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

HEAVY READING
CUSTOM REPORTS

Heavy Reading's 2019 SD-WAN Security Survey

A Custom Research Report Produced for Amdocs, Fortinet, Lavelle Networks, and Nuage Networks

AUTHOR: JIM HODGES, CHIEF ANALYST, HEAVY READING

TABLE OF CONTENTS

1. INTRODUCTION AND KEY FINDINGS

Software-defined wide-area networks (SD-WANs) burst onto the commercial telecom landscape about 4 years ago in response to industry requirements to deliver a lower cost, more programmable connectivity model. This model also had to be capable of exploiting the service potential of cloud networks.

While the early deployments focused on cost models, it did not take long for SD-WAN to also concentrate on enhancing cloud service delivery. In response, SD-WAN is now being positioned as an essential technology to secure the cloud, and the security value proposition is strong. SD-WAN is able to not only manage complex security routing algorithms, but also enhance core and edge networks since it can apply security policy on an application basis. Today, SD-WAN security service adoption is still maturing. However, as 5G networks that utilize an application-centric services model are further commercialized, SD-WAN security capabilities will only increase in value and relevance.

This report presents in detail the key findings of an extensive Heavy Reading market leadership study documenting communications service providers' (CSPs') current and future plans to leverage SD-WAN security services. These CSPs aim to drive the growth of the managed security services they provide to enterprise customers.

1.1 Executive Key Findings

At a minimum, **69% of survey respondents believe it is either "extremely important" (18%-40%) or "important" (42%-55%) that their SD-WAN solution supports security services.**

SD-WAN security services are experiencing strong growth. For a top-ranked capability such as virtual firewall (vFirewall), this translates into 28% of CSPs experiencing an aggressive annual growth rate and 36% experiencing a moderate growth rate.

Only 8% of CSPs plan *not to* integrate their SD-WAN security services into their security as a service (SECaaS) portfolio.

CSPs prefer deploying SD-WAN security services in their telco cloud, but they also see some specific services as well-suited to branch deployments.

The open-source vendor-agnostic orchestration model is the top choice for orchestrating security virtual network functions (VNFs; 34%).

While there is some general support for service-chaining security VNFs, **the range of "may offer" (38%-48%) responses indicate that many CSPs have still not decided if the service-chaining path is viable.**

Approximately **6 out of 10 CSPs already support or plan to implement a broad range of analytics capabilities** to enhance SD-WAN security service delivery.

59% of the respondents believe that integrating automation into SD-WAN will be very complex to implement but overall will have a positive impact. The second largest group indicated it also believes automation will have a positive impact (27%) but does not anticipate a complex implementation process.

1.2 Key Findings

Managed security services are now a fundamental component of SD-WAN deployments. This is in large part due to the broad range of high-value services supported.

Of these "extremely important" high-value services, the top four that resonated with survey respondents were **vFirewall (40%), intrusion prevention (35%), distributed denial-of-service (DDoS) mitigation (34%), and secured SD-branch (30%).**

However, other application-focused services also fared consistently well in the "extremely important" rankings. These include **application control (26%), web filtering (25%), and packet filtering (25%).**

The strategic importance of these services has already resulted in a significant number of implementations. vFirewall (34%) is the most deployed capability, followed by DDoS mitigation and intrusion prevention (both tied at 29%). However, a substantial number of CSPs have also implemented web filtering (26%), application control, and packet filtering (both 24%).

The pace of implementations will continue to aggressively ramp up. Approximately 50% of the CSPs are either currently implementing security services (23%-36%) or plan to implement within 12-18 months (23%-36%). This translates to more than 70% having commercial services in place within 18 months.

Strong business demand is fueling these deployments. CSPs believe their "most aggressive" growth business opportunities are vFirewall (28%), DDoS mitigation and intrusion prevention (both 23%), and application control (21%). These capabilities represent the most potent growth opportunities. Still, it is worth noting that based on "aggressive growth" inputs, all the capabilities had solid levels of support. Based on "moderate growth" inputs, packet filtering (40%) and web filtering (38%) attained the highest scores.

CSPs are also focusing on utilizing security services to differentiate their SD-WAN offerings. The strategy that attained the greatest support level is to offer their enterprise customers a number of security bundles they can select based on their requirements (36%).

However, the second-ranked option is also important since it advocates an even more flexible choice-driven approach. In this case, the option is based on allowing the customers to select from an ecosystem of vendors supported by the CSPs' SD-WAN security bundles (24%). The third-ranked-option (14%) – a "best-of-breed" option – is also important because it reflects the input by many CSPs to move to a more flexible vendor model.

Support for this third option is already starting to affect the vendor selection process. Almost half of the respondents (46%) indicated they prefer to use a mix of embedded security features from their primary vendor, as well as third-party best-of-breed vendor features.

Even more, telling is that 29% of respondents ranked the standalone third-party vendor option (29%) over the primary vendor option (17%). This reinforces the finding that more CSPs favor the flexibility of third-party solutions.

CSPs see three distinct options for how to integrate SD-WAN managed security services into their SECaaS portfolios. The largest group (37%) is in favor of integrating some specific features into their SECaaS portfolios and not others. A second group (28%) advocates an "integrate them all" approach to achieve single pane of glass monitoring and create a single security support team. The third group (28%) is focused on partial integration like the first but plans to transition to a fully integrated model. Taken together, 56% (28% + 28%) of the survey respondents prefer the fully integrated model but will follow different implementation paths.

Most CSPs prefer the security solution for their SD-WAN service to be deployed in their telco cloud while smaller groups support customer site or public cloud deployment models. There are two viable telco cloud options. The first is the approach of deploying SD-WAN security services independently of the basic SD-WAN services platform (34%) followed closely by the integrated SD-WAN telco cloud model (30%). In third place was the customer site deployment model (12%) followed by public cloud (6%).

Despite the telco cloud preference, there is also solid support for deploying some security features in the branch. Of these, the top-ranked service was secure SD-branch (38%), followed by packet filtering and vFirewall (both 36%).

CSPs are making progress in utilizing VNFs for SD-WAN bundled managed security services. Based on the range of "already implemented" (10%-32%) and "plan to implement in 12 months" (27%-40%) responses, the top three priorities are vFirewall (32% + 27%), intrusion prevention (25% + 30%), and DDoS mitigation (24% + 33%). U.S. respondents are well ahead in terms of implementing VNF-based SD-WAN security service bundles.

CSPs see a number of viable options for orchestrating these VNFs. More than a third of the respondents (34%) prefer to utilize a third-party open-source orchestrator that is SD-WAN vendor-agnostic and can be deployed in multiple environments. In second place (30%) is support for a third-party but proprietary network functions virtualization (NFV) orchestrator. Next is the "status quo" option of utilizing the SD-WAN orchestrator followed by the SD-WAN vendor (25%).

Heavy Reading believes that the number one ranking of the open-source vendor-agnostic orchestration option is significant and confirms that CSPs are focused on solutions that minimize vendor lock-in. The process will be gradual given that CSPs have a number of factors to balance. These include balancing vendor relationships with the need to deploy reliable and potentially proprietary cost-effective solutions that work.

CSPs' branch-based security strategies include support of both local internet breakout and all communications services. For example, a greater number of CSPs have already implemented local internet breakout (34%) compared to those that are utilizing SD-WAN branch-based security services to support all communications services (28%). However, based on "currently implementing" response levels, all communications services model leads (40% vs. 34%).

One viable approach to offer SD-WAN security services in the branch is to embed them as VNFs into a universal customer premises equipment (uCPE) appliance. The top three preferences for VNFs in uCPE based on the "already implemented" status are familiar priorities: vFirewall (32%), DDoS mitigation (30%), and intrusion prevention (28%). The top three capabilities "currently being implemented" are vSBC (36%), intrusion prevention (35%), and vFirewall and SSL inspection (both 34%).

However, the ongoing industry push to deploy low-cost devices in the branch will have SD-WAN security service delivery business implications. The gravest concern based on "major challenge" inputs is that low-cost expectations will make it difficult to upsell SD-WAN security services (32%) in the branch.

Low cost, limited intelligence branch devices are not only a business concern, but they also have negative technical implications. Of these, based on "major challenge" responses, the top three areas are concerns about the performance implications on devices when security capabilities are added (27%), lack of security certification for devices (25%), and the diverse set of devices that must be secured (19%).

While some CSPs are considering implementing service-chained security VNFs, others are still not sure if this approach is viable. Based on "will offer" inputs, the leading candidates for service chaining are vFirewall (39%), DDoS mitigation (34%), and intrusion prevention (33%), followed closely by other functions such as application control (32%) and web filtering (28%). However, the range of "may offer" (38%-48%) and "will not offer" (11%-16%) responses identifies that many CSPs have still not decided if the service-chaining path is viable.

The **largest group of CSPs surveyed (39%-51%) believe that they will face a "complex but manageable" path to evolve existing SD-WAN security services** to support new technology rollouts such as multi-access edge computing (MEC) and 5G. In contrast, 15% to 23% indicated that they expect a very complex migration, with the 5G Next-Generation Core (NGC) core implementation representing the greatest challenge.

Approximately 6 out of 10 CSPs already support or plan to implement a broad range of analytics capabilities to enhance SD-WAN security service delivery. The top three capabilities "already supported" are network traffic analysis (37%), URLs accessed (33%), and application usage (30%). The top three capabilities "currently being implemented" include user profile data (37%), regulatory compliance metrics (34%), and threats mitigated or blocked and application usage (both 33%). The top three analytics capabilities that fall into the "may implement" category are incident forensics (49%), geolocation attack data (43%), and regulatory compliance metrics (40%).

59% of the respondents believe that integrating automation into SD-WAN will be very complex to implement but overall will have a positive impact. The second largest group also believes automation will have a positive impact (27%) but does not anticipate a complex implementation process. This leaves two small groups of respondents who believe automation will not have a positive impact (6%) or have yet to form an opinion (7%).

CSPs expect that automation, specifically the implementation of automated security policies, will have a positive impact on SD-WAN managed security service performance. Based on "extremely positive impact" responses, the capabilities that will realize the greatest benefit are vFirewall (33%), intrusion prevention(29%), and DDoS mitigation (27%). However, as seen before, capabilities such as application control, web filtering, and packet filtering are behind only by a few points (24%-26%), emphasizing their overall strong value proposition.

As SD-WAN security services evolve, in addition to automation, they will also need to implement other advanced capabilities. Based on the level of "extremely important" and "important" responses, three capabilities stand out.

The highest-ranked of these is the ability to utilize SD-WAN security policies to steer applications to multiple scanners based on specific application requirements (38%). Very closely behind at 37% is signature-based detection in the SD-WAN device. The third-ranked advanced capability focuses on applying SD-WAN security policies in the branch to first ensure the devices and applications in the branch are fully compliant to the cloud(s) they will run in (32%).

2. SURVEY DEMOGRAPHICS SUMMARY

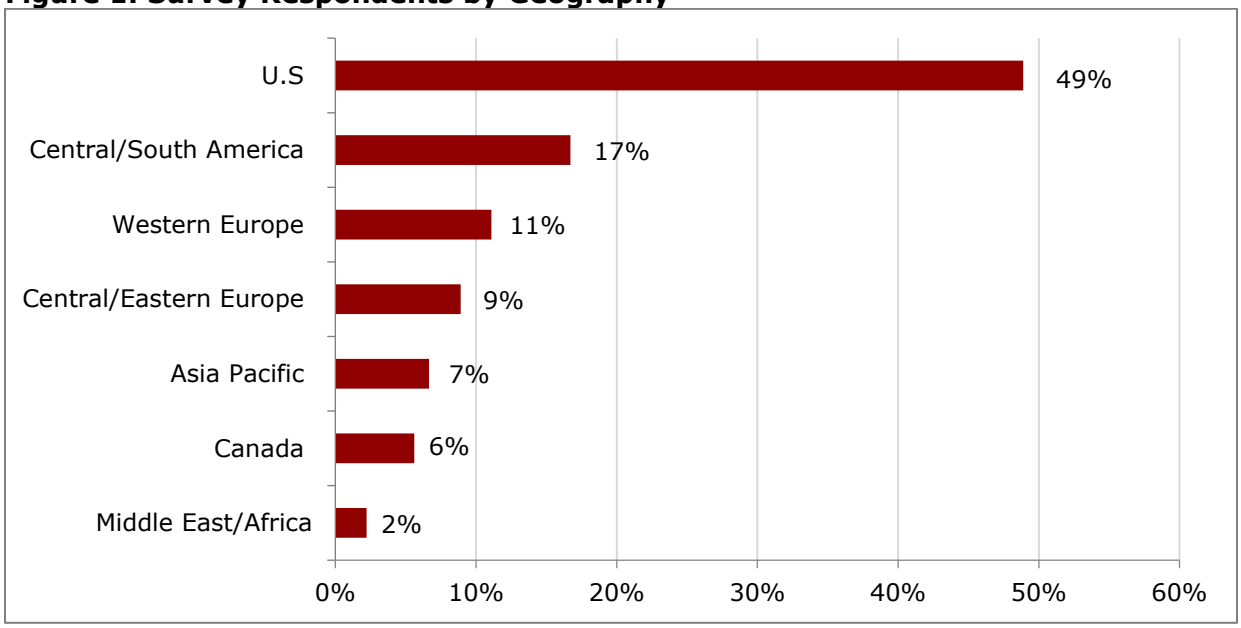
This research report is based on a comprehensive online survey launched in 4Q 2019. The survey created by Heavy Reading in collaboration with research sponsors Amdocs, Fortinet, Lavelle Networks, and Nuage Networks was distributed by email to Light Reading's global list of service provider employees.

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 utilized 26 questions and was promoted to attract a large base of high-value respondents. As shown in **Figure 1**, a global mix of 90 qualified CSP respondents took the survey. Non-qualified, non-CSP responses were deleted. Of these, the largest employee sample was from the U.S. (49%), followed by Central/South America (17%), Western Europe (11%), Central/Eastern Europe (9%), Asia Pacific (7%), Canada (6%), and the Middle East/Africa (2%).

In order to provide further insight, the survey data was filtered using two equal-sized categories: U.S. responses and those from the rest of the world (RoW). This was done to understand on a more granular basis any geographic-specific trends between the U.S. and RoW countries in terms of SD-WAN security service adoption, implementation timelines, business, and implementation challenges. While significant variances in response trends between these two groups are summarized in the body of this report, **Appendix A** provides detailed question-level response data.

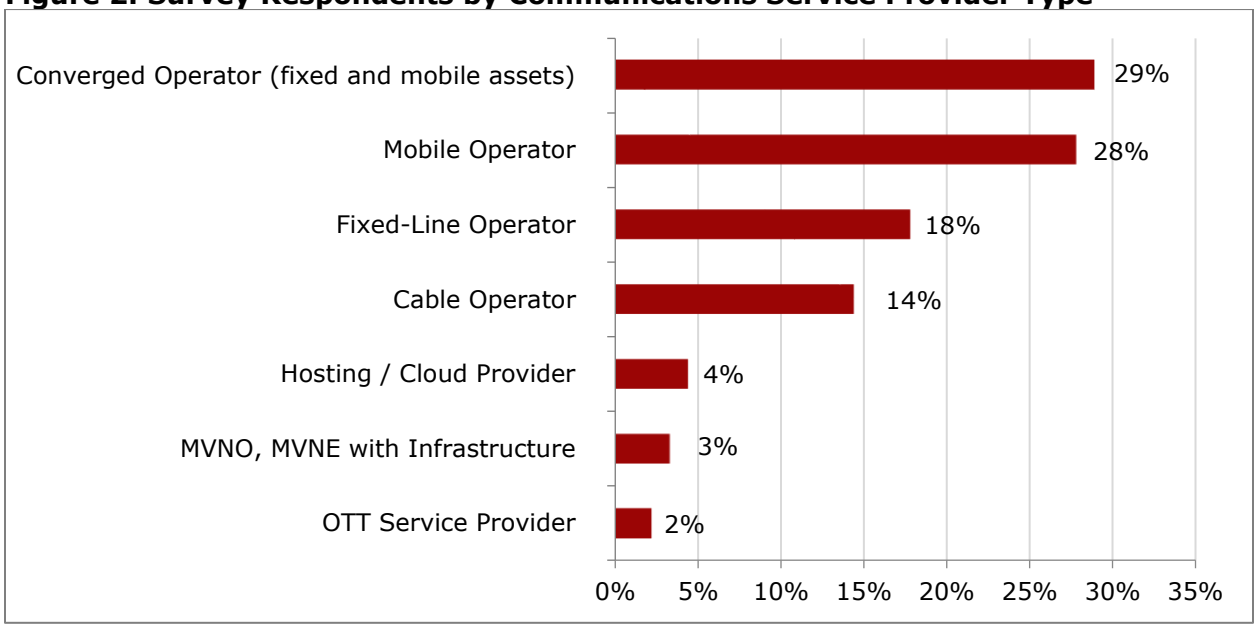
Figure 1: Survey Respondents by Geography



Question: Where is your company located? (N=90)
Source: Heavy Reading

The carrier respondents that provided survey input worked for a range of CSP types. Of these, as shown in **Figure 2**, the two largest groups represented were converged operators (29%) and mobile operators (28%), followed by fixed-line (18%) and cable (14%) operators. Since SD-WAN applies to all these service provider types, this diverse set of inputs is valuable in capturing all the considerations that CSPs must consider in their specific carrier segment.

Figure 2: Survey Respondents by Communications Service Provider Type

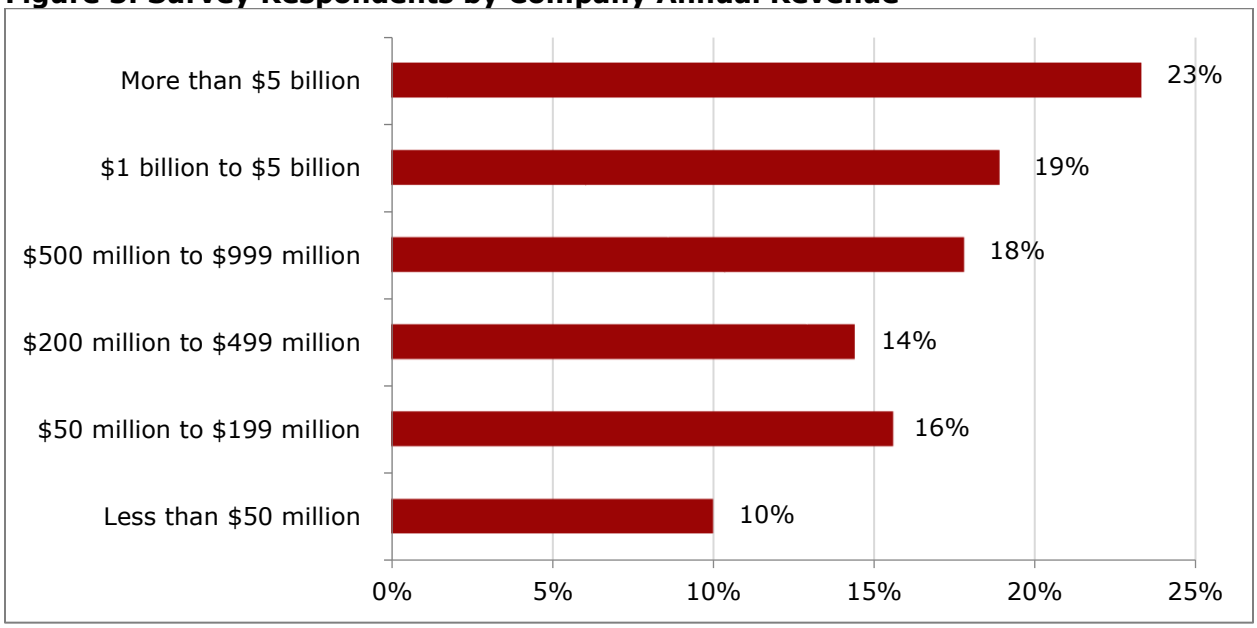


Question: What type of communications service provider (CSP) do you work for? (N=90)
Source: Heavy Reading

Not only were the CSPs diverse segment-wise, but they also represented a diverse mix of carriers based on annual revenue. Of these, as illustrated in **Figure 3** below, the largest group of respondents worked for CSPs that generated more than $5 billion in annual revenue (23%). These were followed by CSPs in the $1 billion to $5 billion range (19%) and the $500 million to $999 million range (18%).

Rounding out the carriers were smaller CSPs that generated revenue of $200 million to $499 million (14%), $50 million to $199 million (16%), and the smallest operators (less than $50 million; 10%). Heavy Reading considers this balanced carrier size distribution as optimal for providing a holistic industry view of SD-WAN security service adoption.

Figure 3: Survey Respondents by Company Annual Revenue

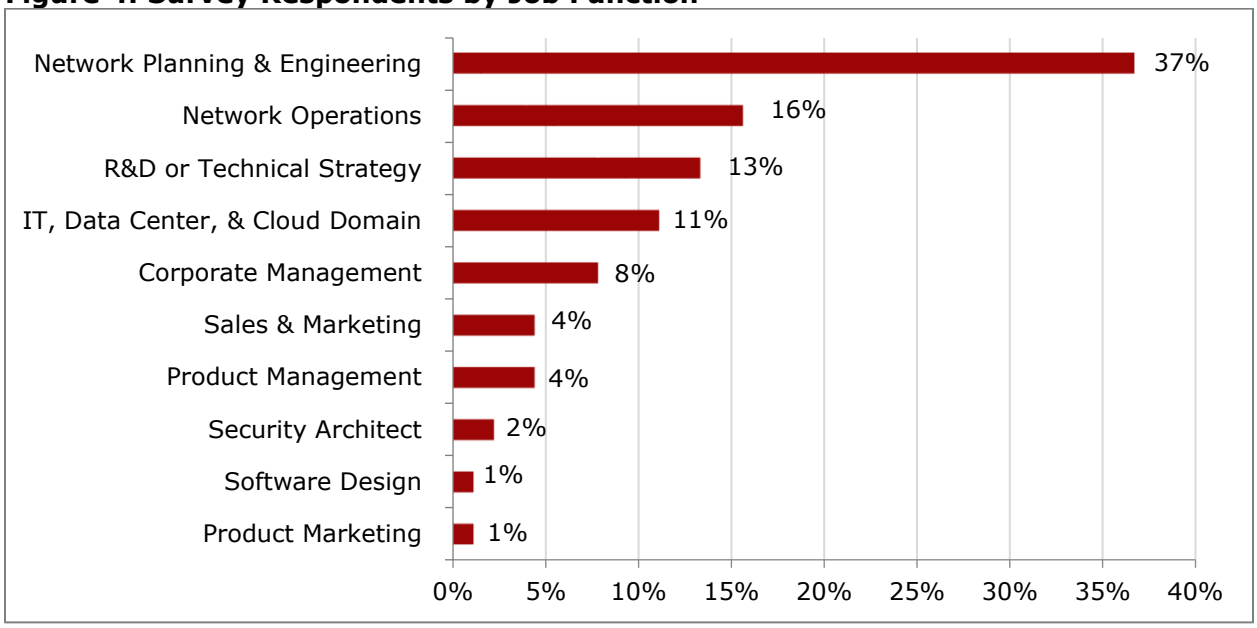


Question: What is your company's annual revenue? (N=90)
Source: Heavy Reading

A final demographic consideration is the job function that the survey respondents performed for the CSPs they represented. **Figure 4** below illustrates the scope of duties performed. Of these, the largest group by a considerable margin were staff from the network planning and engineering group (37%), followed by network operations staff (16%) and R&D or technical strategy team members (13%).

However, as captured in the figure, all the major groups were represented at some level. Given this survey was highly technical, Heavy Reading considers a distribution curve with a greater number of engineering-centric respondents of considerable value for providing granular insights into the considerations associated with deploying and securing SD-WAN services.

Figure 4: Survey Respondents by Job Function



Question: What is your primary job function? (N=90)
Source: Heavy Reading

3. SD-WAN SECURITY SERVICES: IMPLEMENTATION, INTEGRATION, AND IMPACTS

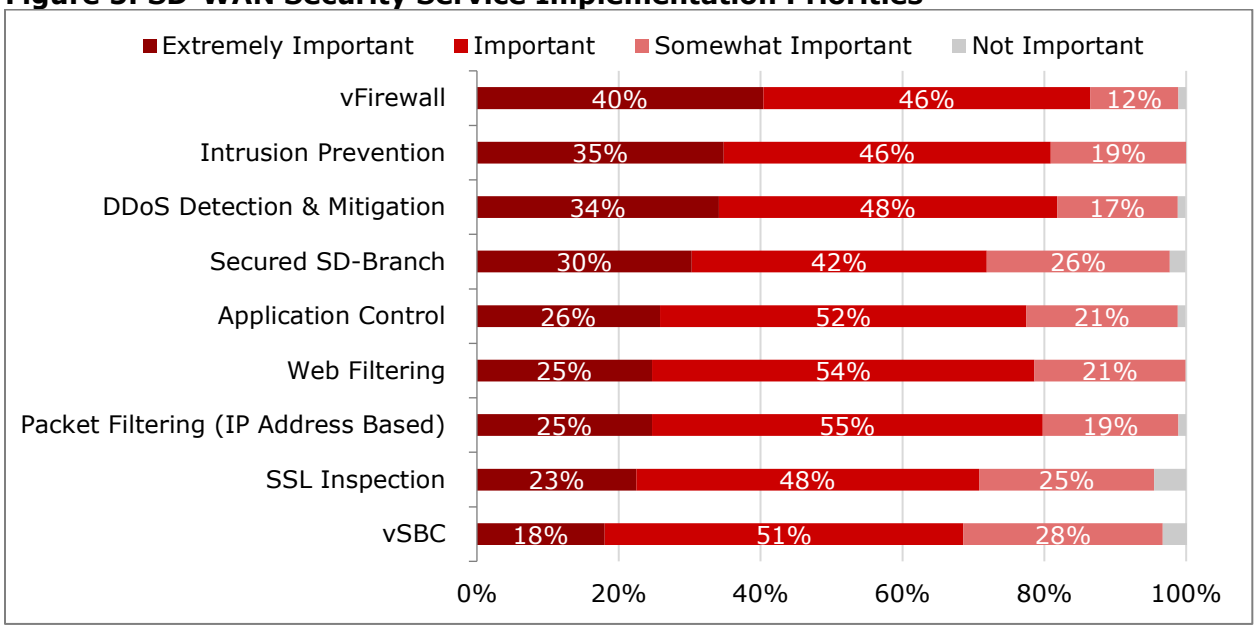
As previously noted, the rapid evolution and demand for SD-WAN services have enabled CSPs to integrate high-value security services into their SD-WAN portfolio.

One reason this represents such a high-value proposition is that there is a broad range of security services supported. These range from virtual firewalls (vFirewalls) to secured SD-branches (which apply advanced management tools), packet filters, and even virtualized session borders controllers (vSBC). As illustrated in **Figure 5**, based on "extremely important" responses, the top four capabilities are vFirewall (40%), intrusion prevention (35%), DDoS mitigation (34%), and secured SD-branch (30%).

This was somewhat expected given these capabilities are considered foundational and mature security capabilities. However, the relatively strong level of "extremely important" support for emerging advanced capabilities such as application control (26%), web filtering (25%), and packet filtering (25%) confirms that effective SD-WAN security service portfolios are multidimensional.

Further evidence of their relative strategic value is that they attained the highest scoring in the "important" band of responses (52%-55%). Overall, this means at least 69% of respondents believe it is either "extremely important" (18%-40%) or "important" (42%-55%) that their SD-WAN solution supports security services.

Figure 5: SD-WAN Security Service Implementation Priorities



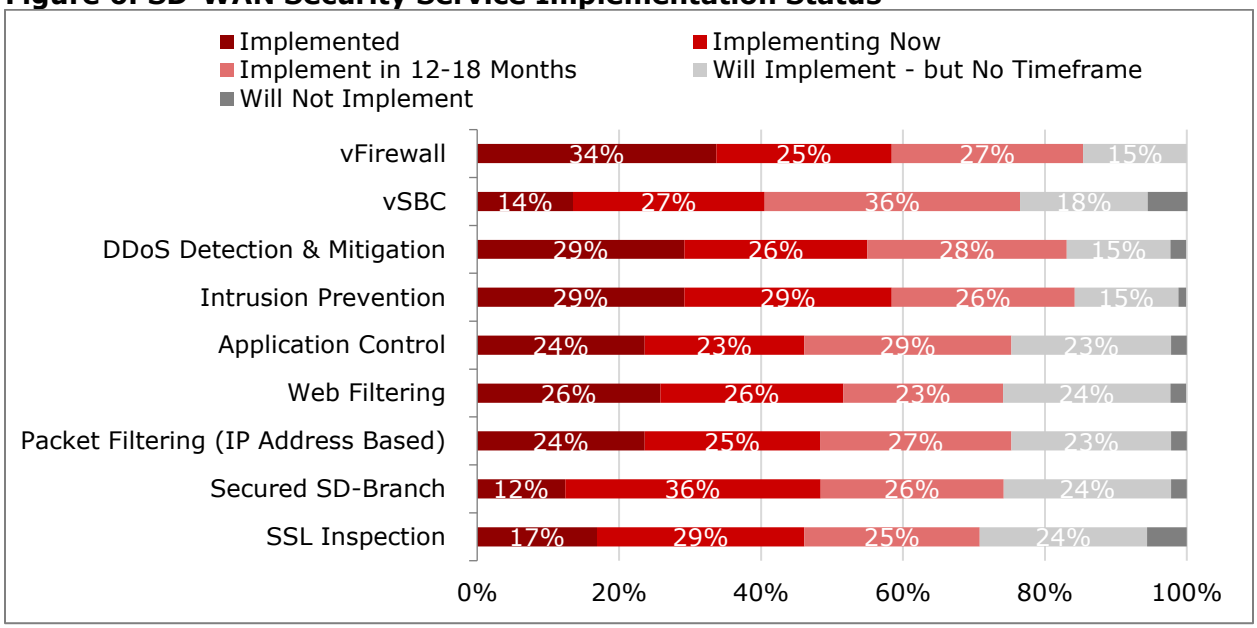
Question: How important is it for your SD-WAN implementation to support the following security services? (N=89)
Source: Heavy Reading

Unsurprisingly, as illustrated in **Figure 6**, CSPs are focused on implementing those capabilities that attained the highest scores in **Figure 5** above. This translates into vFirewall (34%) – the most deployed capability – followed by DDoS mitigation and intrusion prevention (tied both at 29%).

However, consistent with the previous figure, a considerable number of CSPs have also implemented web filtering (26%), application control, and packet filtering (both 24%). Although fewer CSPs have implemented secured SD-branch, it scored highest in the "implementing now" category (36%), confirming its overall importance. U.S. respondents are especially committed to secured SD-branch implementation (see **Figure 26**).

Approximately 50% of the CSPs without commercial SD-WAN security services are either currently implementing them (23%-36%) or plan to implement within 12-18 months (23%-36%). This translates into more than 70% having deployed services within 18 months.

Figure 6: SD-WAN Security Service Implementation Status



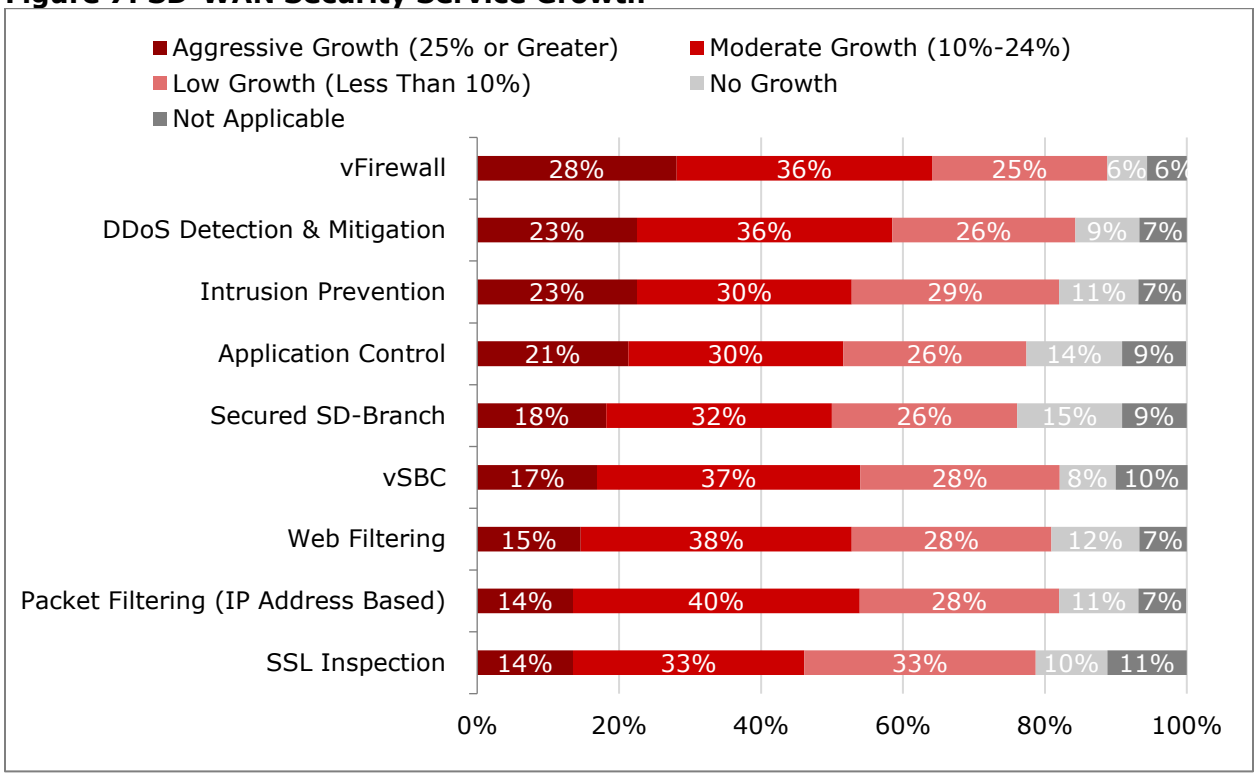
Question: What is the implementation status of the following SD-WAN security services? (N=89)
Source: Heavy Reading

As is often the case, CSP implementation use case priorities are shaped by not only technical benefits but also business case realities. As shown in **Figure 7** below, CSPs see several immediate "aggressive growth" security service business opportunities that directly relate to priorities documented in the preceding figures.

Of these, vFirewall (28%), DDoS mitigation and intrusion prevention (both 23%), and application control (21%) represent the most potent growth opportunities.

Still, it is worth noting that based on "aggressive growth" inputs, all the capabilities had solid levels of support. Based on "moderate growth" inputs, packet filtering (40%) and web filtering (38%) attained the highest scores.

Figure 7: SD-WAN Security Service Growth



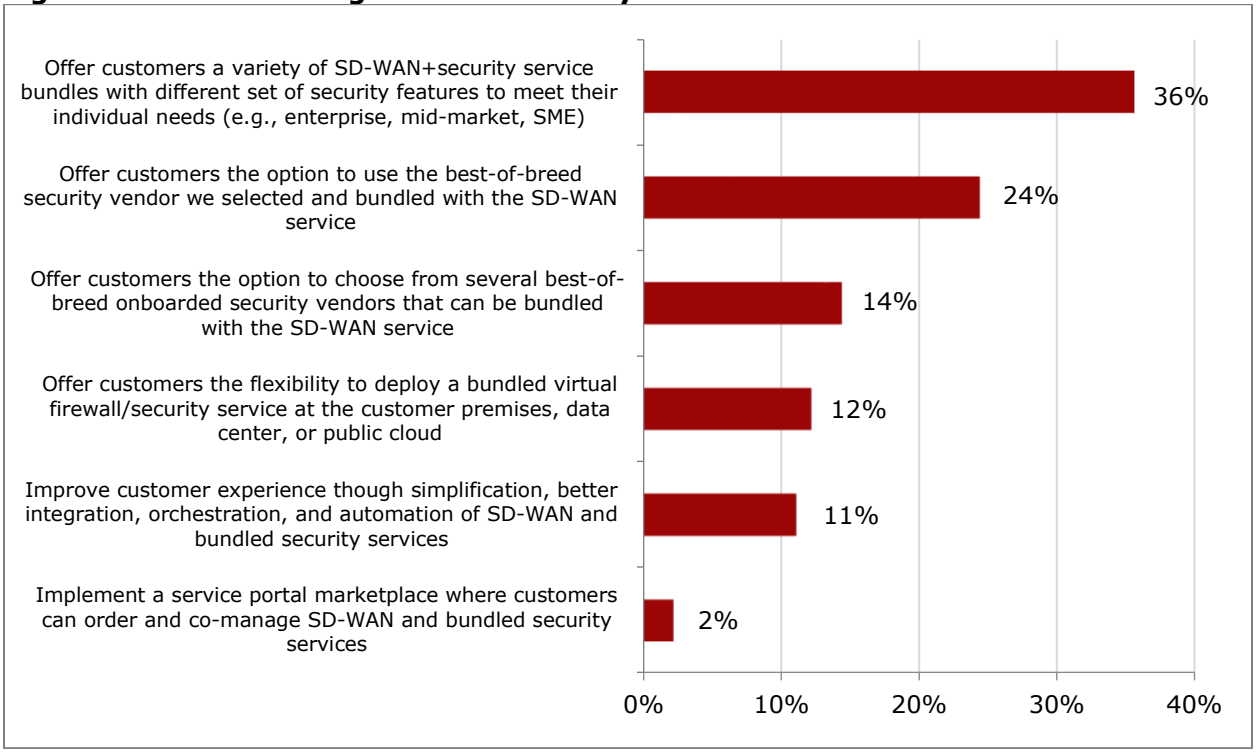
Question: What level of growth are you experiencing for the following SD-WAN security services? (N=89)
Source: Heavy Reading

Another vital business case decision point consideration is not only the revenue potential but also the extent to which the CSP can utilize the service to achieve differentiation from competitors' offerings. Since SD-WAN is highly programmable and software extensible, CSPs have several options to achieve this. One strategy that has considerable merit is the ability to differentiate on a service bundle basis by maximizing the flexibility of choice.

Of these options, as shown in **Figure 8** below, the preferred approach is to offer enterprise customers a number of security bundles they can select based on their requirements (36%). The second-ranked option is also important since it advocates an even more flexible approach. In this case, the option is based on allowing the customers to select from an ecosystem of vendors supported by the CSPs' SD-WAN security bundles (24%).

Heavy Reading believes that as SD-WAN security services mature, this ecosystem option will continue to gain favor. The third-ranked best-of-breed option and the self-service portal marketplace option will also continue to gain favor.

Figure 8: Differentiating SD-WAN Security Services

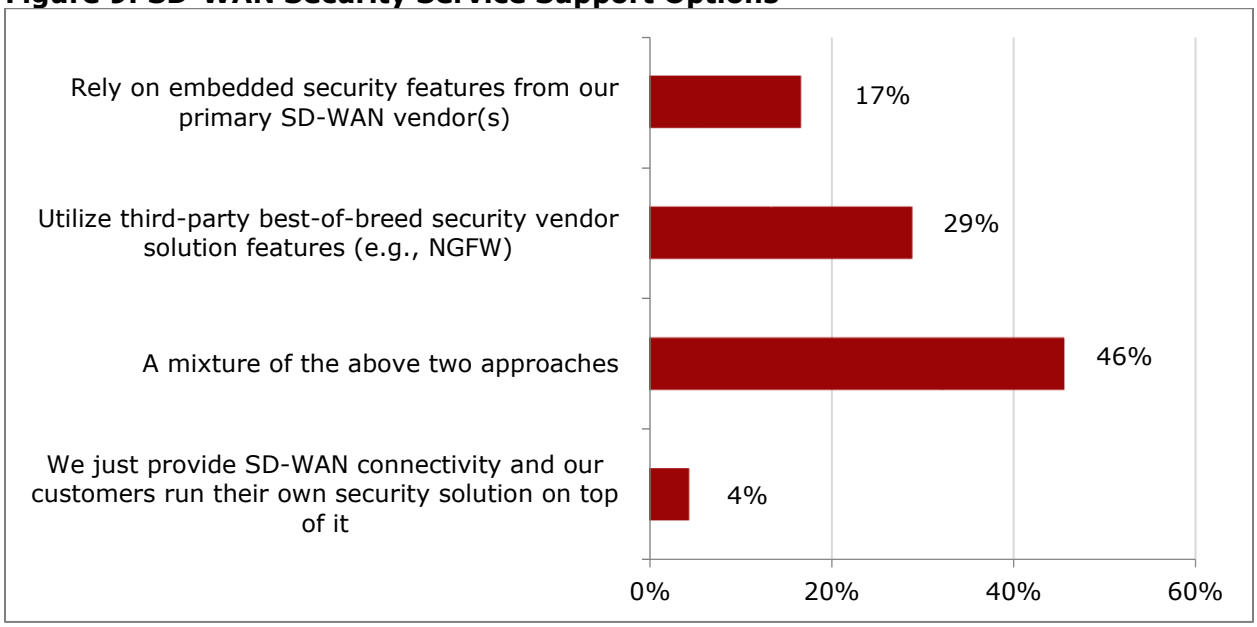


Question: What is your preferred approach for differentiating your managed SD-WAN security services? (N=90)
Source: Heavy Reading

As documented, many CSPs are planning to maximize the flexibility that best-of-breed security vendor solutions provide in managed security service bundles. **Figure 9** below confirms this. As shown in the figure, when asked about preferences, almost half of the respondents (46%) indicated they prefer to use a mix of embedded security features from their primary vendor as well as third-party best-of-breed vendor features.

This was not unexpected since SD-WAN solutions have been deployed for only a few years, which means investment protection is a key consideration. However, Heavy Reading believes that the first-place ranking of the third-party vendor option (29%) over the primary vendor option (17%) indicates that more CSPs favor the flexibility of third-party solutions over relying solely on the primary vendor.

Figure 9: SD-WAN Security Service Support Options



Question: What is your preferred approach for supporting security features in your offered SD-WAN services? (N=90)
Source: Heavy Reading

An upside of the CSPs' cloud transformation has been their ability to sell managed cloud-based managed security services. One service option – SECaaS – has considerable appeal for enterprise customers since it can be delivered transparently to every user regardless of location at a lower cost than deploying hardware and software onsite.

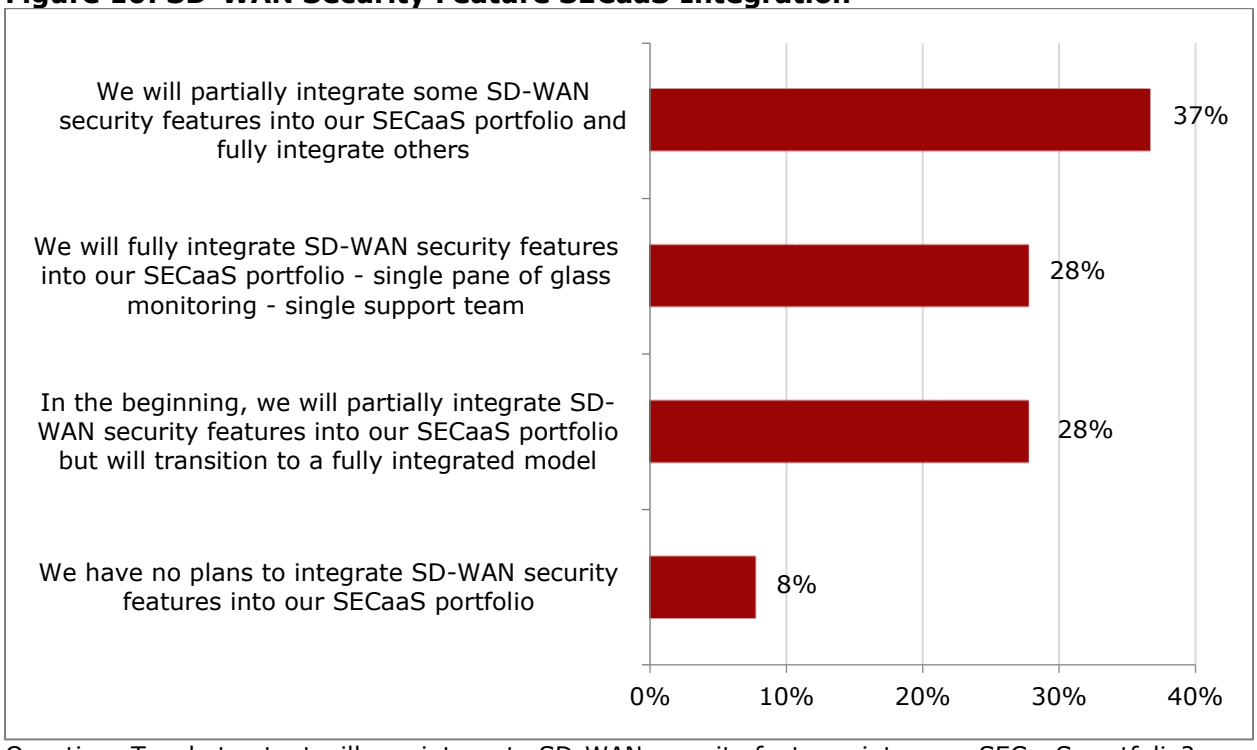
Perhaps another away to look at SECaaS is that it represents a fully integrated managed security services delivery model. The question in an SD-WAN security context then becomes: To what extent do CSPs plan to integrate these SD-WAN security services into the SECaaS domain to achieve a fully integrated holistic delivery model? Alternatively, they could continue in a standalone sales mode by utilizing mature service bundles.

As **Figure 10** below illustrates, CSPs are considering their options. The largest group of respondents (37%) are in favor of integrating some specific features into their SECaaS portfolio and not others. A second group (28%) advocates an "integrate them all" approach to achieve single pane of glass monitoring and create a single security support team. The third group (28%) is focused on partial integration like the first but plans to transition to a fully integrated model.

The key takeaway here is that 56% (28% + 28%) of the survey respondents prefer the fully integrated model but will follow different implementation paths. Meanwhile, the single largest group (37%) prefers to selectively fully integrate based on specific feature requirements.

Looking at the filter groups, U.S. respondents prefer the fully integrated single pane of glass model (39%). RoW respondents are equally split between the selective service integration model and partial to fully integrated transition model approach (both 39%; see **Figure 30**).

Figure 10: SD-WAN Security Feature SECaaS Integration



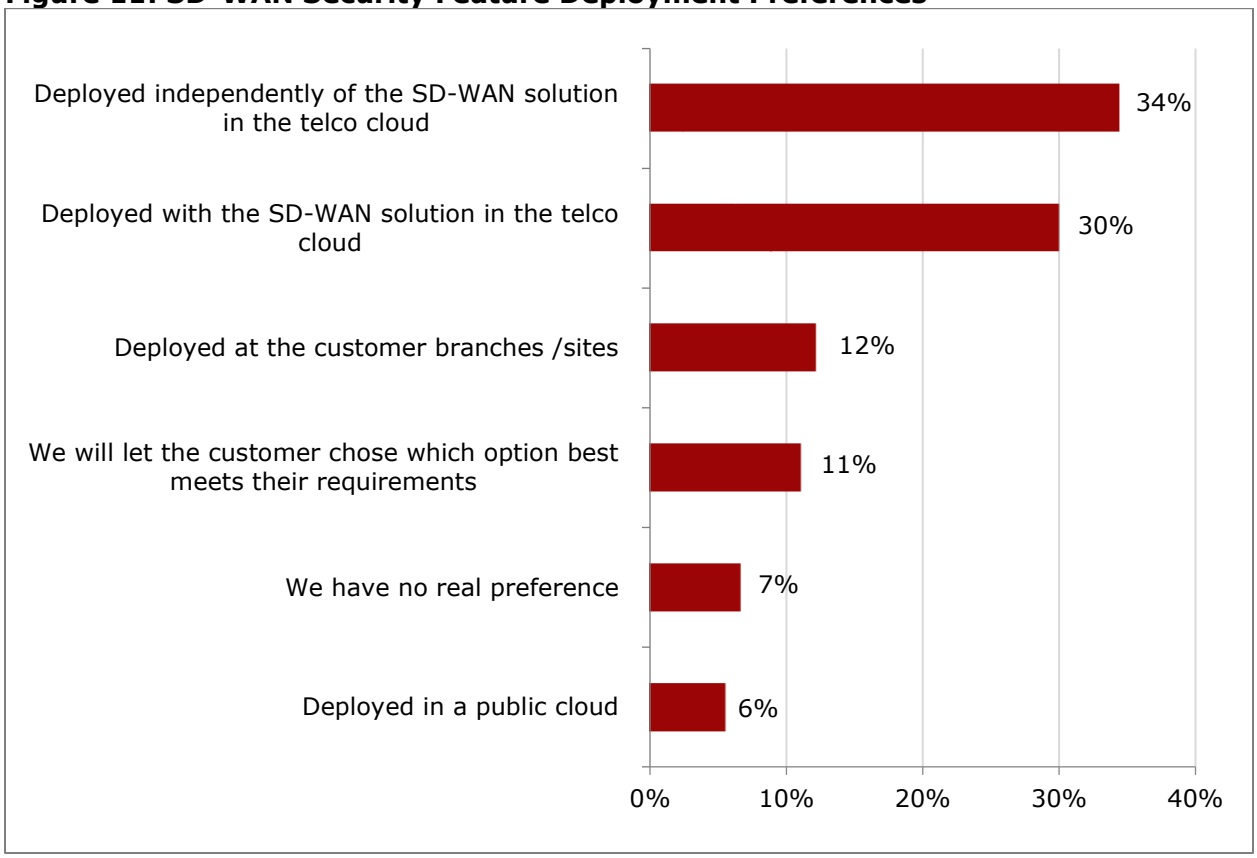
Question: To what extent will you integrate SD-WAN security features into your SECaaS portfolio? (N=90)
Source: Heavy Reading

In addition to an integration strategy, CSPs must also create an SD-WAN security feature deployment strategy. There are several viable options. These include deploying SD-WAN in the telco cloud (either integrated the SD-WAN solution or deployed independently), in branch offices, or even in the public cloud.

As **Figure 11** below shows, both telco options represent the preferred approaches. Leading the way is the independent option (34%), followed closely by the integrated SD-WAN telco cloud model (30%). In third place is the customer branch/site deployment model (12%).

Although the preferences for both filter groups are similar, more U.S. respondents than RoW respondents prefer the independent deployment model. In contrast, more RoW respondents favor the branch site deployment model (see **Figure 31**).

Figure 11: SD-WAN Security Feature Deployment Preferences

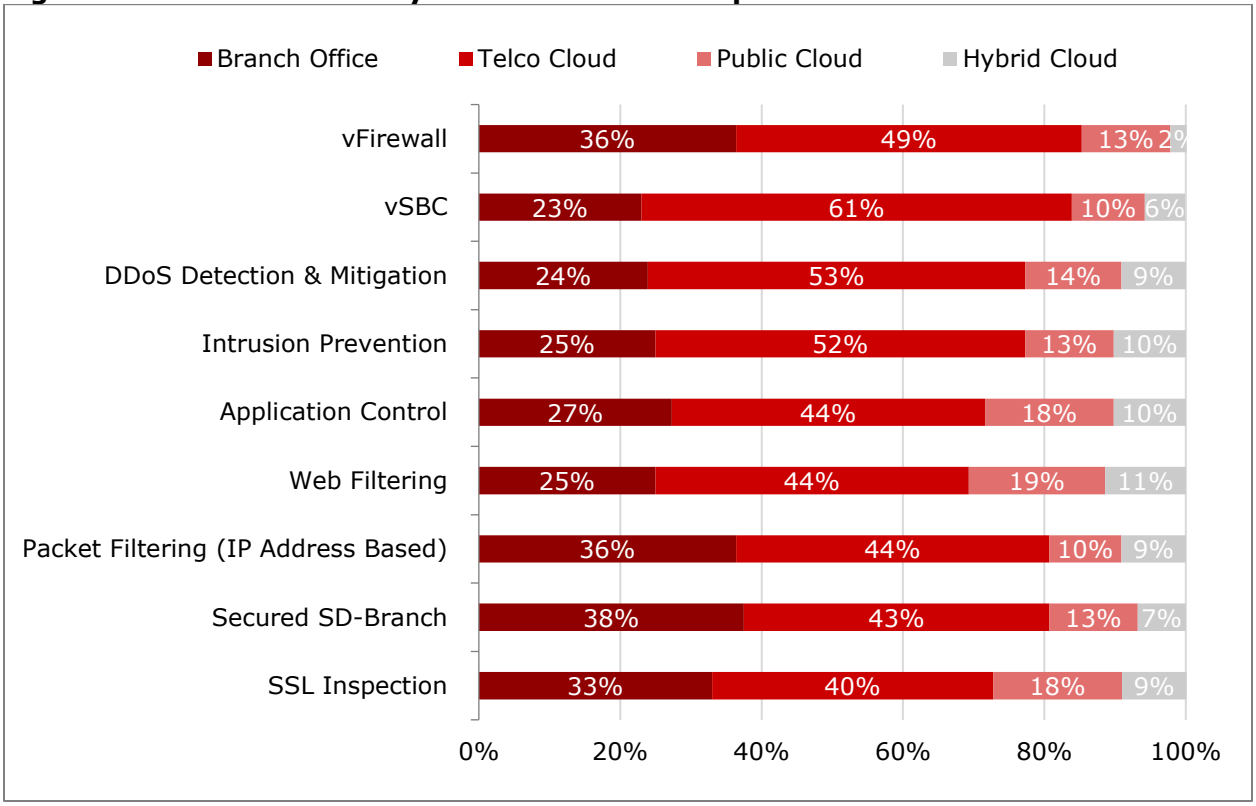


Question: Do you have a preference where the security solution for your SD-WAN service is deployed? (N=90)
Source: Heavy Reading

Figure 12 below reinforces that the telco cloud option is the preferred security deployment option even on a specific service basis (40%-61%). Interestingly, the vSBC – which scored lower as implementation priority (see **Figure 5**) – attained the highest telco cloud score (61%).

However, it is also important to note there is considerable support for deploying some security features in the branch. Of these, leading the scoring was secure SD-branch (38%), followed by packet filtering and vFirewall (both 36%).

Figure 12: SD-WAN Security Service Location Implementation Preferences



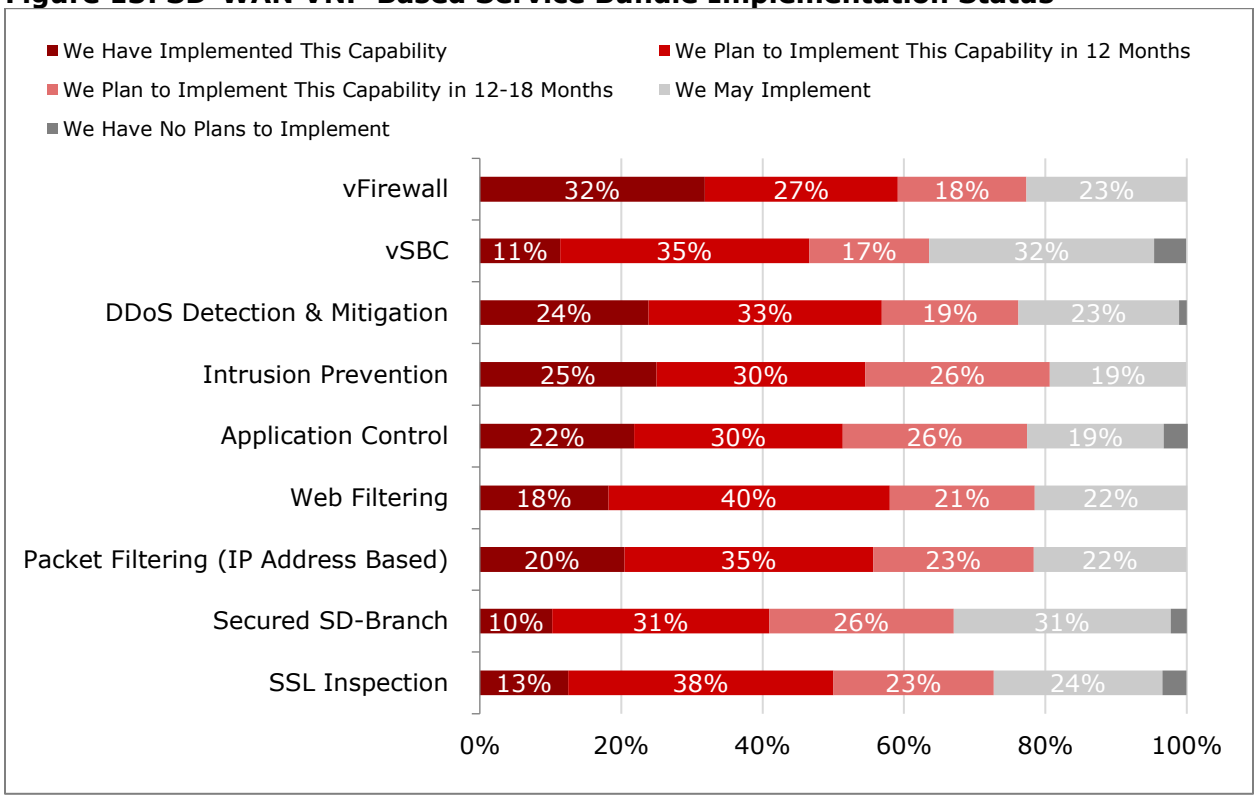
Question: Where is the best place in the network to implement the following SD-WAN security services? (N=88-89)
Source: Heavy Reading

One of the opportunities associated with utilizing VNFs for SD-WAN managed security services is the ability to bundle them into flexible configurations to fuel service differentiation (see **Figure 8**). As captured below in **Figure 13**, there is substantial interest in adopting this approach.

Based on the range of "already implemented" (10%-32%) responses, which provides a view of the number of security VNFs that have already been deployed, and "plan to implement in 12 months" (27%-40%) responses, CSPs are strongly in favor of bundling VNFs. Similar to other input, the top three priorities are vFirewall (32% + 27%), intrusion prevention (25% + 30%), and DDoS mitigation (24% + 33%). U.S. respondents are well ahead in terms of implementing VNF-based SD-WAN security service bundles (see **Figure 33**).

Given this level of support, it is clear that utilizing security VNFs now represents a foundational element of SD-WAN security services, with considerable growth to come in the next 12 to 18 months.

Figure 13: SD-WAN VNF-Based Service Bundle Implementation Status



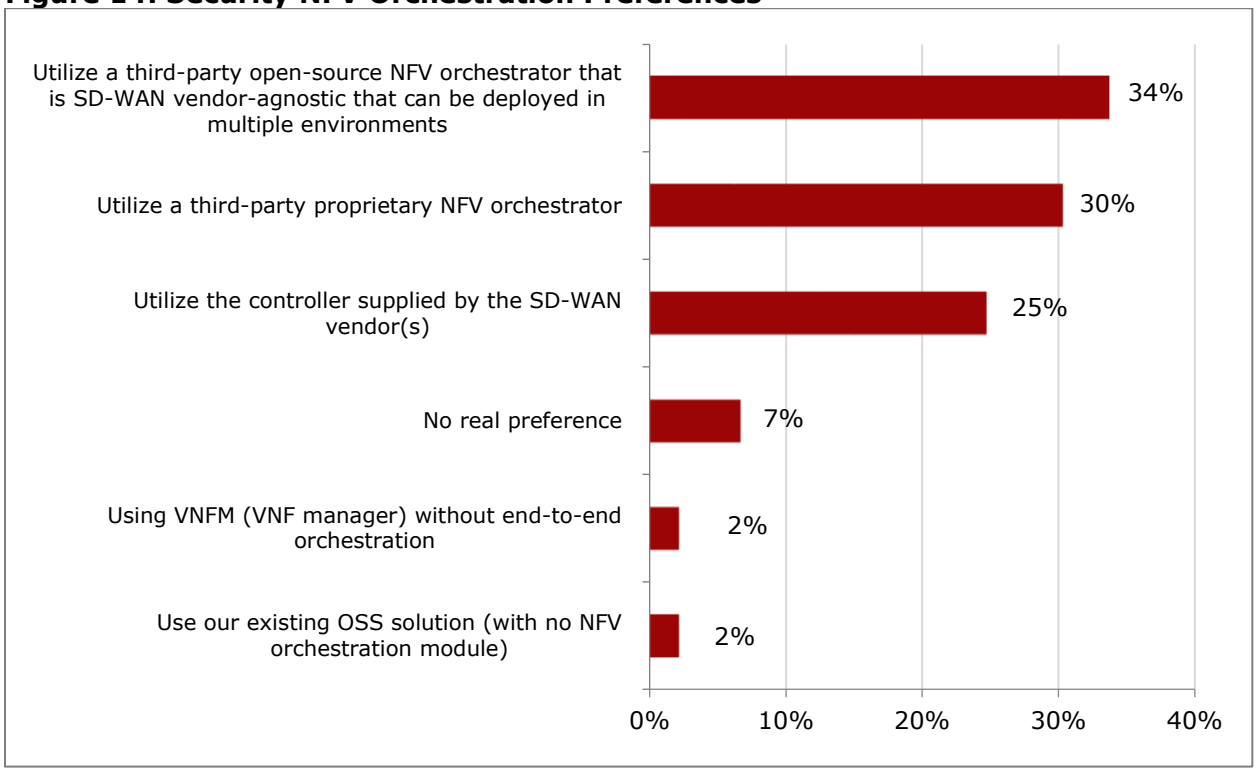
Question: Do you plan to support service bundles/offerings of virtual network functions with your SD-WAN service? (N=88)
Source: Heavy Reading

As documented, a significant number of CSPs are focused on introducing best-of-breed security services into their SD-WAN portfolio (see **Figure 9**). Most of these will be utilizing VNFs in bundles (see **Figure 13**), which will also affect CSPs' NFV orchestrator vendor selection strategies.

For example, as shown in **Figure 14** below, more than a third of the respondents (34%) prefer to utilize a third-party open-source orchestrator that is SD-WAN vendor-agnostic and can be deployed in multiple environments. In second place (30%) is support for a third-party but proprietary NFV orchestrator. Next is the "status quo" option of utilizing the SD-WAN orchestrator followed by the SD-WAN vendor (25%).

Heavy Reading believes that the number one ranking of the open-source vendor-agnostic orchestration option confirms that CSPs are continuing to look for solutions that minimize vendor lock-in. However, the process will be gradual given that CSPs have a number of factors to balance. These include balancing vendor relationships with the need to deploy reliable and potentially proprietary cost-effective solutions that work.

Figure 14: Security NFV Orchestration Preferences



Question: What is your preferred approach for orchestrating security VNFs in an SD-WAN network? (N=89)
Source: Heavy Reading

A central decision point associated with deploying SD-WAN security services in the branch is whether to support only local internet breakout access or to secure *all* communications services originating and terminating within the branch.

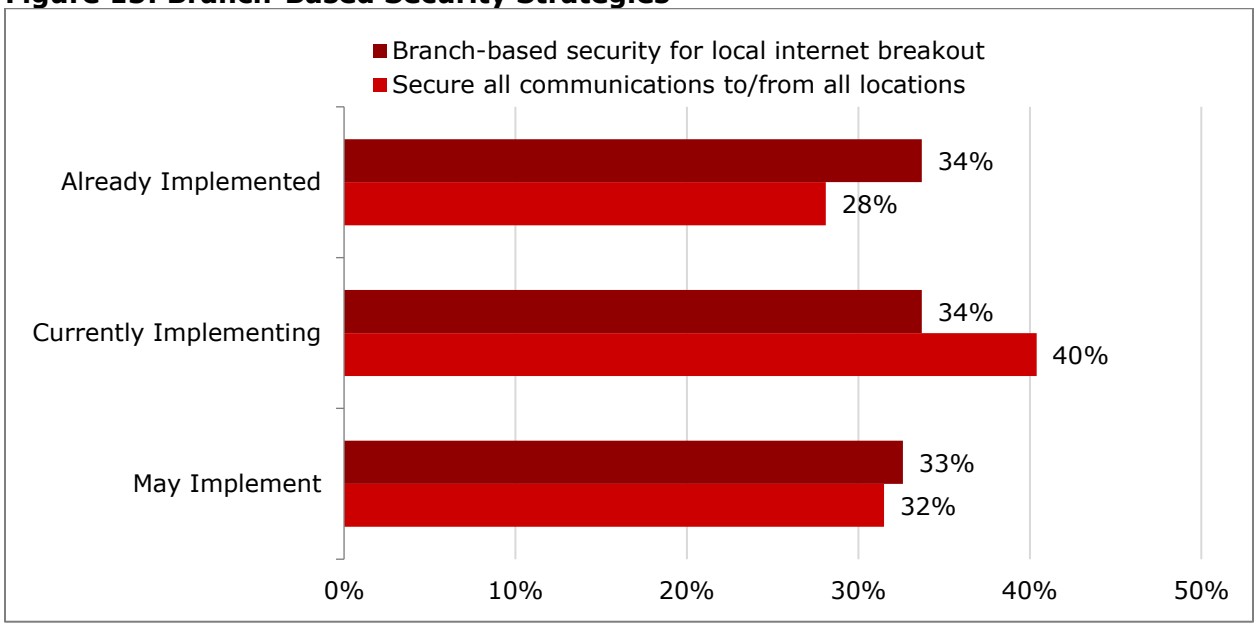
The reason for the renewed interest in local internet breakout is that in the past, Multi-Protocol Label Switching (MPLS) networks often lacked the programmability to support direct internet access in the branch. This meant access could only be supported via a centralized hub configuration, which is less efficient.

In contrast, this represents a straightforward implementation in an SD-WAN network. However, like other SD-WAN services, security must be considered to ensure internet-based attacks do not negatively affect branch services. Since these security services can be delivered via an existing managed SD-WAN security services model, implementation is straightforward.

Given this, as shown in **Figure 15** below, a greater number of CSPs have already implemented local internet breakout (34%). In contrast, 28% of respondents indicated they are utilizing SD-WAN branch-based security services to support all communications services (28%).

Still, based on "currently implementing" response levels, all communications services model leads (40% vs. 34%). Heavy Reading interprets this data as confirming that both the local breakout and all communications service options are relevant components of a systematic branch security strategy.

Figure 15: Branch-Based Security Strategies



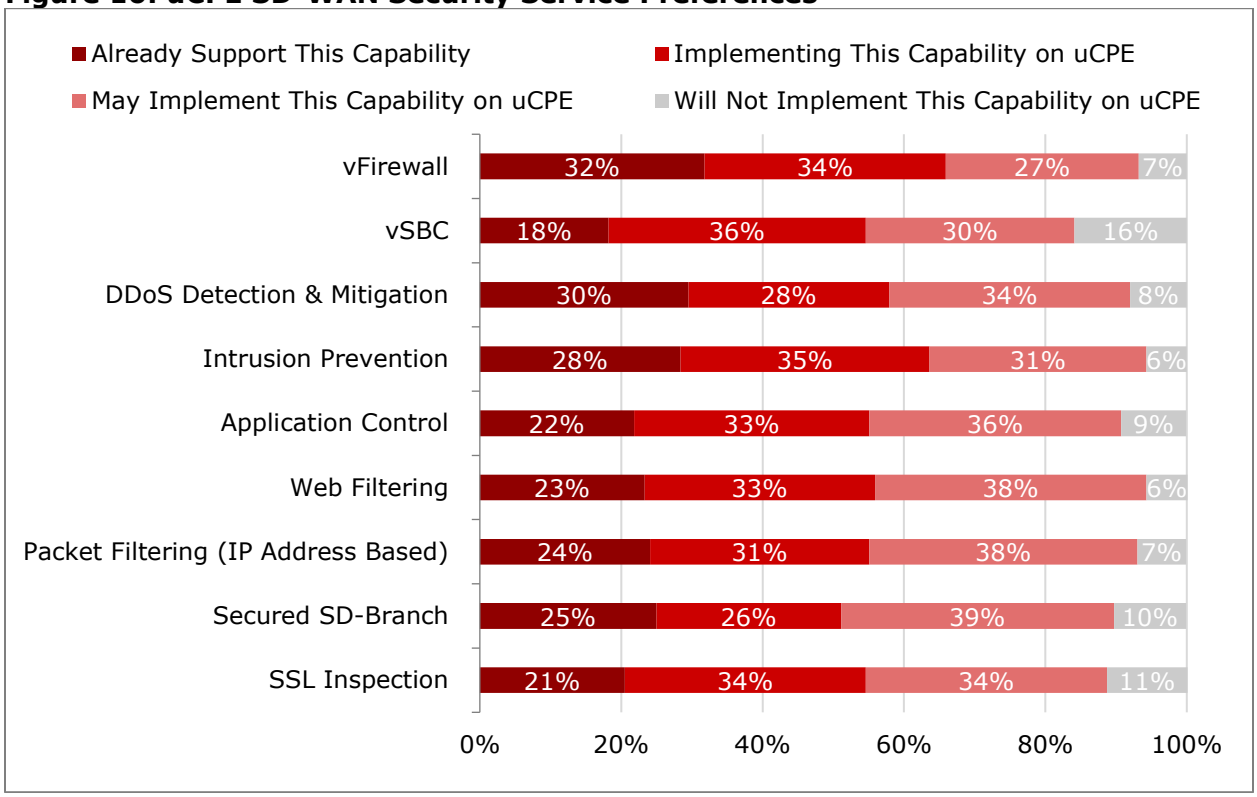
Question: Do you plan to use branch-based security functions for local internet breakout only, or to secure all communications from the branch to other branches, HQ, and cloud?
(N=86-89)
Source: Heavy Reading

One option for offering SD-WAN security services in the branch is to run VNFs on a uCPE appliance. Accordingly, in the next question, the survey investigated which SD-WAN security services the respondents felt were the best fit.

As shown in **Figure 16** below, the top VNFs "already implemented" are familiar priorities: vFirewall (32%), DDoS mitigation (30%), and intrusion prevention (28%). The top three capabilities "currently being implemented" are vSBC (36%), intrusion prevention (35%), and vFirewall and SSL inspection (both 34%).

The first-place scoring of vSBC is interesting given it previously scored higher as a telco cloud than as a branch function (see **Figure 12**). One logical conclusion is customers that implement uCPE see greater value in deploying a vSBC than those that implement a standard SD-WAN branch deployment. Yet, it is also important to note that U.S. respondents are much greater supporters of vSBC VNFs than RoW respondents (see **Figure 36**).

Figure 16: uCPE SD-WAN Security Service Preferences

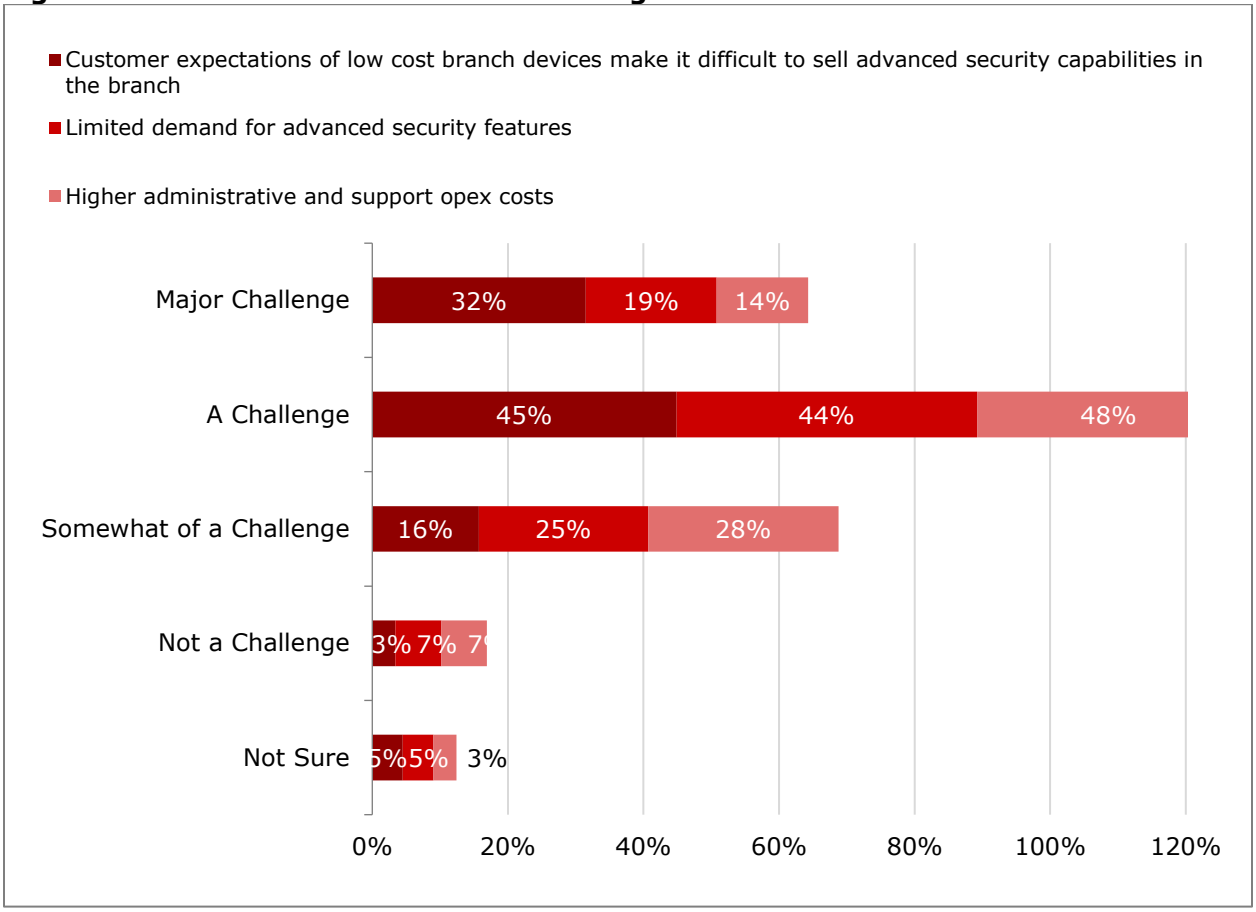


Question: Which security services do you plan to offer as VNFs on uCPE in the branch? (N=86-88)
Source: Heavy Reading

In addition to understanding branch and uCPE security service preferences, the survey also addressed business challenges associated with implementing SD-WAN security in the branch office. As displayed in **Figure 17** below, the gravest concern based on "major challenge" inputs is that customer expectations of low-cost SD-WAN branch devices will make it difficult to upsell advanced SD-WAN security services (32%).

In other words, it is logical that device price points are a major consideration in order to keep costs low when a branch office is deployed. However, the downside is that it makes upselling SD-WAN security services difficult due to the limited intelligence of the devices deployed. Both U.S. and RoW respondents share similar levels of concern (see **Figure 37**).

Figure 17: Branch Office Business Challenges

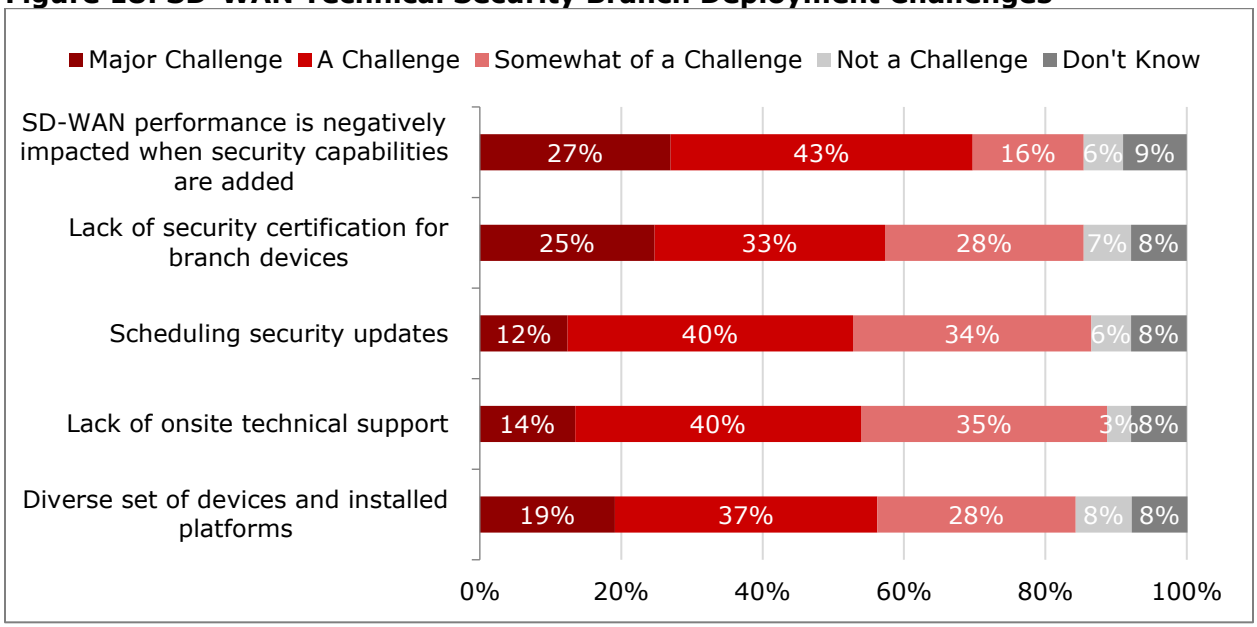


Question: What business challenges have you encountered with implementing SD-WAN security in the branch office? (N=88-89)
Source: Heavy Reading

Low cost, limited intelligence branch devices are not only a business concern, but they also have negative technical implications. As shown in **Figure 18** below, based on "major challenge" responses, the top three areas of concerns revolve around the performance implications on devices when security capabilities are added (27%), lack of security certification for devices (25%), and the diverse set of devices that must be secured (19%).

When the "challenge" responses are added to those three inputs, it equates to a range of 70%, 58%, and 56% of respondents anticipating significant challenges associated with deploying SD-WAN security services in the branch office.

Figure 18: SD-WAN Technical Security Branch Deployment Challenges



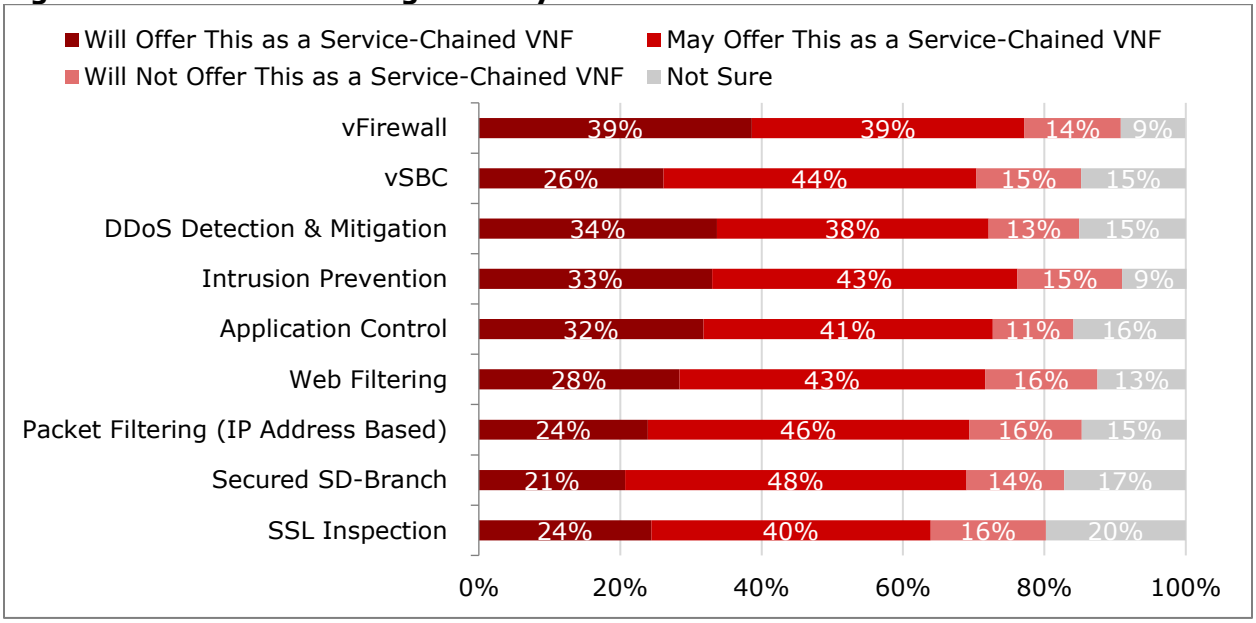
Question: What technical challenges have you encountered with implementing SD-WAN security in the branch office? (N=89)
Source: Heavy Reading

As a highly programmable access fabric, SD-WAN is conceptually well-positioned to support service chaining. The latter enables data streams to selectively utilize specific virtualized resource functions such as web filtering only when the application mandates this function is necessary. This capability is highly desirable because it avoids putting all security resources in the data stream path, thereby optimizing resource usage and minimizing cost.

Similarly, when additional resources are needed due to additional traffic, service chains can be spun up to meet demand. As **Figure 19** below illustrates, there is considerable interest in chaining a diverse range of SD-WAN security functions. Of these, based on "will offer" inputs, the leading candidates are vFirewall (39%), DDoS mitigation (34%), and intrusion prevention (33%). These are followed closely by other functions such as application control (32%) and web filtering (28%).

Although this data does identify clear intent to deploy SD-WAN security services via service chaining, the greater range of "may offer" (38%-48%) and "will not offer" (11%-16%) responses identifies that many CSPs have still not decided if the service-chaining path is viable. Based on filter group input, U.S. respondents are markedly more committed to offering security services as service-chained VNFs in the cloud than RoW respondents (see **Figure 39**).

Figure 19: Service-Chaining Security VNFs



Question: Which security services do you plan to offer as service-chained VNFs in the cloud? (N=86-88)
Source: Heavy Reading

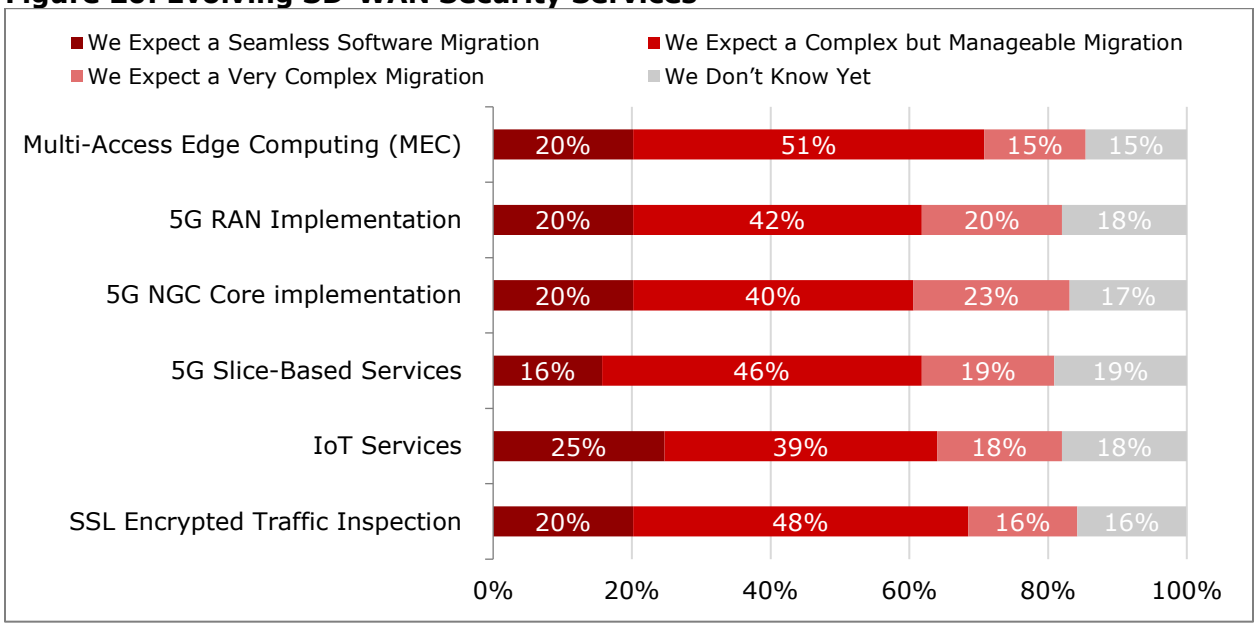
Over the past 8 years, CSPs have faced an unprecedented cadence of technological change encompassing cloud service migration, MEC, and the rollout of 5G networks. Given SD-WAN has rapidly established itself as *the* access technology for all these technologies, it is clear that SD-WAN will need to continue to evolve.

The key question is how well SD-WAN security services already deployed or soon to be deployed will be able to manage these technology-driven transitions. Overall, as shown in **Figure 20** below, most respondents (39%-51%) believe that they will face a "complex but manageable migration" while 16% to 25% expect a "seamless software migration" path to support new technologies.

In contrast, only 15% to 23% expect a "very complex migration," with the 5G NGC core implementation representing the greatest technology of concern. Twice the number of RoW respondents expect a "very complex migration" (15%-33%) compared to their U.S. counterparts (7%-14%; see **Figure 40**).

This range of "very complex migration" concerns should not be taken lightly, given that 60% (20% "seamless migration"; 40% "complex but manageable migration") of survey respondents expect either a seamless or manageable migration for even the most complex technology transition (NGC core, 23%). However, Heavy Reading believes CSPs are comfortable that their SD-WAN security services are up to the task of meeting future technology demands.

Figure 20: Evolving SD-WAN Security Services



Question: How difficult will it be for your current commercial SD-WAN security services implementation to evolve to support the following advanced networking capabilities? (N=89)
Source: Heavy Reading

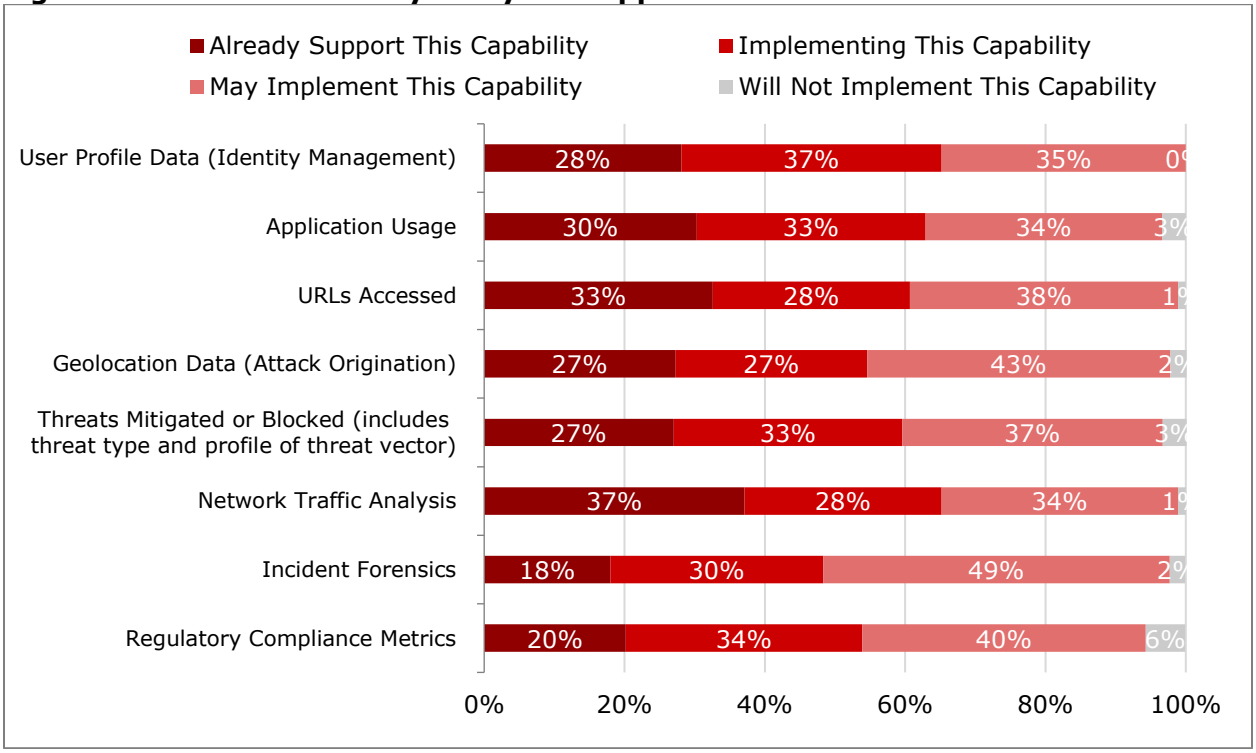
Even before CSPs commenced their virtualized cloud-based service migration, analytics played a key role in providing network administrators with the requisite level of network visibility to maintain network performance. However, in a cloud environment, analytics plays an even greater role, given network data metrics must be collected in more places to provide visibility of overall cloud performance. Therefore, it stands to reason that analytics would place a key role in SD-WAN security service support as well. This relationship is confirmed in **Figure 21** below.

As the figure illustrates, approximately 6 out of 10 CSPs already support or plan to implement a broad range of analytics capabilities to enhance SD-WAN security service delivery. The top three capabilities "already supported" are network traffic analysis (37%), URLs accessed (33%), and application usage (30%). The high ranking of these three capabilities was not unexpected given they provide much-needed visibility into the applications traversing the network and how well the network is able to manage them.

The top three capabilities "currently being implemented" include user profile data (37%), regulatory compliance metrics (34%), and threats mitigated or blocked and application usage (both 33%). The top three analytics capabilities that fall into the "may implement" category are incident forensics (49%), geolocation attack data (43%), and regulatory compliance metrics (40%).

Based on those capabilities already implemented and currently being implemented, it is clear that CSPs will have a broad range of analytics tools at their disposal to ensure SD-WAN security services are not compromised. Looking at the filter group data highlights that U.S. CSPs are generally more committed to implementing analytics to enhance SD-WAN security services than their RoW counterparts (see **Figure 41**).

Figure 21: SD-WAN Security Analytics Support



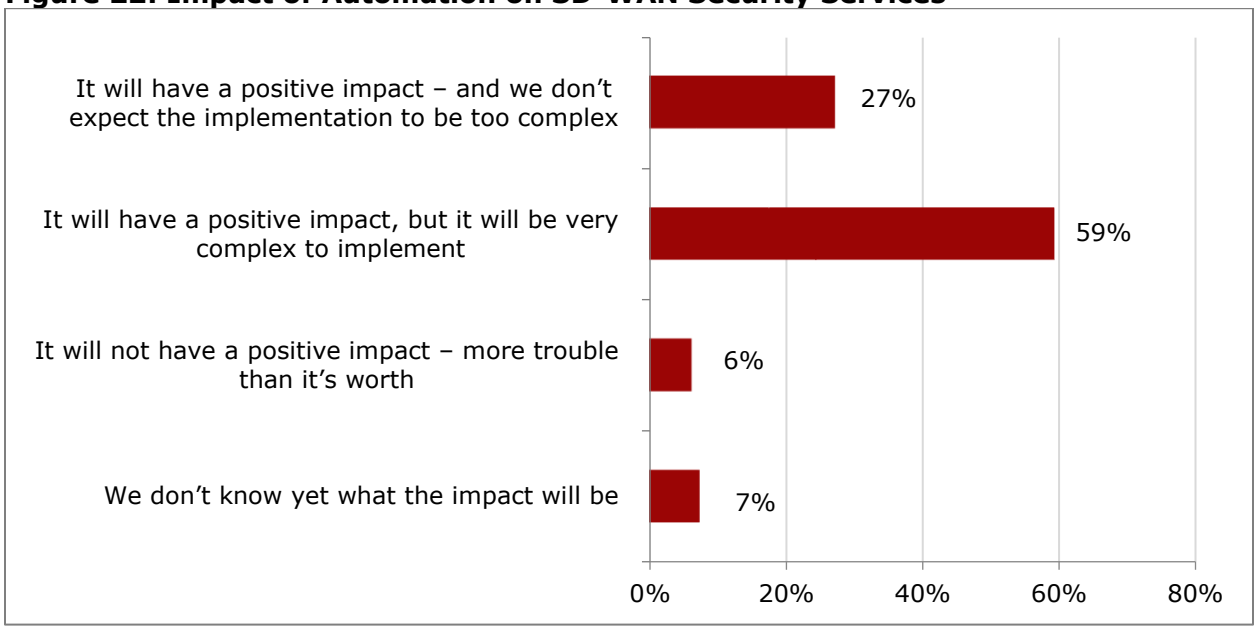
Question: Which security analytics do you support or plan to support in your SD-WAN security offer? (N=89)
Source: Heavy Reading

Like any other new technology, SD-WAN will be affected by the introduction of automated techniques. There is general industry consensus that the benefits that automation will deliver will offset the complexity of implementation since value proposition and integration complexity will vary by technology. However, the survey specifically asked the survey respondents for their insights in an SD-WAN context.

As **Figure 22** below shows, 59% of the respondents believe that integrating automation into SD-WAN will be very complex to implement, but overall, it will have a positive impact. The second largest group also believes automation will have a positive impact (27%) but do not anticipate a complex implementation process. This leaves only two small groups of respondents that believe automation will not have a positive impact (6%) or have yet to form an opinion (7%).

Based on this input, it is readily apparent that 86% (27% + 59%) of the respondents are convinced that automation will deliver value, with the caveat that almost 6 out of 10 (59%) harbor no illusions that the implementation journey will be easy.

Figure 22: Impact of Automation on SD-WAN Security Services

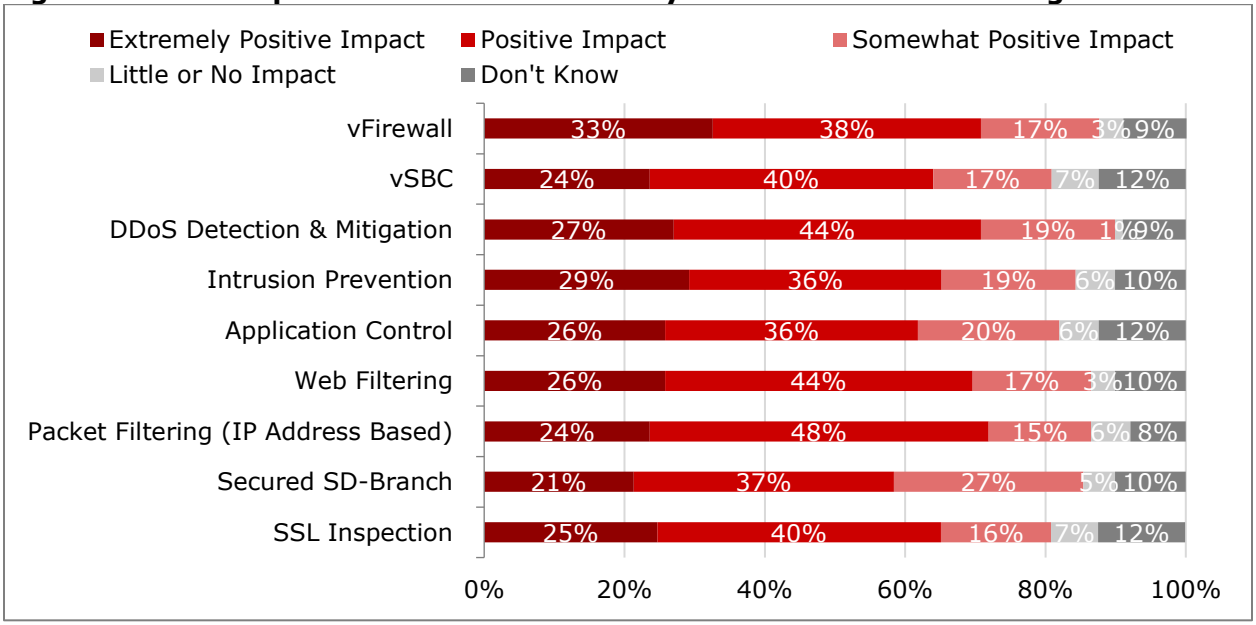


Question: How will automation generally impact your SD-WAN security services? (N=81)
Source: Heavy Reading

Once the relative value proposition of automation was established, the logical next step was to obtain more granular insight into which SD-WAN functions would be most positively affected by the implementation of automated security policies and provisioning processes.

As shown in **Figure 23** below, based on "extremely positive impact" and "positive impact" response levels, the entire standard list of SD-WAN security functions is relevant. Of these, based on the top three "extremely positive impact" responses, the top areas are once again vFirewall (33%), intrusion prevention (29%), and DDoS mitigation (27%). However, as observed in other data distributions, capabilities such as application control, web filtering, and packet filtering are behind only by a few points (24%-26%), emphasizing their overall strong value proposition. Hence, in this case, it is clear that CSPs believe automation will be valuable on many levels.

Figure 23: The Impact of Automated Security Policies and Provisioning



Question: What impact will the implementation of automated security policies and provisioning processes have on the performance of the following SD-WAN security services? (N=89)
Source: Heavy Reading

The richness of SD-WAN's security service offering has unquestionably been one of the factors for managed security service market success. And looking forward, new capabilities will be needed to maintain this position of strength.

Accordingly, in the final question of the survey, Heavy Reading asked the survey respondents to provide insight into which additional capabilities would enhance their ability to upsell managed security services.

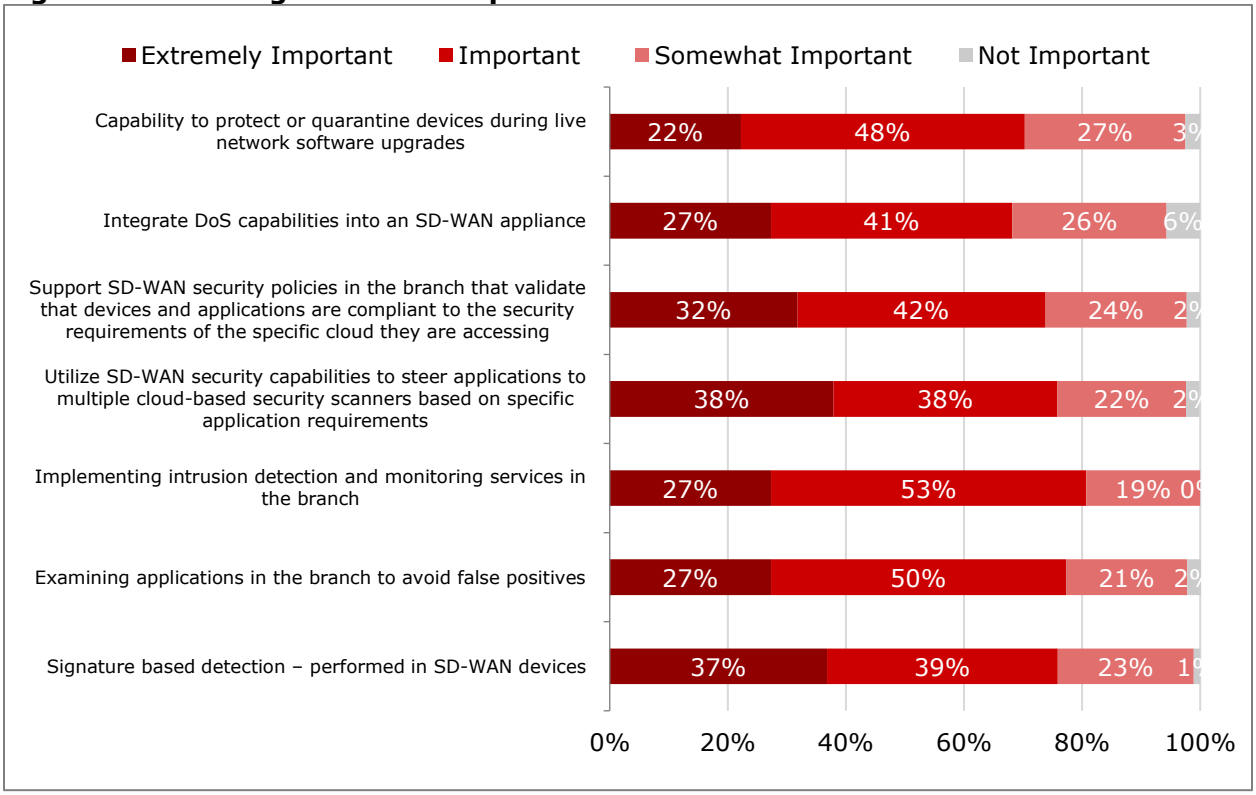
As shown in **Figure 24** below, although all the standard SD-WAN security services fared well based on the level of "extremely important" and "important responses," in looking at the extremely important responses, three capabilities stand out. The highest-ranked of these is the ability to utilize SD-WAN security policies to steer applications to multiple scanners based on specific application requirements (38%).

Heavy Reading believes the high ranking of this capability highlights the realities and challenges associated with moving to an application-centric cloud. Very closely behind at 37% is signature-based detection in SD-WAN devices. This is significant because it not only confirms that devices remain an area of concern for end-users, it also reinforces that CSPs are looking for any unique attack identifiers that can help with the detection of future attack vectors.

The third-ranked advanced capability is branch specific. In this case, the focus is on applying SD-WAN security policies in the branch to first ensure the devices and applications in the branch are fully compliant to the cloud(s) they will run in (32%). Overall, Heavy Reading views this as further validation that the shift to an application environment will demand SD-WAN security services continue to evolve to an application-aware model.

In looking at the two filter group inputs, U.S. respondents are more optimistic than their RoW counterparts about the value of these advanced capabilities to enhance their ability to sell customers managed SD-WAN security services (see **Figure 44**).

Figure 24: Ranking Advanced Capabilities



Question: To what extent would support of the following advanced capabilities enhance your ability to sell your customer-managed SD-WAN security services? (N=81-88)
Source: Heavy Reading

3. APPENDIX A: FILTER GROUP DATA

This appendix provides detailed response data and key findings for each survey question for the two filter groups: the U.S. and the RoW. These filter groups were chosen because they were of similar sizes (U.S. 44 respondents vs. RoW 46 respondents).

Demographically, it is important to note that a greater percentage of the U.S. respondents worked for the largest CSPs – those that generate more than $5 billion in annual revenue. 39% (17 of 44) of U.S. respondents worked for the largest CSPs; only 9% (4 of 46) of RoW respondents worked for these CSPs. This trend helps explain why the U.S. respondents appear more progressive in actual or planned security service implementation schedules.

Figure 25: SD-WAN Security Service Implementation Priorities: U.S. vs. RoW

U.S. (N=42-43)

	Extremely Important	Important	Somewhat Important	Not Important
vFirewall	49%	40%	12%	0%
Intrusion Prevention	33%	54%	14%	0%
DDoS Detection & Mitigation	33%	52%	12%	2%
Secured SD-Branch	37%	47%	16%	0%
Application Control	26%	51%	23%	0%
Web Filtering	33%	47%	21%	0%
Packet Filtering (IP Address Based)	21%	61%	16%	2%
SSL Inspection	26%	51%	21%	2%
vSBC	19%	49%	30%	2%

RoW (N=46)

	Extremely Important	Important	Somewhat Important	Not Important
vFirewall	33%	52%	13%	2%
Intrusion Prevention	37%	39%	24%	0%
DDoS Detection & Mitigation	35%	44%	22%	0%
Secured SD-Branch	24%	37%	35%	4%
Application Control	26%	52%	20%	2%
Web Filtering	17%	61%	22%	0%
Packet Filtering (IP Address Based)	28%	50%	22%	0%
SSL Inspection	20%	46%	28%	7%
vSBC	17%	52%	26%	4%

Question: How important is it for your SD-WAN implementation to support the following security services?

Source: Heavy Reading

Key Findings
While some data points are different, overall, there are several similarities in terms of SD-WAN security service priorities. For example, based on "extremely important" responses, the top three priorities for U.S. respondents are vFirewall (49%), secured SD-branch (37%), and intrusion prevention, DDoS mitigation, and web filtering (all 33%).

For RoW respondents, while the ordering is a little different, the top three priorities of intrusion prevention (37%), DDoS mitigation (35%), and then vFirewall (33%) align with input from their U.S. counterparts.

Figure 26: SD-WAN Security Service Implementation Status: U.S. vs. RoW
U.S. (N=43)

	Implemented	Implementing Now	Implement in 12-18 Months	Will Implement – but No Timeframe	Will Not Implement
vFirewall	42%	21%	28%	9%	0%
vSBC	12%	33%	35%	16%	5%
DDoS Detection & Mitigation	33%	30%	23%	14%	0%
Intrusion Prevention	40%	33%	19%	9%	0%
Application Control	28%	23%	26%	21%	2%
Web Filtering	30%	23%	26%	21%	0%
Packet Filtering (IP Address Based)	26%	30%	26%	16%	2%
Secured SD-Branch	16%	47%	23%	14%	0%
SSL Inspection	26%	37%	21%	14%	2%

RoW (N=47)

	Implemented	Implementing Now	Implement in 12-18 Months	Will Implement – but No Timeframe	Will Not Implement
vFirewall	26%	28%	26%	20%	0%
vSBC	15%	22%	37%	20%	7%
DDoS Detection & Mitigation	26%	22%	33%	15%	4%
Intrusion Prevention	20%	26%	33%	20%	2%
Application Control	20%	22%	33%	24%	2%

	Implemented	Implementing Now	Implement in 12-18 Months	Will Implement – but No Timeframe	Will Not Implement
Web Filtering	22%	28%	20%	26%	4%
Packet Filtering (IP Address Based)	22%	20%	28%	28%	2%
Secured SD-Branch	9%	26%	28%	33%	4%
SSL Inspection	9%	22%	28%	33%	9%

Question: What is the implementation status of the following SD-WAN security services?
Source: Heavy Reading

Key Findings
Based on ranges of comparison data, while U.S. carriers are clearly ahead in terms of implemented service capabilities (12%-42%) versus their RoW counterparts (9%-26%), the top leading implemented service in both groups is vFirewall (U.S. 42% vs. RoW 26%). The second priority for U.S. respondents is intrusion prevention (40%); for RoW respondents, the second priority is DDoS mitigation (26%).

Overall, Heavy Reading views this input as confirming that CSPs globally have made the practical decision to first implement the most mature value-add security services before focusing on advanced capabilities. Examples of the latter include application control and web filtering. Secured SD-branch scored highest by a considerable margin in U.S. "implementing now" response priorities (47%).

Figure 27: SD-WAN Security Service Growth: U.S. vs. RoW
U.S. (N=42-43)

	Aggressive Growth (25% or Greater)	Moderate Growth (10%-24%)	Low Growth (Less Than 10%)	No Growth	Not Applicable
vFirewall	35%	40%	14%	5%	7%
DDoS Detection & Mitigation	23%	42%	14%	12%	9%
Intrusion Prevention	33%	33%	16%	12%	7%
Application Control	26%	33%	19%	12%	12%
Secured SD-Branch	24%	38%	19%	7%	12%
vSBC	30%	33%	16%	7%	14%
Web Filtering	23%	35%	19%	14%	9%
Packet Filtering (IP Address Based)	23%	35%	23%	9%	9%
SSL Inspection	23%	37%	21%	7%	12%

RoW (N=46)

	Aggressive Growth (25% or Greater)	Moderate Growth (10%-24%)	Low Growth (Less Than 10%)	No Growth	Not Applicable
vFirewall	22%	33%	35%	7%	4%
DDoS Detection & Mitigation	22%	30%	37%	7%	4%
Intrusion Prevention	13%	28%	41%	11%	7%
Application Control	17%	28%	33%	15%	7%
Secured SD-Branch	13%	26%	33%	22%	7%
vSBC	4%	41%	39%	9%	7%
Web Filtering	7%	41%	37%	11%	4%
Packet Filtering (IP Address Based)	4%	46%	33%	13%	4%
SSL Inspection	4%	28%	44%	13%	11%

Question: What level of growth are you experiencing for the following SD-WAN security services?
Source: Heavy Reading

Key Findings

U.S. respondents are experiencing higher levels of "aggressive growth," which is likely why they have a more aggressive implementation schedule (see **Figure 26**). In both groups, the vFirewall scored highest in this band (U.S. 35% vs. RoW 22%).

While the two groups tend to rank growth opportunities differently, the range of "moderate growth" inputs are similar for both (U.S. 33%-42% vs. RoW 26%-46%). This confirms that SD-WAN security services represent a global opportunity.

Figure 28: Differentiating SD-WAN Security Services: U.S. vs. RoW

U.S. (N=44)

	Percent
Offer customers a variety of SD-WAN + security service bundles with different set of security features to meet their individual needs (e.g., enterprise, mid-market, SME)	41%
Offer customers the option to use the best-of-breed security vendor we selected and bundled with the SD-WAN service	23%
Offer customers the option to choose from several best-of-breed onboarded security vendors that can be bundled with the SD-WAN service	9%
Offer customers the flexibility to deploy a bundled virtual firewall/security service at the customer premises, data center or public cloud	9%
Improve customer experience through simplification, better integration, orchestration and automation of SD-WAN and bundled security services	16%
Implement a service portal marketplace where customers can order and co-manage SD-WAN and bundled security services	2%

RoW (N=46)

	Percent
Offer customers a variety of SD-WAN + security service bundles with different set of security features to meet their individual needs (e.g., enterprise, mid-market, SME)	30%
Offer customers the option to use the best-of-breed security vendor we selected and bundled with the SD-WAN service	26%
Offer customers the option to choose from several best-of-breed onboarded security vendors that can be bundled with the SD-WAN service	20%
Offer customers the flexibility to deploy a bundled virtual firewall/security service at the customer premises, data center or public cloud	15%
Improve customer experience through simplification, better integration, orchestration and automation of SD-WAN and bundled security services	7%
Implement a service portal marketplace where customers can order and co-manage SD-WAN and bundled security services	2%

Question: What is your preferred approach for differentiating your managed SD-WAN security services?
Source: Heavy Reading

Key Findings
Although U.S. respondents are more bullish on the first option – the individualized security bundle option (U.S. 41% vs. RoW 30%) – it represents the number one response for both groups, confirming its overall importance. Another interesting point is that RoW respondents showed a greater level of support for the best-of-breed customer choice onboarded model compared to U.S. respondents (U.S. 9% vs. RoW 20%).

While it is not clear why this is the case, both groups have similar views, ranking the other best-of-breed option (vendors selected by the CSP) as the second greatest managed security service differentiation opportunity (U.S. 23% vs. RoW 26%).

Figure 29: SD-WAN Security Service Support Option: U.S. vs. RoW
U.S. (N=44)

	Percent
Rely on embedded security features from our primary SD-WAN vendor(s)	18%
Utilize third-party best-of-breed security vendor solution features (e.g., NGFW)	34%
A mixture of the above two approaches	39%
We just provide SD-WAN connectivity and our customers run their own security solution on top of it	2%
Not sure	7%

RoW (N=46)

	Percent
Rely on embedded security features from our primary SD-WAN vendor(s)	15%
Utilize third-party best-of-breed security vendor solution features (e.g., NGFW)	24%
A mixture of the above two approaches	52%
We just provide SD-WAN connectivity and our customers run their own security solution on top of it	7%
Not sure	2%

Question: What is your preferred approach for supporting security features in your offered SD-WAN services?
Source: Heavy Reading

Key Findings
Inputs here are quite similar. Both filter groups ranked the mixture of both approaches the most desirable option (U.S. 39% vs. RoW 52%). While this is a sensible choice to meet immediate service demands, Heavy Reading believes that the second-place ranking of the best-of-breed option (U.S. 34% vs. RoW 24%) confirms that CSPs are increasing their focus on integrating third-party vendor solutions to maximize managed security service delivery agility.

Figure 30: SD-WAN Security Service SECaaS Integration: U.S. vs. RoW
U.S. (N=44)

	Percent
We will partially integrate some SD-WAN security features into our SECaaS portfolio and fully integrate others	34%
We will fully integrate SD-WAN security features into our SECaaS portfolio – single pane of glass monitoring – single support team	39%
In the beginning, we will partially integrate SD-WAN security features into our SECaaS portfolio but will transition to a fully integrated model	16%
We have no plans to integrate SD-WAN security features into our SECaaS portfolio	11%

RoW (N=46)

	Percent
We will partially integrate some SD-WAN security features into our SECaaS portfolio and fully integrate others	39%
We will fully integrate SD-WAN security features into our SECaaS portfolio – single pane of glass monitoring – single support team	17%
In the beginning, we will partially integrate SD-WAN security features into our SECaaS portfolio but will transition to a fully integrated model	39%
We have no plans to integrate SD-WAN security features into our SECaaS portfolio	4%

Question: To what extent will you integrate SD-WAN security features into your SECaaS portfolio?
Source: Heavy Reading

Key Findings
U.S. respondents' preferred SECaaS integration model is the fully integrated single pane of glass model (39%). RoW respondents were equally split between the selective service integration model and partial to fully integrated transition model approach (both 39%).

Figure 31: SD-WAN Security Feature Deployment Preferences: U.S. vs. RoW
U.S. (N=44)

	Percent
Deployed independently of the SD-WAN solution in the telco cloud	41%
Deployed with the SD-WAN solution in the telco cloud	32%
Deployed at the customer branches /sites	9%
We will let the customer chose which option best meets their requirements	9%
We have no real preference	7%
Deployed in a public cloud	2%

RoW (N=46)

	Percent
Deployed independently of the SD-WAN solution in the telco cloud	28%
Deployed with the SD-WAN solution in the telco cloud	28%
Deployed at the customer branches /sites	15%
We will let the customer chose which option best meets their requirements	13%
We have no real preference	7%
Deployed in a public cloud	9%

Question: Do you have a preference where the security solution for your SD-WAN service is deployed?
Source: Heavy Reading

Key Findings
Although the two preferences for both groups are similar, more U.S. respondents than RoW respondents prefer the independent deployment model (U.S. 41% vs. RoW 28%). Also of note is the fact that more RoW respondents prefer the branch deployment model (U.S. 9% vs. RoW 15%). Only a few U.S. and RoW respondents indicated they prefer to deploy SD-WAN security services in a public cloud environment (U.S. 2% vs. RoW 9%).

Figure 32: SD-WAN Security Service Location Implementation Preferences: U.S. vs. RoW

U.S. (N=44)

	Branch Office	Telco Cloud	Public Cloud	Hybrid Cloud
vFirewall	41%	41%	17%	2%
vSBC	29%	49%	15%	7%
DDoS Detection & Mitigation	12%	57%	17%	14%
Intrusion Prevention	24%	43%	19%	14%
Application Control	21%	43%	24%	12%
Web Filtering	21%	48%	17%	14%
Packet Filtering (IP Address Based)	38%	38%	10%	14%
Secured SD-Branch	43%	41%	7%	10%
SSL Inspection	33%	41%	17%	10%

RoW (N=46)

	Branch Office	Telco Cloud	Public Cloud	Hybrid Cloud
vFirewall	33%	57%	9%	2%
vSBC	17%	72%	7%	4%
DDoS Detection & Mitigation	35%	50%	11%	4%
Intrusion Prevention	26%	61%	7%	7%
Application Control	33%	46%	13%	9%
Web Filtering	28%	41%	22%	9%
Packet Filtering (IP Address Based)	35%	50%	11%	4%
Secured SD-Branch	33%	46%	17%	4%
SSL Inspection	33%	39%	20%	9%

Question: Where is the best place in the network to implement the following SD-WAN security services?

Source: Heavy Reading

Key Findings

A clear majority of both U.S. and RoW respondents prefer the telco cloud option for service delivery (U.S. 38%-57% vs. RoW 39%-72%).

While there was considerable deviation in branch office priorities, there were a few similarities as well. For example, the top three branch services for U.S. respondents are secured SD-branch (43%), vFirewall (41%), and packet filtering (38%). For RoW respondents, the priorities are packet filtering and DDoS mitigation (both 35%) and then vFirewall, application control, secured SD-branch, and SSL inspection (all 33%).

Despite the limited general support for deploying SD-WAN security services in the public cloud noted in **Figure 31**, some U.S. and RoW respondents would adopt this model for specific services. For U.S. respondents, the two use cases are application control (24%) and intrusion prevention (19%). RoW respondents focused on web filtering (22%) and SSL inspection (20%).

Figure 33: SD-WAN VNF-Based Service Bundle Implementation Status: U.S. vs. RoW

U.S. (N=42)

	We Have Implemented This Capability	We Plan to Implement This Capability in 12 Months	We Plan to Implement This Capability in 12-18 Months	We May Implement	We Have No Plans to Implement
vFirewall	38%	26%	12%	24%	0%
vSBC	10%	45%	10%	31%	5%
DDoS Detection & Mitigation	29%	43%	12%	14%	2%
Intrusion Prevention	33%	31%	17%	19%	0%
Application Control	29%	31%	21%	17%	2%
Web Filtering	19%	40%	17%	24%	0%
Packet Filtering (IP Address Based)	24%	38%	17%	21%	0%
Secured SD-Branch	14%	40%	17%	26%	2%
SSL Inspection	19%	48%	14%	17%	2%

RoW (N=46)

	We Have Implemented This Capability	We Plan to Implement This Capability in 12 Months	We Plan to Implement This Capability in 12-18 Months	We May Implement	We Have No Plans to Implement
vFirewall	26%	28%	24%	22%	0%
vSBC	13%	26%	24%	33%	4%
DDoS Detection & Mitigation	20%	24%	26%	30%	0%
Intrusion Prevention	17%	28%	35%	20%	0%
Application Control	15%	28%	30%	22%	4%
Web Filtering	17%	39%	24%	20%	0%
Packet Filtering (IP Address Based)	17%	33%	28%	22%	0%

	We Have Implemented This Capability	We Plan to Implement This Capability in 12 Months	We Plan to Implement This Capability in 12-18 Months	We May Implement	We Have No Plans to Implement
Secured SD-Branch	7%	22%	35%	35%	2%
SSL Inspection	7%	28%	30%	30%	4%

Question: Do you plan to support service bundles/offerings of virtual network functions with your SD-WAN service?
Source: Heavy Reading

Key Findings
U.S. respondents are well ahead in terms of implementing VNF-based SD-WAN security service bundles based on the range of already implemented responses (U.S. 14%-38% vs. RoW 7%-26%). In both groups, the leading implemented VNF function is vFirewall (U.S. 38% vs. RoW 26%).

Figure 34: Security NFV Orchestration Preferences: U.S. vs. RoW
U.S. (N=44)

	Percent
Utilize a third-party open-source NFV orchestrator that is SD-WAN vendor-agnostic that can be deployed in multiple environments	32%
Utilize a third-party proprietary NFV orchestrator	30%
Utilize the controller supplied by the SD-WAN vendor(s)	25%
Use our existing OSS solution (with no NFV orchestration module)	5%
No real preference	9%

RoW (N=45)

	Percent
Utilize a third-party open-source NFV orchestrator that is SD-WAN vendor-agnostic that can be deployed in multiple environments	36%
Utilize a third-party proprietary NFV orchestrator	31%
Utilize the controller supplied by the SD-WAN vendor(s)	24%
Using VNFM (VNF manager) without end-to-end orchestration	4%
No real preference	4%

Question: What is your preferred approach for orchestrating security VNFs in an SD-WAN network?
Source: Heavy Reading

Key Findings
In both groups, the preferred approach is the third-party vendor-agnostic orchestration model (U.S. 32% vs. RoW 36%). Similarly, in both groups, the third-party proprietary model is the second favored approach (U.S. 30% vs. RoW 31%).

Figure 35: Branch-Based Security Strategies: U.S. vs. RoW

U.S. (N=41-43)

	Already Implemented	Currently Implementing	May Implement
Branch-based security for local internet breakout	44%	37%	20%
Secure all communications to/from all locations	40%	33%	28%

RoW (N=45-46)

	Already Implemented	Currently Implementing	May Implement
Branch-based security for local internet breakout	24%	31%	44%
Secure all communications to/from all locations	17%	48%	35%

Question: Do you plan to use branch-based security functions for local internet breakout only, or to secure all communications from the branch to other branches, HQ, and cloud?

Source: Heavy Reading

Key Findings

U.S. service providers lead their RoW counterparts from an implementation perspective. While 44% of U.S. respondents have implemented internet breakout, only 24% of RoW service providers have. In looking at the "currently implementing" responses, more RoW respondents are currently implementing the all location option (U.S. 33% vs. RoW 48%). This is likely in part because they lag in "already implementing" responses.

Despite the differences, given the lower levels of "may implement" responses, Heavy Reading interprets the data as confirming that both the local breakout and all locations options are relevant components of a branch-based security strategy for all CSPs.

Figure 36: uCPE SD-WAN Security Service Preferences: U.S. vs. RoW

U.S. (N=41-42)

	Already Support This Capability	Implementing This Capability on uCPE	May Implement This Capability on uCPE	Will Not Implement This Capability on uCPE
vFirewall	38%	43%	12%	7%
vSBC	29%	41%	17%	14%
DDoS Detection & Mitigation	43%	36%	14%	7%
Intrusion Prevention	38%	38%	17%	7%
Application Control	31%	43%	19%	7%
Web Filtering	29%	38%	26%	7%
Packet Filtering (IP Address Based)	34%	37%	22%	7%
Secured SD-Branch	38%	26%	29%	7%
SSL Inspection	29%	48%	14%	10%

RoW (N=44-46)

	Already Support This Capability	Implementing This Capability on uCPE	May Implement This Capability on uCPE	Will Not Implement This Capability on uCPE
vFirewall	26%	26%	41%	7%
vSBC	9%	33%	41%	17%
DDoS Detection & Mitigation	17%	22%	52%	9%
Intrusion Prevention	20%	33%	44%	4%
Application Control	13%	24%	51%	11%
Web Filtering	18%	27%	50%	5%
Packet Filtering (IP Address Based)	15%	26%	52%	7%
Secured SD-Branch	13%	26%	48%	13%
SSL Inspection	13%	22%	52%	13%

Question: Which security services do you plan to offer as VNFs on uCPE in the branch?
Source: Heavy Reading

Key Findings

While roughly 70% or more of U.S. respondents either already support or are implementing VNFs on uCPE, only about 30% to 52% of RoW respondents fall into these two categories. Another notable data point is that support for vSBC VNFs is greater among U.S. respondents

in terms of being an already supported capability (U.S. 29% vs. RoW 9%) as well as an active implementation priority (U.S. 41% vs. RoW 33%).

Figure 37: Branch Office Business Challenges: U.S. vs. RoW

U.S. (N=42-43)

	Major Challenge	A Challenge	Somewhat of a Challenge	Not a Challenge	Not Sure
Customer expectations of low-cost branch devices make it difficult to sell advanced security capabilities in the branch	35%	37%	16%	2%	9%
Limited demand for advanced security features	29%	41%	19%	5%	7%
Higher administrative and support opex costs	14%	51%	23%	5%	7%

RoW (N=46)

	Major Challenge	A Challenge	Somewhat of a Challenge	Not a Challenge	Not Sure
Customer expectations of low-cost branch devices make it difficult to sell advanced security capabilities in the branch	28%	52%	15%	4%	0%
Limited demand for advanced security features	11%	48%	30%	9%	2%
Higher administrative and support opex costs	13%	46%	33%	9%	0%

Question: What business challenges have you encountered with implementing SD-WAN security in the branch office?

Source: Heavy Reading

Key Findings

Based on the similarity of "major challenge" inputs (U.S. 35% vs. RoW 28%), both U.S. and RoW respondents are aligned with the view that customer expectations of low-cost branch devices make it difficult to sell advanced security capabilities in the branch.

Furthermore, the range of "a challenge" inputs from both groups for all three variables are similar as well (U.S. 37%-51% vs. RoW 46%-52%). The one notable exception is that a greater percentage of U.S. respondents view limited demand for advanced security features as a "major challenge" than their RoW counterparts (U.S. 29% vs. RoW 11%).

Figure 38: SD-WAN Technical Security Branch Deployment Challenges: U.S. vs. RoW

U.S. (N=43)

	Major Challenge	A Challenge	Somewhat of a Challenge	Not a Challenge	Don't Know
SD-WAN performance is negatively impacted when security capabilities are added	30%	40%	14%	5%	12%
Lack of security certification for branch devices	28%	35%	19%	7%	12%
Scheduling security updates	19%	42%	21%	7%	12%
Lack of onsite technical support	14%	40%	33%	5%	9%
Diverse set of devices and installed platforms	21%	35%	26%	9%	9%

RoW (N=46)

	Major Challenge	A Challenge	Somewhat of a Challenge	Not a Challenge	Don't Know
SD-WAN performance is negatively impacted when security capabilities are added	24%	46%	17%	7%	7%
Lack of security certification for branch devices	22%	30%	37%	7%	4%
Scheduling security updates	7%	39%	46%	4%	4%
Lack of onsite technical support	13%	41%	37%	2%	7%
Diverse set of devices and installed platforms	17%	39%	30%	7%	7%

Question: What technical challenges have you encountered with implementing SD-WAN security in the branch office?

Source: Heavy Reading

Key Findings

In terms of technical challenges associated with implementing SD-WAN security services in the branch office, based on the level of "major challenge" inputs, both groups are aligned. For example, in both cases, the number one concern is that SD-WAN performance is negatively impacted when security capabilities are added (U.S. 30% vs. RoW 24%). The number two major concern is the same as well and relates to the lack of security certification for branch devices (U.S. 28% vs. RoW 22%). Moreover, the range of "a challenge" responses is also similar (U.S. 35%-42% vs. RoW 30%-46%).

Figure 39: Service-Chaining Security VNFs: U.S. vs. RoW

U.S. (N=40-42)

	Will Offer This as a Service-Chained VNF	May Offer This as a Service-Chained VNF	Will Not Offer This as a Service-Chained VNF	Not Sure
vFirewall	48%	36%	7%	10%
vSBC	33%	41%	12%	14%
DDoS Detection & Mitigation	45%	40%	5%	10%
Intrusion Prevention	41%	41%	10%	10%
Application Control	48%	31%	7%	14%
Web Filtering	36%	43%	7%	14%
Packet Filtering (IP Address Based)	31%	50%	7%	12%
Secured SD-Branch	26%	55%	7%	12%
SSL Inspection	33%	40%	15%	13%

RoW (N=45-46)

	Will Offer This as a Service-Chained VNF	May Offer This as a Service-Chained VNF	Will Not Offer This as a Service-Chained VNF	Not Sure
vFirewall	30%	41%	20%	9%
vSBC	20%	48%	17%	15%
DDoS Detection & Mitigation	24%	37%	20%	20%
Intrusion Prevention	26%	46%	20%	9%
Application Control	17%	50%	15%	17%
Web Filtering	22%	44%	24%	11%
Packet Filtering (IP Address Based)	17%	41%	24%	17%
Secured SD-Branch	16%	42%	20%	22%
SSL Inspection	17%	39%	17%	26%

Question: Which security services do you plan to offer as service-chained VNFs in the cloud?
Source: Heavy Reading

Key Findings

U.S. respondents are more committed to offering security services as service-chained VNFs in the cloud than RoW respondents. For example, the range of "will offer" U.S. inputs is 26% to 48% vs. the RoW input range of 16% to 30%. However, in both cases, vFirewall is the top VNF service-chain capability (U.S. 48% tied for first place with application control

vs. 30% for RoW). The range of "may offer" responses between the two groups is also similar (U.S. 31%-55% vs. RoW 37%-50%).

Figure 40: Evolving SD-WAN Security Services: U.S. vs. RoW

U.S. (N=43)

	We Expect a Seamless Software Migration	We Expect a Complex but Manageable Migration	We Expect a Very Complex Migration	We Don't Know Yet
Multi-Access Edge Computing (MEC)	26%	47%	14%	14%
5G RAN Implementation	28%	40%	14%	19%
5G NGC Core Implementation	28%	42%	12%	19%
5G Slice-Based Services	23%	51%	7%	19%
IoT Services	30%	35%	14%	21%
SSL Encrypted Traffic Inspection	28%	47%	9%	16%

RoW (N=46)

	We Expect a Seamless Software Migration	We Expect a Complex but Manageable Migration	We Expect a Very Complex Migration	We Don't Know Yet
Multi-Access Edge Computing (MEC)	15%	54%	15%	15%
5G RAN Implementation	13%	44%	26%	17%
5G NGC Core Implementation	13%	39%	33%	15%
5G Slice-Based Services	9%	41%	30%	20%
IoT Services	20%	44%	22%	15%
SSL Encrypted Traffic Inspection	13%	50%	22%	15%

Question: How difficult will it be for your current commercial SD-WAN security services implementation to evolve to support the following advanced networking capabilities?
Source: Heavy Reading

Key Findings

A greater number of U.S. respondents believe they will be able to achieve a "seamless software migration" as new technologies roll out (23%-30%) compared to a smaller group of RoW respondents (9%-20%). In contrast, generally, twice the number of RoW respondents expect a "very complex migration" (15%-33%) compared to their U.S. counterparts (7%-14%).

Figure 41: SD-WAN Security Analytics Support: U.S. vs. RoW

U.S. (N=43)

	Already Support This Capability	Implementing This Capability	May Implement This Capability	Will Not Implement This Capability
User Profile Data (Identity Management)	40%	44%	16%	0%
Application Usage	42%	40%	19%	0%
URLs Accessed	37%	35%	26%	2%
Geolocation Data (Attack Origination)	37%	33%	30%	0%
Threats Mitigated or Blocked (includes threat type and profile of threat vector)	28%	42%	28%	2%
Network Traffic Analysis	47%	30%	23%	0%
Incident Forensics	23%	35%	42%	0%
Regulatory Compliance Metrics	23%	37%	35%	5%

RoW (N=45-46)

	Already Support This Capability	Implementing This Capability	May Implement This Capability	Will Not Implement This Capability
User Profile Data (Identity Management)	17%	30%	52%	0%
Application Usage	20%	26%	48%	7%
URLs Accessed	28%	22%	50%	0%
Geolocation Data (Attack Origination)	18%	22%	56%	4%
Threats Mitigated or Blocked (includes threat type and profile of threat vector)	26%	24%	46%	4%
Network Traffic Analysis	28%	26%	44%	2%
Incident Forensics	13%	26%	57%	4%
Regulatory Compliance Metrics	17%	30%	46%	7%

Question: Which security analytics do you support or plan to support in your SD-WAN security offer?
Source: Heavy Reading

Key Findings

Although network traffic analysis is the number one already implemented capability in both groups (U.S. 47% vs. RoW 28%), U.S. CSPs are more committed to implementing analytics to enhance SD-WAN security services. For example, while 16% to 42% of U.S. respondents

fall into the "may implement" group, 44% to 57% of RoW do. Interestingly, in both groups, incident forensics leads the "may implement" responses (U.S. 42% vs. RoW 57%).

Figure 42: Impact of Automation on SD-WAN Security Services: U.S. vs. RoW

U.S. (N=39)

	Percent
It will have a positive impact – and we don't expect the implementation to be too complex	33%
It will have a positive impact, but it will be very complex to implement	49%
It will not have a positive impact – more trouble than it's worth	5%
We don't know yet what the impact will be	13%

RoW (N=42)

	Percent
It will have a positive impact – and we don't expect the implementation to be too complex	21%
It will have a positive impact, but it will be very complex to implement	69%
It will not have a positive impact – more trouble than it's worth	7%
We don't know yet what the impact will be	2%

Question: How will automation generally impact your SD-WAN security services?
Source: Heavy Reading

Key Findings

Both filter groups identify with the positive impact but complex implementation scenario, with a larger group of RoW respondents identifying with this sentiment (U.S. 49% vs. RoW 69%). In contrast, a larger group of U.S. respondents believes the implementation process will not be too complex (U.S. 33% vs. RoW 21%). While specific data points vary, Heavy Reading believes the commonality in data trends indicates there is a common global sentiment: automation will be complex to implement but worth the undertaking.

Figure 43: The Impact of Automated Security Policies and Provisioning: U.S. vs. RoW

U.S. (N=43)

	Extremely Positive Impact	Positive Impact	Somewhat Positive Impact	Little or No Impact	Don't Know
vFirewall	40%	40%	7%	2%	12%
vSBC	33%	33%	14%	2%	19%
DDoS Detection & Mitigation	30%	49%	9%	0%	12%
Intrusion Prevention	33%	42%	14%	0%	12%
Application Control	33%	40%	12%	0%	16%
Web Filtering	33%	49%	5%	2%	12%
Packet Filtering (IP Address Based)	26%	58%	5%	2%	9%
Secured SD-Branch	28%	54%	7%	0%	12%
SSL Inspection	35%	47%	7%	2%	9%

RoW (N=46)

	Extremely Positive Impact	Positive Impact	Somewhat Positive Impact	Little or No Impact	Don't Know
vFirewall	26%	37%	26%	4%	7%
vSBC	15%	48%	20%	11%	7%
DDoS Detection & Mitigation	24%	39%	28%	2%	7%
Intrusion Prevention	26%	30%	24%	11%	9%
Application Control	20%	33%	28%	11%	9%
Web Filtering	20%	39%	28%	4%	9%
Packet Filtering (IP Address Based)	22%	39%	24%	9%	7%
Secured SD-Branch	15%	22%	46%	9%	9%
SSL Inspection	15%	35%	24%	11%	15%

Question: What impact will the implementation of automated security policies and provisioning processes have on the performance of the following SD-WAN security services?
Source: Heavy Reading

Key Findings

A considerably greater range of U.S. respondents assessed the impact as "extremely positive impact" (26%-40%) versus RoW respondents (15%-26%). Once again, in both groups, vFirewall attained the highest response level in the top category, reaffirming just how important this security function is in an SD-WAN context.

Figure 44: Ranking Advanced Capabilities: U.S. vs. RoW

U.S. (N=40-42)

	Extremely Important	Important	Somewhat Important	Not Important
Signature-based detection – performed in SD-WAN devices	44%	42%	12%	2%
Examining applications in the branch to avoid false positives	33%	52%	12%	2%
Implementing intrusion detection and monitoring services in the branch	33%	57%	10%	0%
Utilize SD-WAN security capabilities to steer applications to multiple cloud-based security scanners based on specific application requirements	52%	33%	12%	2%
Support SD-WAN security policies in the branch that validate that devices and applications are compliant to the security requirements of the specific cloud they are accessing	43%	41%	17%	0%
Integrate DoS capabilities into an SD-WAN appliance	33%	45%	19%	2%
Capability to protect or quarantine devices during live network software upgrades	23%	58%	20%	0%

RoW (N=41-46)

	Extremely Important	Important	Somewhat Important	Not Important
Signature-based detection – performed in SD-WAN devices	30%	37%	33%	0%
Examining applications in the branch to avoid false positives	22%	48%	28%	2%
Implementing intrusion detection and monitoring services in the branch	22%	50%	28%	0%
Utilize SD-WAN security capabilities to steer applications to multiple cloud-based security scanners based on specific application requirements	24%	42%	31%	2%

	Extremely Important	Important	Somewhat Important	Not Important
Support SD-WAN security policies in the branch that validate that devices and applications are compliant to the security requirements of the specific cloud they are accessing	22%	44%	30%	4%
Integrate DoS capabilities into an SD-WAN appliance	22%	37%	33%	9%
Capability to protect or quarantine devices during live network software upgrades	22%	39%	34%	5%

Question: To what extent would support of the following advanced capabilities enhance your ability to sell your customer-managed SD-WAN security services?
Source: Heavy Reading

Key Findings
Based on the range of "extremely important" response levels, U.S. respondents are more convinced of the value of advanced capabilities that enhance their ability to sell managed SD-WAN security services (U.S. 23%-52% vs. RoW 22%-30%).

Despite this deviation in the range of scoring of "extremely important" responses, there is some commonality. The top two capacities (albeit in different order) are the same: steering applications to multiple cloud security scanners (U.S. 1st choice vs. RoW 2nd choice) and signature-based detection in SD-WAN devices (U.S. 2nd choice vs. RoW 1st choice).

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