Next-Generation Network Packet Brokers: Defining the Future of Network Visibility Fabrics

REPORT SUMMARY

By Shamus McGillicuddy
ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) Research
August 2018

SPONSORED BY:

NIAGARA NETWORKS

EMA™ IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Report Summary – Next-Generation Network Packet Brokers: Defining the Future of Network Visibility Fabrics

Table of Contents

©2018 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Report Summary – Next-Generation Network Packet Brokers: Defining the Future of Network Visibility Fabrics

Executive Summary

This research summary highlights the findings of a new Enterprise Management Associates study that examines emerging requirements for delivering network traffic data to out-of-band and inline network and security analysis tools. Specifically, it looks at the current usage of and emerging best practices for network visibility fabrics and network packet brokers. Based on a survey of 250 IT professionals, the research also explores next-generation use cases like traffic monitoring in virtualized infrastructure and the public cloud, and it looks at evolving form factors, such as disaggregated "white box" network packet brokers.

Network Traffic Analysis is Essential to IT Operations and Security Teams

Network traffic analysis is arguably the best way to understand what is happening in a network. Packets crossing the wire are the ultimate source of truth. They can tell analysts where traffic came from, where it's going, and what it contains. IT operations and security teams typically use multiple tools that analyze traffic from various segments of the network.

The delivery of traffic to all of these tools can be a significant challenge. Networks, applications, and data centers are constantly growing and evolving, creating more infrastructure and services that must be monitored. Many analysis tools need to collect data from the same network segments, which creates contention over access to traffic. Also, scale and complexity are expanding as enterprises embrace software-defined infrastructure, virtualization, public cloud services, and the Internet of Things to compete in an increasingly digital economy. In fact, this year EMA research found that enterprise network management decision-making is driven primarily by software-defined data center initiatives, server virtualization, public cloud infrastructure as a service (IaaS) migration, and private cloud architecture.[1]

Many enterprises install a network visibility fabric to connect their traffic analysis tools with traffic data. A visibility fabric mirrors traffic from the production network for out-of-band monitoring, but it can also connect live traffic with inline security tools like firewalls and intrusion prevention systems. These fabrics consist of port mirroring solutions, inline bypass solutions, and network packet brokers. Mature IT organizations deploy and use these network visibility fabrics to provide tools with consistent access to traffic, but they also leverage the advanced traffic grooming and filtering features of network packet brokers to right-size data flows to individual tools.

[1] EMA, "Network Management Megatrends 2018: Exploring NetSecOps Convergence, Network Automation, and Cloud Networking," April 2018.

©2018 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Research Goal

This research study looks at the current state of enterprise network visibility fabrics, with a particular emphasis and focus on network packet brokers, which form the core of any large and complex fabric. The goal is to identify the features, architecture, and administrative capabilities that enterprises most value in network packet brokers. This research also identifies how enterprises are adapting their visibility fabrics to new technology trends, such as virtualization, public cloud, and hardware-software disaggregation. Enterprise Management Associates (EMA) last examined this topic with the October 2013 research study "Network Visibility Controllers: Best Practices for Mainstreaming Monitoring Fabrics." The new research will refer to the 2013 study occasionally to draw trendlines between then and now.

This research study looks at the current state of enterprise network visibility fabrics, with a particular emphasis and focus on network packet brokers.

Research Methodology

For this research, EMA surveyed a random sample of 250 enterprise technology professionals who are directly involved in multiple aspects of their organization's network visibility fabric. In fact, majorities of the respondents are involved in every aspect of the visibility fabric lifecycle, from product evaluation to deployment to actual use of the solutions. Most frequently, respondents are users of network monitoring tools connected to a visibility fabric (69 percent) and security monitoring tools connected to a fabric (70 percent). A significant majority of them are also responsible for managing and maintaining the visibility fabric itself. Slightly more than half of respondents indicated that they are involved in researching these solutions, purchasing them, and implementing them.

While this research examines network visibility fabrics broadly, it is particularly focused on the use of network packet brokers, which are the core element of any mature and sophisticated visibility fabric. Thus, to qualify for this research, participants had to have a packet broker currently deployed in his or her environment. To gain a sense of how much experience an enterprise has with these solutions, EMA asked participants to reveal how long they have had these devices deployed. **Figure 2** reveals that the plurality of respondents (47 percent) have had NPBs deployed for one to five years. Another significant portion (41 percent) only deployed NPBs in the last year. A small minority (12 percent) have had them in place for more than five years.

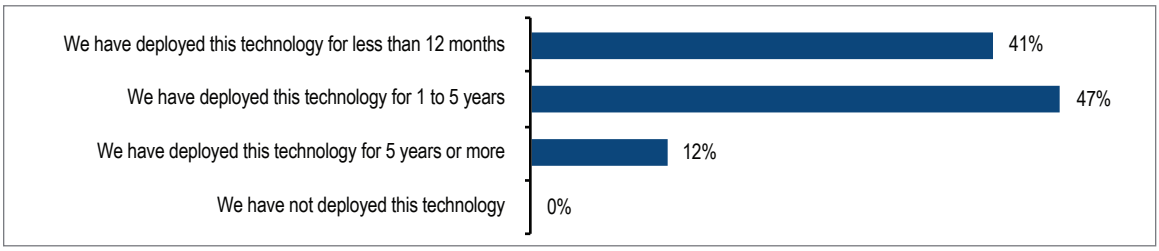

Figure 2. Current status of deployment of Network Packet Brokers (NPBs) within an organization's infrastructure

©2018 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Demographics

Participants in this research all work within an enterprise IT organization. EMA collected demographic data about them.

Role: Thirty-seven percent are IT executives and 63 percent are subject matter experts or middle management.

Function: Twenty-five percent of participants work in security functions, either as a chief information security officer or as a member of the security operations or security engineering teams. The other 75 percent serve in the rest of the IT organization, including the CIO suite, network engineering, network operations, data center operations, application management, IT architecture, and project management.

Size of company (global employees): Fifty percent of respondents work for a midmarket company (250-2,499 employees), and the other half work for a large enterprise (2,500 or more employees).

Size of company (revenue): Sixty-three percent of respondents work for organizations that earn $100 million or more in annual revenue. Thirty-four percent are with organizations that earn from $1 million to less than $100 million. The remainder were either unaware of revenue numbers or worked for government or nonprofit agencies where revenue doesn't apply.

Geography: Fifty-one percent of respondents are located in North America and 49 percent are located in Europe (United Kingdom, France, or Germany).

Network Packet Broker Deployments

Overall, enterprises tend to deploy network packet brokers in data centers more than anywhere else. **Figure 6** reveals where packet brokers are deployed currently and where enterprises intend to deploy them in the next 12 months. At the top of the list is the core of the data center network, where 48 percent of enterprises have them deployed already and another 23 percent plan to deploy them over the next year. The campus backbone is the least likely place for a network packet broker, although the number who have such deployments will nearly double in the next year.

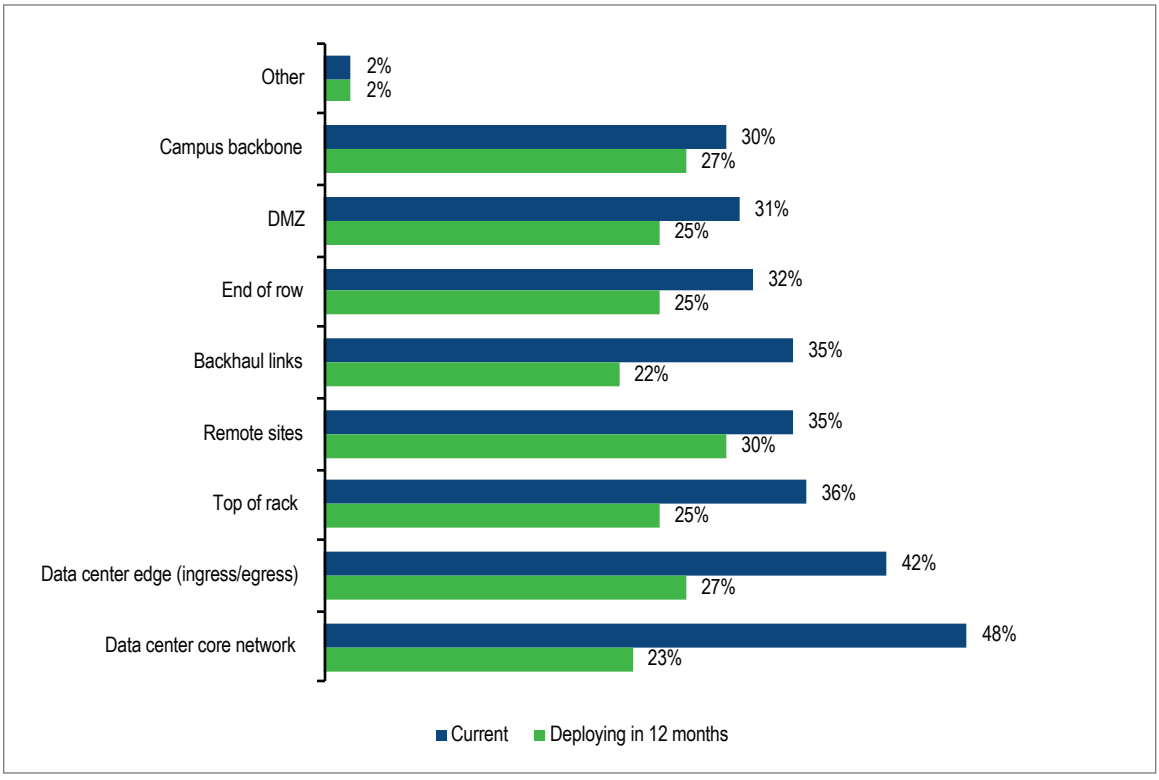

Figure 6. Where NPBs are deployed today, versus 12 months from now

©2018 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Bear in mind, this chart refers to where packet brokers are deployed, not where the visibility fabric is deployed. Many enterprises may have the data center core tapped for monitoring, but not have an actual packet broker there. EMA will address the total coverage of visibility fabrics later in this report.

The data center edge (the egress and ingress point) is the second most common deployment scenario for packet brokers. Remote sites, backhaul links, and data center top-of-rack are all secondarily common deployments for these devices. Remote sites on the WAN will see a significant increase in deployments over the next year, which suggests a strong requirement for improved visibility and security at branch offices and other distributed sites on the WAN.

Security personnel (60 percent) were more likely than IT personnel (45 percent) to say they have packet brokers deployed in the data center core, which suggests a focus on packet-based security over performance management in the data center network. North American respondents (50 percent) were more likely to have a packet broker deployed at the data center edge, versus 35 percent of Europeans. Organizations that have had packet brokers deployed for more than one year were more likely than those with younger deployments to have the devices installed in the campus backbone (36 percent to 22 percent) and remote sites (41 percent versus 27 percent).

Overall Coverage of Packet-Based Visibility Tools

In theory, every network operations and security operations team would monitor 100 percent of the network to ensure that every event is detected and fully analyzed. Very few actually do so.

EMA asked research participants to reveal the percentage of their network segments covered by network performance monitoring tools and security monitoring tools. **Figure 7** shows the depth of coverage for network performance monitoring tools. **Figure 8** shows coverage for security tools.

Enterprises cover a larger portion of their network with security tools than they do with performance management tools.

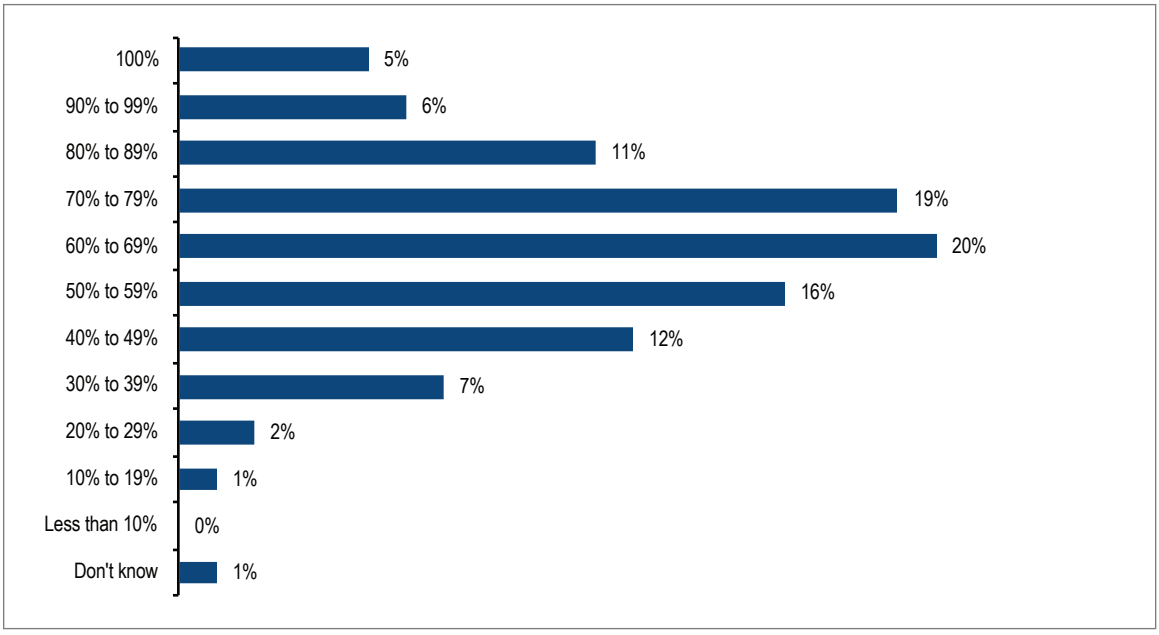

Figure 7. Percentage of network segments currently monitored by network performance monitoring tools

©2018 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

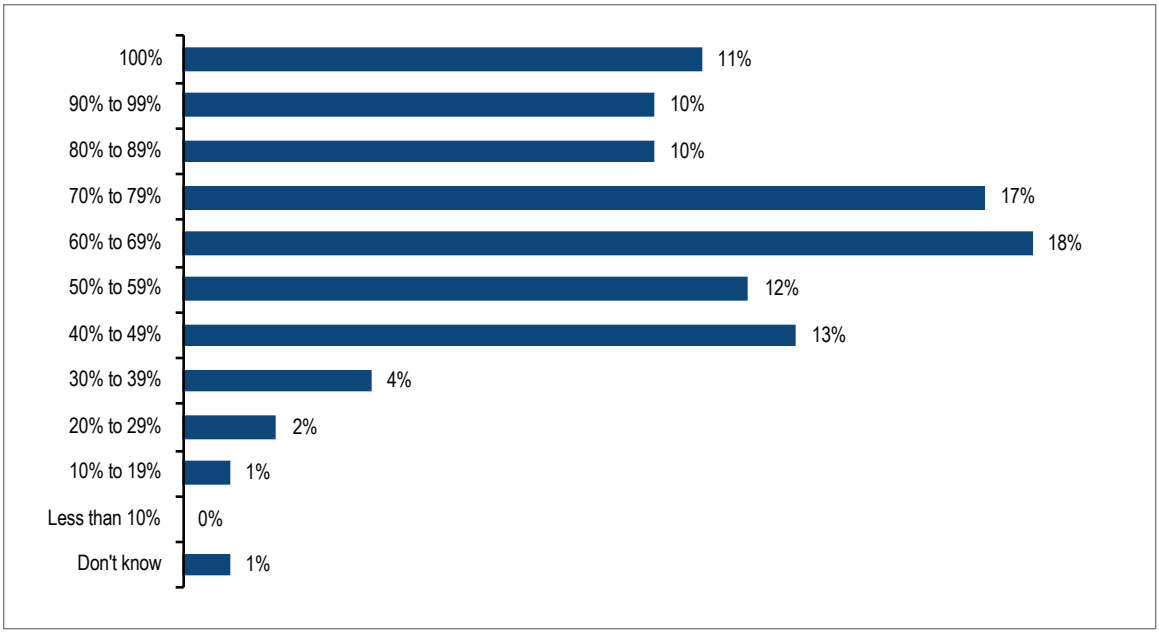

Figure 8. Percentage of network segments currently monitored by security tools

Overall, it's clear that enterprises tend to cover a larger portion of their network with security tools than they do with performance management tools. Figure 7 is a nearly perfect "bell curve," with a majority of enterprises (55 percent) monitoring between 50 percent and 80 percent of their network segments with performance management tools. Only 11 percent of enterprises cover 90 percent or more of network segments with performance management tools, and just ten percent monitor less than 40 percent of network segments.

Responses in Figure 8 present a less perfect bell curve, but a comparison to Figure 7 shows that enterprises clearly prioritize broader coverage with their security tools. For instance, the number of enterprises that monitor 100 percent of network segments with security tools is double the number who monitor 100 percent of segments with performance management tools. Another 20 percent monitor between 80 percent to 99 percent of segments, and 35 percent monitor between 60 percent and 80 percent.

©2018 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

The majority of enterprises monitor a large portion of their network segments with performance management and security tools, but very few cover 100 percent of the network. **Figure 9** explores why 100 percent coverage is so rare. Thirty percent of respondents say they don't need to monitor 100 percent of the network because their current level of coverage meets their needs. Healthcare companies (54 percent) and IT-related professional services firms (56 percent) were very likely to say current coverage is sufficient, versus only 14 percent of financial companies.

Thirty percent of respondents say they don't need to monitor 100 percent of the network because their current level of coverage meets their needs.

The other 70 percent of research participants identified several challenges. Network complexity (38 percent) is the top barrier. European respondents (54 percent) struggle with this complexity issue more often than North Americans (32 percent). Theoretically, a well-architected fabric with advanced network package broker technology should help address complexity. However, visibility fabrics can only do so much. Sometimes the architecture of a network is so arcane that the engineering team can't even quantify the number of segments the network has.

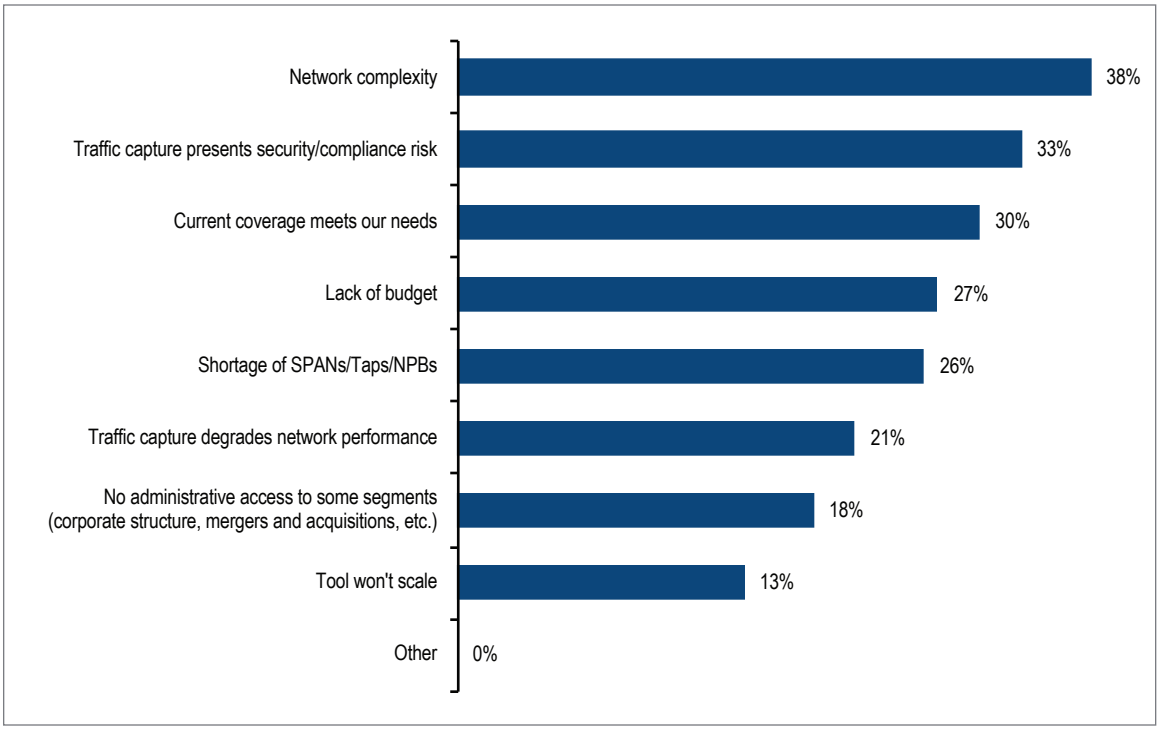

Figure 9. Why organizations do not monitor 100% of network segments

Another common inhibitor of 100 percent coverage is the security or compliance risk posed by traffic capture. Some parts of the network are too sensitive, and the instrumentation of those segments for data access is unacceptable to risk management and compliance teams. They would rather "fly blind" than capture the data, or they may use other data sources for monitoring. For instance, the network engineering team could use active test monitoring solutions, which inject synthetic data into the network and observe its behavior and how infrastructure responds to it. These solutions can provide insight into performance and asset security. NetFlow and other flow technologies are another alternative. This data provides summary data for traffic rather than packet data, so enterprises can monitor traffic behavior without looking at payload data.

©2018 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Lack of budget is a challenge for a little more than a quarter of respondents. Nearly the same number also said they struggle with a shortage of SPAN ports, taps, or network packet brokers. IT executives (35 percent) selected this challenge more often than staff (21 percent).

The least common challenges were degradation of network performance caused by traffic capture (something more applicable to inline security solutions than out-of-band monitoring tools), a lack of administrative access to some network segments, and tools that do not scale.

Given that all of these enterprises use network packet brokers, it's not surprising that tool scalability is such a non-factor. Packet brokers excel at solving this problem by filtering traffic and by load balancing across multiple instances of a tool. Organizations with strong IT budget growth were less than half as likely (ten percent) to struggle with a lack of administrative access, while those with flat or shrinking IT budgets (31 percent) truly struggle with this issue.

Finally, security personnel (37 percent) are twice as likely as IT personnel (16 percent) to be inhibited by network performance degradation. Again, this is indicative of inline security tools, which can impact performance. Out-of-band network performance monitoring tools are rarely going to cause such a problem.

Network Visibility Fabric Procurement and Implementation

Visibility Fabric Procurement Strategies

Network visibility fabrics, packet-based network operations monitoring tools, and packet-based security tools are three very distinct industries. However, they are deeply intertwined. Network operations and security tools live or die by the quality of the visibility fabric that feeds them traffic. Network monitoring vendors and security vendors have strong influence over network visibility fabric implementations. **Figure 15** takes a high-level view of how traffic-based visibility solutions are procured.

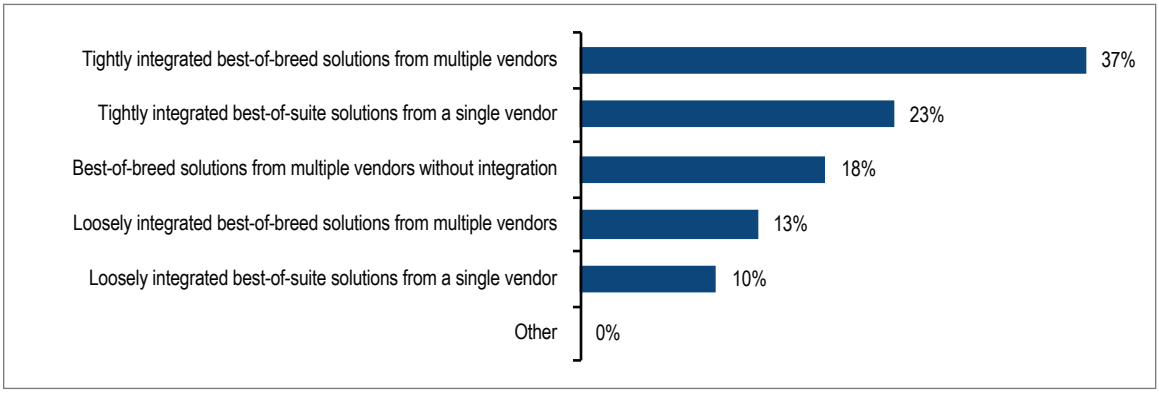

Figure 15. Preferred strategy for selecting and implementing NPBs and visibility fabrics, network monitoring tools, and security monitoring solutions

The data shows that tight integration is essential. The majority of enterprises (60 percent) procure tightly integrated solutions, either best-of-breed solutions from multiple vendors or best-of-suite solutions from a single vendor. Only 18 percent prefer unintegrated solutions and 23 percent prefer loosely integrated solutions.

This data suggests that go-to-market integration between security vendors, network operations tool vendors, and visibility fabric vendors is essential. Also, vendors that can offer all of these pieces in a tightly integrated suite will offer strong value to a specific segment of the market.

©2018 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Visibility Fabric and Network Packet Broker Management

Like any layer of infrastructure, the network visibility fabric requires ongoing management. Network packet brokers have complex software images that require maintenance and upgrades. And their broad, advanced feature sets require configuration management capabilities. **Figure 17** reveals preferred approaches to managing packet brokers and the broader visibility fabric.

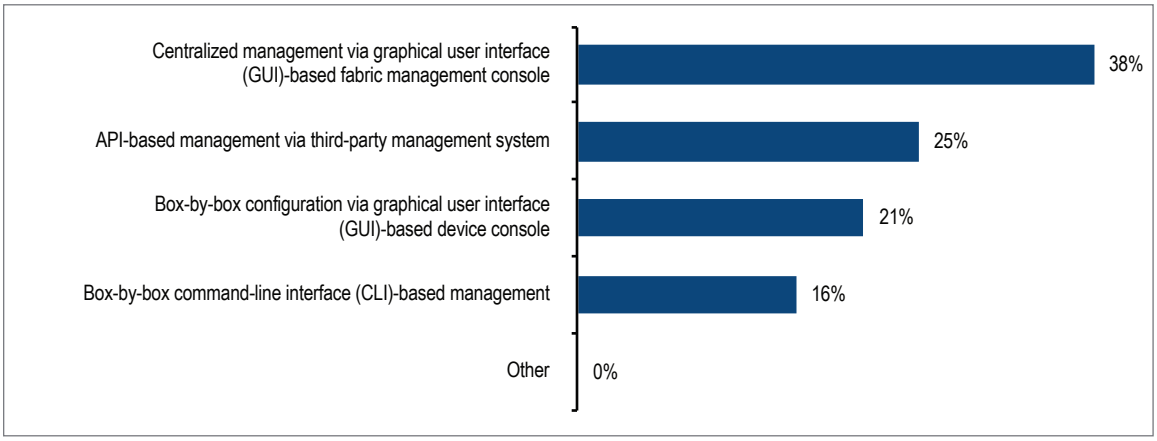

Figure 17. Primary approaches to managing NPBs and the network visibility fabric

Centralized management with a graphical user interface is the most popular approach. Manufacturers of non-IT goods (67 percent) particularly prefer this approach, while application/cloud service providers are unlikely (19 percent).

Centralized management with a graphical user interface is the most popular approach to network visibility fabric management.

The second most popular management approach is API-based management through third-party systems. This could include an IT operations tool that not only consumes traffic from the fabric but also manages the fabric itself. Or it might include an infrastructure orchestration system. Security personnel (32 percent) are more likely than IT personnel (22 percent) to prefer this approach. Cloud/application service providers (41 percent) also like this management approach.

Around one in five enterprises prefer box-by-box GUI management of packet brokers, which is a more granular approach than a GUI-based central management console. IT personnel (24 percent) found this style more appealing than security personnel (11 percent). Government agencies (40 percent) and IT hardware manufacturers (33 percent) also liked this approach. IT staff (26 percent) selected this preference more often than staff (12 percent), which suggests a fundamental difference of opinion from IT leadership. Executives are probably pushing for more efficiency, which means a preference for API-based management or central GUI-based consoles, although we observed no statistically relevant variation there for now.

Box-by-box CLI-based management is definitely the least popular approach to fabric management. This is the least efficient approach, and it also requires product expertise that many personnel will lack.

©2018 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Using the Network Visibility Fabric

Network and Security Teams Sharing the Visibility Fabric

Network operations and security operations teams are increasing their collaboration. In fact, earlier this year, EMA discovered that 40 percent of enterprises have fully converged these groups with shared tools and processes.[2] This convergence is more common among small and midsized enterprises (SMEs), where silos are less prominent. Still, very few enterprises in general continue to keep their security and network operations teams fully siloed. For instance, 35 percent of enterprises have integrated their security and network operations tools to facilitate collaboration across the two groups. Another 16 percent have deployed shared tools across these two groups to enable collaboration.

This collaboration drives cost efficiencies in operational expenses, but it's about more than money. Enterprises told EMA that convergence and collaboration across the two groups reduces overall security risk, improves IT productivity, and makes the IT organization more responsive to business change.

Cross-team collaboration is important in the context of network packet brokers and network visibility fabrics, too. These two groups, whether converged or not, need access to the same traffic. To avoid conflicts over that access, they need to collaborate. **Figure 19** reveals the overall approach enterprises take to visibility fabric collaboration. Overall, 90 percent of network and security teams are collaborating, but only 51 percent have formal processes and best practices. The rest take an ad hoc approach. A very small number use a third-party intermediary to facilitate instrumentation for both groups.

Overall, 90 percent of network and security teams are collaborating, but only 51 percent have formal processes and best practices.

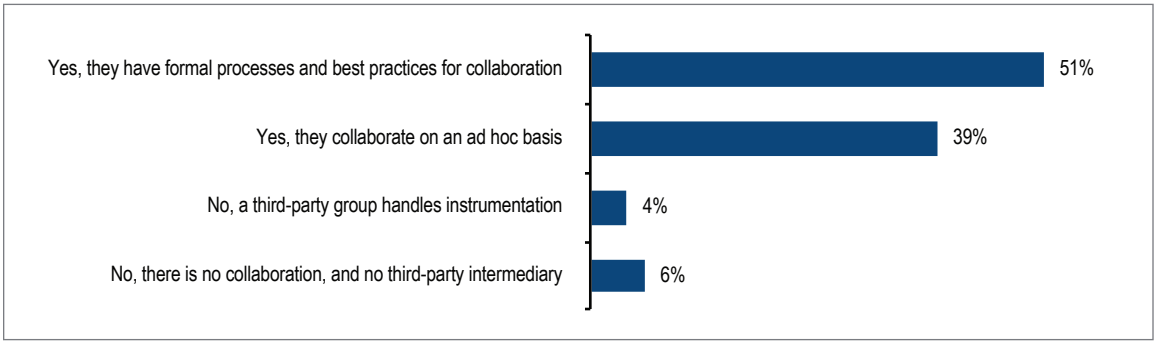

Figure 19. The nature of collaboration between network operations and security operations teams on instrumentation of the network via NPBs and other visibility technology

Security personnel were more likely (66 percent) than other respondents (46 percent) to report formal collaboration between networking and security. EMA surveyed security personnel only if they had direct involvement in some aspect of their organization's use of network packet brokers and visibility fabrics. Formal collaboration probably drives security personnel toward deeper involvement with visibility fabrics, thus leading to a bias toward formal collaboration among security pros in this research.

IT executives (48 percent) were more likely than staff (34 percent) to say these groups collaborate only on an ad hoc basis. Financial companies (63 percent) and manufacturers of non-IT goods (67 percent) reported higher rates of formal collaboration between networking and security. IT manufacturers (67 percent) and retail (58 percent) were more likely to rely on ad hoc collaboration. Government agencies had a very strong preference for a third-party intermediary (30 percent).

[2] EMA, "Network Management Megatrends 2018: Exploring NetSecOps Convergence, Network Automation, and Cloud Networking," April 2018.

©2018 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

EMA recommends that security and network teams establish best practices and processes for collaboration. If these groups don't have controls and processes in place, conflicts over traffic access will arise. In the case of inline security use cases, a lack of collaboration could lead to configuration and provisioning errors that lead to service problems or security breaches.

This collaboration isn't easy. In fact, 92 percent of the respondents in this research claimed to be dealing with east least one significant challenge to successfully balancing the traffic instrumentation needs of the network and security teams. **Figure 20** details those problems.

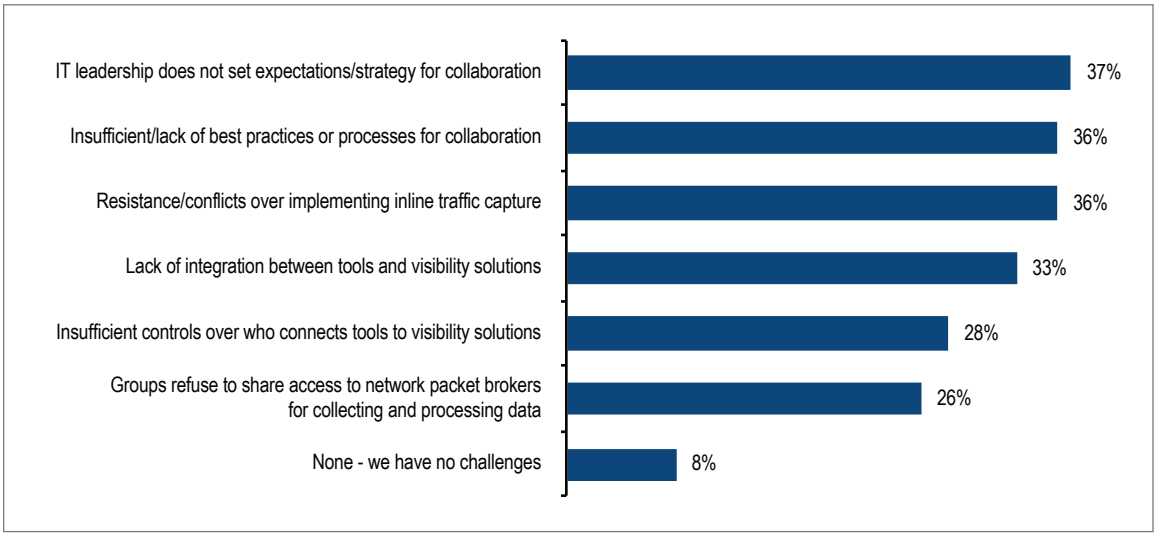

Figure 20. Greatest challenges to balancing the network visibility requirements of the security group and the network operations group

Four challenges are particularly prominent. At the top of the list is poor leadership. The IT executive suite has failed to set expectations or establish a strategy for successful collaboration. Notably, EMA observed no statistical variation on the response between IT executives and IT staff. Both groups agree that this is a problem, and IT leaders are just as hard on themselves as staff are.

The IT executive suite has failed to set expectations or establish a strategy for successful collaboration.

Another significant challenge is the lack of good best practices or processes for this collaboration. Outside consultants are relatively low on the list of trusted external partners for visibility fabrics, but process consultants could be a major help in this particular area. The IT service management group could also support the network and security teams on this topic, given its focus on formal processes and best practices.

Conflicts over inline traffic capture are also a major challenge. The network and security teams have different goals here. The security team wants to lock things down with inline tools. The network team is concerned with keeping traffic flowing through the inline device. The security team needs to balance the network team's concerns about performance and reliability. Bypass solutions will be an important technology to address this conflict area. Also, the two groups will need to come to an agreement about maintenance windows for inline devices. The security team may need to invest in redundant tools for high-availability deployments, for instance. IT executives (44 percent) selected this challenge more often than staff (31 percent), which suggests that they are hearing complaints more often and being asked to mediate or perhaps provide leadership.

©2018 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Finally, a lack of integration between tool vendors and visibility solutions is a significant challenge for many enterprises. Integration of security tools with visibility solutions, for instance, will facilitate cooperation between the network team (frequently the owner of visibility fabrics) and the security team. Most companies prefer to acquire solutions with tight integration between tools and visibility products. Clearly, this is an area that some vendors could improve upon. Organizations with strong growth (37 percent) and moderate growth (35 percent) in their IT budgets are more likely to struggle with insufficient integration, versus just 15 percent of organizations with flat or shrinking budgets. It's unclear to EMA what would drive this disparity. One possibility is that organizations with tighter IT budgets focus on low-cost, all-in-one solutions where tools are hosted on network packet brokers.

Network Packet Brokers in Inline Security

Seventy-eight percent of enterprises have connected security technology to inline network packet brokers. Enterprises that have formal processes for network and security team collaboration are more likely to do this (86 percent).

Seventy-eight percent of enterprises have connected security technology to inline network packet brokers.

EMA will identify the inline security tools most commonly attached to visibility fabrics in the next section, but will first examine the administrative implications of inline tools. Inline security technologies inspect live traffic. When they are plugged into an inline network packet broker, the enterprise has some options when it comes to maintenance. EMA asked respondents to identify their primary approach to applying patches and updates to inline security systems. **Figure 21** reveals that a plurality rely on high-availability architecture. They simply divert traffic to a secondary tool. This requires a larger investment in security tools, with the installation of a secondary appliance. It also requires a security vendor that supports high-availability architecture.

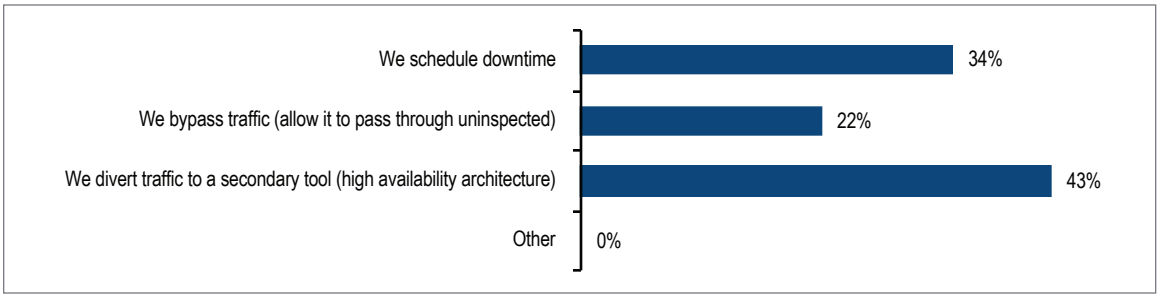

Figure 21. Primary approach to applying patches and updates to inline security tools connected to an NPB

One-third of enterprises schedule downtime for a security appliance update. This approach usually happens overnight or on weekends, and the work must be completed within a specified window. The administrative team will be under pressure to complete the work. This is bad for morale, but more importantly, it's a major disruption. As a consequence, some enterprises often delay patches and updates, which translates into increased security risks.

Finally, a small amount of enterprises simply bypasses traffic, allowing it to pass through without inspection. This might be acceptable to low-risk traffic, such as guest Internet access at a branch office, but most enterprise network traffic is sensitive in some way, and it's always risky to let down one's defenses. Enterprises play with fire by following this approach.

©2018 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Tools Connected to Network Packet Brokers

Figure 22 reveals the tools that are connected to enterprises' network packet brokers presently and what will be added within 12 months. Firewalls are the most popular, connected to packet brokers now by 55 percent of enterprises. Naturally, given the high rate of connection to packet brokers, relatively few have plans to connect firewalls to them by next year.

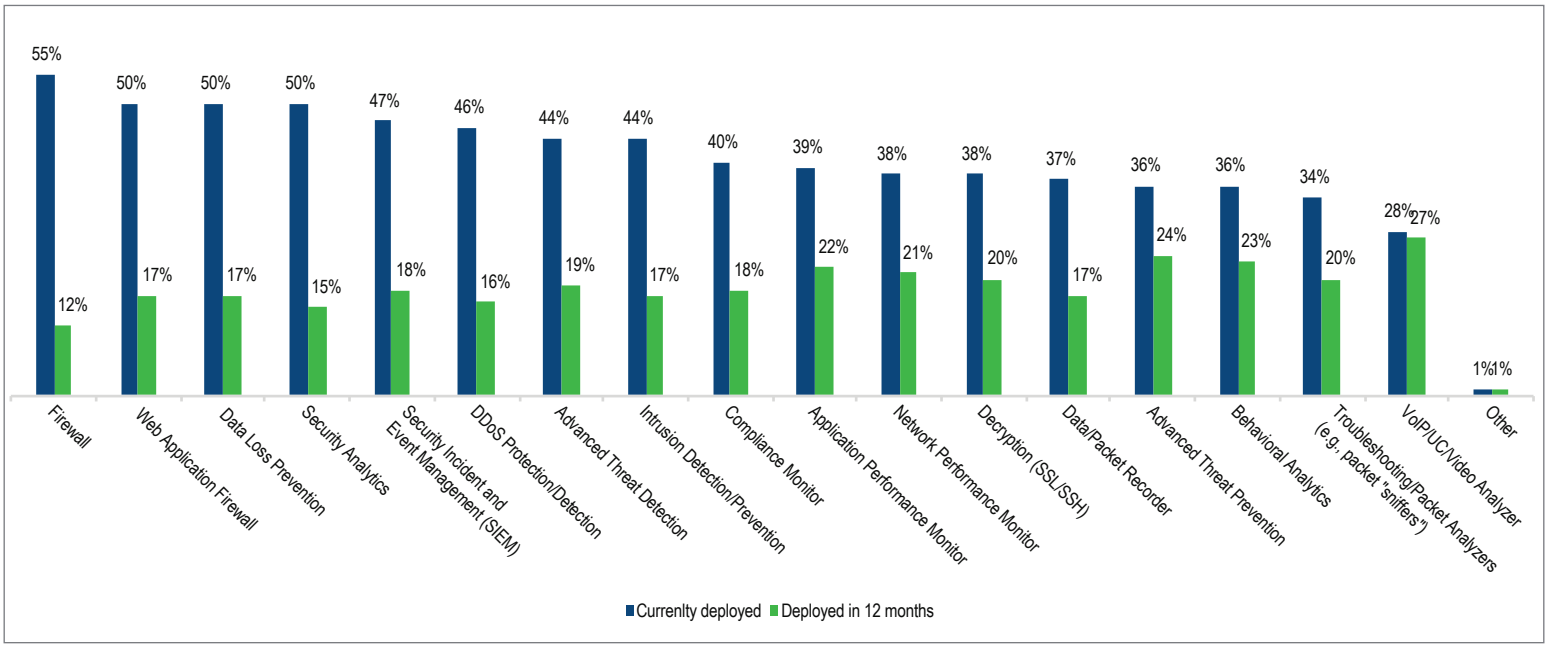

Figure 22. Tools connected to network packet brokers, today and in 12 months

Overall, security technologies (both inline systems like firewalls, web application firewalls, and data loss prevention, and out-of-band systems like security analytics and SIEM systems) are the most ubiquitously connected technologies.

IT operations tools are toward the middle or the bottom of the list. For instance, application performance monitoring tools are connected in only 39 percent of enterprises and network performance monitoring tools are connected in only 38 percent. Basic troubleshooting tools like packet analyzers are rarely connected (34 percent), probably because these tools are often deployed in response to an incident. If a problem is detected, a network engineer will connect a packet sniffer to a specific mirrored port and capture packets. However, organizations with strong IT budget growth (41 percent) are more likely to have such devices connected, suggesting that they have the resources for ongoing packet capture for forensic analysis.

Overall, security technologies (both inline systems and out-of-band systems) are the most ubiquitously connected technologies.

VoIP/UC/video analyzers are also rarely connected, but a relatively large number of enterprises (27 percent) plan to connect these next year, suggesting such tools are becoming more important in the context of visibility fabrics.

Overall, these findings suggest that the network packet brokers are serving a wide array of security technologies and are less often supporting IT operations tools. Security personnel were more likely to report certain security systems connecting to packet brokers, especially firewalls (66 percent), data loss prevention (63 percent), security analytics (66 percent), and DDoS protection/detection (63 percent). However, they also see VoIP/UC/video analyzers more frequently connected (45 percent).

©2018 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Defining the Network Packet Broker of the Future

Network packet brokers are evolving in a number of ways. Vendors are adding and enhancing packet manipulation features to deliver the correct data in the perfect volume and in the right format to each tool. Vendors are also enhancing the architectural and administrative features of these devices and innovating their form factors to support use cases in public and private clouds. Also, some vendors introduced disaggregated network packet broker software that can run on off-the-shelf, open network hardware, which offers some enterprises flexibility and affordability. This chapter explores what enterprises want from their network packet brokers in each of these areas.

Critical Packet Manipulation Features for Network Operations Monitoring

One thing that sets network packet brokers apart from standard aggregation devices is the set of advanced packet manipulation features the packet broker offers. These packet manipulation features are often essential for the proper functioning of network operations tools, out-of-band security tools, and inline security systems.

Figure 24 highlights the criticality of more than a score of common packet manipulation and other advanced features to network operations monitoring tools. Decryption tops the list, which reflects the ongoing challenge that network managers have with the rise of encrypted traffic on enterprise networks. Many network monitoring and performance management tools need visibility into packets. With SSL encryption on the rise in enterprise networks, a decryption feature on network packet brokers is essential.

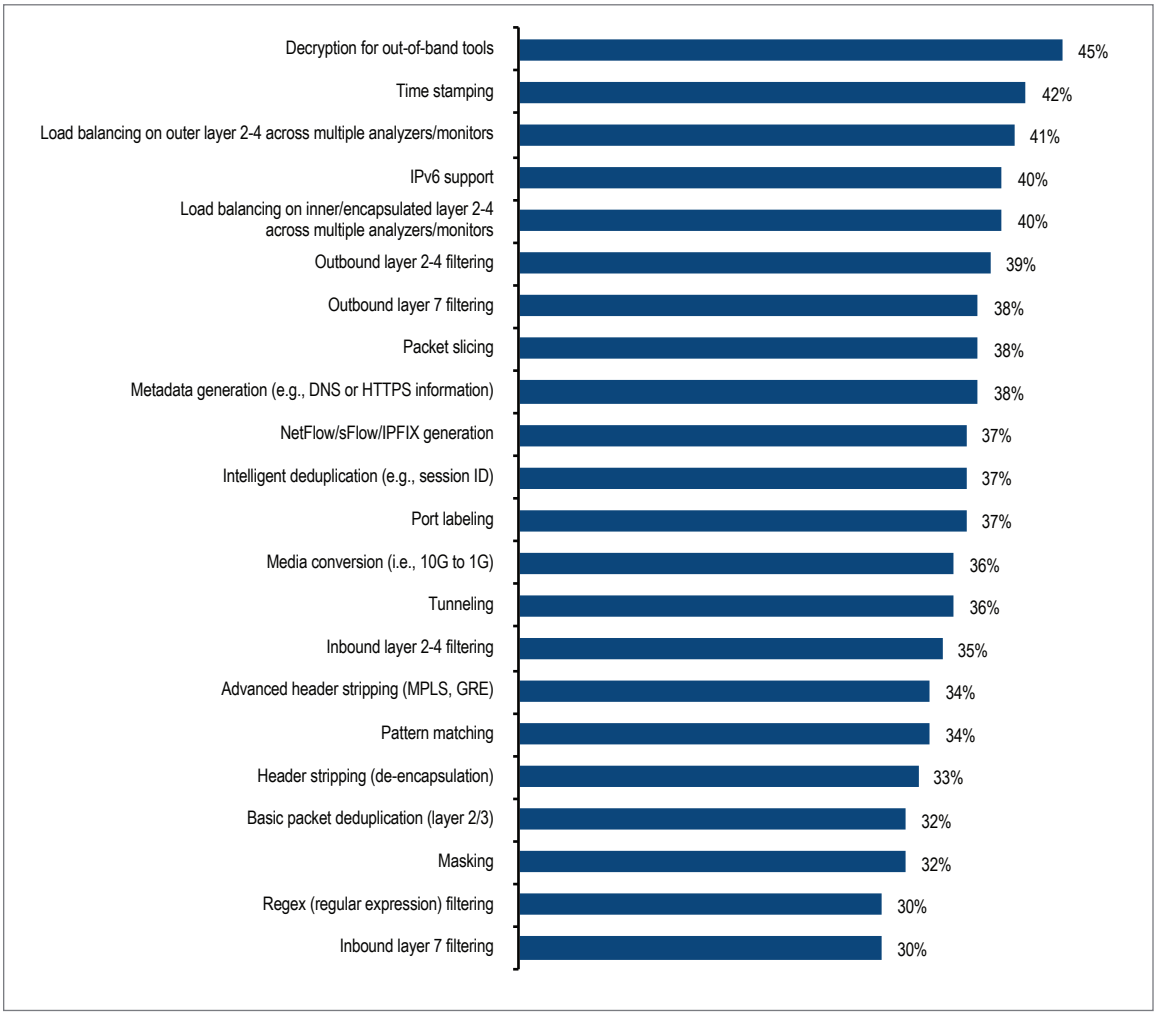

Figure 24. Critical NPB packet manipulation features for network operations monitoring

©2018 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Time stamping, Layer 2-4 load balancing based on non-encapsulated (outer) packets, IPv6 support, and Layer 2-4 load balancing based on encapsulated (inner) packets round out the top five most critical features for network operations monitoring. The popularity of the two load balancing capabilities indicates a focus on distributed traffic data across multiple instances of a tools. This is unsurprising given the number of enterprises who had 40 Gbps or higher links in their networks at the time of this research.

Outbound filtering, both Layer 2-4 and Layer 7, are also relatively critical features for network monitoring. These filtering capabilities can reduce the number of packets that go to a tool. For instance, Layer 4 filtering can filter out packets by port number and Layer 7 filtering can filter by application type.

Critical Packet Manipulation Features for Out-of-Band Security Monitoring

Figure 25 lists the criticality of network packet broker features for out-of-band security monitoring use cases. Here, decryption takes a backseat to more than a dozen other features. Intelligent deduplication (e.g., by session ID) and metadata generation (e.g., insertion of DNS or HTTPS information) sit at the top of the list. Intelligent deduplication allows security tools to reduce data volumes while zooming in on specific network conversations and other areas of interest in traffic data. Metadata generation will tag traffic with information that adds context to security analysis, making security tools more effective.

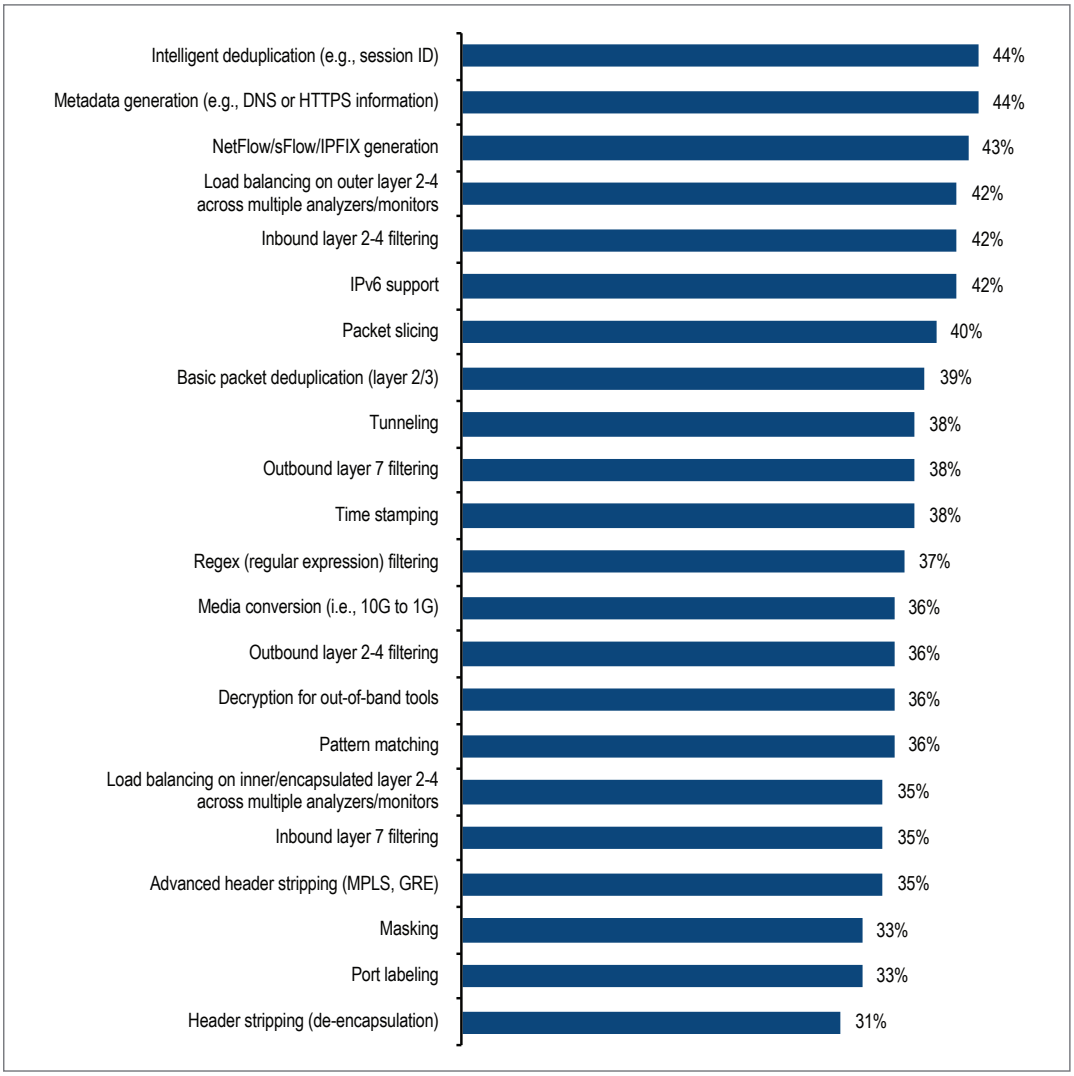

Figure 25. Critical NPB packet manipulation features for out-of-band security monitoring and analysis

©2018 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

NetFlow/sFlow/IPFIX generation are also high on the list of critical features. Flow monitoring and analysis tools have become increasingly important to both network performance management and security monitoring, but not all network devices have the ability to generate flow records. In some cases, they don't support the technology, and in other cases, generation of flows as a certain level of granularity impacts the performance of a network device. Increasingly, network packet broker vendors added the ability to create flow records based on a summary of the network sessions that pass through the device, thus closing the visibility gap that some enterprises are dealing with.

Load balancing on Layer 2-4, non-encapsulated packets, and inbound Layer 2-4 filtering round out the top five most critical features of out-of-band security monitoring. Actually, they are in a three-way tie for fourth place with IPv6 support. Layer 2-4 load balancing based on encapsulated data is relatively less important here than it was for network operations monitoring.

Critical Packet Manipulation Features for Inline Security Monitoring and Controls

Critical network packet broker features for inline security use cases are quite different from those of out-of-band security. **Figure 26** shows that load balancing is less important than it is to out-of-band features, which indicates that enterprises are connecting extremely powerful appliances to inline network packet brokers. Instead, IPv6 is more important here, which suggests a focus on inline security in an enterprise DMZ or network ingress/egress points. Decryption also leaps to the top, whereas it was relatively unimportant to out-of-band security. Inline security appliances place a premium on performance and efficiency, so offloading decryption to the network packet broker is valuable.

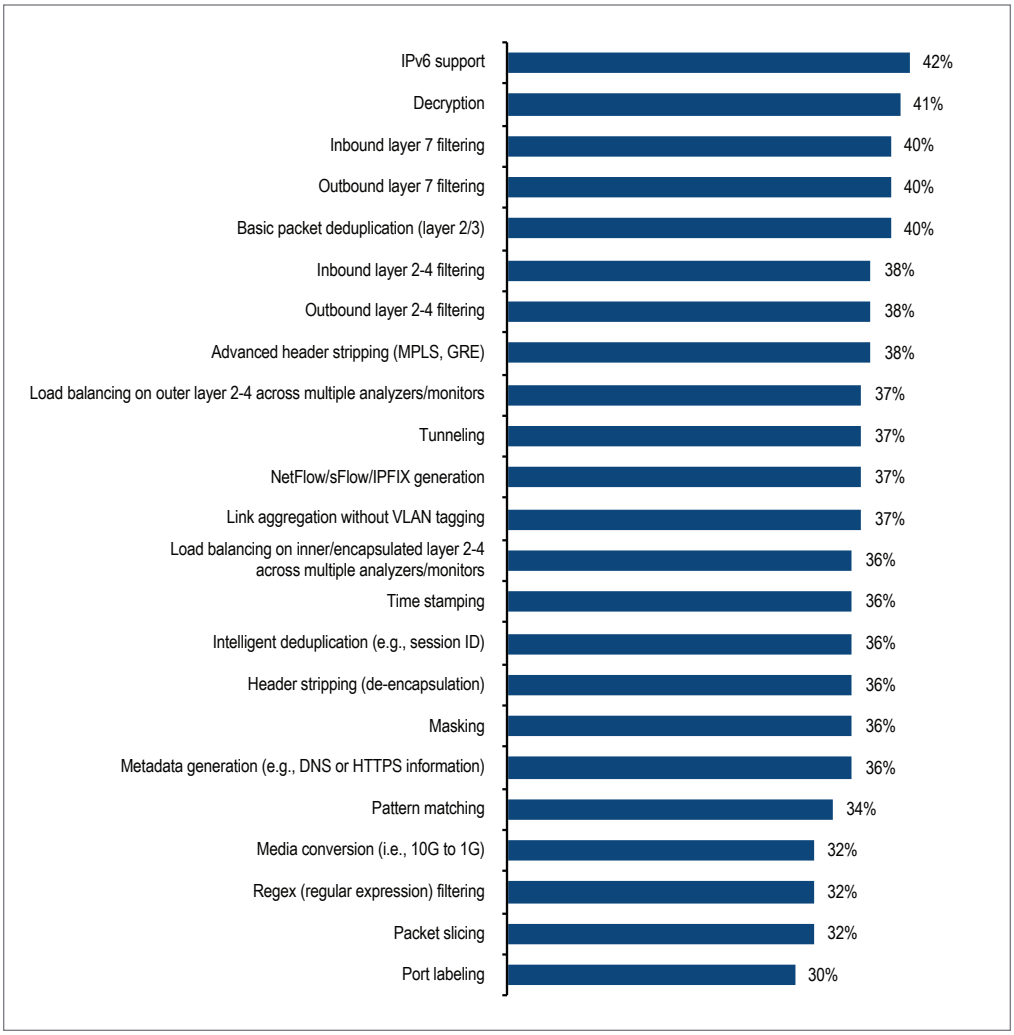

Figure 26. Critical NPB packet manipulation features for inline security monitoring and controls

©2018 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Inbound and outbound Layer 7 filtering are also very important, which suggests an extreme focus on filtering traffic by application for inspection by inline devices. Finally, basic packet deduplication rounds out the top five most critical features. Inbound and outbound Layer 2-4 filtering and advanced header stripping (removing MPLS labels, for instance), are also quite critical. Organizations with moderate IT budget growth were more likely (35 percent) to select port labeling, versus 15 percent of companies with flat or shrinking budgets.

Critical Network Packet Broker Architectural Features

Enterprises have very specific architectural requirements of the network packet brokers they deploy in their environments. **Figure 28** reveals which architectural features are most critical in network packet brokers. High availability and fault tolerance top the list by a slim margin. Whether it's a chassis with redundant systems or dual fixed appliances in a high-availability configuration, enterprises demand packet brokers that will stay up and running at all times. This feature was also the most important feature in the 2013 research on this subject.

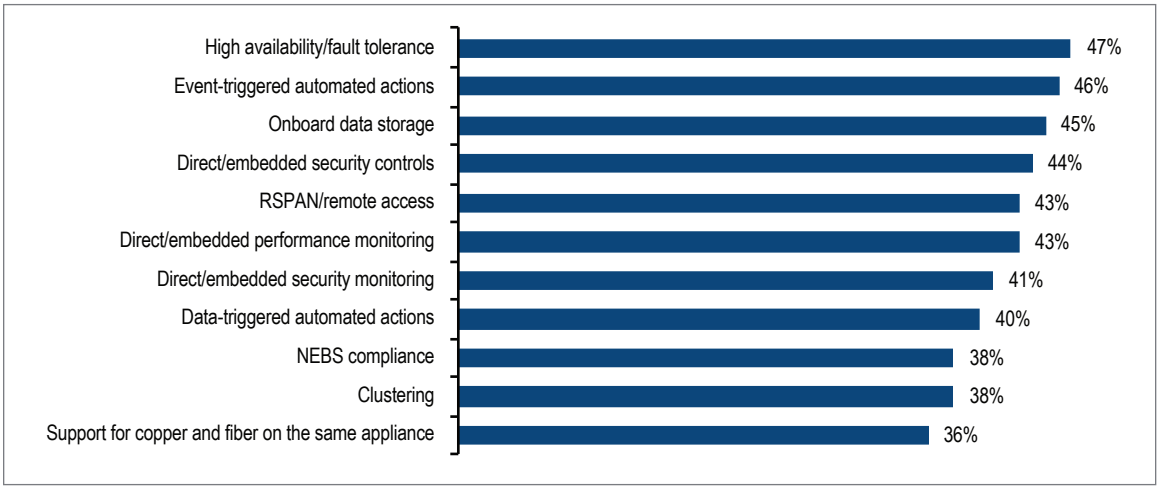

Figure 28. Critical NPB architectural features

The number-two feature is the ability to take automated actions triggered by events. An example of this would be forwarding traffic to a data recorder after it or a third-party security solution detects a security incident or performance problem. This assures that engineers have relevant data for forensic analysis. This feature was also the second most important feature in the 2013 research.

Onboard data storage, direct/embedded security controls, and RSPAN/remote access round out the top five features. Onboard storage removes the need for a separate data recording device, which reduces costs and simplifies architecture. Likewise, embedded security controls allow an enterprise to consolidate some security functions onto an inline packet broker. RSPAN (remote SPAN)/remote access involves support for configuring and collecting mirrored traffic from multiple SPAN ports.

NEBS compliance, clustering, and copper and fiber support on the same appliance are the least important features, although still strongly favored by more than one-third of enterprises.

Security personnel have priorities that are very different from the rest of the IT organization. More than half of them identified the following as critical:

- **Event-triggered automated actions**: 58 percent
- **Direct/embedded security monitoring:** 56 percent
- **RSPAN/remote access:** 55 percent
- **NEBS compliance:** 53 percent

©2018 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Certain industries have distinct architectural preferences, too. Retail firms are more likely to value direct or embedded security monitoring (52 percent), high availability/fault tolerance (65 percent), and NEBS compliance (52 percent). IT-related professional services firms have a strong need for onboard data storage (65 percent), high availability/fault tolerance (65 percent), and data-triggered automated actions (65 percent). Cloud/application service providers require data-triggered automated actions (59 percent) and high availability/fault tolerance (56 percent).

Disaggregated and White Box Network Packet Brokers

Much like the switches and routers from which they collect traffic, network packet brokers have traditionally been vertically integrated systems. Vendors deliver these systems through an inextricable combination of software and hardware innovation. However, the networking industry is evolving, and the network packet broker industry is, too.

A growing number of network switch vendors are offering disaggregated solutions, such as network operating systems that can run on off-the-shelf hardware, either "white box" hardware from original design manufacturers (ODMs) or "britebox" hardware from mainstream network hardware manufacturers. In parallel, many vendors have started offering disaggregated network packet brokers, too. Typically, these solutions are software-based, capable of running on the same switch hardware that network operating systems vendors support.

In an industry where vertically-integrated solutions have always been the norm, there are challenges and benefits to such an approach to network visibility solutions. For instance, commodity hardware typically can't support the advanced packet processing features offered by vertically-integrated network packet brokers. Adopters of these solutions need to find a workaround. Also, network engineers will now find themselves functioning as system integrators of hardware and software, which could open up some skill gaps.

Enterprises have strong interest in disaggregated network packet brokers, with 94 percent acknowledging some level of activity with the technology.

Figure 30 shows that enterprises have strong interest in disaggregated network packet brokers, with 94 percent acknowledging some level of activity with the technology. While only 29 percent have deployed such systems, many more have plans to do so within the next three years. A small number (ten percent) have no specific plans, but they are researching and evaluating the technology.

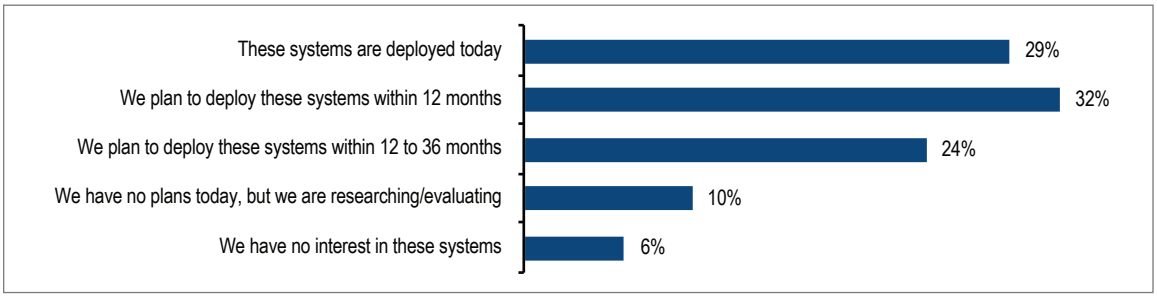

Figure 30. Use of network packet broker software deployed on commodity, off-the-shelf hardware

Conventional wisdom says that disaggregated network packet brokers are more affordable than specialized appliances. However, IT organizations with money to spend tend to be more aggressive with these solutions. For instance, enterprises with strong IT budget growth are more likely to have these systems deployed currently (38 percent), versus just 21 percent of enterprises with flat or shrinking budgets. Strong budget growth actually drives an expansion of network visibility requirements, since enterprises with fat wallets are usually deploying new applications and new infrastructure that need to be monitored and secured. Disaggregated packet brokers offer them a way to scale their visibility fabrics economically, although price is not a major driver of investment in disaggregation.

©2018 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Figure 31 reveals why enterprises are adopting these disaggregated systems. Reduced operational expenses and reduced capital expenses are at the bottom of the list. They are not focused on saving money and resources. Instead, flexibility of software options is at the top of their priorities, along with flexible hardware options. Large enterprises (53 percent) are particularly interested in flexible software options. Enterprises with strong IT budget growth (46 percent) are much more likely to see hardware flexibility as a driver, versus just 24 percent of enterprises with flat or shrinking budgets. Thus, as their visibility fabric requirements expand, they need hardware flexibility.

Figure 31. Primary drivers for using disaggregated network packet broker systems

Hardware and software flexibility can play out in a number of ways. In some circumstances, enterprises can switch network packet brokers' software vendors without changing hardware. They can simply install a new software package on existing installed hardware. On the other hand, when expanding the visibility fabric, an enterprise can choose from multiple hardware providers, but continue using their existing software vendor across the fabric.

The third most popular driver is reduced complexity. Security personnel are especially interested in this driver (48 percent) versus just 29 percent of the IT organization.

These disaggregated systems run on commodity hardware. They lack the specialized silicon required to support advanced flow processing features like header stripping, packet slicing, packet deduplication, and Layer 7 filtering. Thus, many enterprises will need to find a workaround. **Figure 32** reveals that there is no consensus on a preferred approach yet. There is consensus on one thing. Only five percent say they have no use for advanced flow processing. Thus, 95 percent need a solution.

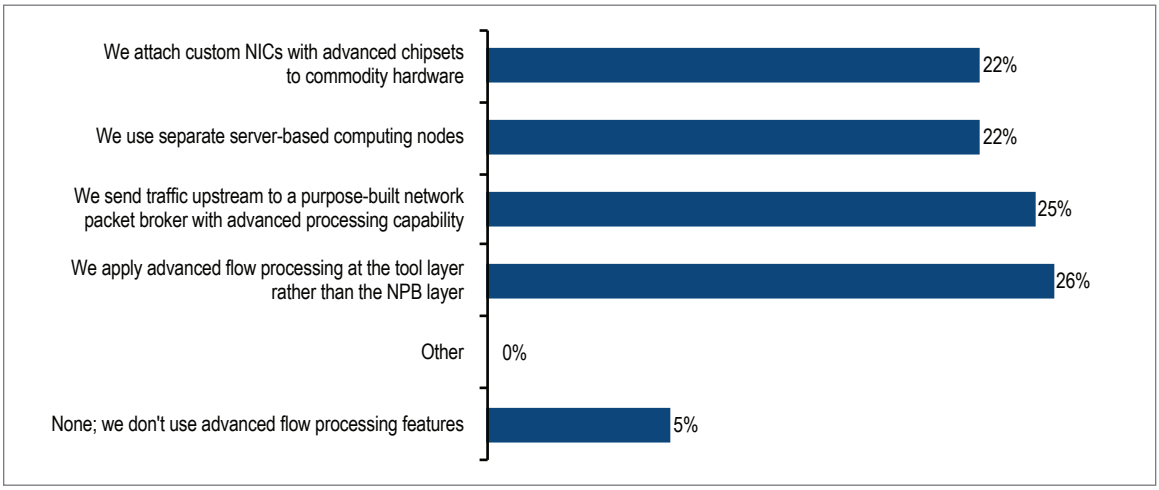

Figure 32. Preferences for implementing advanced flow processing capabilities with disaggregated network packet brokers

©2018 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Just over a quarter apply or plan to apply advanced flow processing at the tool layer rather than the packet broker. This will place a heavy burden on tools, particularly inline security tools that will find their overall throughput diminish. Education (50 percent), healthcare (54 percent), and manufacturers of non-IT products (53 percent) tend to prefer this approach.

Another quarter of enterprise send traffic upstream to a vertically-integrated network packet broker for advanced processing. This suggests that many enterprises will deploy a mix of specialized appliances and disaggregated solutions. Such an approach could add complexity to the network visibility fabric, unless the packet broker vendor has an end-to-end architecture for such solutions. Government agencies (67 percent) and non-IT professional services firms (50 percent) are more likely to follow this path.

A smaller number of enterprises prefer to use separate server-based computing nodes, another potential source of complexity. Given the low cost of servers lately, a good end-to-end software solution could scale quite well with this approach. Software companies (32 percent) and retail firms (33 percent) are more likely to pursue this. Finally, another small cohort attach custom network interface cards (NICs) with advanced chipsets to their commodity hardware. This approach will particularly appeal to inline use cases.

Finally, EMA asked enterprises to identify the biggest barriers to their adoption of disaggregated network packet brokers. Overall, only 19 percent said they see no business case or technical reason for deploying the technology. This means that 81 percent see value in the solutions, if they can overcome the barriers.
A fortunate few (ten percent) said they saw no barriers to adoption, so they are good to go.

The biggest problem, as revealed in **Figure 33,** is an internal skills gap. Disaggregation forces the IT organization to be internal system integrators. They must pair hardware and software, then implement and maintain a fabric with these systems. Many enterprises already lack the necessary skills to support a traditionally-built network visibility fabric. Disaggregated systems will stretch their skilled engineers even further and force them to acquire some new skills. Adopters of disaggregated systems will probably lean heavily on the professional services and customer support organizations of their vendors, at least at the beginning.

Adopters of disaggregated systems will probably lean heavily on the professional services and customer support organizations of their vendors, at least at the beginning.

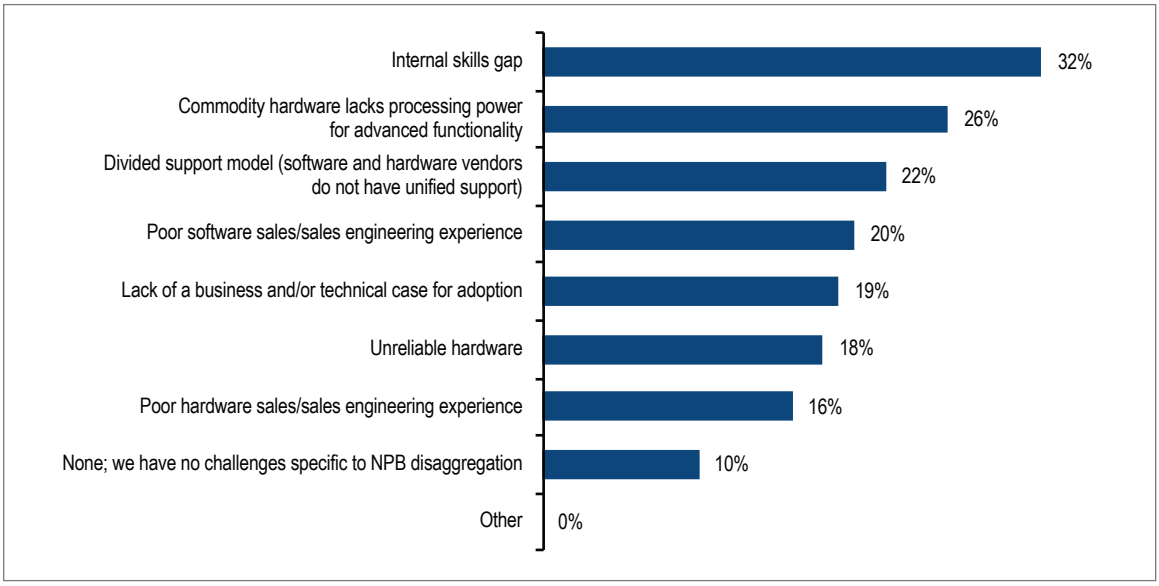

Figure 33. Biggest barriers to adopting disaggregated network packet brokers

©2018 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

The second most common barrier is a lack of processing power in commodity hardware for advanced functionality. Vendor selection will drive this to some degree, since disaggregated vendors take different approaches to the advanced flow processing requirements of customers. For now, it's clear that there is some uncertainty on the best course of action.

The next-most common barrier is a divided support model. There is no so-called "one throat to choke" with disaggregation. The hardware and software vendors usually have separate customer support organizations. However, they sometimes partner to provide some integration. For instance, many software vendors will serve as the first line of support, with warm handoffs to a hardware vendor when applicable.

The fourth-most common barrier is a poor software sales and sales engineering experience. EMA suspects this is a maturity issue. This is a young market, with startups still building out their go-to market capabilities and incumbent vendors shifting from an appliance-centric business model to a software-centric one. Many vendors will improve their performance in this area over time, especially if they are committed to disaggregation as a core strategy.

Extending Visibility Fabrics to the Public Cloud

Thirty-seven percent of enterprises are collecting traffic data in their public cloud environments, as **Figure 37** shows. IT executives (46 percent) were more likely to report having a solution in place already, versus just 32 percent of staff. This discrepancy is possibly attributable to the fact that IT executives have broader awareness of cloud deployments than engineering and operational staff. Many public cloud deployments are led by application developers or line of business organizations. They may be instrumenting traffic monitoring without involving the traditional owners of the internal visibility fabric.

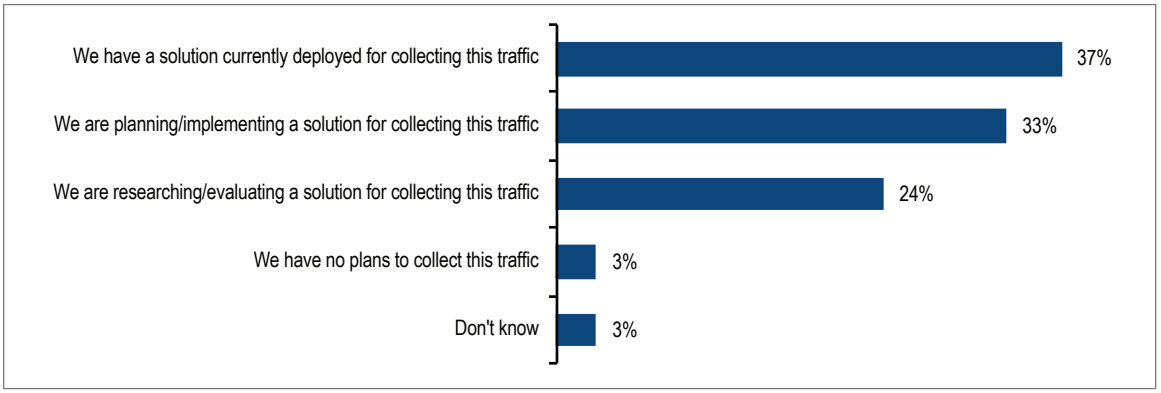

Figure 37. The state of collecting traffic data within public cloud environments for analysis by IT operations and security tools

Another 33 percent are planning to implement or are in the process of implementing a solution for traffic collection, and 24 percent are researching and evaluating the possibility. Government agencies are the least likely (ten percent) to have a solution currently deployed, but very likely (50 percent) to be researching and evaluating solutions. Transportation companies (71 percent) are very likely to have a solution deployed. Application/cloud service providers (41 percent), IT manufacturers (42 percent), and non-IT manufacturers (48 percent) are all more likely to be planning or implementing a solution.

Network infrastructure and security-related problems (e.g., breaches) are the most common root causes of complex service issues and outages.

©2018 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

The market for traffic monitoring in public cloud services is still immature. Public cloud providers offer some limited traffic monitoring services. Network visibility fabric vendors have started offering native solutions over the last couple of years. As a result, there is no consensus approach to public cloud traffic monitoring. **Figure 38** reveals that enterprises are almost evenly split across three approaches. About one-third are each using native traffic capture solutions offered by providers, third-party tap, or packet broker software implemented via a cloud provider's market place, or third-party tap or packet broker software installed directly in a cloud workload.

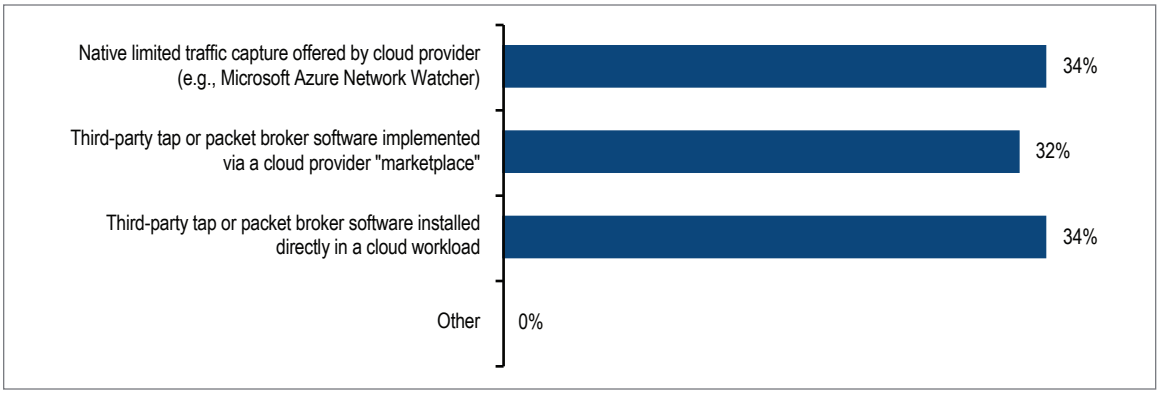

Figure 38. Primary technique used or planned for use in capturing traffic between IaaS workloads for analysis by IT operations and security tools

Finally, EMA asked research participants to reveal the types of traffic data they capture from public cloud environments. **Figure 39** shows that majorities collect all three classes of data. Packet metadata, packet header information, and full packets are all nearly identical in popularity. The question that remains is which use cases they are pursuing with all of this data. EMA suspects that full packets are collected somewhat rarely in the public cloud, only triggered during an event that requires a forensic investigation.

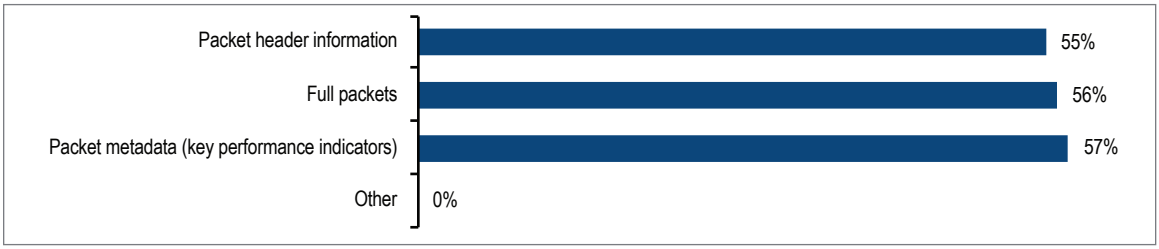

Figure 39. Types of traffic data collected in the public cloud

Financial companies are more likely (73 percent) to capture header information. Enterprises that have had a network visibility fabric deployed for more than one year (61 percent) are also more likely to collect header information. Manufacturers of non-IT products (74 percent), application/cloud service providers (65 percent) and retail firms (64 percent) are most likely to monitor full packets. Retail firms are also more likely to capture packet metadata (75 percent).

©2018 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Impacts and Challenges of a Network Packet Brokers and Visibility Fabrics

Network Visibility Fabric Challenges

Generally, enterprises encounter four primary challenges to their successful use of network packet brokers and visibility fabrics, as **Figure 40** details. Architectural complexity tops the list, followed by a lack of personnel with visibility fabric skills. Complexity could come from the network itself, which can be too complex or too poorly understood to properly instrument, or it could trace to the visibility solution itself, which is too complex to work with. The lack of skilled personnel is unsurprising, since EMA identified network skills gaps as the number one challenge enterprises face in overall network operations. IT executives (41 percent) are more likely to see the skills gap as a challenge, versus just 27 percent of staff. Certain industries are also more likely to struggle with skills gaps, including manufacturers of non-IT goods (62 percent) and IT hardware manufacturers (58 percent).

Generally, enterprises encounter two primary challenges to their successful use of network packet brokers and visibility fabrics. Architectural complexity tops the list, followed by a lack of personnel with visibility fabric skills.

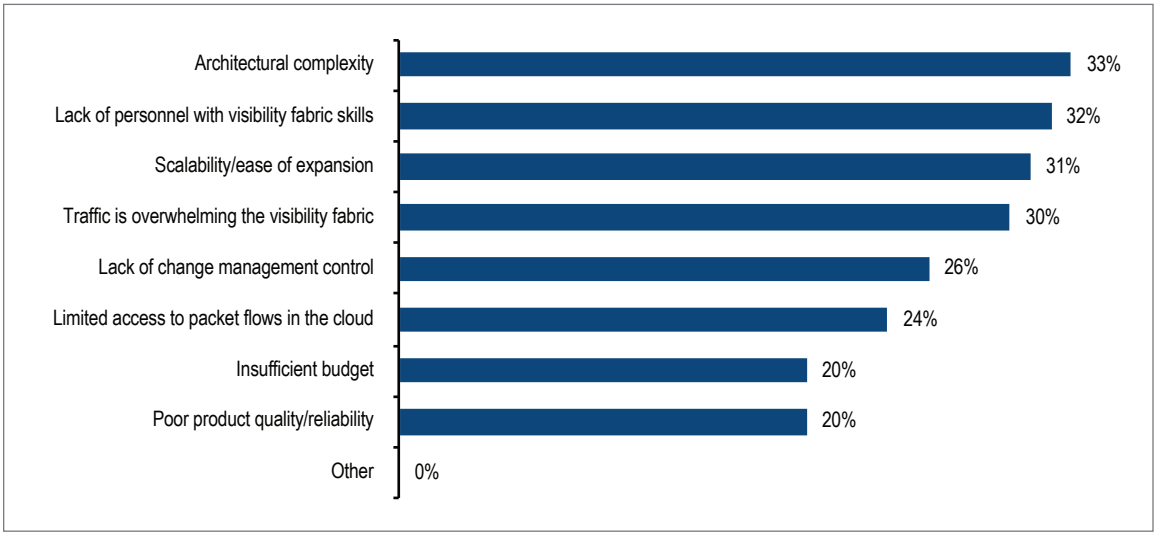

Figure 40. The most difficult challenges organizations face with overall use of network visibility fabrics and NPBs

Problems with scalability or ease of expansion is the third top challenge with visibility fabrics. This challenge can involve struggles with accommodating growth in traffic flows, from 10Gbps to 100Gbps, or it can involve the difficulty in adding more network segments to a visibility fabric.

Finally, heavy traffic overwhelming the visibility fabric rounds out the top four problems. Rather than upgrades to networks, this involves a growth in traffic, which leads to oversubscription on the existing visibility fabric.

A lack of change management control and limited access to packet flows in the public cloud are both mid-level problems, only a major issue for about a quarter of enterprises. However, organizations with strong IT budget growth (33 percent) struggle with this more often. This latter statistic is attributable to the fact that robust budgets will lead to more aggressive investment in digital initiatives like cloud migration.

Finally, budget problems and poor product quality are the least common challenges. IT professional services organizations (41 percent) are more likely to struggle with the product quality issue.

©2018 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Benefits of a Network Visibility Fabric

Obviously, an enterprise deploys network packet brokers and a visibility fabric to provide analysis tools with access to traffic. That is top of mind for any IT organization that invests in such technology, but EMA believes that is just a technical goal for investment. The benefits of such an implementation can be broader and more multi-dimensional, as **Figure 41** details.

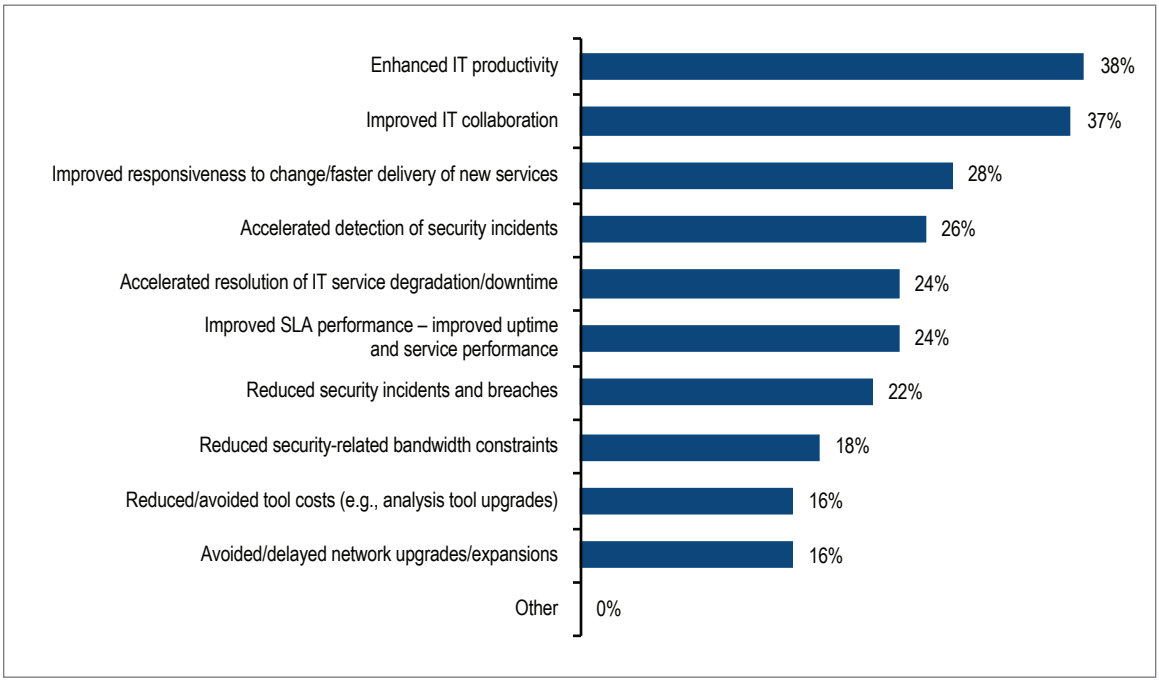

Figure 41. Most valuable benefits from using NPBs and network visibility fabrics

Two benefits stand out from the rest. First, enterprises reported enhanced IT productivity. Visibility fabrics can streamline the workflows involved in collecting data for analysis during a troubleshooting process or security incident response. Many visibility fabrics have frontline analysis capabilities, too. These provide dashboard views of events that, for instance, give network operators and security personnel the context they need to identify which tool they should use for an investigation.

The second most valuable benefit of a visibility fabric is improved IT collaboration. These fabrics give IT operations and security personnel access to the right data at the right time, allowing them to get more value out of their tools and empowering them to bring valuable insight to multidisciplinary teams, whether for capacity planning or incident response. Visibility fabrics also make it easier for multiple teams to share access to traffic data, which reduces conflicts and encourages better collaboration. Notably, organizations whose network and security groups have formal processes for collaborating on the instrumentation of the network with a visibility fabric were more likely to say improved IT collaboration is a benefit (43 percent), versus those who don't have formal processes for collaboration (30 percent).

Enterprises identified five secondary benefits of visibility fabrics. First, these solutions improve a team's responsiveness to change or the speed with which they can deliver a new service. With a fabric in place, it becomes easier for the infrastructure and security teams to instrument new or evolving services with monitoring and security tools.

These solutions improve a team's responsiveness to change or the speed with which they can deliver a new service.

©2018 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

The next two secondary benefits are accelerated detection of security incidents and accelerated resolutions of IT service degradation and downtime. These are examples of how IT and security teams are simply more effective detecting and resolving problems. The last two secondary benefits are improved SLA performance and reduced security incidents and breaches. In other words, not only are the operations and security teams better able to fix problems; they're also good at preventing problems before the business is negatively impacted.

The least important benefits of a visibility fabric are reduced security-related bandwidth constraints, reduced/avoided tool costs, and avoided/delayed network upgrades or expansions. Security-related bandwidth constraints are reducible through the use of inline fabric capabilities, such as bypass switches and inline network packet brokers. These solutions can filter and load balance traffic so that the packet processing power and throughput of inline security tools don't become a bottleneck.

EMA Perspective

Enterprises do not spare budget when it comes to network visibility fabrics and network packet brokers. Performance management and security are critical priorities in the digital economy, and traffic data is an essential data source. Enterprises are moving away from low-cost options like SPAN-based traffic mirroring in favor of taps. They are also making heavy use of advanced traffic manipulation features that are only found in premium network packet brokers.

They are also investing in new visibility solutions like public cloud, virtual fabric technologies, and disaggregated packet brokers. All of this is aimed at providing data to a growing set of inline and out-of-band analysis tools. The need for packet data will only increase. The growth in overall network speeds and feeds suggests that growth in network visibility fabric investments will continue to grow, too.

There are many pitfalls along the way. Networks and the visibility fabrics that tap into them are becoming more complex. IT organizations are also dealing with a shortage of the skilled personnel required to keep up with visibility requirements. Fortunately, this research shows that enterprises have identified trusted external partners for the implementation of fabrics. Also, collaboration on visibility fabrics across silos in the IT organization appears to be broadening. With strong support from internal and external partners, and with the right best practices and processes, enterprises are poised for success with network visibility fabrics and network packet brokers.

©2018 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blog.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. "EMA" and "Enterprise Management Associates" are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2018 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3761-Niagara_SUMMARY.091218