Enterprise Strategy Group | Getting to the bigger truth.™

White Paper

The Modern Network Monitoring Mandate

By Bob Laliberte, Senior Analyst

April 2014

This ESG White Paper was commissioned by Emulex and is distributed under license from ESG.

Contents

Executive Summary

Enterprise networks are becoming larger and more complex, driven by data center consolidation, the need to virtualize the compute layer, new application architectures, and the shift to 10GbE or higher network infrastructure. As a result of this transformation, it is imperative that organizations have higher levels of visibility and more granular network information in order to manage the network effectively. By embracing network visibility (the ability to collect, store, search, and present network data), enterprises are better equipped to ensure network and application performance, security, and compliance, as well as reduce the time needed to find and fix critical problems.

To better understand the needs of the network to support these highly virtualized and dynamic environments, on the behalf of Emulex, ESG surveyed 150 IT professionals currently responsible for evaluating, purchasing, and managing network infrastructure technologies for their organizations. All respondents were currently using some form of network-based monitoring or management tools and were employed at enterprise organizations (defined as organizations with 1,000 employees or more) across multiple industries (including financial, business services, manufacturing, and retail) in North America.[1]

Modern Networks Increase Complexity and Risk

Most organizations are transforming their IT environments in order to be more responsive to the needs of the business. The ability to rapidly provision new or upgraded applications or deliver IT services in minutes instead of months is becoming the standard. As a result, organizations have implemented a number of initiatives that will help them reach their end goal of a more agile environment. Unfortunately, while some of these initiatives are driving efficiencies in one domain, they are creating more complexity and rapid growth for the network. These initiatives include:

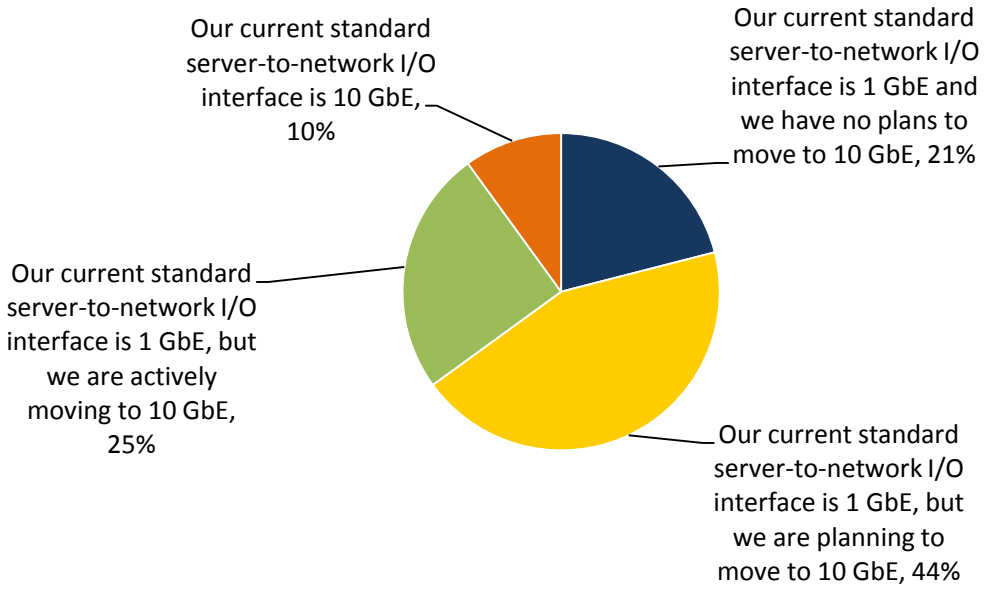
- **Data center consolidation**. ESG research has shown this to be a top ten most-cited priority for surveyed organizations over the last five years.[2] Organizations have been actively consolidating data centers to centralize applications, processes, and infrastructure in an effort to reduce costs and drive higher levels of efficiency. As a result, enterprises have fewer, but much larger and more complex data center environments. This means the network environment has to cope with rapid scale and higher levels of complexity. Also, this consolidation of many of the regional data centers into centralized sites requires remote and branch offices to be dependent on WAN links to deliver applications and services.
- **Server virtualization/the use of private cloud**. As organizations continued to increase their use of server virtualization technology and take advantage of its dynamic capabilities, networked storage environments were required. Thus, previously standalone servers are now being connected to networked storage. Although many of these network connections are in the data center today, some organizations are bursting to public clouds or between multiple corporately owned data centers.
- **Installing modern applications**. Many modern applications are built on multiple tiers and with a modular architecture. They are also becoming applications of engagement instead of applications of record, so performance is critical. While the modular approach accelerates development time, it also means a far greater reliance on the network to handle a large amount of server-to-server or east-west traffic. Also, unified communications applications are driving more video traffic across the network and even to mobile devices.
- **Upgrading to 10GbE networks**. In large part due to the initiatives outlined and a general anticipation of more traffic, a significant number of organizations have either transitioned or have begun the transition to 10GbE interfaces. Ten percent of the respondents to the ESG research survey reported they have already

[1] All ESG research references and charts in this white paper have been taken from this research survey, unless otherwise noted.
[2] Source: ESG Research Report, *2014 IT Spending Intentions Survey*, February 2014.

transitioned to 10 GbE, with another 69% either actively moving to it or planning to do so (see Figure 1). In many large organizations, the core network may already be moving to 40 GbE.

Figure 1. Upgrading to 10GbE Environment

Which of the following best represents your organization's server-to-network I/O interface standards? (Percent of respondents, N=150)



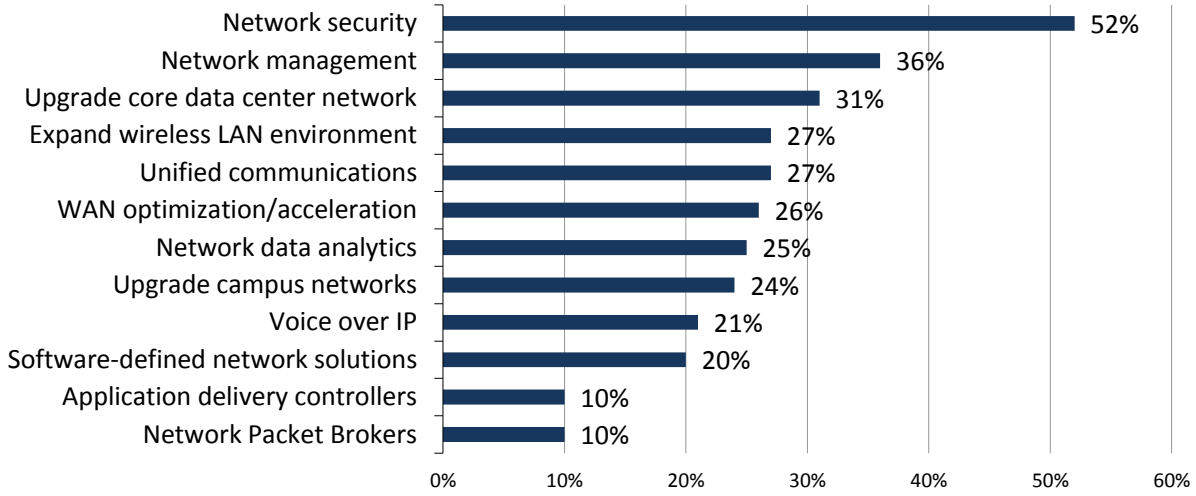
Source: Enterprise Strategy Group, 2014.

These initiatives have made it much harder for operations teams to effectively monitor, manage, and secure the network environment. Fortunately, most organizations recognize the need to accomplish these tasks and are allocating their budgets accordingly. ESG research in Figure 2 highlights specific spending plans for network infrastructure reported by respondents.[3] Clearly, network security is a top concern for these organizations, followed by network management and upgrades of data center, campus, and wireless networks. However, while allocating budget is a decent start, it doesn't always guarantee success.

[3] Source: ESG Research Report, *2014 IT Spending Intentions Survey*, February 2014.

Figure 2. Network Investments for 2014

We would like to learn a bit more about your specific spending plans for network infrastructure in 2014. In which of the following areas will your organization make the most significant investments over the next 12 months? (Percent of respondents, N=301, five responses accepted)

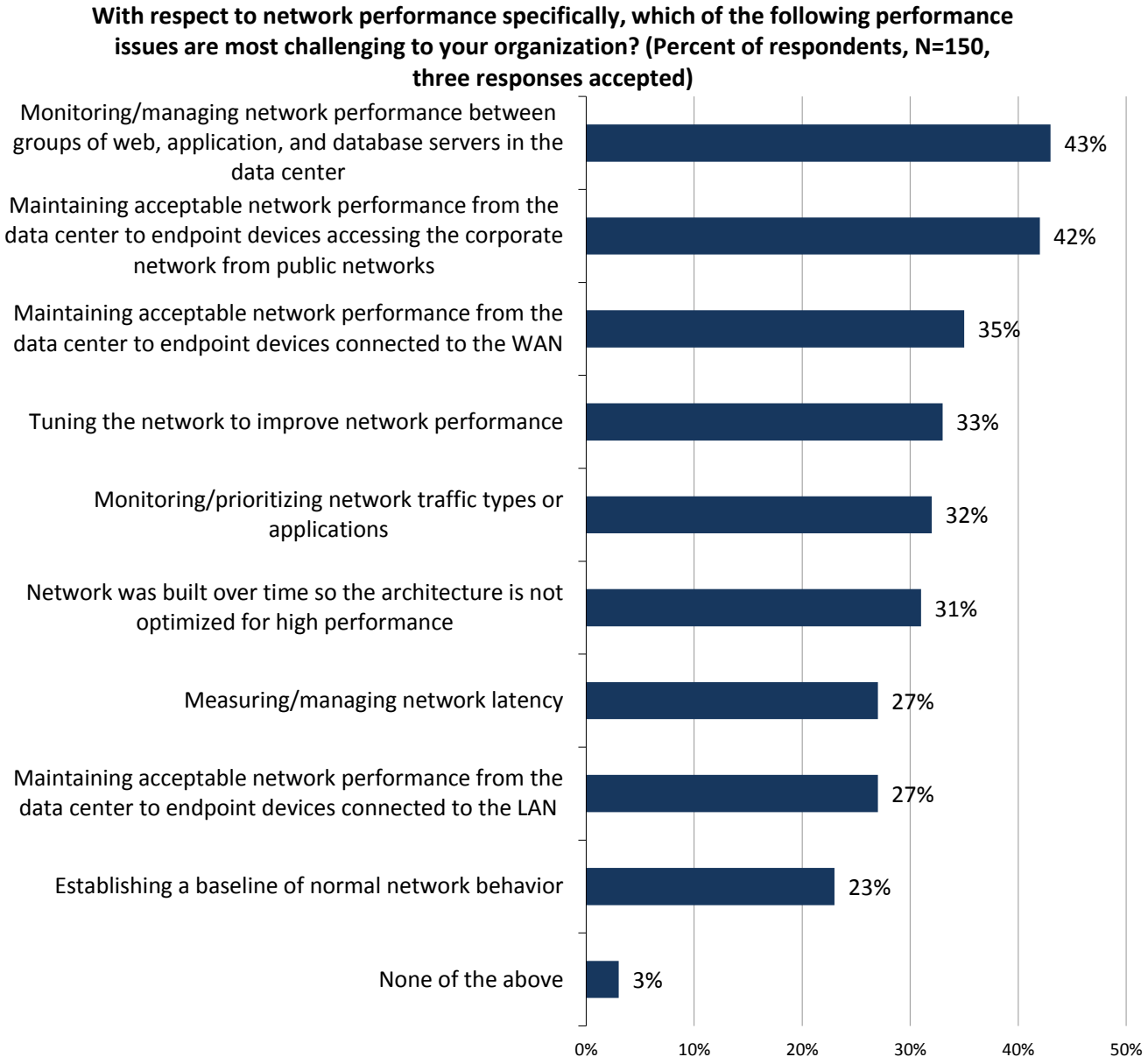


Source: Enterprise Strategy Group, 2014.

Challenges Organizations Encounter

As might be expected, these rapidly growing and complex network environments represent significant challenges for organizations. Their sheer size and complexity make it difficult for operations teams to ensure optimal performance and high levels of security. To better understand these challenges, ESG asked respondents to cite their specific network performance and security challenges. As seen in Figure 3, the most-cited performance challenge highlights the problems faced with new multi-tier and modular software architecture. After that, organizations struggle to maintain end-to-end network performance to endpoint devices connecting either via public networks or wide area networks (WAN). These challenges reflect a rapidly changing environment marked by centralized data centers and an increasingly mobile workforce. This extends the boundary of end-to-end management to mobile devices. Other challenges include tuning the network, providing QoS based on traffic or applications, and understanding network latency.

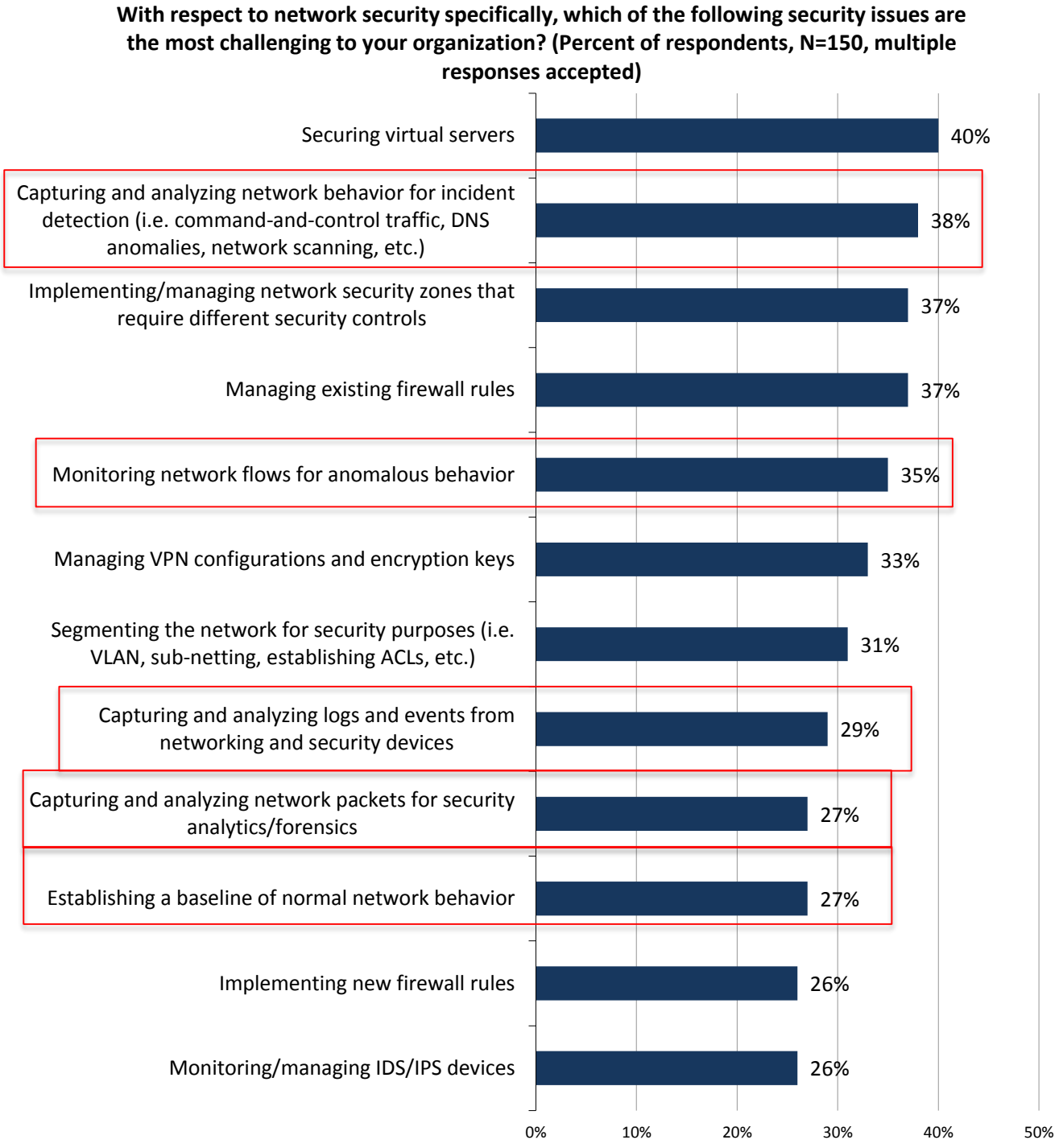
Figure 3. Network Performance Challenges



Source: Enterprise Strategy Group, 2014.

When it comes to security, organizations highlighted a number of challenges. While a number of other challenges were cited, we have highlighted those that clearly point out the need for network visibility in order to improve security. This includes the struggle to capture network behavior for incident detection, monitoring network flows for anomalous behavior, the ability to capture and analyze logs from network and security devices, and network packets for security analytics or forensics as well as the ability to establish a baseline of normal network behavior.

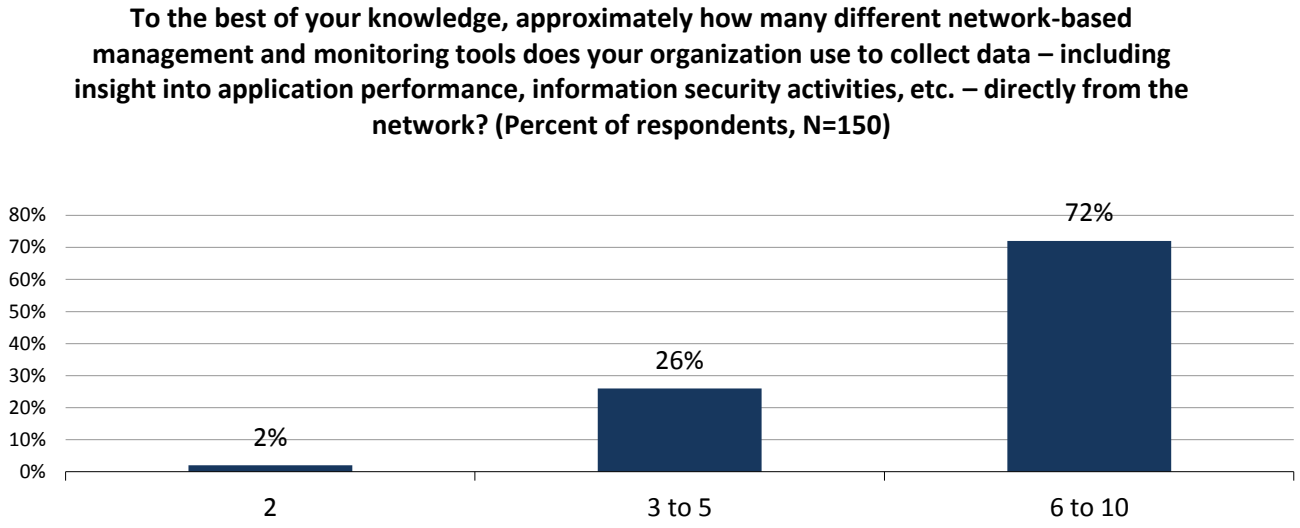
Figure 4. Security Challenges



Source: Enterprise Strategy Group, 2014.

In order to overcome these challenges, organizations are instrumenting and deploying monitoring tools in their environments, but is it enough? Of the organizations ESG surveyed, 72% of them reported that they already have between six and ten tools deployed to monitor the network (see Figure 5).

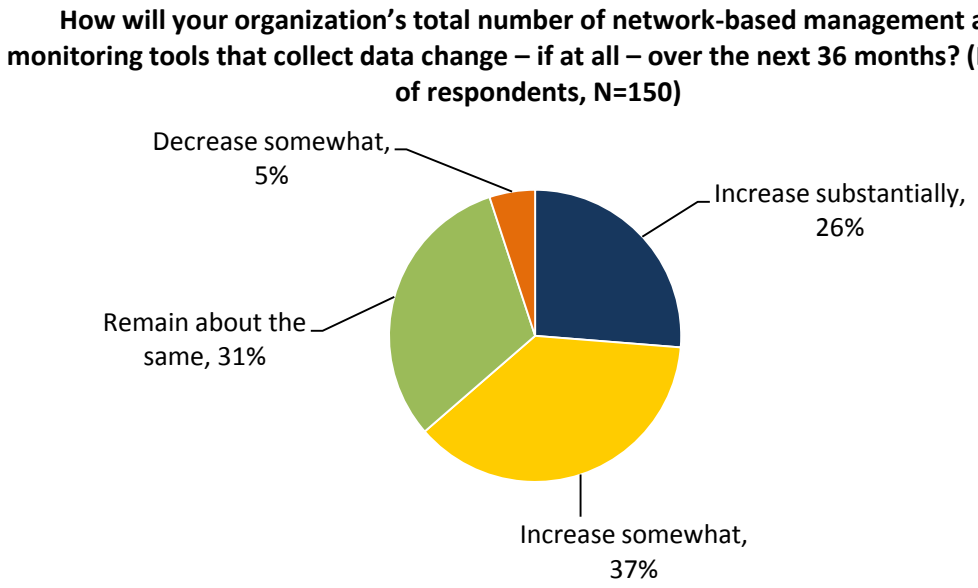
Figure 5. Number of Network-based Management and Monitoring Tools



Source: Enterprise Strategy Group, 2014.

Even more telling is the fact that 63% expect that the number of tools they use to monitor their network environment will increase either somewhat or substantially in the near future (see Figure 6).

Figure 6. Increase in the Number of Tools Deployed



Source: Enterprise Strategy Group, 2014.

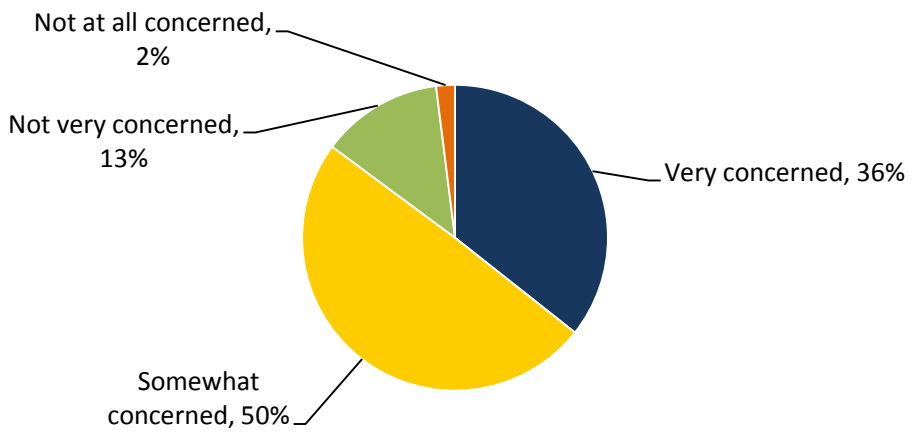
Again, these are telltale signs of a rapidly growing network environment. And the need for more information is also continuing to grow. More than two-thirds (69%) of respondents stated that they expected the number of requests to capture network data (not just meta-data but packets) to increase dramatically. Keep in mind that the number of internal departments requesting this information is also increasing. The requests are not just from the network

operations team: Respondents to the survey indicated that the network architecture, security, compliance, and IT audit and application teams were also requesting this data.

Unfortunately, the ability to fulfill all of these requests is becoming more difficult, especially with organizations upgrading their networks to 10 GbE. Should organizations be concerned? According to the research, 86% of organizations planning to go to 10 GbE are concerned about their traditional monitoring tools and methodologies ability to cope with the increased throughput (see Figure 7).

Figure 7. Concern about Dropped Packets with Existing Tools

When thinking about your organization's transition to 10 GbE as its standard network I/O interface, are you concerned about any of your organization's network-based management and monitoring tools dropping packets or being unable cope with the increased throughput? (Percent of respondents, N=103)

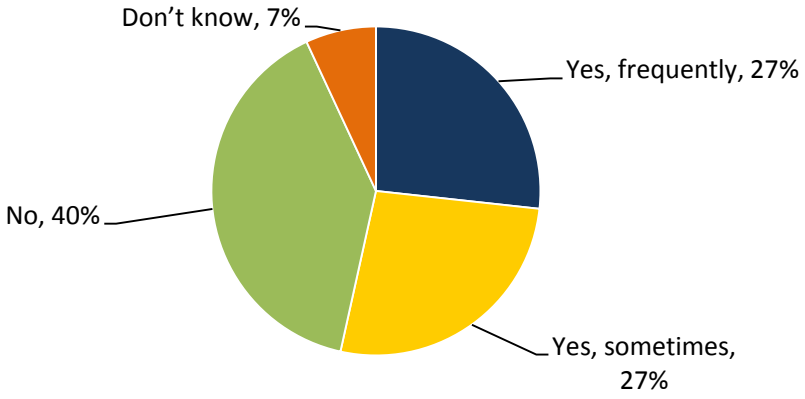


Source: Enterprise Strategy Group, 2014.

To better understand the impact that this transition could potentially have, organizations that have already standardized on 10 GbE networks were asked about the impact of the move. Figure 8 demonstrates that more than half (54%) of those organizations find that their traditional monitoring tools and methodologies either sometimes or frequently cannot cope with the increased throughput or are dropping packets due to the increased throughput. Organizations actively transitioning or planning to go to 10 GbE networks should learn from those organizations that have gone before them so they don't struggle with the same challenges.

Figure 8. Monitoring Tools Having Difficulty with 10 GbE Network Throughput

Since transitioning to 10 GbE as its standard network I/O interface, has your organization encountered situations where any of its network-based management and monitoring tools are dropping packets or cannot cope with the increased throughput?



Source: Enterprise Strategy Group, 2014.

Why It's Important to Capture Network Data

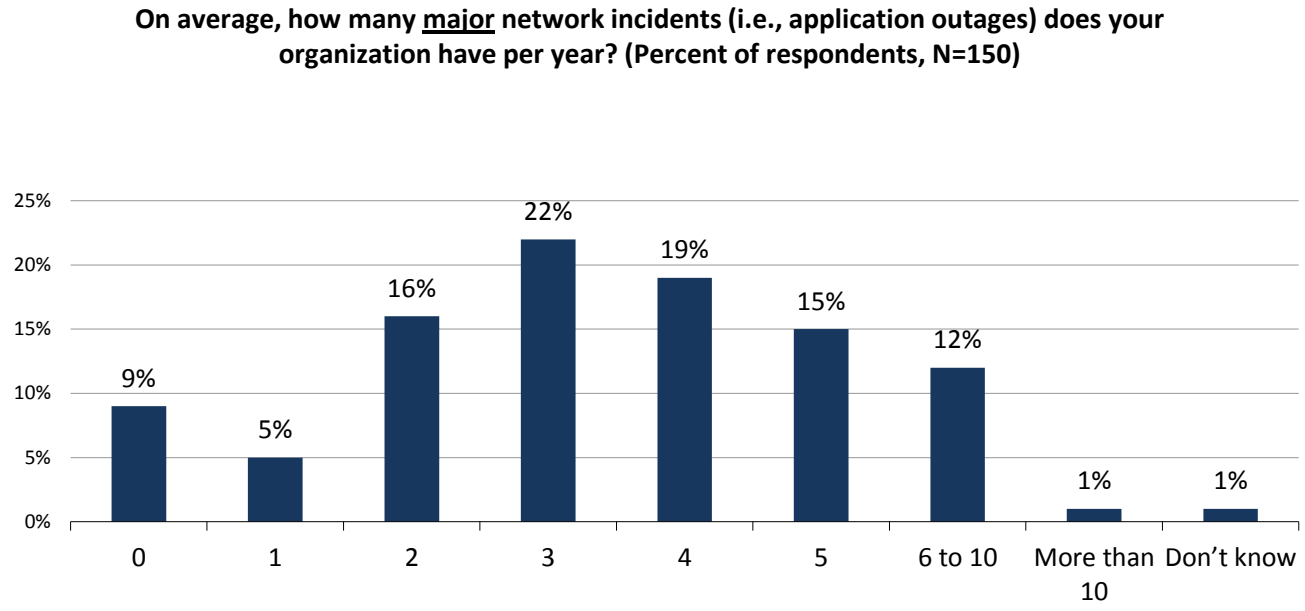
Despite the challenges faced by organizations with rapidly growing and complex network environments, the ability to capture network data has never been more important. More frequently, organizations are relying on network data (meta-data and packets) to provide insight into network performance or problems, and to deliver increased levels of security. When done correctly, a plethora of information is available for collection and analysis.

Organizations also need to think about collection metrics: Does real time mean that a sample is taken every five minutes, or does it involve capturing every packet? The obvious implication is that a problem could come and go outside of a collection window, so an application would be impacted without the collection tool being aware. Having granular information will help to quickly identify and resolve those intermittent or sporadic problems. Having this data accessible could be the difference between identifying a problem immediately and requiring several hours or days to track it down.

Historical data can be extremely important as well because the ability to establish baselines and see trends will help to identify areas that need attention before they actually cause a problem. It also enables organizations to review capacity based on seasonality or the end of the week, month, quarter, or year in order to plan appropriately. Organizations can also leverage this data to help optimize the network for specific applications or eliminate bottlenecks. Having both historical and real-time granular data will enable organizations to become more proactive in addressing both intermittent issues and in responding more quickly to major problems.

The reality is that major network problems do occur, and the majority of ESG research respondents (64%) indicated that their organization experienced three or more major network incidents per year (see Figure 9). And just over a quarter of the respondents (27%) reported between five and ten major network incidents per year.

Figure 9. Major Network Incidents



Source: Enterprise Strategy Group, 2014.

Each of these outages has consequences for the business. Depending on the length of time required to find and fix the problem, the ramifications of these outages could be disastrous: Not only is there the cost of downtime, which ranges anywhere from tens of thousands to over a million dollars per hour depending on the industry, but organizations also have to consider the residual impact of an extended outage—i.e., loss of customer confidence, potential impact to stock price (if public), etc. Plus, without detailed information isolating the root cause, these outages impact efficiency as organizations dedicate resources to find and fix the problem. More than half of the respondents (55%) to ESG's survey indicated that they dedicate four or more staff members to resolving major incidents.

The Mandate

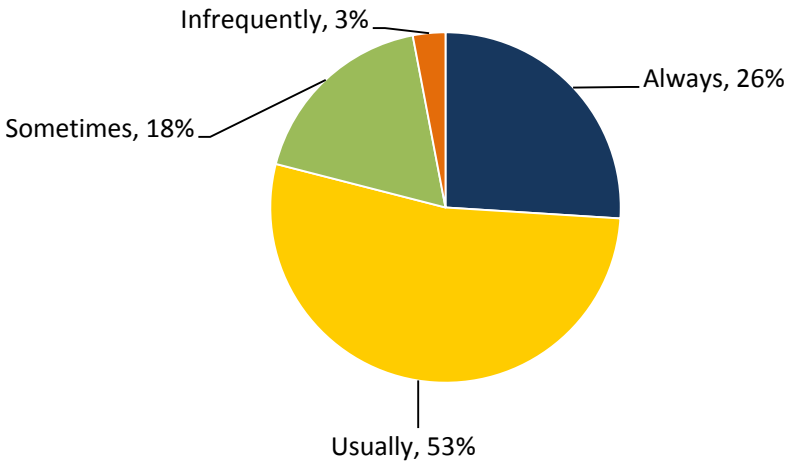
The perfect storm of increasing network scale, higher levels of complexity, and the requirement to be always on has resulted in network monitoring and capture evolving from a "nice to have" feature into a corporate mandate. Organizations have to be able to quickly find and fix problems, and the key is the ability to quickly isolate the root cause of network issues so valuable time is not lost.

How important is identifying the root cause of network issues? Well, 40% of respondents deemed identifying root cause to be critical to them, while another 49% stated it was very important. With the overwhelming majority of respondents assigning a high level of importance to determining root cause, it is clear that having this capability has moved beyond a nice to have feature and is now a virtual mandate.

After realizing the importance of root cause analysis, the next step is understanding how capturing network information can help to accelerate that process. More than three-quarters (79%) of respondents indicated that the network, security, and application operations teams need to access packet-level network traffic in order to successfully identify the root cause of network issues (see Figure 10). In fact, only 3% of respondents indicated they infrequently access network traffic to identify root causes of network issues.

Figure 10. Need to Access Packet-level Network Traffic

How frequently do network, security, or application operations personnel need to access packet-level traffic data in order to successfully identify the root cause of network issues? (Percent of respondents, N=150)



Source: Enterprise Strategy Group, 2014.

While every organization has a different network environment and will make the transition to 10 GbE at their own pace, all organizations should be able to ask themselves some fairly basic questions about their monitoring environments, specifically:

- Is your organization currently monitoring and capturing all network traffic effectively?
- Can your existing network performance, security, compliance, and application monitoring tools readily access that data?
- Will current monitoring solutions be able to handle all the network traffic being generated from modern network environments (including 10 GbE, modular or multi-tier applications, end-to-end, etc.), without dropping any data?
- Are you able to quickly and efficiently identify the root cause for major, minor, and intermittent network problems?

Organizations need to ensure they have effective monitoring solutions in place that will enable the transformation to modern network environments. If your answer to any of these questions is not an emphatic "yes," then perhaps it is time to create a network monitoring mandate for your organization.

The Bigger Truth

The truth is that organizations are rapidly transforming their IT environments to better handle the requirements of the businesses they serve. A number of the initiatives driving this transformation, while delivering significant benefits, are also creating new challenges, and specifically new network challenges. In order to retain control, organizations need to implement solutions that enable operations teams to more effectively monitor and manage these complex, modern network environments.

It is also important to understand that as the network becomes viewed as a source of valuable information, organizations should anticipate that additional requests will be made to access that data. ESG survey data indicates that the number of different internal operations and audit teams that require access to this information and the number of tools deployed to analyze this data will only continue to grow. As the network transitions from 1GbE to 10 GbE (and eventually up to 40 and 100 GbE), these requirements will only intensify. It will be imperative for organizations to deploy solutions that can handle not only current, but also future needs.

Organizations should consider network visibility (the ability to collect, store, search, and present network data) to be a mandate, so they will be better prepared to ensure network performance, security, and compliance, as well as dramatically reduce the time to find and fix critical problems in modern network environments.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0218 | www.esg-global.com