Report Summary: Network Management Megatrends 2016

Managing Networks in the Era of the Internet of Things, Hybrid Clouds and Advanced Network Analytics

By Shamus McGillicuddy
An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) End-User Research Report
April 2016

This research has been sponsored by:

riverbed®

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

Report Summary:
Network Management Megatrends 2016

Table of Contents

EMA

Report Summary:
Network Management Megatrends 2016

Executive Summary

This ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) research summary highlights some of the key findings of EMA's landmark report, "Network Management Megatrends 2016: Managing Networks in the Era of the Internet of Things, Hybrid Cloud, and Advanced Network Analytics." It examines several major areas of change and evolution affecting network management, or what EMA calls "megatrends." These megatrends include hybrid cloud networking, the Internet of Things, advanced network analytics, network management outsourcing, and network management tool consolidation.

Introduction

Enterprise Management Associates (EMA) analysts closely follow the evolutions and revolutions of managed enterprise network environments and how they affect best practices for monitoring, troubleshooting, and designing modern networks. Network availability and performance are, more than ever before, a critical part of the way in which IT supports the enterprise. As new initiatives such as hybrid cloud, the Internet of Things, and advanced network analytics gain traction in the enterprise, the network engineering and operations teams must ensure that network services can adapt.

Over the past several years, EMA has conducted a series of research studies called "Network Management Megatrends" reviews. They are designed to examine how both micro and macro technology trends are affecting network management tools, technologies, and practices. This study is our fourth megatrends study. For this latest version, we have carried forward a number of ongoing questions and threads that are designed to track how the network management landscape is changing over time. We've also included many new questions and queries intended to help us characterize and quantify the very latest technology trends. In particular, new questions were added in this report to begin assessing whether hybrid clouds, advanced analytics, and/or the Internet of Things were having an impact on network management tools and practices.

Key Findings of Network Management Megatrends 2016

- **Enterprises continue to use far too many tools to monitor and troubleshoot their networks.** This has a direct impact on the effectiveness of network operations. Enterprises need to strategically consolidate network management tools wherever possible.
- **Most enterprise networking teams are already supporting multiple Internet of Things (IoT) initiatives.** To support them, they are implementing new security controls, IoT device management systems, and network expansions and upgrades.
- **Most enterprise networking teams have either completed a production hybrid cloud deployment or are in the process of doing so.** Many of them are implementing network virtualization overlays and new network performance management software to support these clouds.
- **Roughly half of enterprise network teams are applying advanced analytics to network data.** These network analytics projects are helping them with network security monitoring, network optimization, and business process optimization.
- **The number of enterprises that outsource some aspects of network management is rising, particularly among large enterprises.** One function that has become a bigger target for outsourcing is Layer 1 support (help desk calls).

The following pages offer some highlights of the Network Megatrends 2016 study. For a more comprehensive look at these megatrends and for more data on enterprises' evolving requirements for network management tools, please download the full report.

Demographics

EMA surveyed North American IT professionals at 150 enterprises for this research. Survey respondents hailed from a diverse group of companies. In terms of company size, there was broad distribution. Twenty-eight percent (28%) of respondents worked at small enterprises (250 to 999 global employees), 38% worked at midsized enterprises (1,000 to 4,999 global employees), and 34% worked for large enterprises (more than 5,000 global employees).

From a vertical industry perspective, three industries were represented by a statistically significant number of respondents: 17% were from finance/banking/insurance firms, 11% were from software companies, and 11% were from the retail/wholesale/distribution industries.

Finally, to qualify for the survey underpinning this research, respondents had to be involved in the selection, implementation, and/or use of network management products and solutions. As seen in **Figure 1**, the respondents were involved in all stages of a network management solution's lifecycle within their enterprises. They reported involvement ranging from evaluation, approval/purchase, and deployment/support of the products to using the products to plan, manage/monitor, and troubleshoot networks. The typical respondent was involved in four aspects of a network management product's lifecycle within their organization. With only 51% of the research sample involved in network troubleshooting, it was the least common activity reported.

Figure 1. How are you involved with network management products and solutions within your organization?

Megatrend #1: The Internet of Things Is Already Pervasive in Enterprises

Over the last couple years, several major technology companies, particularly infrastructure product vendors, have started promoting the marketing term "Internet of Things" (IoT) to describe a network of everyday objects that network operators have not traditionally thought of as network endpoints. These objects, or "things," have sensors, controls, and network connectivity, which they use to collect, send, and receive data. These things can include consumer devices, durable goods, industrial equipment, buildings, vehicles, transportation systems, and public utilities.

While the concept of IoT is relatively new, the actual network it describes has been around longer. Utility companies had already developed smart grids. Industrial companies had already connected their control and monitoring systems to IP networks. Agricultural companies were already deploying network-connected sensors on livestock and crops. IoT awareness has risen, however, and this awareness has led enterprises and technology providers to take a more strategic approach to connecting objects to networks.

For this study, EMA explored whether network infrastructure teams were supporting enterprise IoT initiatives. Eighty-seven percent (87%) of the network management professionals surveyed in this study said they were providing connectivity to devices—i.e. "things"—as part of an IoT initiative.

87% of network management professionals were providing connectivity to devices—i.e. "things"—as part of an IoT initiative.

As **Figure 2** demonstrates, "networks and communications" is the top application category that enterprises are adopting with IoT. Networks are primarily thought of as enablers of IoT, but here enterprises have identified networks and communications as an actual IoT application. Examples of such IoT applications may include advanced power management and so-called "green IT" initiatives aimed at making network infrastructure more efficient. It may also include advanced mobile technologies such as location-based services. Networking may also be prominent as an application category because every enterprise today has a network, whereas many of the other IoT applications that EMA polled users on are very specific to vertical industries. Agriculture, municipal and utilities, environmental monitoring, and health and body were all niche applications, supported by less than 20% of survey respondents.

Aside from networks and communications, five other applications emerged as prominent. Security and public safety led the way with 35% of respondents, followed by retail, logistics and transportation, buildings and facilities, and consumer goods. Each of these have more applicability across vertical industries. Finally, industrial controls, which can include manufacturing facilities and energy production, were supported by nearly one-quarter of survey respondents.

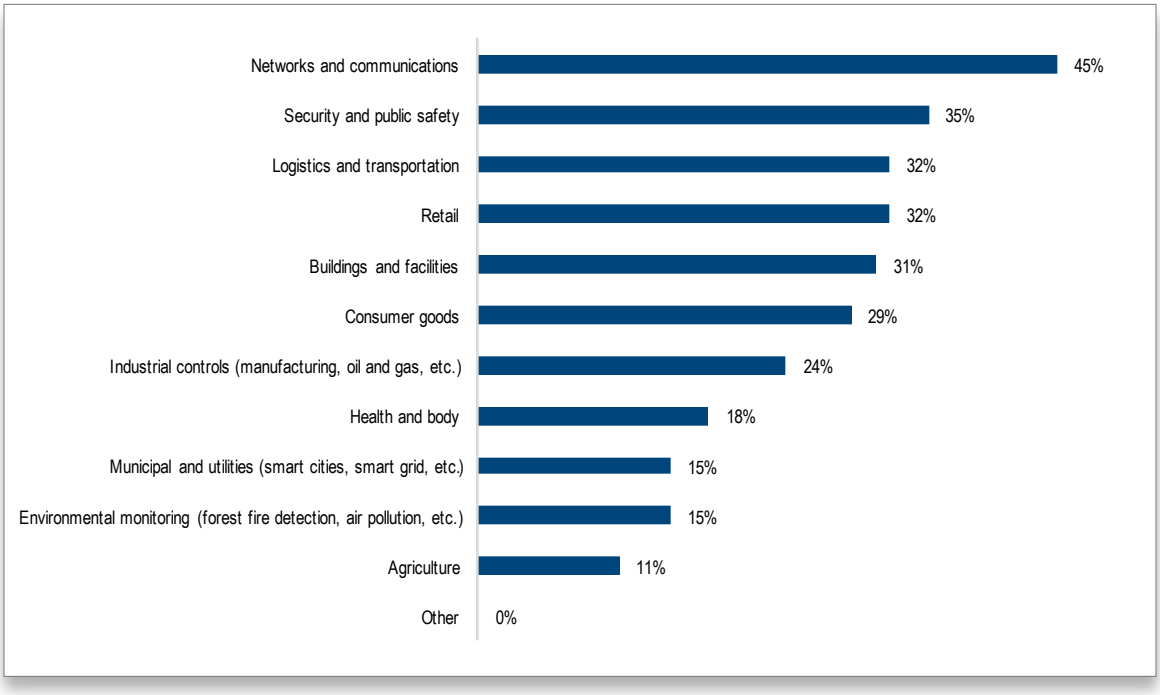

Figure 2. What applications is your organization pursuing with its IoT initiative?

IoT Impacts on Network Infrastructure Teams

We asked network managers from organizations that have adopted IoT to identify which technologies they had implemented in support of these initiatives. New security controls were the only technology installed by a majority (55%) of enterprises.

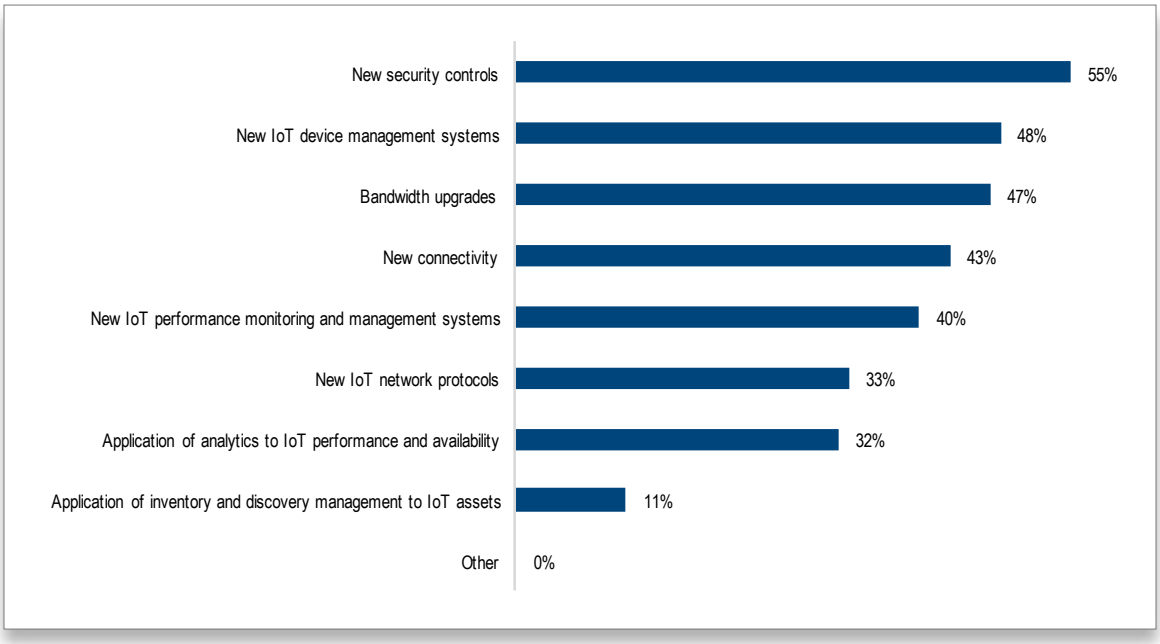

Figure 3. Have you implemented any of the following in support of your organization's Internet of Things initiative?

New management tools were also popular among IoT adopters. Forty-eight percent (48%) had added new IoT device management systems, and 40% had added new IoT performance monitoring and management systems. Forty-seven percent (47%) of enterprises were implementing bandwidth upgrades to support IoT and 43% were adding new connectivity.

New IoT network protocols were less popular, with just one-third of respondents implementing them. This number may rise in subsequent market studies, given that there is a wide variety of emerging protocols in the industry today, many of which are being promulgated by vendor consortiums rather than the standards bodies that traditionally codify network protocols. It is unclear today which ones the industry will embrace as standards.

The application of analytics to IoT performance and availability and the application of inventory and discovery tools to IoT assets were also relatively unpopular among networking pros supporting these initiatives.

Megatrend #2: Hybrid Cloud's Moment Has Arrived

In past research, EMA has studied how networking professionals support cloud computing initiatives, in both the public cloud and the private cloud. Increasingly, we have focused on how hybrid cloud affects the networking organization. For this research, EMA defined "hybrid cloud" as "a cloud computing environment that combines private, internal cloud infrastructure with public, external cloud infrastructure." It is also characterized by connectivity and orchestration across internal and external cloud domains to support use cases such as cloud bursting, geographic workload distribution, and disaster recovery.

As shown in **Figure 4,** 70% of the network management professionals who participated in this research project worked for organizations that had a launched hybrid cloud deployment, including 35% that had already completed a production hybrid cloud deployment and another 35% that were in the process of deploying their hybrid cloud. Twenty percent (20%) were in various stages of planning, and just 9% had no immediate plans for hybrid cloud.

70% of the network management professionals who participated in this research project worked for organizations that had a launched hybrid cloud deployment

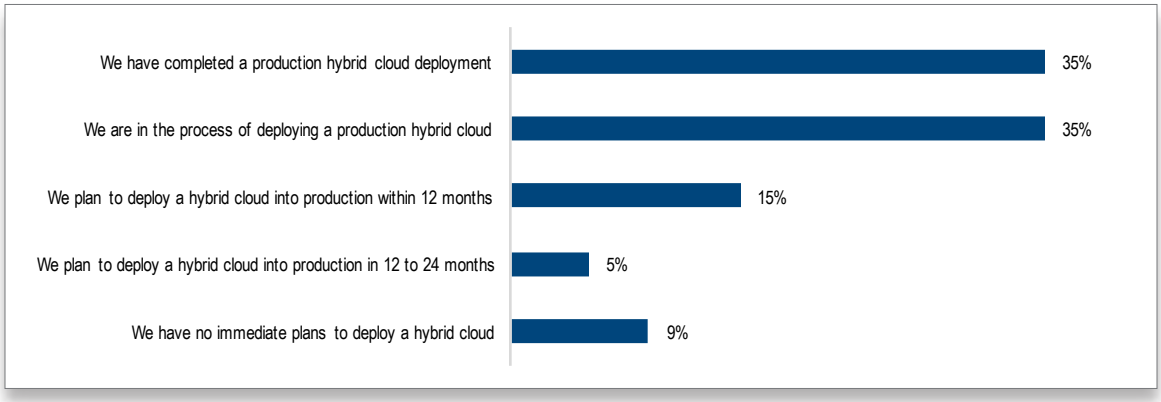

Figure 4. At what stage of activity is your organization with respect to hybrid cloud infrastructure?

Budget growth is a major indicator of aggressive adoption of hybrid cloud. This research found that 61% of enterprises with high-growth IT budgets (budgets that grew by more than 25% this year) were already in production with their hybrid cloud. Company size also influenced hybrid cloud adoption. Small companies were much less likely to be in production (just 26%) and were the most likely to say they had no immediate plans for hybrid cloud (19%). Medium-sized companies were the most likely to be in the middle of their production deployment (44%), while large firms were most likely to have completed their production deployment (41%). Financial firms appear to be early adopters of hybrid cloud, with 50% of them already in production. Retail companies are mostly in the deployment phase, with 56% in the midst of their production implementation today.

The majority of hybrid cloud organizations are adopting network virtualization overlays and new network performance monitoring and management software to support this infrastructure.

Networking Teams and Hybrid Cloud

EMA asked research participants whose organizations were planning, deploying, or operating production hybrid clouds to identify the networking technologies that they were adopting to support these initiatives. As **Figure 5** reveals, the majority of hybrid cloud organizations are adopting network virtualization overlays and new network performance monitoring and management software to support this infrastructure.

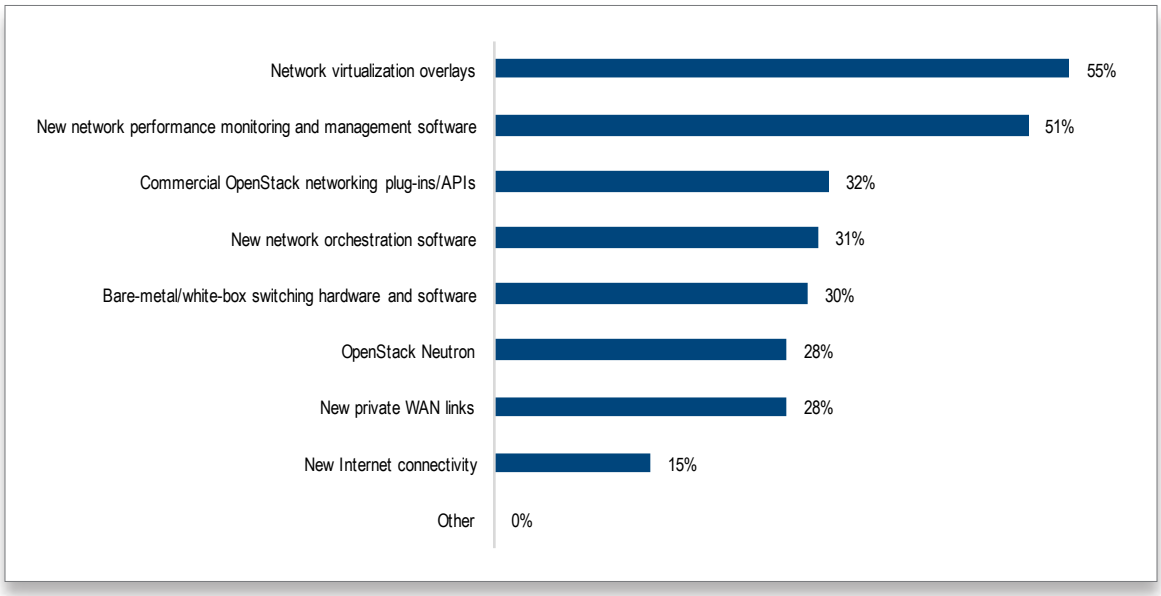

Figure 5. Are you implementing any of the following technologies to support hybrid cloud networking?

The research identified five other technologies that are secondary for hybrid cloud networking. Roughly one-quarter to one-third of organizations were implementing new private WAN links, new network orchestration software, bare-metal or white-box switching hardware and software, commercial OpenStack networking plug-ins or APIs, and OpenStack Neutron.

With 30% of the research pool indicating adoption of bare-metal switching, the level of adoption for this technology was surprisingly high, and it may be a statistical aberration. However, three mainstream network equipment manufacturers (Hewlett Packard Enterprise, Dell, and Juniper Networks) have introduced bare-metal switch solutions over the last couple years, which has significantly lowered the barriers to adoption among enterprises. This high adoption rate may also be partly driven by the retail companies represented in the survey, which reported a 47% adoption rate of bare-metal switching.

With 32% of these organizations using commercial OpenStack APIs and 28% of them using OpenStack Neutron, it is quite clear that OpenStack is a significant element of an enterprise hybrid cloud architecture. Financial companies appear to be particularly aggressive with OpenStack. Forty-two percent (42%) have implemented OpenStack Neutron, and 50% have implemented commercial OpenStack APIs.

EMA also asked respondents to identify the top networking challenges they were facing with their organizations' hybrid cloud initiatives. As **Figure 6** demonstrates, there was no consensus on the top challenge for networking teams. Instead, enterprises appear to be grappling with a wide range of issues. However, the complexity of provisioning interconnections between public and private cloud environments inched ahead of other issues to emerge as the foremost problem networking teams are dealing with. Otherwise, all other networking headaches were felt equally, from a lack of end-to-end, multisite visibility to the problem of latency between internal and external cloud resources.

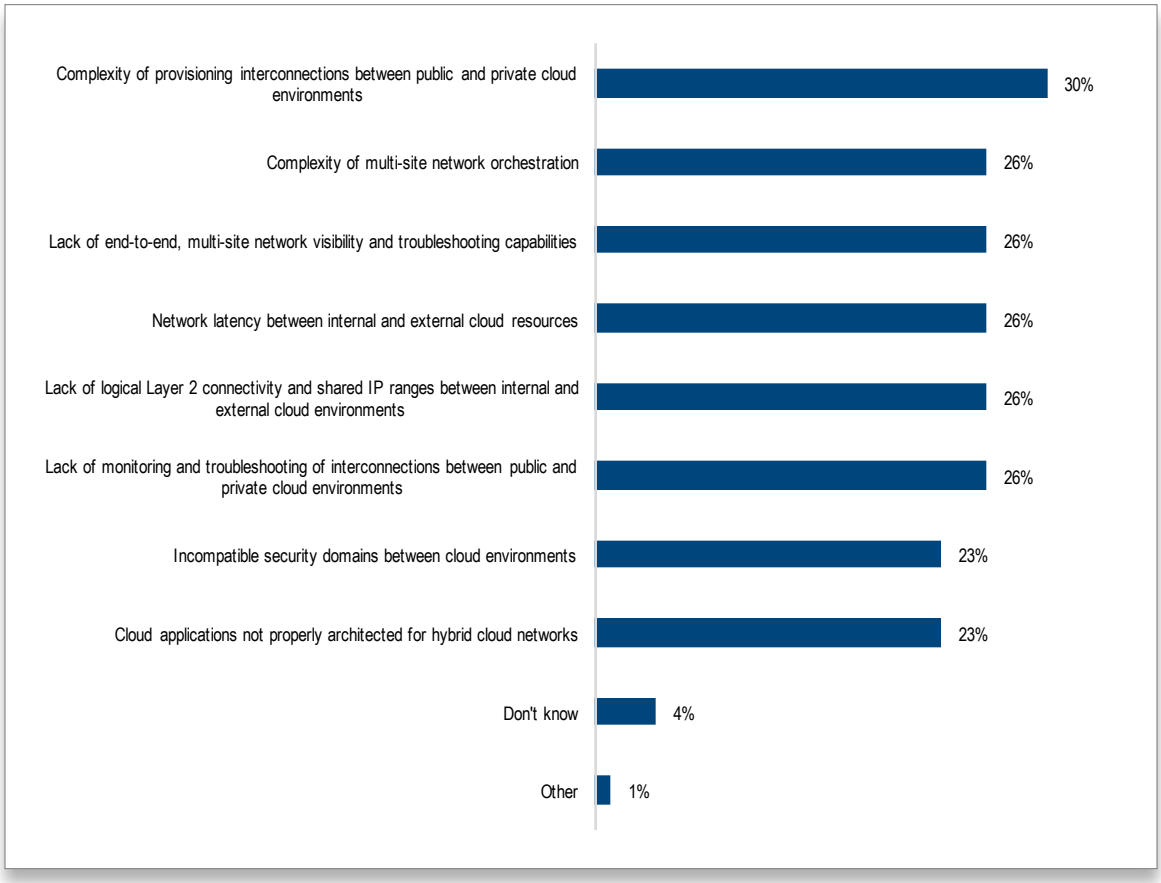

Figure 6. What are the top networking challenges you are facing with your organization's hybrid cloud?

Megatrend #3: Applying Advanced Analytics to Network Data

Today's digital economy has elevated the status of data to new heights. In the abstract, data has always had value to enterprises, whether it included customer information, employee communications, intellectual property, or something else. But with the emergence of advanced analytical techniques such as big data, the utility of data and the business and operational insights it can provide have expanded. Networking data is no exception to this trend.

In a digital enterprise, everything crosses the network wire, including transactions, processes, and communications. With the right analytical tool, an enterprise should be able to glean valuable insight from that network data. In this research project, EMA asked network management professionals to share their experience with the application of advanced analytics to network data.

Network flows (NetFlow, IPFIX, etc.) and network security data are the two types of data most popular for inclusion in network analytics initiative.

Forty-nine percent (49%) of research participants said their organizations were applying advanced analytics to network data today, and another 40% said they had plans to do this within 12 months.

Network flows (NetFlow, IPFIX, etc.) and network security data are the two types of data most popular for inclusion in network analytics initiative. **Figure 7** shows that nearly half of network analytics adopters were applying analytics to both of those data sources. From a vertical industry perspective, retail companies (69%) were especially reliant on network security data for advanced network analytics, but software companies (31%) were only light users of security data.

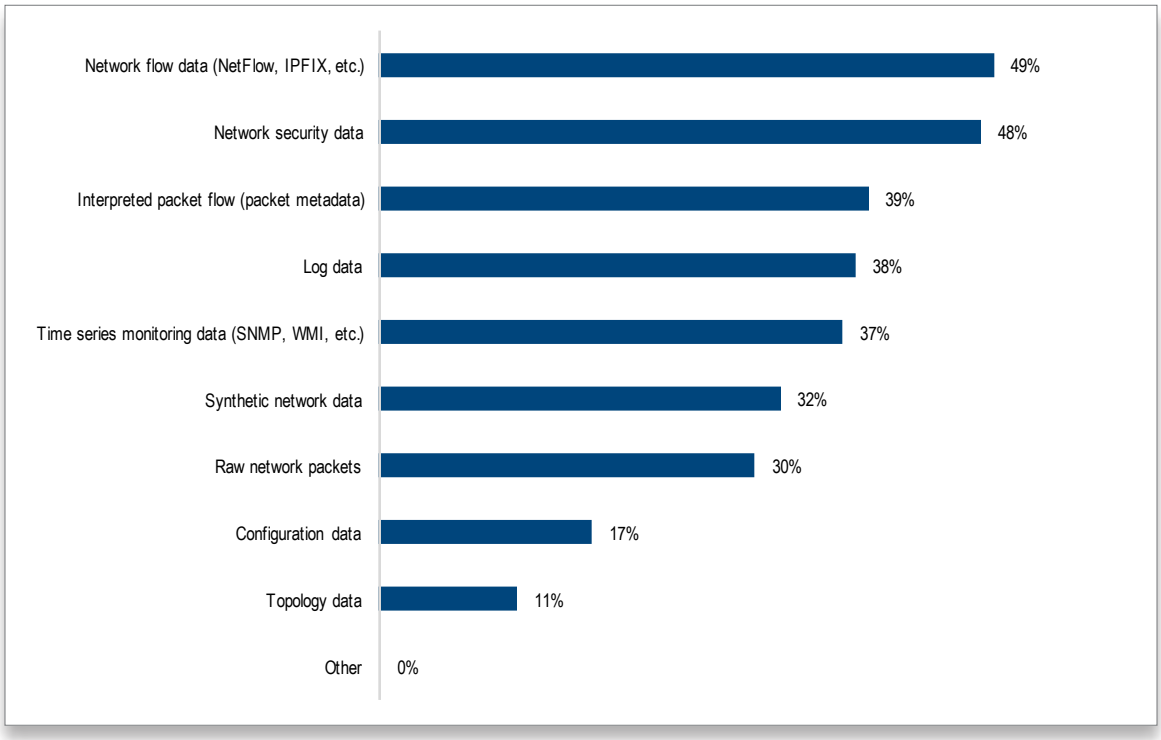

Figure 7. What network infrastructure data do you include in this network analytics initiative?

Interpreted packet flows (packet metadata), log data, and time-series monitoring data (SNMP, WMI, etc.) all emerged as secondary data sources for advanced analytics. Small companies (47%) were especially focused on including log data in network analytics, and large companies (47%) were making heavy use of interpreted packet flows. Raw network packets and synthetic network data (e.g., test traffic) fell into a more distant third category of data types used by less than one-third of organizations. However, more large companies (39%) were using raw network packets than small (25%) and medium (24%) organizations. Finally, topology and configuration data were almost never used in advanced network analytics.

Advanced Network Analytics Use Cases

Figure 8 reveals which advanced network analytics use cases were most important to enterprises. Network security monitoring was clearly the number one use case, which isn't a shock given that network security data and network flows (which are often used for security monitoring) were the two most popular types of data assimilated in network analytics initiatives.

Network optimization, business process optimization, predictive network analysis, predictive security analytics, and business process monitoring were all identified as secondary use cases. Network optimization was actually the top use case for small companies (47%), which makes sense since small companies have fewer resources and must maximize the useful life of existing infrastructure. In fact, organizations with flat-to-negative IT budget growth were also much more likely to use analytics for network optimization (42%), whereas just 15% of organizations with high-growth IT budgets bothered with this use case.

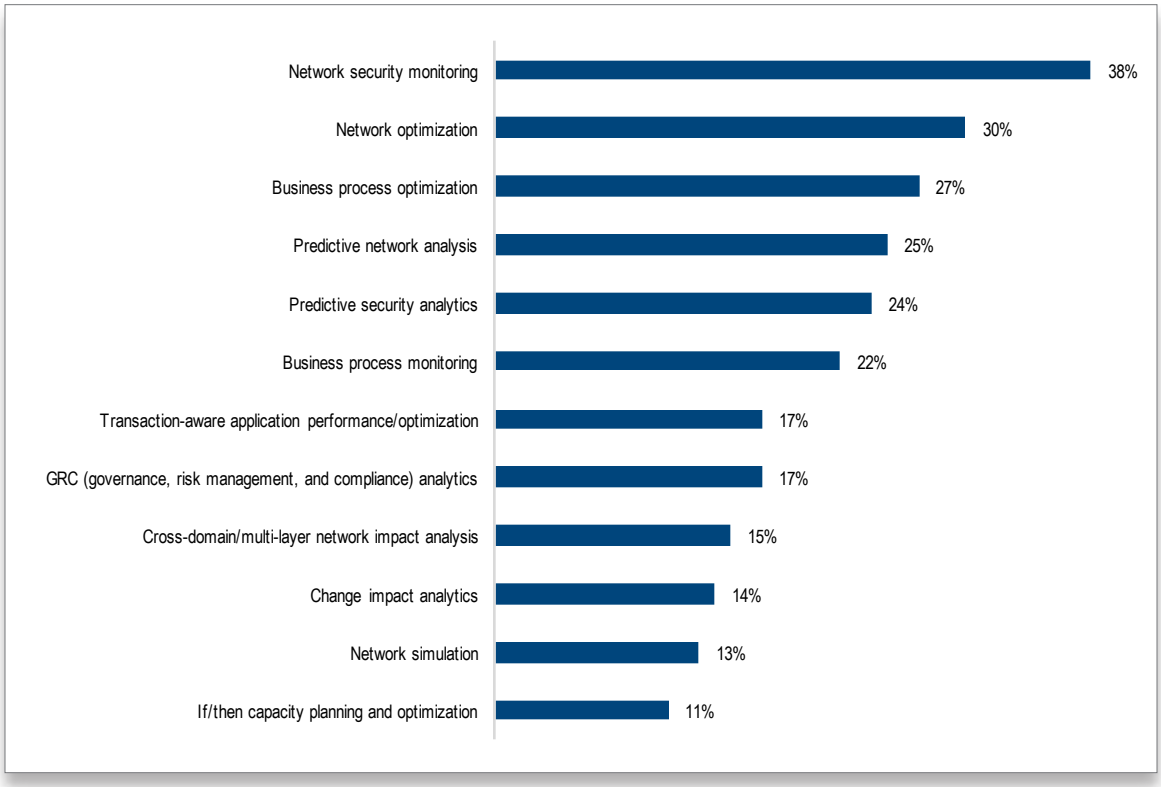

Figure 8. Which advanced network analytics use cases are most important to you?

Small enterprises were also more active with predictive security analytics as 36% of small companies were using them versus only 20% of medium and large enterprises. Large enterprises were more likely to be doing predictive network analysis (31%) and transaction-aware application performance optimization (31%). Organizations with high-growth IT budgets were also more likely (30%) to use analytics for transaction-aware application performance optimization, which was otherwise a minor use case.

Finally, business process optimization emerged as the number two use case for medium-sized enterprises. Thirty-three percent (33%) of them were pursuing this use case versus just 24% of large companies and 22% of small companies.

Overall, network security monitoring appears to be the low-hanging fruit for advanced network analytics use cases. Companies of all sizes were pursuing it. Network optimization was a target use case for companies with limited resources, while more ambitious organizations were tackling more ambitious use cases that support overall IT operations. Given the amount of business-relevant data that crosses an enterprise, EMA suspects that there is more potential for organizations to apply advanced network analytics to business process monitoring and business process optimization. Relatively few organizations are doing this today. With more experience and more resources, network infrastructure teams should be able to demonstrate their ability to more directly support business initiatives.

Network security monitoring appears to be the low-hanging fruit for advanced network analytics use cases. Companies of all sizes were pursuing it. Network optimization was a target use case for companies with limited resources.

Megatrend #4: The Impact of Overcrowded Network Management Toolsets

Network Management Toolkits: The Creeping Terror of Too Many Tools

EMA has long advocated that enterprises maintain a streamlined network management toolset for the sake of operational efficiency. Most modern network management products consolidate a variety of functional capabilities that were once available only as discrete tools. If a network management team hasn't taken a formal approach to consolidating tools over the years, their tool belts can get overcrowded and network operations can become tremendously inefficient.

In 2014, EMA found that the typical network operations team actively used three to 10 tools for network monitoring and troubleshooting. Our conclusion at the time was that enterprises needed to consolidate. In the current research, we asked the same question. **Figure 9** shows a comparison between the 2014 and 2016 results. The chart reveals that network operations teams have actually grown the number of monitoring and troubleshooting tools they use. Now the typical enterprise network management toolset ranges from four to 15 tools. This is a disappointing result.

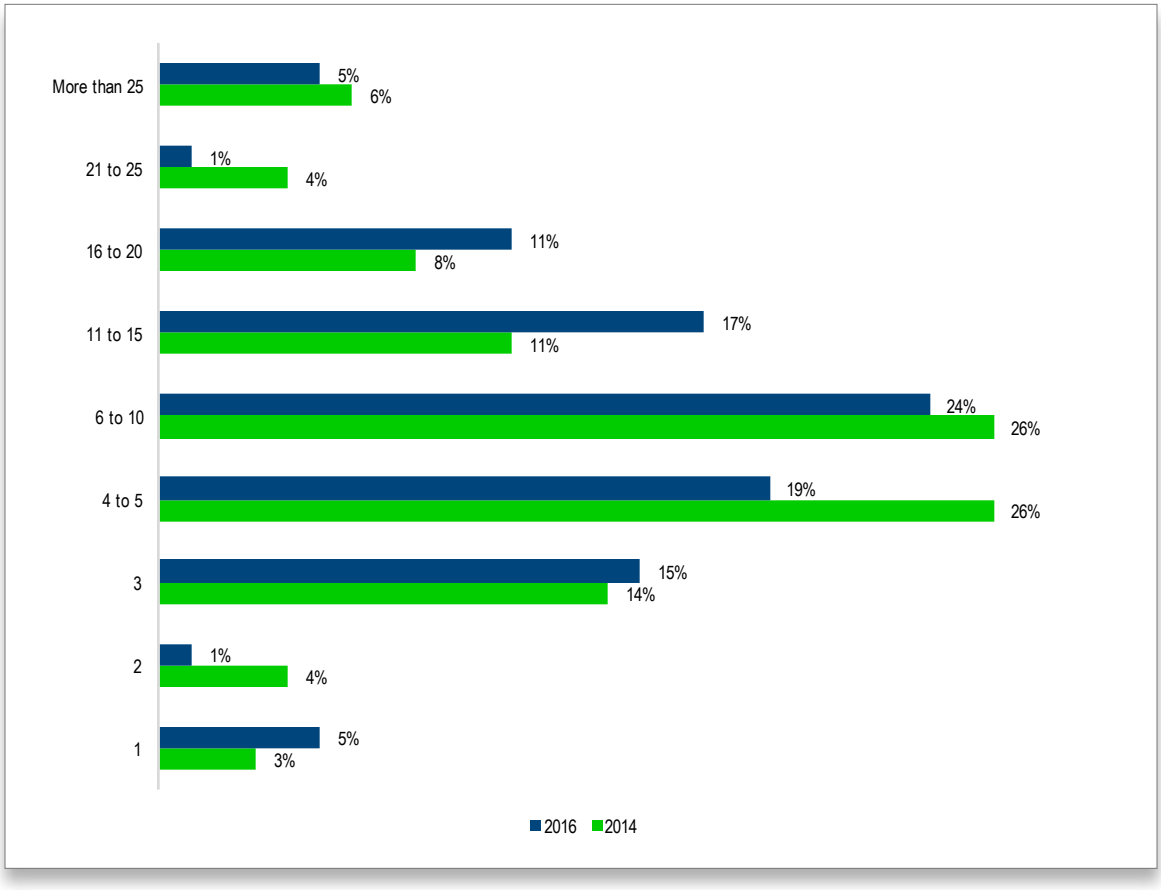

Figure 9. In total, how many tools would you estimate the network operations team uses for network monitoring and troubleshooting? (2014 versus 2016)

How Overcrowded Toolkits Affect Network Monitoring and Troubleshooting

EMA research has found over the years that a successful network management team should be able to detect most infrastructure problems before they impact end users. If an end user is the one who is first reporting a network problem, he or she is inevitably being impacted by that problem. Either applications and services are performing poorly or they aren't working at all. It is critical that network operations detect as many problems as possible before they impact user experience. Otherwise, business productivity is degraded.

EMA asked research participants to reveal how often end users tip them off to network trouble. Overall, the average network management professional revealed that around 40% of problems are first detected and reported by end users. This number is actually identical to the rate EMA uncovered in the 2014 Network Megatrends study.

Figure 10 reveals that organizations with larger network monitoring toolsets catch fewer network problems. Consider enterprises with 11 or more network monitoring and troubleshooting tools in active use. End users detect network problems about half of the time (52%). However, end users only detect about 29% of network problems in organizations where the network operations team uses only one to three tools. Meanwhile, network operations teams with four to 10 tools fall in the middle. Their end users catch problems first about 36% of the time.

Organizations with larger network monitoring toolsets catch fewer network problems.

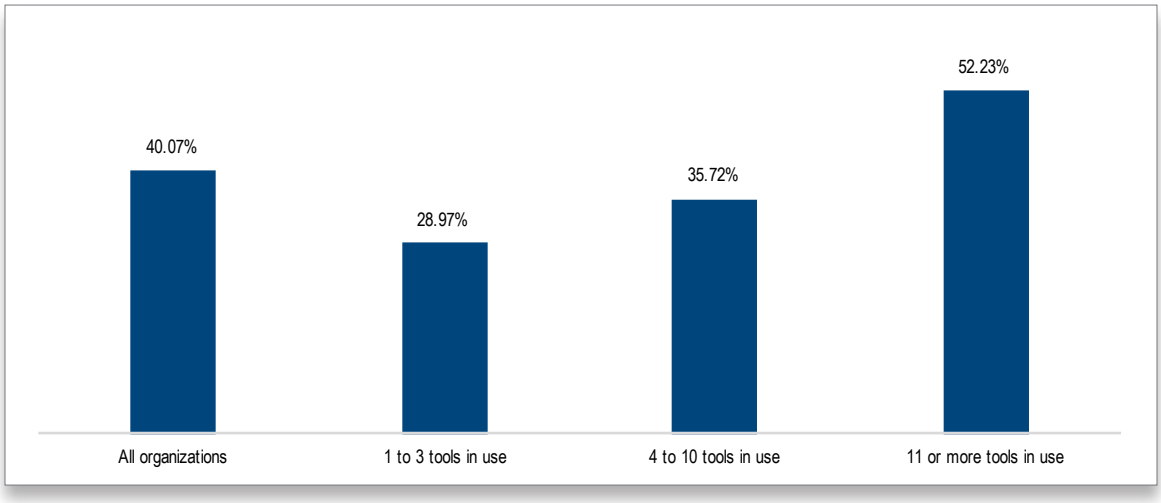

Figure 10. Currently, what percentage of issues or outages are first recognized and reported by end users, versus being recognized first by network operations?

To further understand the effectiveness of network operations, EMA next asked respondents to describe the percentage of their work time that was occupied by the following three general functions: reactive troubleshooting, proactive problem prevention, and all other tasks and projects. Ideally, EMA would like to see network teams devoting most of their time to "all other tasks and projects." If they spend less time fixing problems, they can devote more time to projects that directly support business initiatives. Also, we would like to see network management teams spending more time on proactive problem prevention and less time on reactive troubleshooting since this will translate to fewer impacts on end-user experience.

Unfortunately, **Figure 11** shows that network teams spend most of their time on reactive troubleshooting, a trend that has persisted for years in EMA's research. Also, network teams spend the least time on all other tasks and projects, which reduces their ability to deliver value to the business.

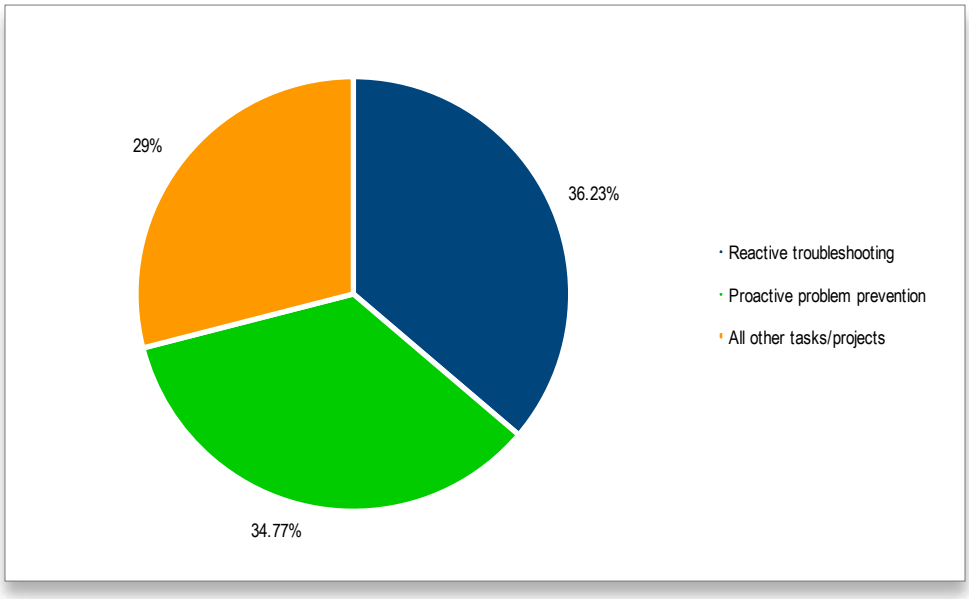

Figure 11. What percentage of total work time does your organization's network team spend per week on the following activities?

Figure 12 shows how the size of a network monitoring and troubleshooting toolkit affects these ratios. Networking teams with the smallest toolsets spend the least time on reactive troubleshooting and the most time on other projects. Organizations with 11 or more tools spend the most time on reactive troubleshooting. The data reveals a quirk among organizations in the middle, which use four to 10 tools. They spend the least amount of time on other projects and the most time on proactive problem prevention. Although their management toolkits are more consolidated than companies with 11 or more tools, this hasn't translated into more time spent on other projects. On the other hand, by doing more proactive problem prevention, they are likely to deliver improved network availability and performance.

Networking teams with the smallest toolsets spend the least time on reactive troubleshooting and the most time on other projects.

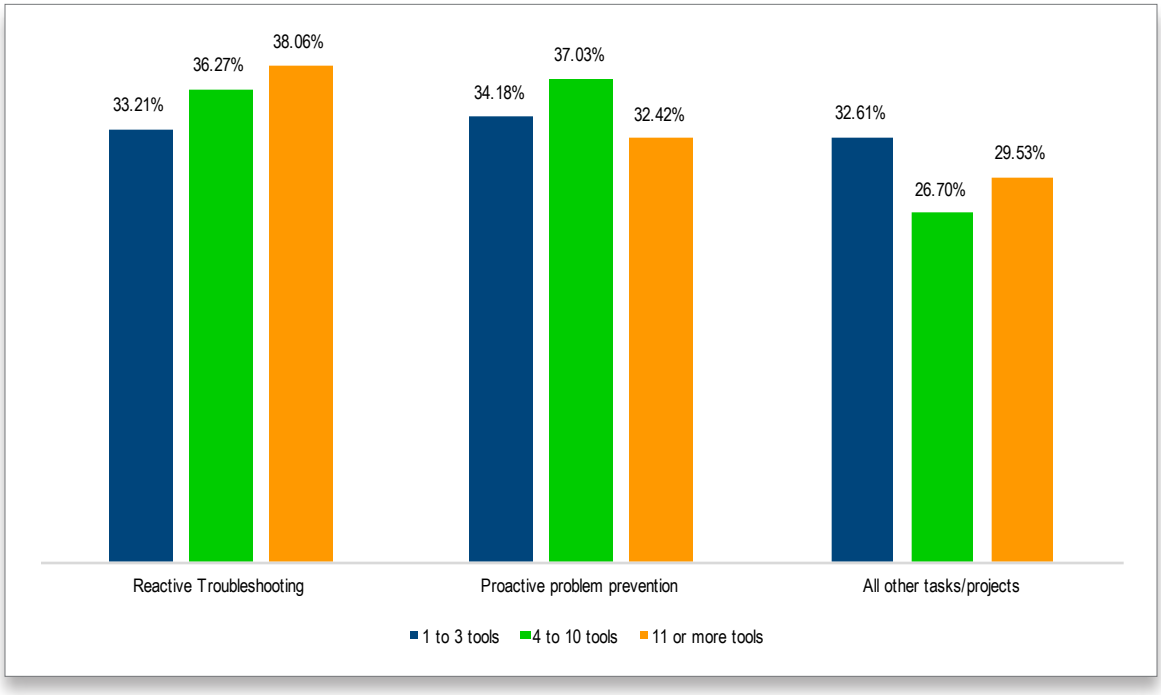

Figure 12. What percentage of total work time does your organization's network team spend per week on the following activities? (By number of networking tools)

These statistics show that network management teams that use larger toolsets are slower to detect and solve network problems. When network management teams maintain a complex set of discrete monitoring and troubleshooting tools, their workflows are inevitably inefficient and their toolsets are prone to gaps in visibility. EMA does not argue that simply removing network management tools from use will address this issue. Instead, when network management teams are procuring new tools or upgrading existing tools, they should be mindful of opportunities to consolidate. Many modern network management systems are multifunctional platforms that can replace several discrete management tools. However, network management teams often neglect these opportunities for consolidation. They maintain crowded arrays of discrete tools, both commercial and open source, due to personal preferences or a lack of planning. With a more disciplined approach, network management teams can become more effective.

Megatrend #5: Majority of Enterprises Outsource Some Network Management Functions

For the first time since EMA started tracking such activity in 2012, the majority of enterprises now outsource at least some network management functions. In EMA's 2014 Megatrends research, only 36% of network management professionals said their organizations were outsourcing aspects of network monitoring and management to a management services provider (MSP). This year that percentage jumped to 51%.

Figure 13 reveals that a much of the growth in outsourcing was driven by large enterprises. In fact, 55% of small companies indicated they still don't outsource any network management. Financial companies (65%) were also outsourcing network management more aggressively.

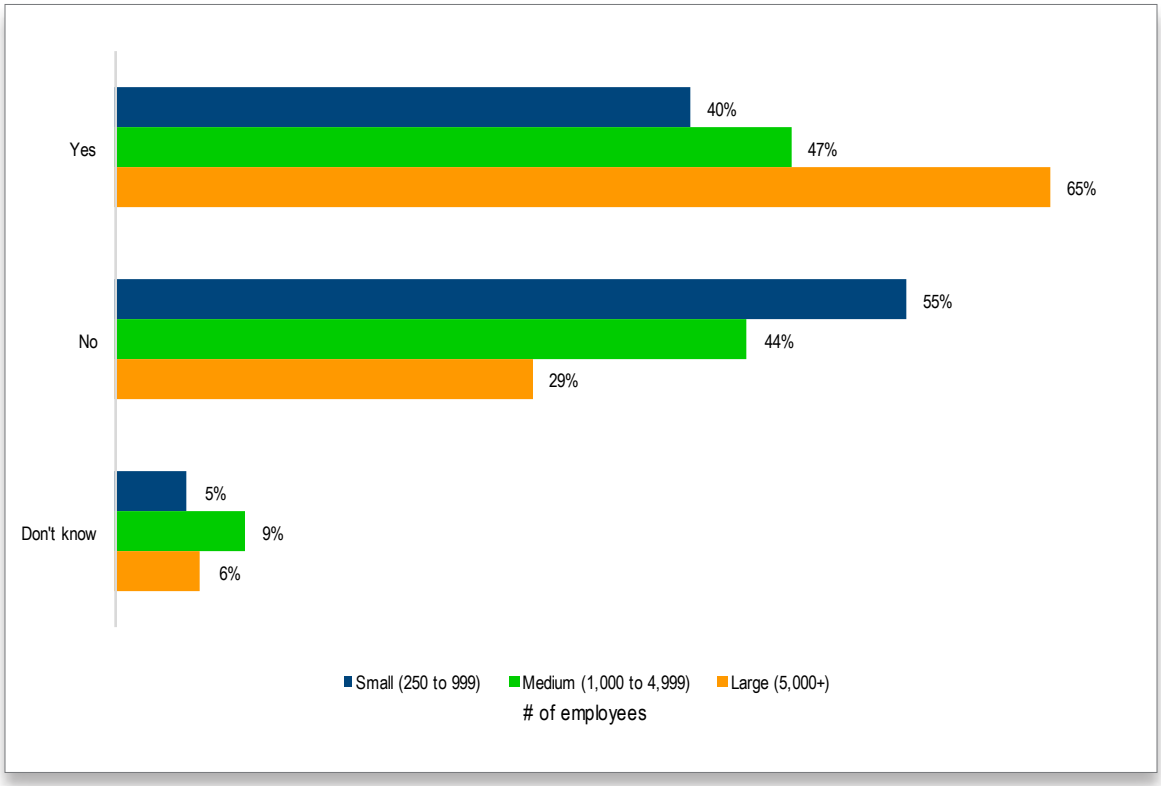

Figure 13. Are any aspects of your organization's network monitoring and management activities provided by an MSP (Management Services Provider)?

The two management functions that were the most popular targets for outsourcing—24x7 network health monitoring and remote site networking—remain unchanged from 2014. However, **Figure 14** reveals that Layer 1 support (help desk calls) emerged as a much more likely target for outsourcing. In 2014, it was the least likely function to be outsourced. In 2016, it was the third most popular.

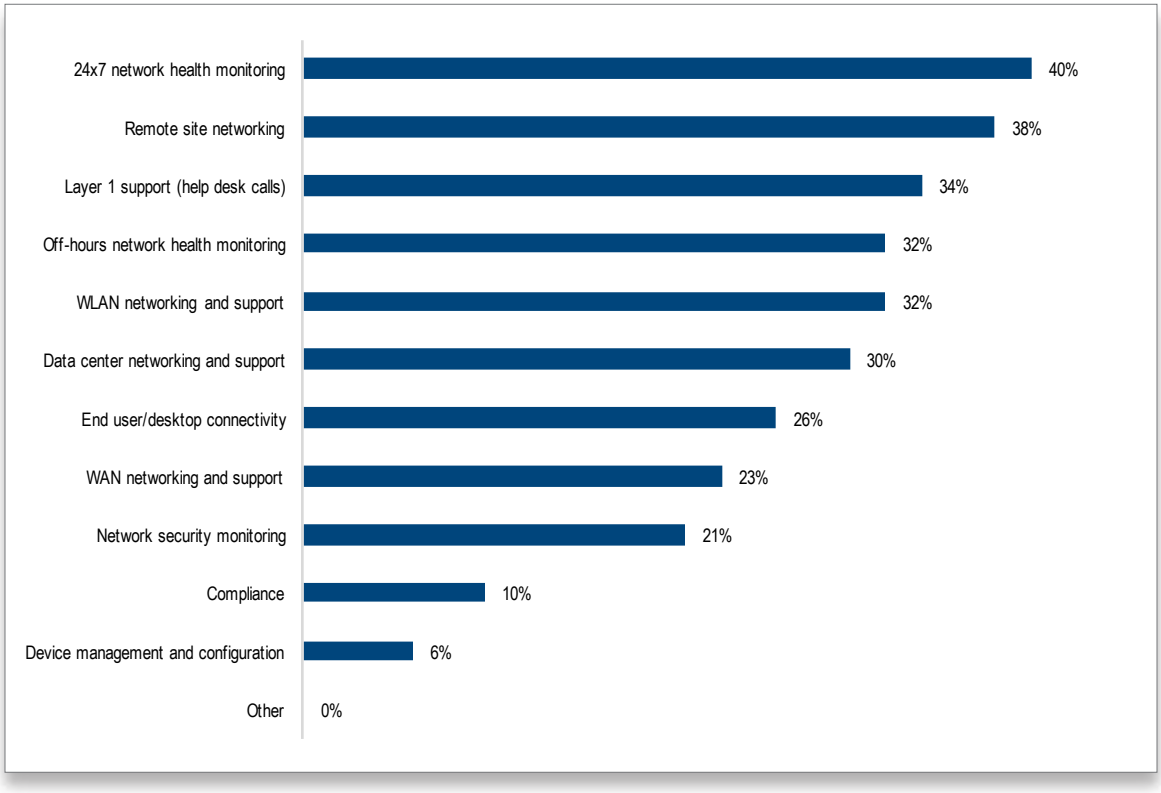

Figure 14. Which of the following network management functions are outsourced?

Large firms were the most likely to outsource 24x7 network health monitoring (52%), off-hours network health monitoring (48%), and WLAN networking and support (42%). The small enterprises that outsourced network management tended to have very different functional priorities. Forty-seven percent (47%) of them were outsourcing remote site networking, and 41% were outsourcing data center networking and support.

Given the rise in network management outsourcing detected this year, further research into network management outsourcing is warranted. In a future study, EMA will examine the challenges and benefits of such outsourcing more thoroughly.

The two management functions that were the most popular targets for outsourcing—24x7 network health monitoring and remote site networking.

Data Sources for Network Management: Log Files Decline in Priority

In EMA's 2014 Network Megatrends study, log files emerged as the most commonly used data source for network capacity planning and engineering, sustained network availability and performance monitoring, and network troubleshooting. Sixty-five percent (65%) were using or planning to use log files for network troubleshooting, 52% were using log files for planning and engineering, and 59% were using them for availability and performance monitoring.

Log files have declined in popularity in favor of increased use of synthetic test traffic data.

This year's research shows a significant shift in priorities. Log files have declined in popularity in favor of increased use of synthetic test traffic data. **Figure 15** reveals the data that enterprises are using or planning to use for sustained network availability and performance monitoring. In 2014 log files topped the list of data sources used for this management function, but in 2016 it slipped to sixth place. Packet inspection and network flow data (NetFlow, sFlow, IPFIX, etc.) remain very popular for monitoring, but synthetic test traffic data emerged from obscurity to become the number two data source for monitoring in 2016.

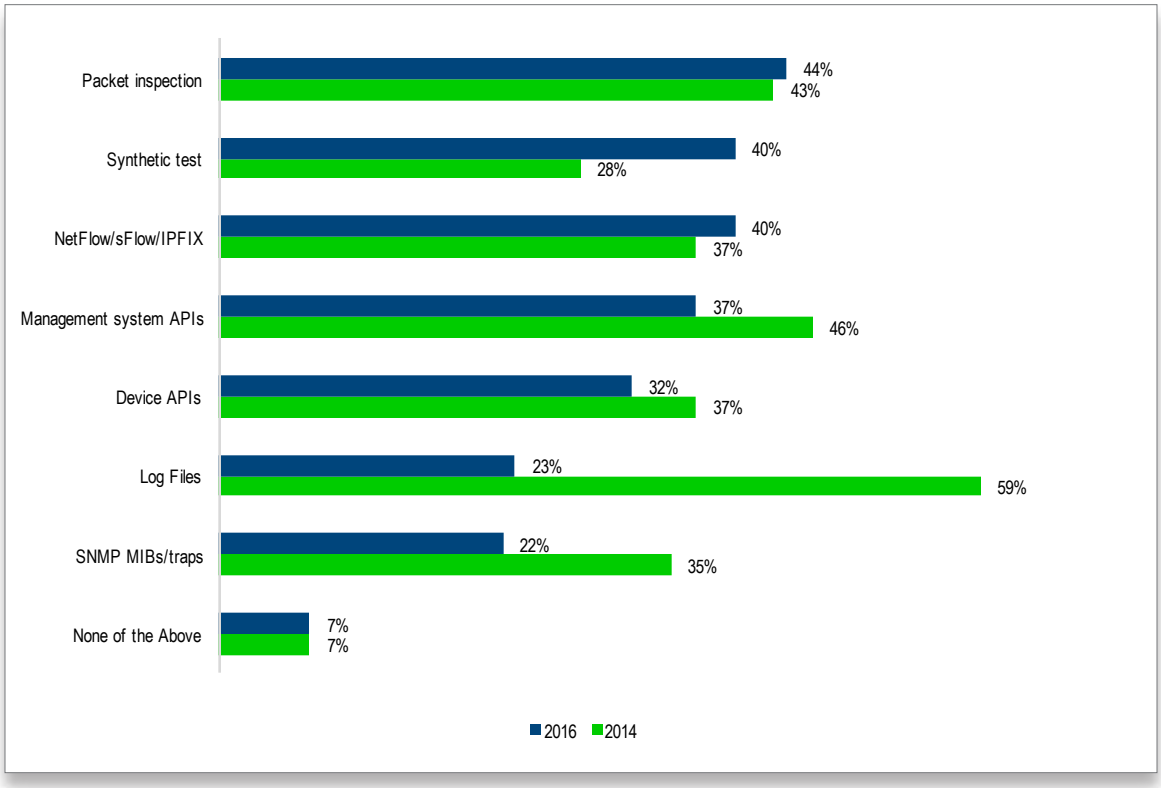

Figure 15. Which of the following data sources is your organization using/planning for sustained network availability and performance monitoring?

EMA suspects that the growing popularity of cloud-based services, particularly software-as-a-service (SaaS) applications, is a driver of the synthetic test data as a source for monitoring. Given that enterprises have limited visibility into the infrastructure of SaaS application providers, several solutions have emerged in the last few years that use synthetic test data to emulate SaaS end-user experience. As enterprises make more strategic use of SaaS applications, they need better visibility into the health and performance of these applications.

To a lesser extent than log files, SNMP MIBs and traps also declined significantly in importance, going from 35% in 2014 to 22% in 2016. EMA has long observed that network management professionals consider SNMP to be an imperfect technology for collecting network metrics due to concerns about scalability and impacts on infrastructure performance. This decline in SNMP's utility could be a reflection of this simmering dissatisfaction, especially in light of the fact that several network infrastructure vendors have introduced new streaming telemetry features on their switches and routers that could serve as SNMP replacements in some circumstances.

Log files also declined in importance as a data type used for network capacity planning and engineering. With more than half of enterprises using or planning to use it for capacity planning and engineering in 2014, it was the top data source two years ago. This year, log files are only the sixth most popular data source for this use case.

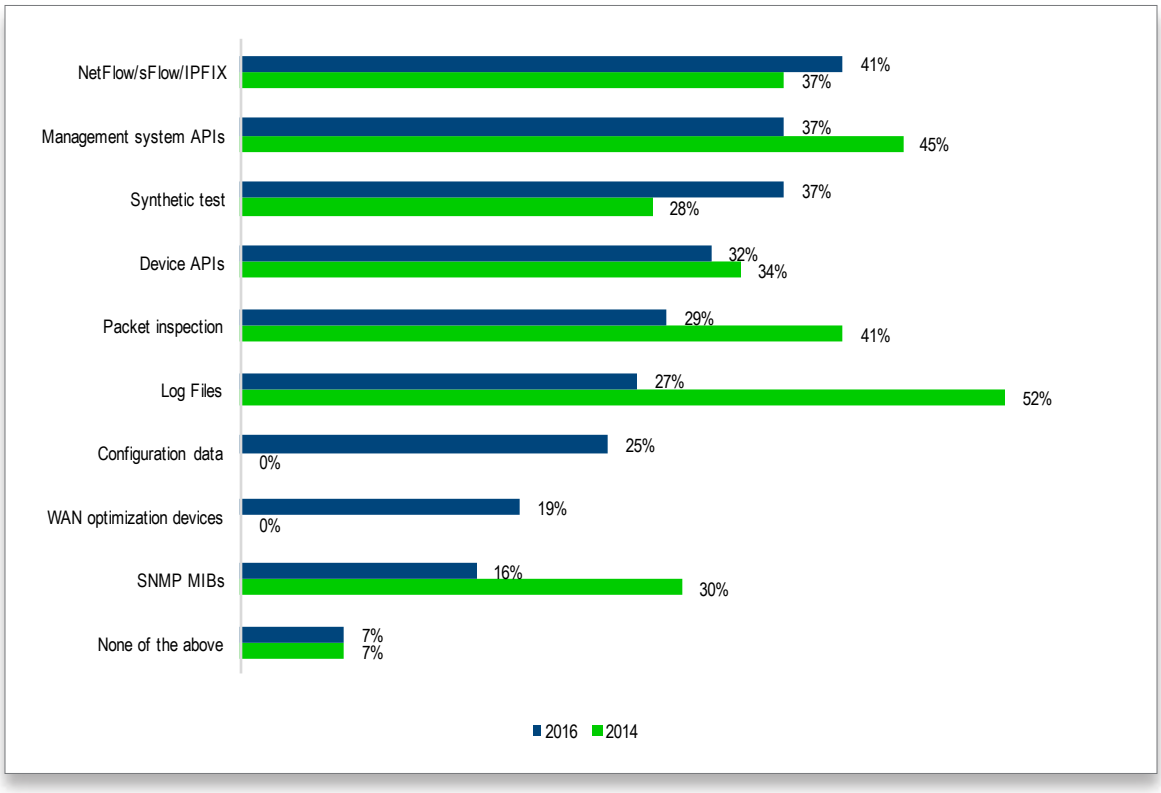

Figure 16. Which of the following data sources is your organization using/ planning for network capacity planning and engineering purposes?

Synthetic test data emerged from obscurity for capacity planning and engineering use cases, much as it did for monitoring. In 2014, it was the least popular data source for planning and engineering, and in 2016 it ranked third. Meanwhile, network flow data emerged as the most popular data source in this category, and management system APIs maintained their position as the second most popular. The popularity of NetFlow and other network flow technologies makes sense, given this technology's ability to provide application-aware insights into network traffic patterns, a critical consideration when planning network capacity. One would expect packet inspection data to also be valuable for the same reason; however, it remained relatively less popular.

Based on input from the industry, EMA decided to poll users on configuration data and WAN optimization device data for the first time. Both data sources proved to be of minor importance for planning and engineering tasks.

Finally, EMA explored the data sources enterprises are using for network troubleshooting. **Figure 17** shows the variation in responses from 2014 to 2016. Two years ago, log files emerged as the top data source, just as it had for monitoring, planning, and engineering. The oft-used ping function was the number two data source. This year, ping declined tremendously in value. Log files and packet capture and analysis remained relatively as important, although the overall percentage of enterprises that use both has dropped significantly.

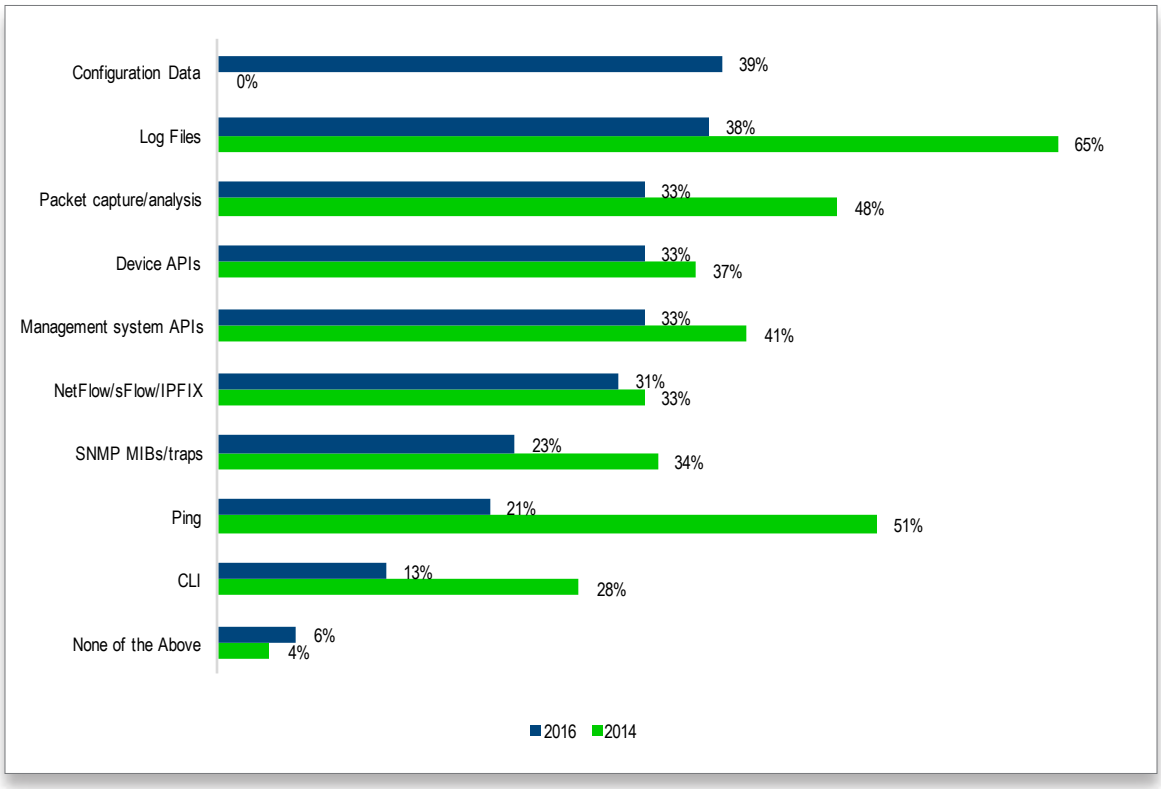

Figure 17. Which of the following data sources is your organization using/planning for network troubleshooting purposes?

Based on industry feedback, EMA added "configuration data" as an option for this question, and it emerged as the top data source for troubleshooting. The popularity of configuration data may be tied, in part, to the rising use of the NETCONF protocol and the YANG modeling language for network infrastructure management. NETCONF can retrieve a variety of configuration data from network devices, and YANG-based management systems can model network state based on that configuration data. Such a capability can be valuable in network troubleshooting.

The popularity of configuration data may be tied, in part, to the rising use of the NETCONF protocol.

Network Operations Success

EMA asked respondents to assess their overall level of success. Nearly half of companies (49%) rated their network operations as "successful" while many others (41%) rated themselves as only "somewhat successful." The rest (10%) were neutral, saying they were "neither successful nor unsuccessful."

This high rate of success emerged despite the fact that earlier in this research EMA discovered that 40% of all network problems were detected and reported by end users before network operations was aware of them. And, as noted earlier, network teams spend more than 70% of their time fixing problems (either in reactive or proactive postures) and just 29% of their time on tasks and projects that could deliver additional value to the business. From EMA's point of view, these statistics reveal a troubling lack of operational effectiveness. But given the context provided by years of research, these numbers also represent a status quo that network operations teams are extremely familiar with. From their perspective, they are doing as well as can be expected. However, EMA argues that there is significant room for improvement.

Nearly half of companies (49%) rated their network operations as "successful" while many others (41%) rated themselves as only "somewhat successful."

The full Network Megatrends 2016 report contains data on the top challenges to and the top benefits of network operations success. It also examines evolving network management tool requirements and organizational trends in network operations. Finally, it examines each of the above megatrends in more detail. For a deeper look at the findings of this research, download the full report.

Case Study: Leading Financial Software Company Unifies Network and Application Monitoring with Riverbed SteelCentral

Riverbed's SteelCentral suite of network performance management (NPM) and application performance management (APM) solutions has become essential to hybrid cloud operations at one of the world's leading financial software companies. IT operations uses the SteelCentral suite to monitor and troubleshoot end-to-end application and network performance for a hybrid cloud infrastructure that comprises nearly 20,000 on-premises servers, 2,500 switches and routers, and 14,000 public cloud workloads.

The company, which offers dozens of financial software products and SaaS services, uses SteelCentral AppResponse for network-based application performance monitoring; SteelCentral AppTransaction Analyzer for transaction trace analysis and performance prediction; SteelCentral AppInternals for code-level application performance management; and SteelCentral NetSensor for SNMP-based and network flow–based network availability and performance monitoring. Finally, the company uses SteelCentral Portal to integrate these various monitoring solutions into a unified platform that provides end-to-end infrastructure visibility.

SteelCentral Portal Unifies NPM and APM

According to a lead network engineer at the company, Portal's ability to unify SteelCentral solutions is especially critical because the IT organization uses 75 individual tools to monitor its infrastructure.

"On the application side, when we have an event at an application tier, we have so many tools and alerts that it's hard to find what is specifically impacting that application," the engineer said. "We end up with a lot of alerts that can be cumbersome to correlate."

SteelCentral Portal features an application dependency map view that correlates and displays data from all installed SteelCentral monitoring products in a unified manner. This unified view can see through the alert storms generated by the company's many other monitoring products. The company's engineer said he is also able to build customized dashboards in Portal that other groups in the IT organization can use to better understand application and network events.

How SteelCentral Improves Application and Network Troubleshooting

The engineer said SteelCentral was recently instrumental in troubleshooting a performance issue that degraded a variety of core enterprise applications.

"We used Riverbed AppResponse [to analyze networked application performance] and reviewed it in Portal," he said. "We found a whole bunch of servers that were processing data that used similar naming conventions and tracked down where the data was coming from."

The engineer traced the issue to a flood of data that was streaming into the company's internal infrastructure from the public cloud. The company's fraud analysis team was analyzing end-user transaction records for one of its SaaS-based financial applications. The analysis involved collecting metadata from hundreds of thousands of transactions that had been processed in the public cloud and sending it to an internal data center for analysis. While the company's hybrid cloud infrastructure is designed to scale rapidly, this influx of transaction data grew too fast and flooded one of the company's network interlinks.

"One of our interlinks that was scheduled for an upgrade was choked," the engineer said. "We were doing 7 gigabits per second for the fraud analysis plus the 2 gigabits we need just for day-to-day operations. We cut off that data, which annoyed the fraud analysis guys. Then we negotiated with them that they could do 200 megabits of data collection during the day and then an overnight period of 1 gigabit collection. It took them longer to get all the data, but they got it in time."

As the company consolidates application architectures, this unified approach to network and application monitoring only continues to become more valuable. For instance, each of the company's dozens of SaaS products once had siloed architectures, but now the company is centralizing many back-end services. This approach delivers a unified experience to end customers, but it also makes effective network operations more essential.

"When I started here, every business unit had its own authentication scheme and customer service connection," the engineer said. "We've tied all that together, so when you log in we know who you are and we can link different types of data from different applications together. When a core service like identity management is slow, it can have a cascading impact across multiple businesses and customers."

The engineer said he is able to identify critical core network and application services problems with SteelCentral Portal, where he can combine network (AppResponse) and code-level application performance visibility (AppInternals) with SNMP-level network visibility (NetSensor). Portal's dependency mapping can show him how all these different infrastructure layers combine to deliver core services, which allows him to detect and troubleshoot problems quickly.

The company's SteelCenral installation fulfills more than just monitoring and troubleshooting functions. The custom dashboards the engineer builds in Portal are also consumed by the engineering team.

"I build stuff for them from a capacity planning perspective," the engineer said. "They will want to build this or that, and they can see whether bandwidth needs upgrading or a load balancer or firewall needs replacing. We're trying to lead the [financial software] industry, and this visibility supports that. By building these customized dashboards in Portal, I can allow other groups to consume it. They can access the data without having to learn [the process of acquiring] the data."

Megatrends Experiences

Hybrid Cloud – With 20,000 servers in its internal data centers and 14,000 workloads in the public cloud, this financial software company has clearly embraced the hybrid cloud. Its multi-tiered applications span internal and external cloud infrastructure, which makes end-to-end visibility across public and private clouds essential to infrastructure operations.

The Overcrowded Network Management Toolset – The IT organization has clearly identified the challenges it faces with more than 75 IT monitoring tools in use today. The unified visibility offered by the SteelCentral suite monitoring and SteelCentral Portal has helped IT operations see past alert storms and get to the bottom of what's affecting application performance.

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 blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn.

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

3362-Riverbed_SUMMARY.042616