, in Heavy Reading's view, highlights that many CSPs need to adopt new DDoS attack management strategies, given they are currently unable to avoid blocking legitimate traffic or even report what traffic is being blocked.

Overall, U.S. CSPs are considerably more confident than their RoW counterparts. For example, while only 18% of U.S. respondents are either "somewhat confident" (13%) or "not confident" (5%) in their ability to automatically block DDoS attacks, in this same category, RoW response levels hit the 56% mark (34% and 22%, respectively – see **Figure 35**). A factor that likely comes into play here is the fact that U.S. respondents are experiencing greater success in hiring skilled resources (see **Figure 7**).

Figure 14: Security Capability Support Confidence Levels

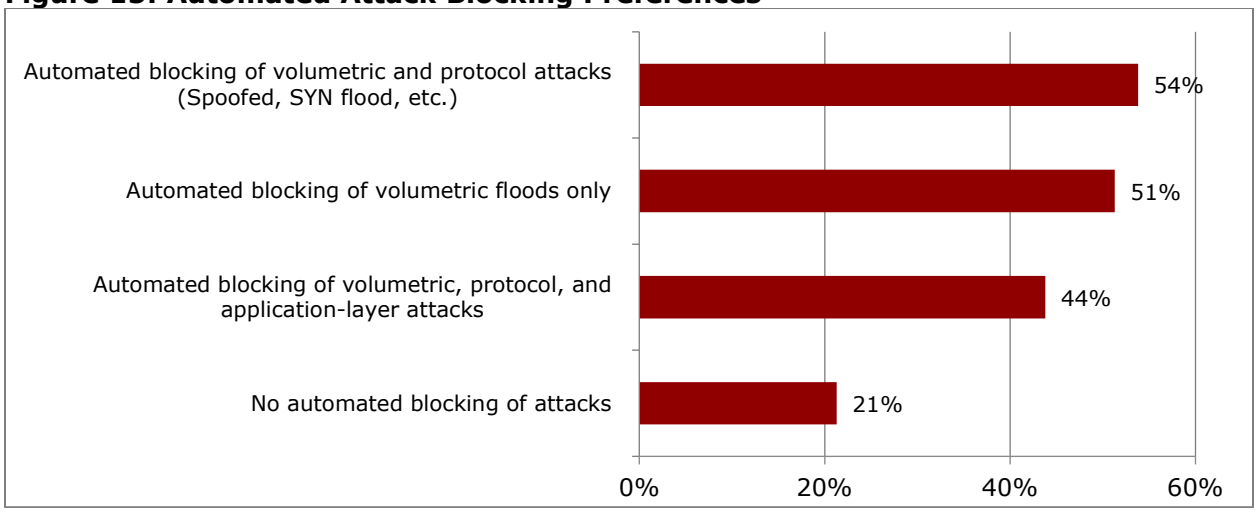


Question: How confident are you in your current ability to support the following security capabilities? (N=78-80)
Source: Heavy Reading

As previously noted, the complexity and various types of DDoS attacks will mandate a multifaceted technology deployment strategy. This is reinforced in **Figure 15**, which captures that CSPs will use a number of DDoS attack block strategies. Of these, the approach that attained the highest scoring was to leverage automation for blocking of both volumetric and protocol-level attacks (54%).

There is no single right answer for which technology should be deployed by all operators. Yet, the low scoring (21%) of the "no automated blocking of attacks" confirms that roughly 8 out 10 CSPs view automation as a foundational component of whichever DDoS mitigation strategy they do implement.

Figure 15: Automated Attack Blocking Preferences



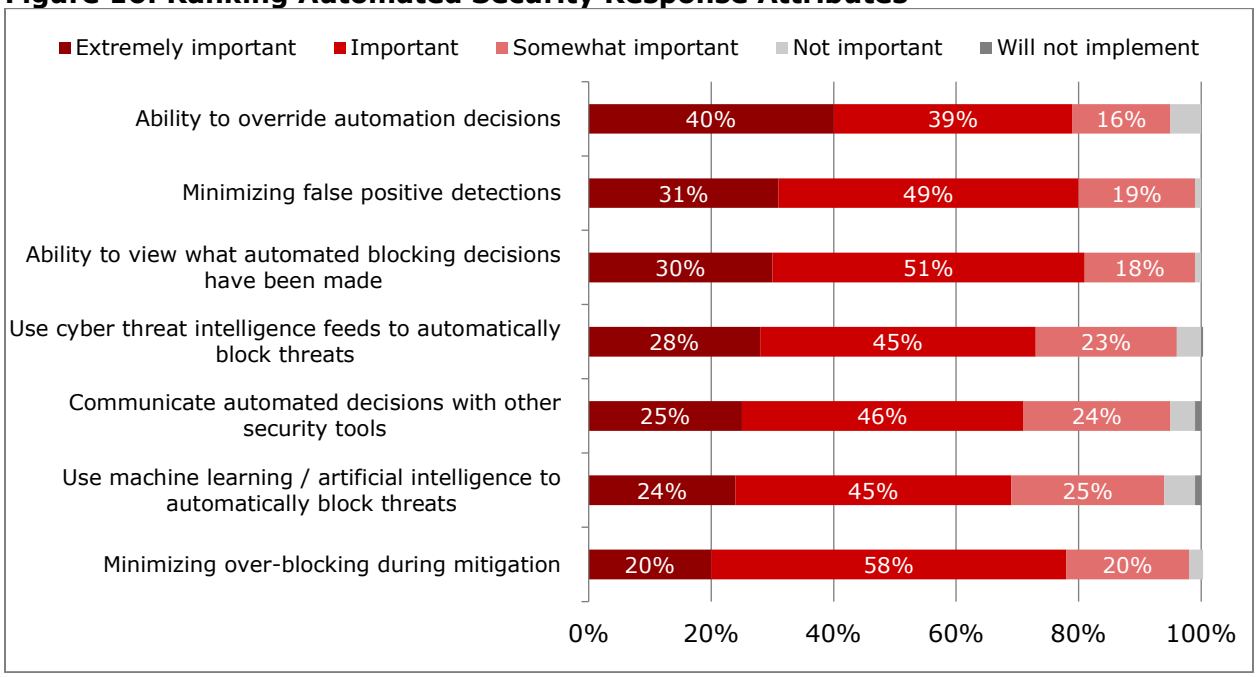
Question: There are different degrees of automated blocking of attacks that can be achieved. Please indicate which degree(s) of automated blocking you find desirable (Select all that apply) (N=80)
Source: Heavy Reading

The next question in the survey continued the automation discussion and sought more detailed information on the relative value of a number of automated DDoS response security capabilities. As shown in **Figure 16**, these capabilities include automatic threat blocking, security tool interaction, minimizing false positives, and even minimizing over-blocking.

Of these, based on "extremely important" response rates, the highest ranking is the "ability to override automation decisions" (40%). This is logical. In order to maintain network control, CSPs must be able to override automated decisions in cases where it is clear that automation, for some reason, is making unsound security decisions.

Still, the high scoring of the other capabilities shown in **Figure 16** also confirms that techniques to minimize false positives and document DDoS blocking decisions are also very important capabilities. Minimizing over-blocking during DDoS mitigation was the lowest ranking response based on "extremely important" responses. However, it scored highest in "important" responses (58%), which confirms this is also an important consideration for CSPs.

Figure 16: Ranking Automated Security Response Attributes



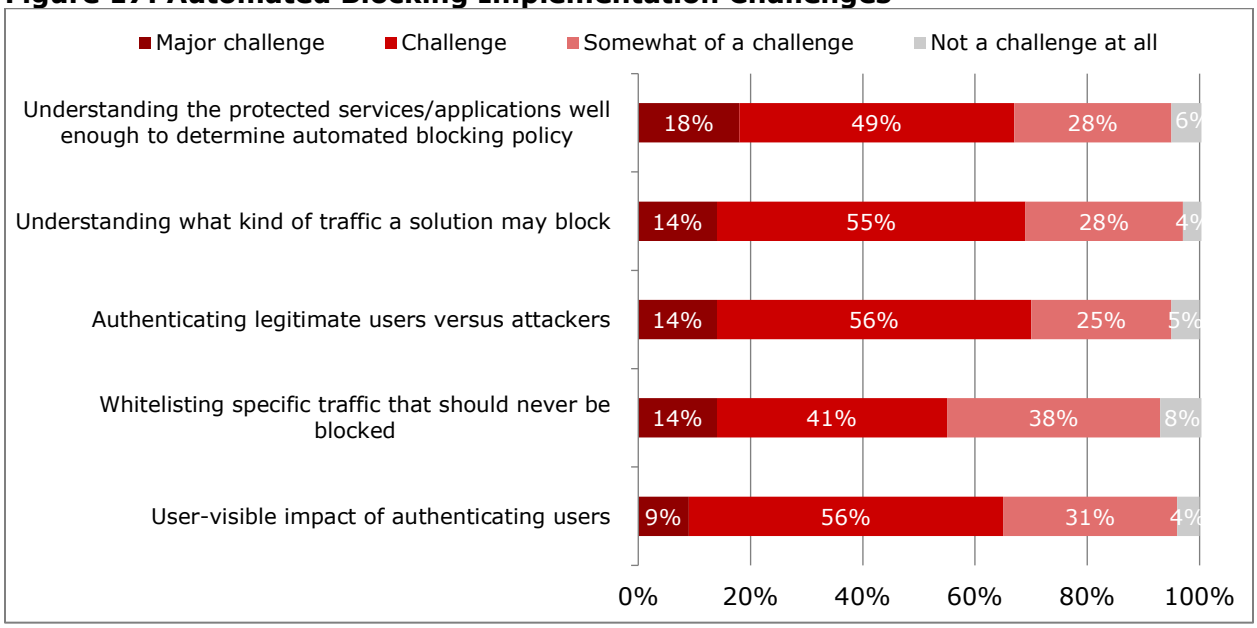
Question: How important are the following attributes in the implementation of an automated security response system? (N=80)
Source: Heavy Reading

One of the reasons Heavy Reading believes that CSPs highly rank the ability to override automated decisions is that they understand the complexity and associated challenges of implementing automated DDoS security systems. As shown in **Figure 17** below, based on both "major challenge" and "challenge" responses, there is no shortage of concerns.

CSPs expect significant DDoS mitigation challenges because they possess a limited understanding of the protected applications/services, the types of traffic they need to block, and even the ability to correctly authenticate legitimate users and block attackers. As a proof point, typically, more than 60% of CSPs are concerned that automation will make it

difficult to prevent blocking legitimate traffic. Some of the concerns are visibility related due to limited insight of the applications/services running in the network (67% "major challenge" and "challenge") or even the ability to correctly authenticate legitimate users and block attackers (70% "major challenge" and "challenge").

Figure 17: Automated Blocking Implementation Challenges

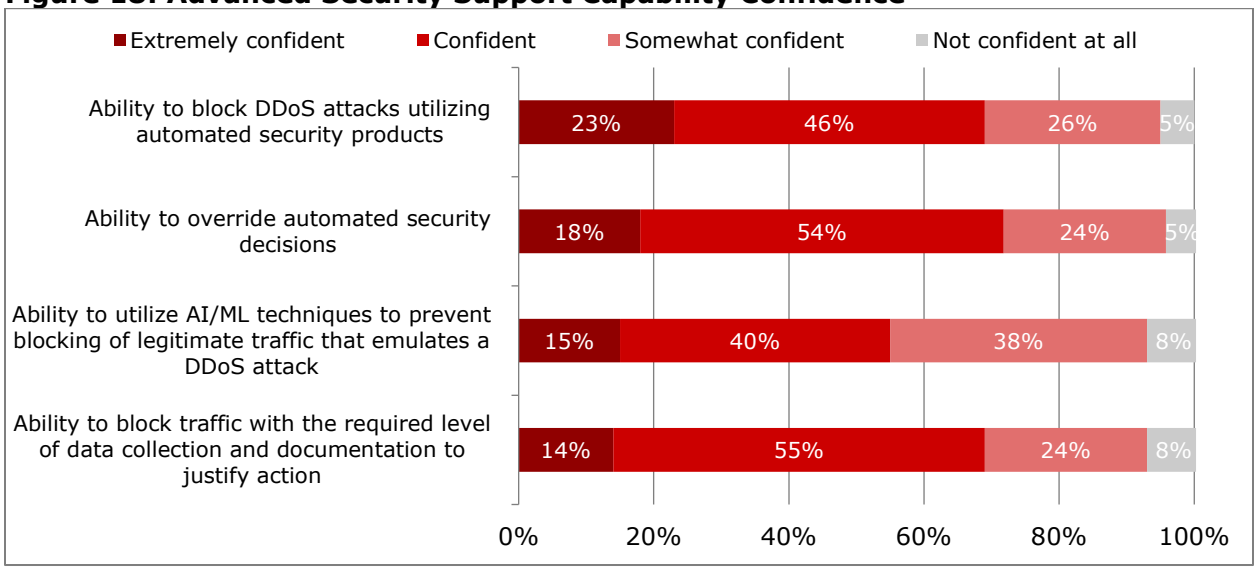


Question: Please rate the following challenges you face in implementing automation-based solutions to prevent blocking of legitimate traffic? (N=80)
Source: Heavy Reading

Considering the challenges associated with using automation, logically, CSPs should also be less confident in their ability to support automation capabilities. This premise is validated in **Figure 18** below, with many key automation functions scoring lower in the "extremely confident" range (14% to 23%) and higher in the aggregated "somewhat confident" and "not confident at all" ranges (29% to 46%).

While there is a solid band of "confident" responses (40% to 55%), it is hard not to be concerned that 29% of respondents have limited or no confidence in supporting a foundational capability, such as the ability to override automated security decisions (see **Figure 16**). Even more concerning is that 46% of respondents have limited or no confidence they will be able to utilize AI/ML techniques to prevent blocking of legitimate traffic that emulates a DDoS attack.

Figure 18: Advanced Security Support Capability Confidence



Question: What is your level of confidence for supporting the following capabilities? (N=80)
Source: Heavy Reading

One of the impacts of deploying services in distributed clouds is that authentication becomes more complex given user mobility and a distributed software reference architecture. In response, CSPs need to implement more advanced authentication capabilities to ensure that only legitimate users can access specific services.

Moreover, it is no longer simply a matter of blocking bad human actors. They must also use authentication to block automated bots from accessing the network to launch DDoS attacks. To protect their networks, as illustrated in **Figure 19** below, CSPs plan to rely on a broad range of authentication capabilities.

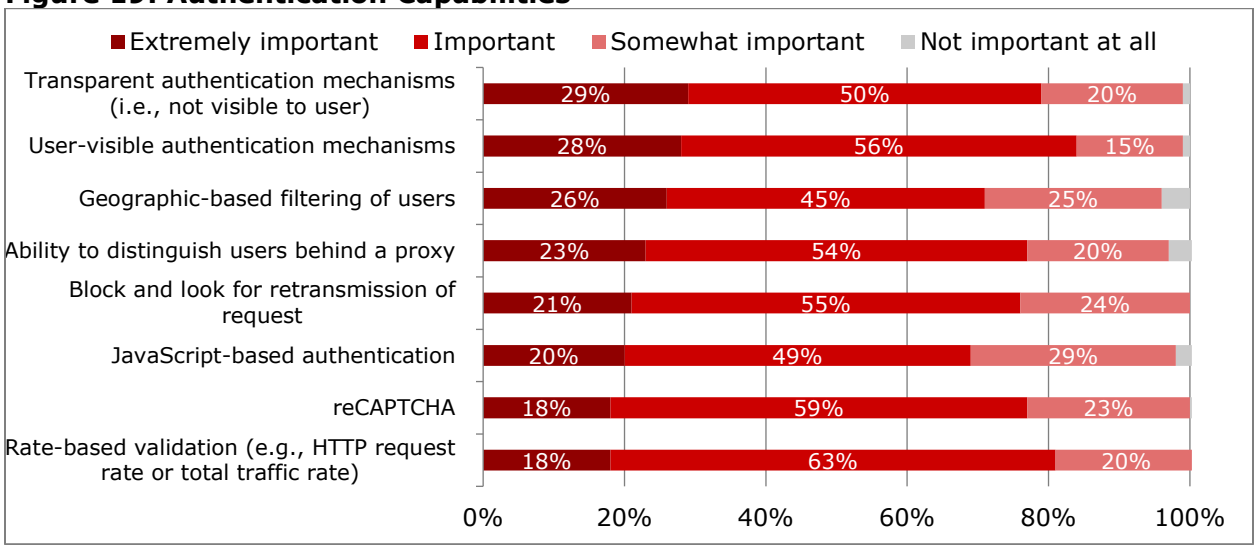
Based on "extremely important" responses, the top three preferred capabilities are "transparent authentication mechanisms" (29%), "user-visible authentication mechanisms" (28%), and "geographic-based filtering of users" (26%).

However, all the listed capabilities, including reCAPTCHA (18%), are still considered valid options based on the range of "important" response levels. The message here is that authentication also requires a multifaceted approach that is seamlessly integrated.

Examining filter group responses reveals there are some unique geographic preferences. For example, based on "extremely important" response levels, the top three U.S. respondent-preferred approaches are "user-visible authentication mechanisms," "block and look for retransmission of request" (both 28%), and "reCAPTCHA" (26%).

In contrast, RoW respondents' top three authentication capabilities are "transparent authentication mechanisms" (34%), "geographic-based filtering of users" (29%), and "user-visible authentication mechanisms" and "ability to distinguish users behind a proxy" (both 27%) (see **Figure 40**).

Figure 19: Authentication Capabilities

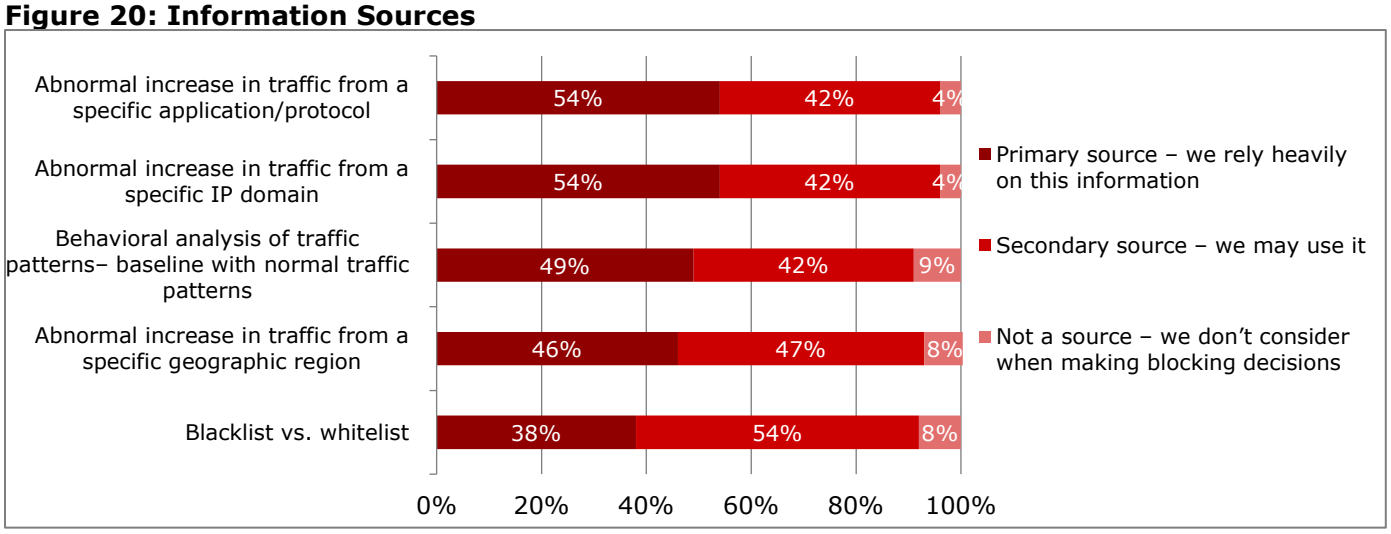


Question: How important are the following capabilities for enabling authentication of legitimate user traffic versus a traffic generating bot in protected applications? (N=80)
Source: Heavy Reading

Another DDoS complexity that CSPs must address is deciding on which information sources they will rely upon when making traffic blocking decisions. Here again, as illustrated in **Figure 20** below, CSPs will need to rely on a multiples-based approach. Based on "primary source" inputs, the two top preferred approaches by a slight margin are "abnormal increase in traffic from a specific application/protocol" and "abnormal increase in traffic from a specific IP domain" (both 54%). Rounding out the top three is "behavioral traffic analysis of traffic patterns – baseline with normal traffic patterns" (49%).

Given the complexity and challenges they face, CSPs now seem to be moving away from relying heavily on a traditional blacklist versus whitelist approach (38%).

Figure 20: Information Sources

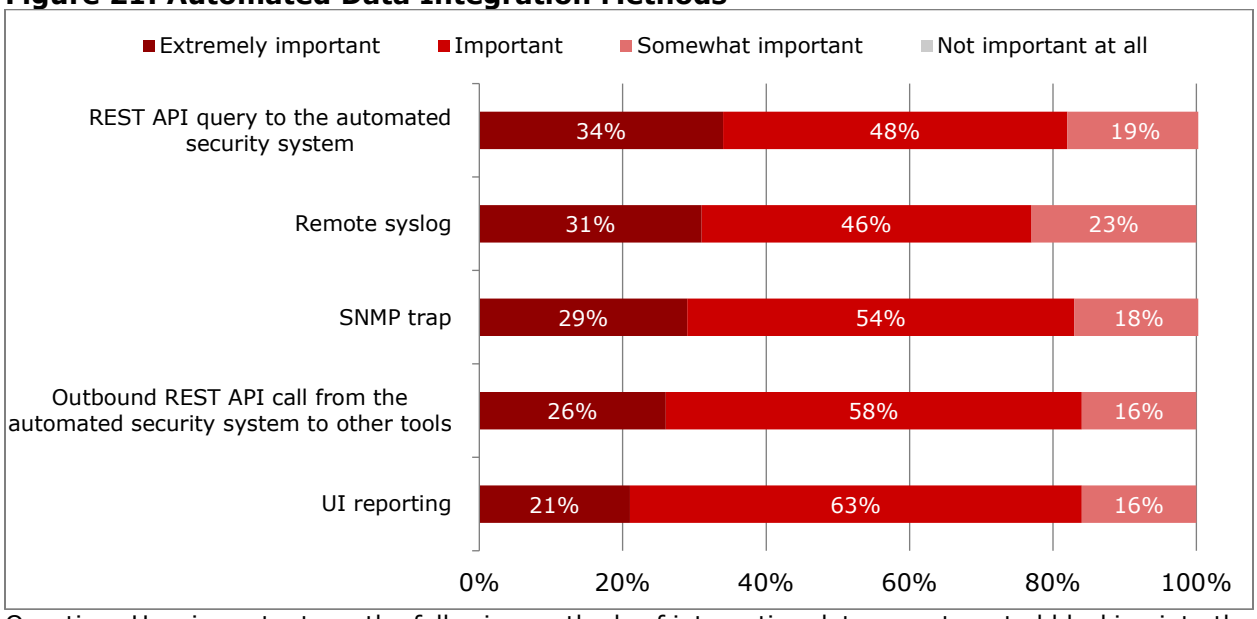


Question: To what extent do you currently rely on the following information when deciding to block traffic? (N=79-80)
Source: Heavy Reading

One of the considerations associated with using automated DDoS blocking is how to feed automated decision data into existing security and reporting systems. In this regard, as shown in **Figure 21**, based on "extremely important" responses, CSPs believe that the top three integration methods are to first look at application programming interface (API) query data (34%), then consider remote syslog (31%) and SNMP trap data (29%).

However, even the bottom two ranking methods of outbound REST API (26%) and user interface (UI) system reporting (21%) have enough support to constitute valid approaches.

Figure 21: Automated Data Integration Methods



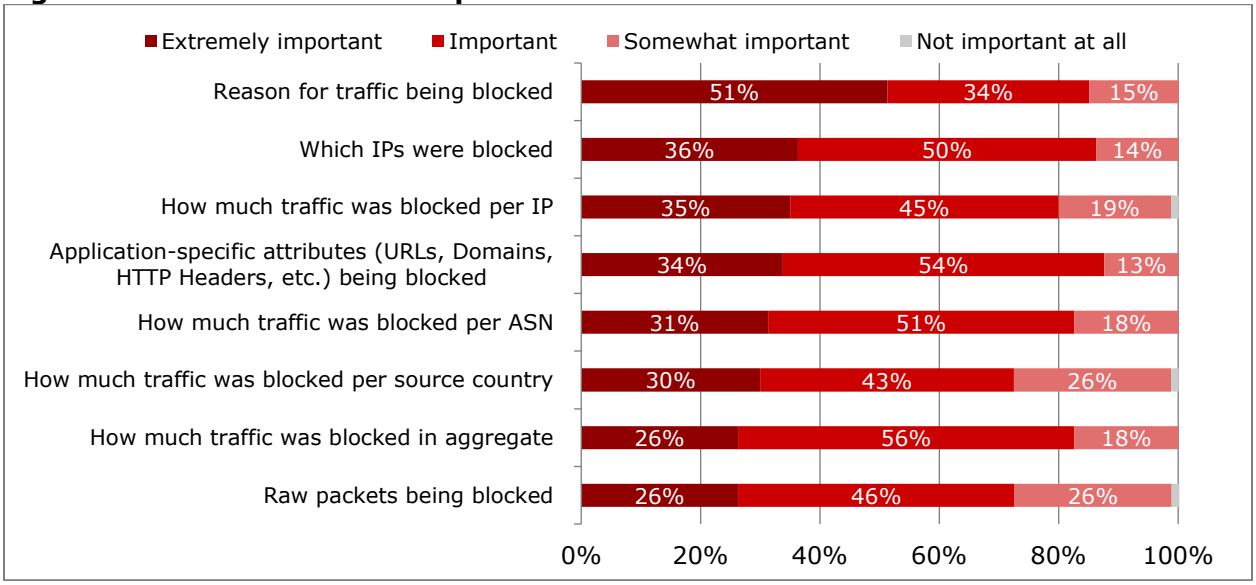
Question: How important are the following methods of integrating data on automated blocking into the rest of your security and reporting systems? (N=80)
Source: Heavy Reading

A related consideration in terms of managing the data generated by automated DDoS systems is what data should be exported to other security systems. Here, as shown in **Figure 22**, the survey respondents have a clear preference.

In this case, the leading data source based on "extremely important" response levels is the reason for the traffic being blocked (51%). This ranking also aligns with **Figure 13**, which documented this data as an "extremely important" component of an automated DDoS system.

Other vital data considerations rounding out the top three captured in **Figure 22** were "which IPs were blocked" (36%) and "how much traffic was blocked per IP address" (35%).

Figure 22: Automated Data Export



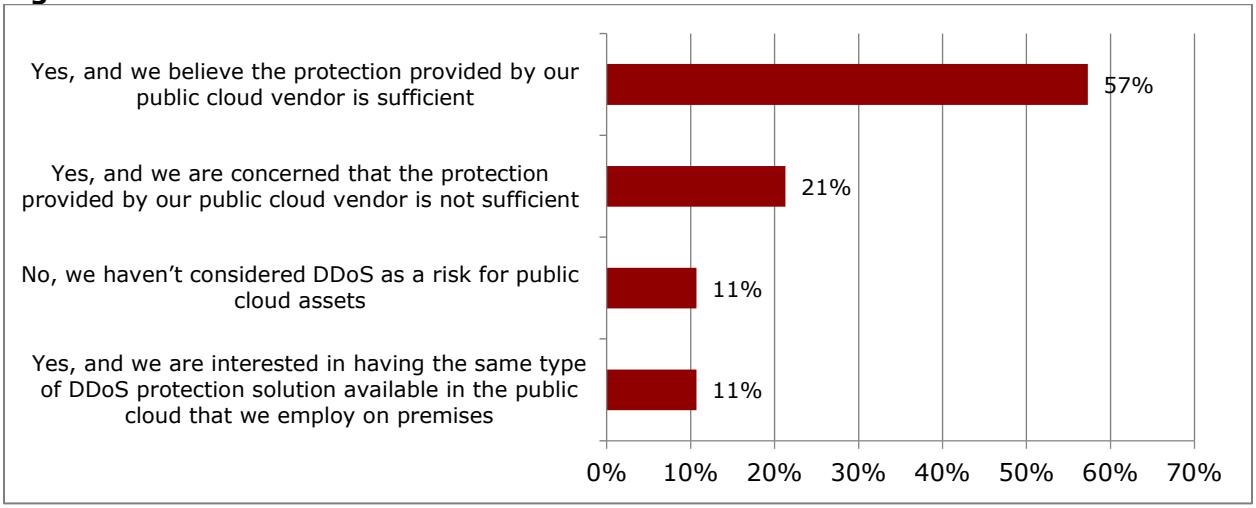
Question: When exporting information to other systems, how important is it for the automated security system to export the following types of information? (N=80)
Source: Heavy Reading

One emerging issue that CSPs must address is increasing customer demand to run business applications in the public cloud. While this is desirable because it provides greater access to low cost compute resources, it does have DDoS mitigation ramifications. The greatest concern is that, because these applications are no longer running in the telco cloud domain, the same level of security enforcement is not readily transportable to public cloud domain.

Instead, CSPs must rely solely on the public cloud provider to protect their applications from DDoS attacks. Interestingly, even in this "zero trust" age, as shown in **Figure 23** below, 57% of the respondents believe that their selected public cloud vendor will be able to provide adequate DDoS protection – even though there is little, if any, history to suggest this is the case.

Although relying on public cloud providers' security capabilities does simplify the transition of telco applications to the public cloud, Heavy Reading believes this approach will put CSPs in an even more vulnerable position if they have zero visibility into the nature of DDoS attacks or response strategies. But **only 21% of the survey respondents** shared this view and **are concerned that their public cloud partner will not be able to meet their requirements**.

Figure 23: DDoS and the Public Cloud

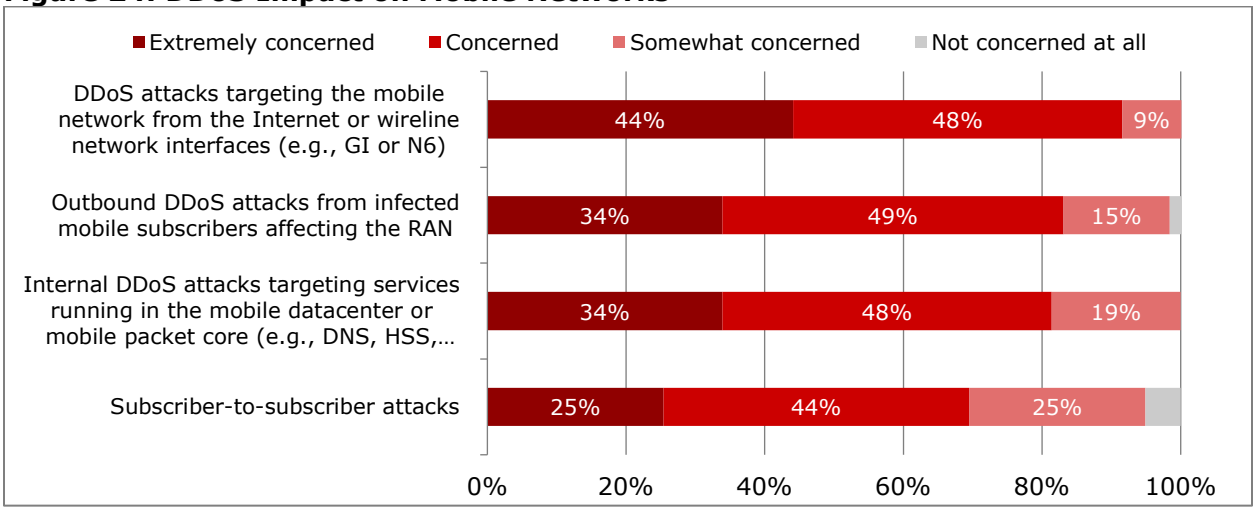


Question: Have you considered the risk of DDoS attacks for business applications you are migrating to the public cloud? (N=75)
Source: Heavy Reading

In order to provide a more granular view of DDoS impacts on mobile networks, the survey requested mobile and converged operators to provide insight into their concern levels associated with managing a range of DDoS attacks (e.g., internal attacks, outbound, and internet-based attacks). Of these various threat types, in this smaller sample of mobile operators only based on "extremely concerned" response levels, there is no shortage of internal or external threat types.

For example, as illustrated in **Figure 24**, while DDoS attacks originating from wireline network or the internet was the greatest concern (44%), the ranking and scoring of mobile-infected devices and internal attacks targeting the data center or core networks (both 34%) are also formidable concerns.

Figure 24: DDoS Impact on Mobile Networks



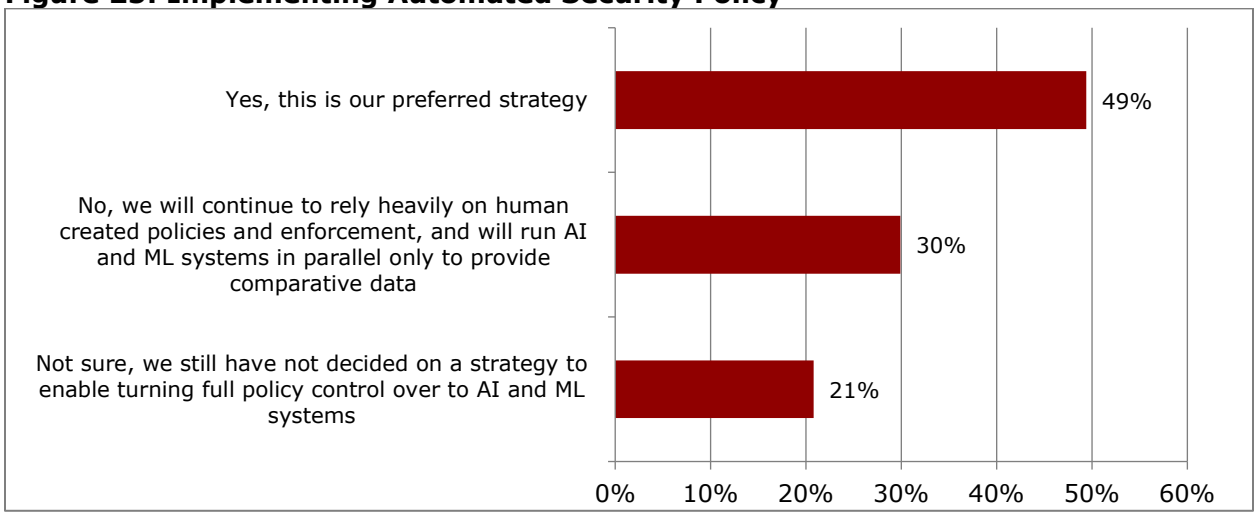
Question: If you are a mobile network provider, how concerned are you about the following potential DDoS threats affecting your mobile network? (N=59)
Source: Heavy Reading

The final question of the survey addressed implementing automated security policy. There are essentially two ways this can be approached. The first approach is to create security policies manually to create a foundation and then allow AI systems to assume full control of monitoring, tuning, and updating. As shown in **Figure 25**, this AI full control strategy is the preferred approach of almost half (49%) of the respondents.

The benefit of this approach is that it leverages the inherent strength of AI early in the implementation process. However, it does involve "a leap of faith" that the technology is ready for commercial deployment. Heavy Reading believes this willingness to trust automation to manage DDoS threats is why, as documented in **Figure 16**, a similar percentage of the survey respondents (40%) believe it is "extremely important" that they retain the ability to override automation decisions to maintain overall system control.

In contrast, the second approach, which attracted only 30% of the responses, involves continued reliance on manually created human processes, with AI and ML systems running in the background for comparative purposes only. While this more measured approach reduces the risk of ML-based error, it is realistically only sustainable for a short period of time given the additional expense and resources it consumes. It is also worth noting that a significant portion of the population (21%) have yet to decide on the optimal approach.

Figure 25: Implementing Automated Security Policy



Question: To what extent do you agree with the following statement? "Our approach to implementing automated security will be to create security policies manually but then turn over full control to AI systems for monitoring, tuning, and updating." (N=77)
Source: Heavy Reading

In comparing the U.S. and RoW filter groups, a number of observations stand out. The first is that while both groups prefer the full control option, U.S. respondents are more committed to this approach (63% vs. 36%). This is, in part, because a much larger group of RoW respondents (39%) fall into the "not sure" category versus only 3% of their U.S. counterparts (see **Figure 46**).

5. APPENDIX A: FILTER GROUP DATA

This appendix provides question response data for the two filter groups: the U.S. and the RoW. Key findings documenting response similarity and differences are also provided.

Figure 26: Security Team Hiring: U.S. vs. RoW
U.S. (N=39)

	Percent
We plan to grow our security team based on resources available	51%
We will stay as-is and only hire to maintain headcount	41%
We will likely reduce headcount	7%
Not sure/Don't know	7%

RoW (N=41)

	Percent
We plan to grow our security team based on resources available	34%
We will stay as-is and only hire to maintain headcount	44%
We will likely reduce headcount	12%
Not sure/Don't know	10%

Question: Which statement best reflects the hiring status of your security team resources over the next 12 months?
Source: Heavy Reading

Key Findings

While U.S. and RoW respondents are aligned in the sense that only a small percentage of respondents expect their companies to reduce security team headcount (7% vs. 12%), 51% of U.S. respondents expect to grow team resources compared to only 34% of RoW respondents. These are several factors in play here, including, as noted below, that U.S. respondents consider it less of a challenge to hire qualified security resources (see **Figure 28**).

Figure 27: OPSEC Development Team Challenges: U.S. vs. RoW
U.S. (N=39)

	Percent
Lack of headcount or resources	36%
Capital expenditure (capex) funding	44%
Operational expenditure (opex) funding	39%
Lack of internal stakeholder support	33%
Lack of management support	18%

RoW (N=41)

	Percent
Lack of headcount or resources	63%
Capital expenditure (capex) funding	49%
Operational expenditure (opex) funding	42%
Lack of internal stakeholder support	42%
Lack of management support	39%

Question: What challenges do you face in building and maintaining an effective OPSEC team? (Select all that apply)
Source: Heavy Reading

Key Findings

While RoW and U.S. respondents are generally aligned on the impact of capex and opex funding challenges, a much larger percentage of the RoW cited a lack of headcount resources (63% vs. 36% U.S.) and a lack of management support (39% vs. 18%) as two key challenge areas.

Figure 28: Hiring Qualified Security Team Resources: U.S. vs. RoW
U.S. (N=39)

	Percent
It is difficult to find and hire the right personnel	31%
Somewhat difficult, but we manage to find personnel	54%
Not difficult at all	15%

RoW (N=41)

	Percent
It is difficult to find and hire the right personnel	66%
Somewhat difficult, but we manage to find personnel	34%
Not difficult at all	0%

Question: How difficult is it to hire qualified security team resources for your organization?
Source: Heavy Reading

Key Findings

Similar to the input of the previous question, a much larger group of RoW respondents are encountering challenges in securing the team resources they vitally require (66% vs. 31%).

Figure 29: DDoS Protection Concern: U.S. vs. RoW

U.S. (N=39)

	Percent
Concerned	56%
Somewhat concerned	23%
Extremely concerned	21%
Not concerned at all	0%

RoW (N=40)

	Percent
Concerned	43%
Somewhat concerned	28%
Extremely concerned	28%
Not concerned at all	3%

Question: How concerned is your team/organization about protecting your infrastructure and application/services from a DDoS attack?
Source: Heavy Reading

Key Findings

Both groups displayed similar "somewhat concerned" and "extremely concerned" response levels. One notable difference was a higher level of "concerned" responses from U.S. respondents (56% vs. 43%). Heavy Reading believes this is, in part, attributable to the fact they had a slightly lower rate of "extremely concerned" responses (21% vs. 28%) than their RoW colleagues.

Overall, given the consistency in the distribution trend, Heavy Reading views the data as confirming that U.S. and RoW service providers have a similar level of concern about the threat that DDoS attacks present.

Figure 30: DDoS Attack Blocking Confidence: U.S. vs. RoW

U.S. (N=38)

	Percent
Very confident	29%
Confident	52%
Somewhat confident	18%

RoW (N=40)

	Percent
Very confident	13%
Confident	40%
Somewhat confident	48%

Question: To what extent are you confident in your ability to block DDoS attacks?
Source: Heavy Reading

Key Findings

There is considerable deviation here between the groups. While 81% of U.S. respondents are either "very confident" (29%) or "confident" (52%) in their ability to block DDoS attacks, only 53% of RoW respondents have similar views (13% and 40%, respectively).

As a result, a much greater percentage of RoW respondents (48%) assess their abilities as only "somewhat confident" versus 18% of U.S. respondents.

Figure 31: DDoS Blocking – Customer Perspective: U.S. vs. RoW
U.S. (N=38)

	Percent
Extremely important	40%
Important	58%
Somewhat important	3%

RoW (N=40)

	Percent
Extremely important	40%
Important	38%
Somewhat important	23%

Question: How important to your customers is your ability to block DDoS attacks?
Source: Heavy Reading

Key Findings

An identical number of U.S. and RoW (40%) respondents believe that it is "extremely important" to their customers that CSP networks block DDoS attacks. In Heavy Reading's view, this confirms the importance of protecting the customer from DDoS-initiated service outages.

Interestingly, RoW respondents had a considerably higher level of "somewhat important" response rates (23% vs. 3% for U.S. respondents). This suggests that, in some RoW markets, customers are less concerned about protection from DDoS attacks. One potential factor related to DDoS attack trends is discussed directly below in **Figure 32**.

Figure 32: DDoS 12-Month Attack Trends: U.S. vs. RoW

U.S. (N=39)

	Strong growth	Measured growth	No growth	Decrease in attacks	Not sure – we have no visibility in DDoS growth levels
Volume-based attacks (reflection / amplification attacks, other flooding attacks)	26%	51%	23%	0%	0%
Application-layer DDoS attacks (DNS, HTTP, etc.)	21%	54%	23%	3%	0%
Protocol attacks (state exhaustion, spoof SYN / TCP flood)	21%	54%	26%	0%	0%

RoW (N=41)

	Strong growth	Measured growth	No growth	Decrease in attacks	Not sure – we have no visibility in DDoS growth levels
Volume-based attacks (reflection / amplification attacks, other flooding attacks)	15%	61%	20%	0%	5%
Application-layer DDoS attacks (DNS, HTTP, etc.)	17%	56%	20%	2%	5%
Protocol attacks (state exhaustion, spoof SYN / TCP flood)	12%	59%	22%	2%	5%

Question: What has been the trend for the following types of DDoS attacks in your environment over the last 12 months?

Source: Heavy Reading

Key Findings

In looking at data by distinct groups, the percentage of "strong growth" metrics is higher among U.S. respondents (21% to 26% vs. 12% to 17% for RoW respondents). However, when the two growth categories are combined, the ranges are quite similar (75% to 77% for the U.S. vs. 71% to 76% for RoW), which indicates that growth in DDoS attacks is a global issue.

Figure 33: Implementing Automated DDoS Response: U.S. vs. RoW

U.S. (N=38)

	Percent
We have already implemented	40%
We will implement in less than 12 months	26%
We will implement in 12-18 months	18%
We will implement at some point	13%
We have no plans to implement	3%

RoW (N=41)

	Percent
We have already implemented	27%
We will implement in less than 12 months	12%
We will implement in 12-18 months	32%
We will implement at some point	27%
We have no plans to implement	2%

Question: When do you plan to implement automated technologies to respond to DDoS attacks without human intervention?

Source: Heavy Reading

Key Findings

While 40% of U.S. respondents have already implemented some form of automation, only 27% of RoW respondents have. However, within a 12- to 18-month window, the results are very similar (26% + 18% = 44% U.S. vs. 12% + 32% = 44% RoW), which reinforces the expectation that automation-based DDoS detection will be aggressively deployed globally.

Figure 34: DDoS Strategy Enforcement Strategy Factors: U.S. vs. RoW

U.S. (N=37-39)

	Extremely important	Important	Somewhat important	Not important	Will not implement
Automatically detect DDoS attacks	46%	44%	10%	0%	0%
Automatically block DDoS attacks	49%	39%	10%	3%	0%
Not blocking legitimate traffic	38%	41%	22%	0%	0%
Reporting what is being blocked and why	41%	38%	22%	0%	0%

RoW (N=40-41)

	Extremely important	Important	Somewhat important	Not important	Will not implement
Automatically detect DDoS attacks	44%	37%	20%	0%	0%
Automatically block DDoS attacks	39%	49%	12%	0%	0%
Not blocking legitimate traffic	50%	33%	18%	0%	0%
Reporting what is being blocked and why	37%	39%	15%	10%	0%

Question: How important are the following to your DDoS security enforcement strategy?
Source: Heavy Reading

Key Findings

The strong level of alignment between RoW and U.S. "extremely important" responses (U.S. 38% to 49% vs. RoW 37% to 50%) confirms that these capabilities are vital components of an effective DDoS security enforcement strategy for all service providers.

Figure 35: Security Capability Support Confidence Levels: U.S. vs. RoW
U.S. (N=37-39)

	Extremely confident	Confident	Somewhat confident	Not confident	Will not implement
Automatically detect DDoS attacks	28%	49%	18%	5%	0%
Automatically block DDoS attacks	26%	56%	13%	5%	0%
Not block legitimate traffic	21%	50%	18%	11%	0%
Report what is being blocked and why	22%	41%	32%	5%	0%

RoW (N=40-41)

	Extremely confident	Confident	Somewhat confident	Not confident	Will not implement
Automatically detect DDoS attacks	15%	39%	32%	12%	2%
Automatically block DDoS attacks	10%	34%	34%	22%	0%
Not block legitimate traffic	10%	37%	44%	10%	0%
Report what is being blocked and why	10%	40%	40%	10%	0%

Question: How confident are you in your current ability to support the following security capabilities?
Source: Heavy Reading

Key Findings

Overall, U.S. CSPs are considerably more confident than their RoW counterparts. For example, while only 18% of U.S. respondents are either "somewhat confident" (13%) or "not confident" (5%) in their ability to automatically block DDoS attacks, RoW response levels hit the 56% mark (34% and 22%, respectively).

Figure 36: Automated Attack Blocking Preferences: U.S. vs. RoW

U.S. (N=39)

	Percent
No automated blocking of attacks	18%
Automated blocking of volumetric floods only	54%
Automated blocking of volumetric and protocol attacks (spoofed, SYN flood, etc.)	44%
Automated blocking of volumetric, protocol, and application-layer attacks	39%

RoW (N=41)

	Percent
No automated blocking of attacks	24%
Automated blocking of volumetric floods only	49%
Automated blocking of volumetric and protocol attacks (spoofed, SYN flood, etc.)	63%
Automated blocking of volumetric, protocol, and application-layer attacks	49%

Question: There are different degrees of automated blocking of attacks that can be achieved. Please indicate which degree(s) of automated blocking you find desirable? (Select all that apply)
Source: Heavy Reading

Key Findings

Although RoW survey respondents prefer the automated blocking of both volumetric and protocol attacks (63% vs. 44% U.S.), the overall trends are quite similar, especially with respect to the no automated blocking option (18% U.S. vs. 24% RoW).

Figure 37: Ranking Automated Security Response Attributes: U.S. vs. RoW

U.S. (N=39)

	Extremely important	Important	Somewhat important	Not important	Will not implement
Ability to override automation decisions	41%	39%	18%	3%	0%
Minimizing false positive detections	28%	51%	21%	0%	0%
Ability to view what automated blocking decisions have been made	26%	56%	18%	0%	0%

	Extremely important	Important	Somewhat important	Not important	Will not implement
Use cyber threat intelligence feeds to automatically block threats	33%	36%	31%	0%	0%
Communicate automated decisions with other security tools	31%	36%	28%	5%	0%
Use machine learning/artificial intelligence to automatically block threats	31%	46%	23%	0%	0%
Minimizing over-blocking during mitigation	26%	54%	18%	3%	0%

RoW (N=41)

	Extremely important	Important	Somewhat important	Not important	Will not implement
Ability to override automation decisions	39%	39%	15%	7%	0%
Minimizing false positive detections	34%	46%	17%	2%	0%
Ability to view what automated blocking decisions have been made	34%	46%	17%	2%	0%
Use cyber threat intelligence feeds to automatically block threats	22%	54%	15%	7%	2%
Communicate automated decisions with other security tools	20%	56%	20%	2%	2%
Use machine learning/artificial intelligence to automatically block threats	17%	44%	27%	10%	2%
Minimizing over-blocking during mitigation	15%	61%	22%	2%	0%

Question: How important are the following attributes in the implementation of an automated security response system?
Source: Heavy Reading

Key Findings

Although U.S. respondents displayed a greater tendency to characterize more of the security attributes as "extremely important," overall, there are a number of similarities. One example is that both groups assessed the ability to override automation decisions as the

number one most important automaton attribute (U.S. 41% vs. RoW 39%). Similarly, in both cases, minimizing over-blocking achieved the lowest ranking of "extremely important" responses (U.S. 26% vs. RoW 15%).

Figure 38: Automated Blocking Implementation Challenges: U.S. vs. RoW

U.S. (N=39)

	Major challenge	Challenge	Somewhat of a challenge	Not a challenge at all
Understanding the protected services/applications well enough to determine automated blocking policy	15%	56%	23%	5%
Understanding what kind of traffic a solution may block	21%	56%	23%	0%
Authenticating legitimate users versus attackers	10%	67%	21%	3%
Whitelisting specific traffic that should never be blocked	15%	49%	31%	5%
User-visible impact of authenticating users	13%	64%	23%	0%

RoW (N=41)

	Major challenge	Challenge	Somewhat of a challenge	Not a challenge at all
Understanding the protected services/applications well enough to determine automated blocking policy	20%	42%	32%	7%
Understanding what kind of traffic a solution may block	7%	54%	32%	7%
Authenticating legitimate users versus attackers	17%	46%	29%	7%
Whitelisting specific traffic that should never be blocked	12%	34%	44%	10%
User-visible impact of authenticating users	5%	49%	39%	7%

Question: Please rate the following challenges you face in implementing automation-based solutions to prevent blocking of legitimate traffic?

Source: Heavy Reading

Key Findings

Both groups are aligned in that they anticipate a very similar range of "major challenges" (U.S. 10% to 21% vs. RoW 5% to 20%). Beyond this, more RoW responses fall into the "somewhat of a challenge" category, which indicates they are less concerned about them.

Figure 39: Advanced Security Support Capability Confidence: U.S. vs. RoW

U.S. (N=39)

	Extremely confident	Confident	Somewhat confident	Not confident at all
Ability to utilize AI/ML techniques to prevent blocking of legitimate traffic that emulates a DDoS attack	23%	54%	21%	3%
Ability to block DDoS attacks utilizing automated security products	31%	49%	21%	0%
Ability to override automated security decisions	26%	62%	10%	3%
Ability to block traffic with the required level of data collection and documentation to justify action	18%	62%	15%	5%

RoW (N=41)

	Extremely confident	Confident	Somewhat confident	Not confident at all
Ability to utilize AI/ML techniques to prevent blocking of legitimate traffic that emulates a DDoS attack	7%	27%	54%	12%
Ability to block DDoS attacks utilizing automated security products	15%	44%	32%	10%
Ability to override automated security decisions	10%	46%	37%	7%
Ability to block traffic with the required level of data collection and documentation to justify action	10%	49%	32%	10%

Question: What is your level of confidence for supporting the following capabilities?
Source: Heavy Reading

Key Findings

U.S. respondents are more confident in their ability to support automated capabilities based on range of "extremely confident" responses (U.S. 18% to 31% vs. RoW 7% to 15%). Moreover, a significantly greater percentage of U.S. respondents are "confident" (U.S. 49% to 62% vs. RoW 27% to 49%). In contrast, a greater percentage of RoW CSPs view themselves as "not confident at all" (U.S. 0% to 5% vs. RoW 7% to 12%).

Figure 40: Authentication Capabilities: U.S. vs. RoW

U.S. (N=39)

	Extremely important	Important	Somewhat important	Not important at all
Transparent authentication mechanisms (i.e., not visible to user)	23%	59%	18%	0%
User-visible authentication mechanisms	28%	59%	13%	0%
Geographic-based filtering of users	23%	44%	31%	3%
Ability to distinguish users behind a proxy	18%	67%	13%	3%
Block and look for retransmission of request	28%	56%	15%	0%
JavaScript-based authentication	21%	56%	23%	0%
reCAPTCHA	26%	54%	18%	3%
Rate-based validation (e.g., HTTP request rate or total traffic rate)	21%	67%	13%	0%

RoW (N=41)

	Extremely important	Important	Somewhat important	Not important at all
Transparent authentication mechanisms (i.e., not visible to user)	34%	42%	22%	2%
User-visible authentication mechanisms	27%	54%	17%	2%
Geographic-based filtering of users	29%	46%	20%	5%
Ability to distinguish users behind a proxy	27%	42%	27%	5%
Block and look for retransmission of request	15%	54%	32%	0%

	Extremely important	Important	Somewhat important	Not important at all
JavaScript-based authentication	20%	42%	34%	5%
reCAPTCHA	10%	63%	27%	0%
Rate-based validation (e.g., HTTP request rate or total traffic rate)	15%	59%	27%	0%

Question: How important are the following capabilities for enabling authentication of legitimate user traffic versus a traffic generating bot in protected applications?
Source: Heavy Reading

Key Findings

Based on "extremely important" response levels, the top three preferred approaches for U.S. respondents are user-visible authentication and block, look for transmission request (both 28%), and reCAPTCHA (26%).

In contrast, RoW respondents' top three authentication capabilities are transparent authentication mechanisms (34%), geographic-based filtering of users (29%), and user-visible authentication and ability to distinguish users behind a proxy (both 27%).

Figure 41: Information Sources: U.S. vs. RoW
U.S. (N=38)

	Primary source – we rely heavily on this information	Secondary source – we may use it	Not a source – we don't consider when making blocking decisions
Abnormal increase in traffic from a specific application/protocol	55%	45%	0%
Abnormal increase in traffic from a specific IP domain	45%	50%	5%
Behavioral analysis of traffic patterns – baseline with normal traffic patterns	53%	37%	11%
Abnormal increase in traffic from a specific geographic region	47%	47%	5%
Blacklist versus whitelist	34%	58%	8%

RoW (N=40-41)

	Primary source – we rely heavily on this information	Secondary source – we may use it	Not a source – we don't consider when making blocking decisions
Abnormal increase in traffic from a specific application/protocol	54%	39%	7%
Abnormal increase in traffic from a specific IP domain	63%	35%	3%
Behavioral analysis of traffic patterns – baseline with normal traffic patterns	46%	46%	7%
Abnormal increase in traffic from a specific geographic region	44%	46%	10%
Blacklist versus whitelist	42%	51%	7%

Question: To what extent do you currently rely on the following information when deciding to block traffic?
Source: Heavy Reading

Key Findings

Primary data source preferences between the two filter groups are somewhat similar, except that RoW respondents are more committed to the abnormal traffic increase from a specific IP domain (RoW 63% vs. U.S. 45%) and usage of blacklists and whitelists (RoW 42% and U.S. 34%).

Figure 42: Automated Data Integration Methods: U.S. vs. RoW
U.S. (N=39)

	Extremely important	Important	Somewhat important	Not important at all
REST API query to the automated security system	41%	44%	15%	0%
Remote syslog	33%	49%	18%	0%
SNMP trap	36%	49%	15%	0%
Outbound REST API call from the automated security system to other tools	33%	51%	15%	0%
UI reporting	31%	51%	18%	0%

RoW (N=40-41)

	Extremely important	Important	Somewhat important	Not important at all
REST API query to the automated security system	27%	51%	22%	0%
Remote syslog	29%	44%	27%	0%
SNMP trap	22%	59%	20%	0%
Outbound REST API call from the automated security system to other tools	20%	63%	17%	0%
UI reporting	12%	73%	15%	0%

Question: How important are the following methods of integrating data on automated blocking into the rest of your security and reporting systems?
Source: Heavy Reading

Key Findings

While the range of "extremely important" responses is higher for U.S. respondents (31% to 41% vs. RoW 12% to 29%), the priority rankings are similar. For example, the top three ranked data integration methods for U.S. respondents are API query (41%), SNMP trap (36%), and remote syslog and outbound API (both 33%). The top three priorities for RoW respondents in order are remote syslog (29%), API query (27%), and SNMP trap (22%).

Figure 43: Automated Data Export: U.S. vs. RoW
U.S. (N=39)

	Extremely important	Important	Somewhat important	Not important at all
Reason for traffic being blocked	54%	36%	10%	0%
Which IPs were blocked	31%	59%	10%	0%
How much traffic was blocked per IP	31%	51%	18%	0%
Application-specific attributes (URLs, domains, HTTP headers, etc.) being blocked	36%	54%	10%	0%
How much traffic was blocked per ASN	31%	54%	15%	0%
How much traffic was blocked per source country	28%	44%	28%	0%
How much traffic was blocked in aggregate	33%	54%	13%	0%
Raw packets being blocked	33%	46%	21%	0%

RoW (N=41)

	Extremely important	Important	Somewhat important	Not important at all
Reason for traffic being blocked	49%	32%	20%	0%
Which IPs were blocked	42%	42%	17%	0%
How much traffic was blocked per IP	39%	39%	20%	2%
Application-specific attributes (URLs, domains, HTTP headers, etc.) being blocked	32%	54%	15%	0%
How much traffic was blocked per ASN	32%	49%	20%	0%
How much traffic was blocked per source country	32%	42%	24%	2%
How much traffic was blocked in aggregate	20%	59%	22%	0%
Raw packets being blocked	20%	46%	32%	2%

Question: When exporting information to other systems, how important is it for the automated security system to export the following types of information?
Source: Heavy Reading

Key Findings

For both filter groups, the reason for blocking traffic attained the highest level of "extremely important" responses (U.S. 54% vs. RoW 49%). For U.S. respondents, the second and third priorities were application-specific attributes (36%) and aggregate blocked traffic and raw packets blocked (both 33%). For the RoW, the second and third priorities were which IPs were blocked (42%) and the amount of traffic blocked per IP address (39%).

Figure 44: DDoS and the Public Cloud: U.S. vs. RoW
U.S. (N=35)

	Percent
Yes, and we believe the protection provided by our public cloud vendor is sufficient	63%
Yes, and we are concerned that the protection provided by our public cloud vendor is not sufficient	26%
No, we haven't considered DDoS as a risk for public cloud assets	6%
Yes, and we are interested in having the same type of DDoS protection solution available in the public cloud that we employ on premises	6%

RoW (N=40)

	Percent
Yes, and we believe the protection provided by our public cloud vendor is sufficient	53%
Yes, and we are concerned that the protection provided by our public cloud vendor is not sufficient	18%
No, we haven't considered DDoS as a risk for public cloud assets	15%
Yes, and we are interested in having the same type of DDoS protection solution available in the public cloud that we employ on premises	15%

Question: Have you considered the risk of DDoS attacks for business applications you are migrating to the public cloud?
Source: Heavy Reading

Key Findings

Although a greater percentage of RoW respondents do not consider DDoS a risk for applications running in the public cloud (15% vs. U.S. 6%), both groups are generally comfortable that the DDoS protection provided by the public cloud vendor is sufficient (U.S. 63% vs. RoW 53%).

Figure 45: DDoS Impact on Mobile Networks: U.S. vs. RoW
U.S. (N=29)

	Extremely concerned	Concerned	Somewhat concerned	Not concerned at all
DDoS attacks targeting the mobile network from the Internet or wireline network interfaces (e.g., GI or N6)	45%	52%	3%	0%
Outbound DDoS attacks from infected mobile subscribers affecting the RAN	38%	48%	14%	0%
Internal DDoS attacks targeting services running in the mobile datacenter or mobile packet core (e.g., DNS, HSS, content caching servers)	24%	59%	17%	0%
Subscriber-to-subscriber attacks	31%	41%	24%	3%

RoW (N=30)

	Extremely concerned	Concerned	Somewhat concerned	Not concerned at all
DDoS attacks targeting the mobile network from the Internet or wireline network interfaces (e.g., GI or N6)	43%	43%	13%	0%
Outbound DDoS attacks from infected mobile subscribers affecting the RAN	30%	50%	17%	3%
Internal DDoS attacks targeting services running in the mobile datacenter or mobile packet core (e.g., DNS, HSS, content caching servers)	43%	37%	20%	0%
Subscriber-to-subscriber attacks	20%	47%	27%	7%

Question: If you are a mobile network provider, how concerned are you about the following potential DDoS threats affecting your mobile network?
Source: Heavy Reading

Key Findings

Given the consistency in response weighting, it is clear that, globally, many CSPs harbor similar concerns about the serious impacts that both internal and external DDoS attacks could have on their mobile networks.

Figure 46: Implementing Automated Security Policy: U.S. vs. RoW
U.S. (N=38)

	Percent
Yes, this is our preferred strategy	63%
No, we will continue to rely heavily on human-created policies and enforcement and will run AI and ML systems in parallel only to provide comparative data	34%
Not sure, we still have not decided on a strategy to enable turning full policy control over to AI and ML systems	3%

RoW (N=39)

	Percent
Yes, this is our preferred strategy	36%
No, we will continue to rely heavily on human-created policies and enforcement and will run AI and ML systems in parallel only to provide comparative data	26%
Not sure, we still have not decided on a strategy to enable turning full policy control over to AI and ML systems	39%

Question: To what extent do you agree with the following statement? "Our approach to implementing automated security will be to create security policies manually but then turn over full control to AI systems for monitoring, tuning, and updating."
Source: Heavy Reading

Key Findings

In comparing the two filter groups, a number of observations stand out to Heavy Reading. The first is that while both groups prefer the "full control" option, U.S. respondents are more committed to this approach (63% vs. 36%). This is, in part, because (as also noted) a much larger group of RoW respondents (39%) fall into the "not sure" category versus only 3% of their U.S. counterparts.

TERMS OF USE

LICENSE AGREEMENT
This report and the information therein are the property of or licensed to Heavy Reading, and permission to use the same is granted to purchasers under the terms of this License Agreement ("Agreement"), which may be amended from time to time without notice. The purchaser acknowledges that it is bound by the terms and conditions of this Agreement and any amendments thereto.

OWNERSHIP RIGHTS
All Reports are owned by Heavy Reading and protected by United States Copyright and international copyright/intellectual property laws under applicable treaties and/or conventions. The purchaser agrees not to export this report into a country that does not have copyright/intellectual property laws that will protect Heavy Reading's rights therein.

GRANT OF LICENSE RIGHTS
Heavy Reading hereby grants the purchaser a non-exclusive, non-refundable, non-transferable license to use the report for research purposes only pursuant to the terms and conditions of this Agreement. Heavy Reading retains exclusive and sole ownership of all reports disseminated under this Agreement. The purchaser agrees not to permit any unauthorized use, reproduction, distribution, publication or electronic transmission of this report or the information/forecasts therein without the express written permission of Heavy Reading.

DISCLAIMER OF WARRANTY AND LIABILITY
Heavy Reading has used its best efforts in collecting and preparing this report. Heavy Reading, its employees, affiliates, agents and licensors do not warrant the accuracy, completeness, currentness, noninfringement, merchantability or fitness for a particular purpose of any material covered by this Agreement. Heavy Reading, its employees, affiliates, agents or licensors shall not be liable to the purchaser or any third party for losses or injury caused in whole or part by Heavy Reading's negligence or by contingencies beyond Heavy Reading's control in compiling, preparing or disseminating this report, or for any decision made or action taken by the purchaser or any third party in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if Heavy Reading was advised of the possibility of the same. The purchaser agrees that the liability of Heavy Reading, its employees, affiliates, agents and licensors, if any, arising out of any kind of legal claim (whether in contract, tort or otherwise) in connection with its goods/services under this Agreement shall not exceed the amount the purchaser paid to Heavy Reading for use of this report.

DISPUTE RESOLUTION
This License will be governed by the laws of the State of New York. In case of a dispute arising under or related to this License, the parties agree to binding arbitration before a single arbitrator in the New York City office of the American Arbitration Association. The prevailing party will be entitled to recover its reasonable attorney fees and costs.

Heavy Reading
P.O. Box 1953
New York, NY 10156
Phone: +1 212-600-3000
www.heavyreading.com