EMA RESEARCH REPORT: NETWORK PERFORMANCE MANAGEMENT FOR TODAY'S DIGITAL ENTERPRISE

ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) Research Report
Written by Shamus McGillicuddy
May 2019

SPONSORED BY: ManageEngine
Powering IT ahead

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

TABLE OF CONTENTS

TABLE OF CONTENTS

Executive Summary

IT operations teams often struggle to assemble an effective network performance management (NPM) toolkit, because the market is increasingly complex. There are at least half a dozen classes of technologies that claim to manage network performance, yet they all offer very different views of the network. Moreover, the number of NPM use cases is expanding. Network operations monitoring, network troubleshooting, and network capacity planning remain core use cases. However, enterprises also use NPM tools for security monitoring and cloud application migration assessments.

This summary of new EMA research offers a guide to evaluating NPM technologies and establishing a tool strategy that meets every use case an enterprise might have for such solutions. However, it is not a vendor comparison study. In fact, the reader will find almost no mention of specific vendors. The research draws on survey data and one-on-one interviews with IT professionals to understand how IT organizations are selecting, implementing, and using NPM tools. It identifies key technology requirements, industry challenges, and potential best practices. The key finding is this: There is no such thing as the ideal NPM platform. Every enterprise has its own unique needs that defy the possibility of a silver bullet for all. Instead, this research shows how enterprises assemble their own ideal NPM platforms based on partnerships with key vendors and some good old-fashioned hard work.

> ***This research will not establish that there is a single, ideal NPM platform that will address the needs of the universal enterprise. Rather, enterprises must assemble that platform themselves through vendor partnerships, systems integration, and rigorous best practices.***

Introduction

The term “network performance management” (NPM) has always been imperfect and imprecise. EMA research typically finds that enterprises vary widely in their approach to “managing” network performance. Enterprises today apply at least half a dozen classes of technology to the task.

Some network operators will tell you that the most important NPM tool in their enterprise is a system that collects metrics from switches and routers via Simple Network Management Protocol (SNMP) polling and traps. Meanwhile, many network engineers will scoff at this, telling you that visibility into network performance requires network traffic monitoring…but how deep does that visibility into traffic need to be? While some network managers can succeed with a tool that analyzes NetFlow records, others require packet analysis.

Moreover, the use cases that NPM tools serve are diverse. The first thing that comes to mind is the sustained monitoring of the health and performance of networks and networked applications.[1] Of course, NPM tools are also essential to troubleshooting health and performance problems. Next up, many enterprises use these tools to plan and manage network capacity. More recently, EMA found that NPM tools are important to security monitoring. Also, with so many applications migrating to external public clouds, network engineers are using NPM tools to assess the network requirements of applications targeted for cloud migration.

In reality, IT organizations combine multiple tools to address their NPM use cases, which presents a complicated picture. If there isn’t a silver bullet for addressing the various NPM use cases, who is going to help them cobble together a solution?

That’s the question EMA wants to answer. Given the diversity of tools and use cases, EMA is launching ongoing research that takes a deep, comprehensive look at how enterprises use NPM technologies. This inaugural study, based on a survey of 250 enterprises and one-on-one interviews with half a dozen subject-matter experts, answers fundamental questions about NPM technology strategies and best practices. This research will not establish that there is a single, ideal NPM platform that will address the needs of the universal enterprise. Rather, enterprises must assemble that platform themselves through vendor partnerships, systems integration, and rigorous best practices. Vendors are here to help, but it’s really up to your IT organization to identify the best path forward. This research , based on a survey of 250 North American and European enterprise IT professionals and one-on-one interviews with a half-dozen NPM practitioners, offers a map to help you find that path.

[1] For the rest of this report, EMA will refer to that monitoring as “network operations monitoring.”

Key Findings

- The top drivers of NPM strategies today are network security, the Internet of Things, AIOps, hybrid and public clouds, and data center software-defined networking.
- The majority of enterprises are significantly expanding their NPM investments in the next 24 months, primarily to address requirements for new functionality.
- Security monitoring and incident response have emerged as critical use cases.
- Enterprises prefer fully-integrated, multi-function NPM tools over multi-tool strategies. However, they rarely achieve this goal. The typical enterprise has three to six tools installed.
- Management system APIs are an essential source of data for NPM platforms. While device metrics and traffic data are extremely valuable, data pulled from other systems provides essential context. Other data priorities vary by use case and the specific requirements of individual enterprises.
- Enterprises are integrating NPM tools with IT service management, security monitoring, IT/cloud orchestration, DevOps automation, and cloud monitoring systems.
- An NPM tool must be able to correlate multiple sources of data. This correlation assists with assessing application performance, detecting security incidents, and understanding end-user experience.
- Correlating insights across multiple NPM tools is also a priority, and enterprises vary in how they do this.
- Top functional requirements of NPM tools include traffic volume analysis, network traffic visualization, advanced analytics, and end-to-end path analysis.
- Enterprises are using embedded AIOps features in their NPM tools for a variety of use cases.
- Top challenges to NPM tool usability are lack of real-time insights, lack of granular data, and conflicting or inaccurate data.
- Enterprises are particularly concerned with the security risks associated with collecting data from the network.

Drivers of NPM Tool Strategy

Technical Initiatives That Influence NPM Decisions

The technology initiative on which an enterprise focuses will influence an IT organization's NPM tool strategy. For instance, public cloud investments will force the IT operations team to update its tools to provide visibility into cloud resources. **Figure 1** shows the general technology initiatives that are most influential on NPM tool strategies today.

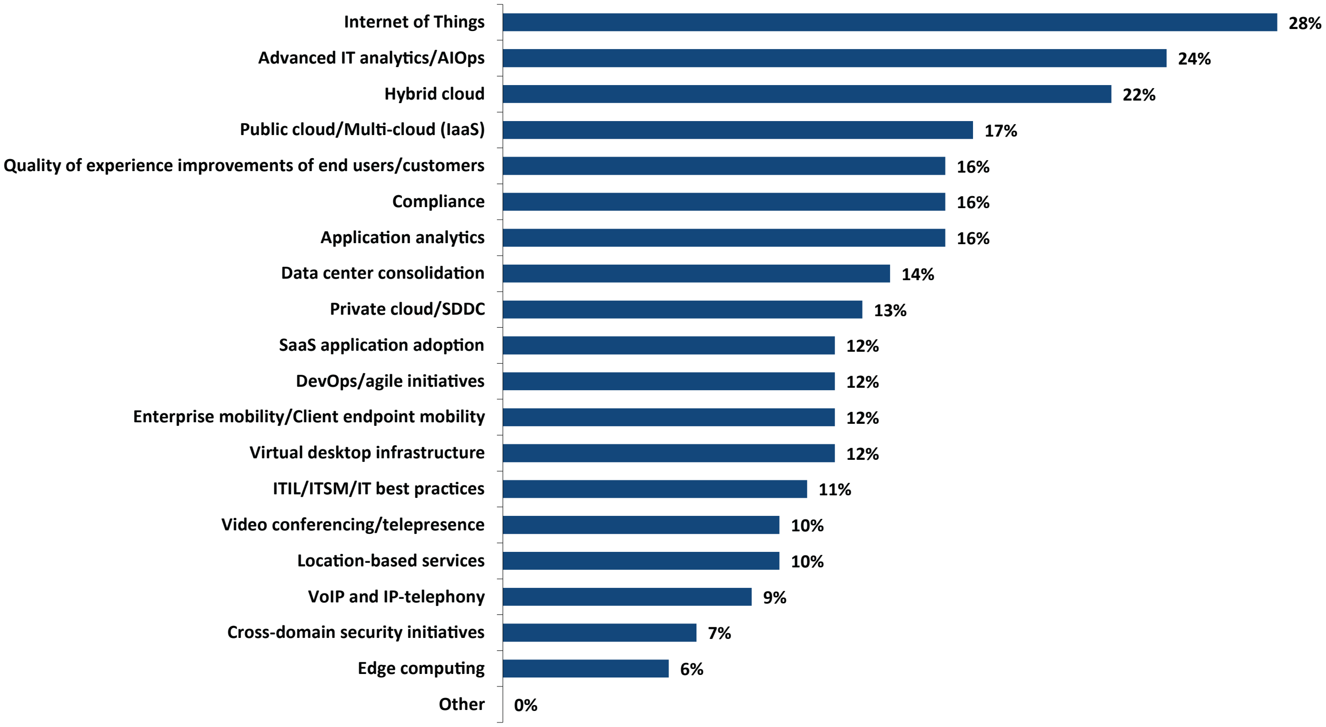

Figure 1. General technology initiatives most responsible for driving NPM tool strategies

The Internet of Things (IoT) is the most prominent driver. From an NPM perspective IoT can, among other things, increase network traffic, introduce new application protocols, and present new security and compliance challenges.

Advanced IT analytics (or AIOps) is another major driver, which suggests that network managers are streaming their data to analytics tools, or they are adding AIOps capabilities directly to their tool to enhance their value.

Hybrid cloud and public/multi-cloud round out the top four initiatives. EMA research consistently finds that cloud projects are disrupting network operations and NPM tool strategies. The lack of administrative access that IT organizations have to public cloud infrastructure forces them to evolve their tools.

Given the nominal networking focus of NPM tools, **Figure 2** zooms in on the network technology initiatives most influential on NPM strategies. Network security is the standout driver on this list, which is a bit unexpected given the low priority of cross-domain security initiatives revealed by Figure 9. This distinction suggests that NPM experts are thinking about network security technology in particular, such as remote access solutions, firewalls, and intrusion prevention. Cyber security projects like threat monitoring and data loss prevention are probably less relevant. Respondents from the IT analytics group were very likely to cite network security as a driver (59%), but only 19% of people in the IT management tool architecture and engineering group called it out, suggesting that the people who actually buy and implement NPM tools don't give network security a lot of thought while evaluating solutions.

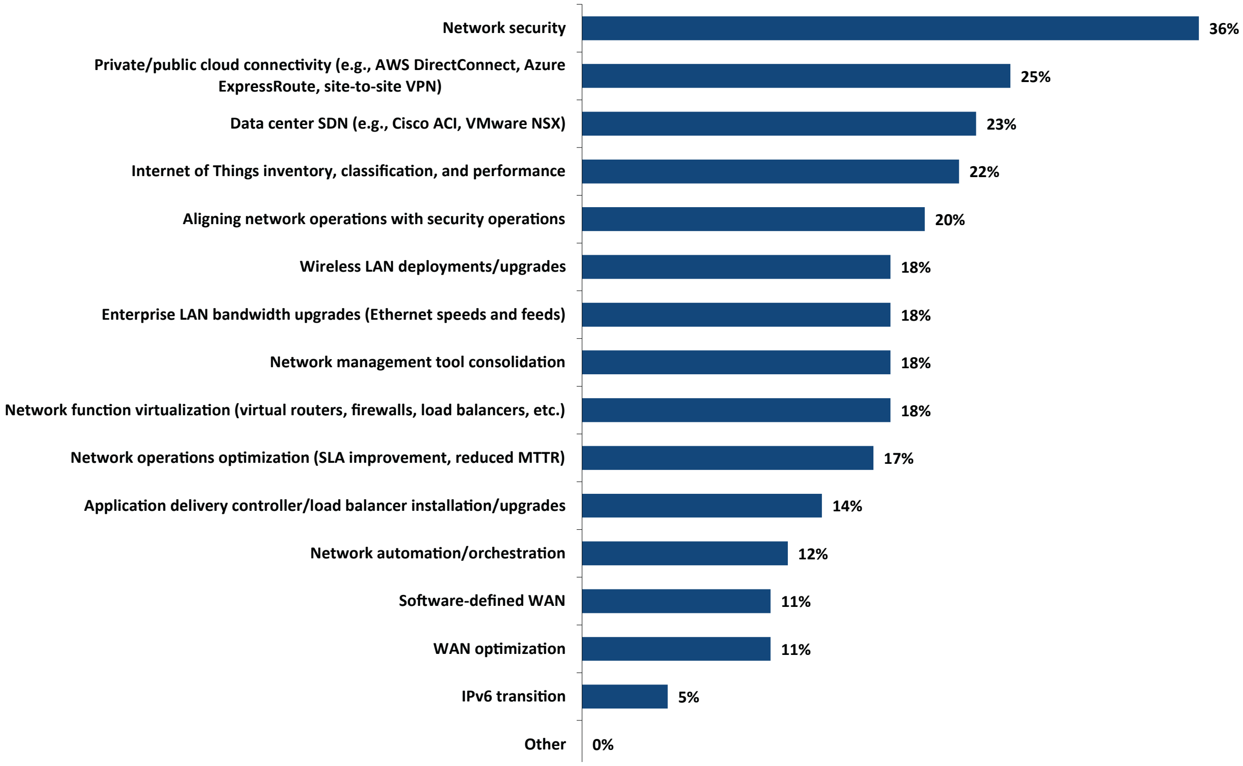

Figure 2. Network technology initiatives most responsible for driving NPM tool strategy

Cloud interconnects between private data centers and public clouds, such as AWS DirectConnect, are also influential, and cross over with the cloud initiatives observed in Figure 10. Network engineers have repeatedly told EMA in previous cloud-focused research projects that these cloud interconnects require constant monitoring.

Data center software-defined networking (e.g., Cisco ACI and VMware NSX) are also highly influential. These solutions tend to support a major uptick in East-West traffic in highly virtualized environments, which can be hard to manage and monitor with NPM solutions.

IoT inventory, classification, and performance are significant drivers, as is alignment of network operations and security operations. In the latter case, EMA previously found that more than 90% of network managers are formally collaborating with their security operations team, and they identified NPM as the number-one tool in their toolkit for enabling that collaboration.[2]

[2] EMA, “Network Management Megatrends 2018: Exploring NetSecOps Convergence, Network Automation, and Cloud Networking,” April 2016.

NPM Tool Business Requirements

Figure 3 reveals the business requirements that currently shape an enterprise's NPM tool strategy. Four things stand out as most important: ease of use, affordability, flexible deployment options, and scalability. Highly distributed enterprises (500 or more remote sites) were particularly interested in flexible deployment options (39%), and also active user communities (26%), which are otherwise a low priority.

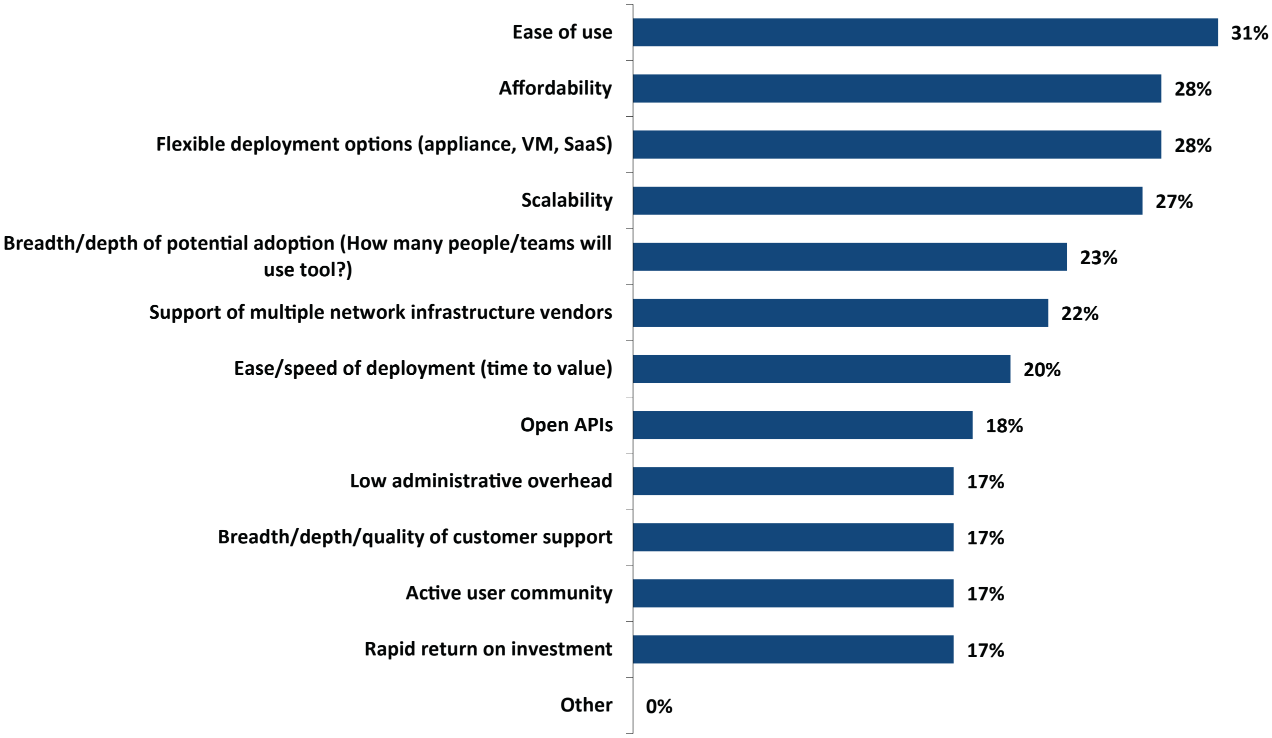

Figure 3. Most important business requirements for NPM tools

Ease of use was the clear standout among requirements. Not every user of an NPM tool is going to be a certified engineer. IT generalists responding to help desk tickets need to get something out these tools, too.

"User friendliness is important. I'm looking for innovation in the user interface to have better-defined workflows and the ability to adapt it," said a network operations analyst with a midsized North American transportation company.

"We have some fairly large teams with varying levels of skill, so the last thing we want is a complex tool that overwhelms junior engineers," said a senior network engineer with a large North American retailer.

This sentiment also applies to one of the secondary prominent business drivers: breadth and depth of potential adoption. Some enterprises look for NPM tools that can be used by the widest number of people. Larger networks will demand broader adoption, as the network teams become more tiered and different skillsets attack different responsibilities in large networks. In fact, 30% of enterprises with larger networks (1,000 to 4,999 network devices) prioritize potential user adoption, versus only 18% of enterprises with fewer than 1,000 devices.

The business requirements that currently shape an enterprise's NPM tool strategy are ease of use, affordability, flexible deployment options, and scalability.

Affordability is a big factor in the NPM industry, where tools can range wildly in price. Some enterprises take an open-source approach, using free tools to minimize cost, while others will spend millions on the tools and millions more on data acquisition solutions like network packet brokers. Interestingly, respondents working in a network operations center place a higher priority on affordability (50%), versus only 19% of IT tool architects and engineers, who are more likely to manage NPM tool budgets.

"It just goes without saying that [price] is one of the challenges I have. [My packet monitoring solution] is very good, but they have a price premium. It is difficult to get a vendor to realize that a price premium can be challenging," said the managing director of infrastructure at a very large North American financial services company.

Scalability isn't just an issue for the largest networks. Any network engineer will tell you that they need a tool that can scale when the time comes, especially as they shift into the public cloud, where infrastructure can scale out rapidly.

"NPM solutions must scale their data collection and reporting functions to meet ever-increasing network size and speed requirements. The scalability bottleneck in most solutions is the central reporting server. No matter how big a server is used, it can never scale to keep up with the demands of an increasing number of data collectors, storage, and reporting demands. The larger the system deployment, the slower a report can take to generate," said an IT analyst with a very large North American government agency.

Multi-Vendor vs. Single Vendor

One complexing factor in the NPM market is vendor diversity. No one vendor offers best-of-breed solutions across the board. Some excel at analyzing one or two data sources, but not others. Enterprises with a broad set of NPM requirements will often have to compromise between best-of-breed solutions and best-of-suite. Sometimes it's very difficult to know which way to go.

"That's the million-dollar question. You can do best-of-breed, where you evaluate each specific silo that you're working with and get the best tool that does that. Unfortunately, in many cases, those end up being smaller companies and sometimes they get absorbed by large companies that make changes or lose focus on the products. Or, you can go with a solution from a larger, viable vendor that has a unified architecture, where everything was developed in-house, but that's very hard to find," said a senior principal tool engineer with a large North American aeronautics enterprise.

Figure 4 identifies strategic priorities. Nearly half of enterprises prefer a fully-integrated, multifunction platform. Respondents who work in an IT executive suite (58%) and the NOC (63%) are particularly interested in this approach. Of course, strategies don't always translate to reality. In the next chapter, the research will find that very, very few enterprises are able to manage with a single NPM tool. Other groups are more realistic. People from network engineering (0%), the cross-domain support group (0%), network architecture (11%), and the IT tool architecture and engineering team (16%) are often much less focused on adopting a single, multifunction platform.

No one vendor offers best-of-breed solutions across the board. Enterprises with a broad set of NPM requirements will often have to compromise between best-of-breed solutions and best-of-suite.

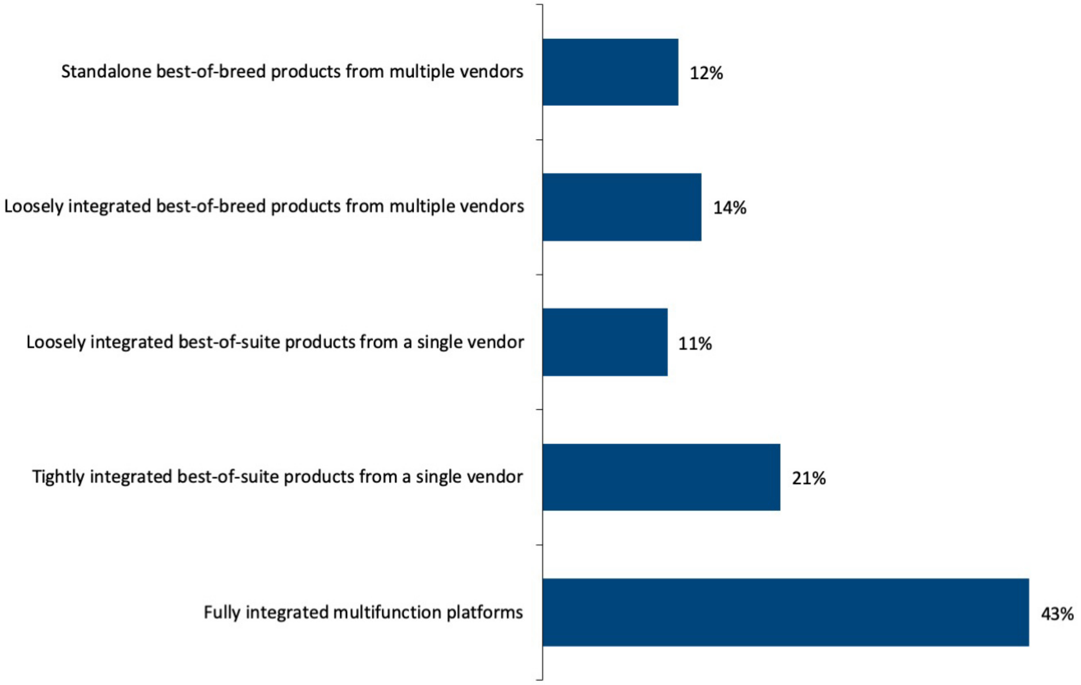

Figure 4. Primary strategy for acquiring, deploying, and using NPM tools

“I prefer best-of-breed tools. They’re aggregated into a custom-built solution designed around my company. I’m not going to get a competitive advantage based on buying stuff off the shelf. It’s about bringing together the power of multiple best-of-breed tools,” said the managing director of infrastructure at a very large North American financial company.

If one tool to rule them all isn’t realistic, enterprises should look for ways to integrate NPM tools to create unified workflows and correlate diverse datasets. There are several ways to approach this. The most popular is a tightly-integrated, best-of-suite strategy from a single vendor, as Figure 15 shows. This is the preferred approach for individuals who consider NPM tools critical to their job (30%) versus only 15% of those who consider NPM tools merely relevant to their role. Many best-of-breed vendors of point NPM solutions now partner with complementary vendors to offer similar benefits. Loosely integrated best-of-breed products from multiple vendors is the number-three priority in this research.

Using standalone best-of-breed products from multiple vendors is the least advisable course, because it can lead to inefficiency in IT operations. Regardless, EMA suspects this is a very common outcome for many vendors, even if it’s a low strategic priority. Some groups even have a pronounced affinity for this approach, including the IT management tool architecture and engineering team (23%), data center operations (22%), and application management (21%).

NPM Tools: What Enterprises Use Today

Data Drives the Platform

NPM means many things to many people. One way to understand an enterprise's approach to NPM tools is by identifying the data the tools collect and analyze. EMA assumes that enterprises typically use multiple tools that collect multiple types of network data. However, EMA asked survey participants to identify the single most relevant and important source of data collected and analyzed by their NPM toolsets.

Critical NPM Data Sources

Figure 5 shows that management system APIs are the most important source of data. This is interesting on multiple levels. First, enterprises see tremendous value in data generated by other IT management systems, whether it's a trouble ticket from a service management platform, configuration data from a network change and configuration management system, or events generated by a tool that monitors other infrastructure domains, such as application performance or security. Second, multiple classes of NPM tools can be modified to consume and correlate this data, whether it's a packet monitoring tool or an SNMP polling system. Essentially, management system APIs are a secondary data source for any number of NPM tools, used to enrich and contextualize the data that the tool collects directly from the network.

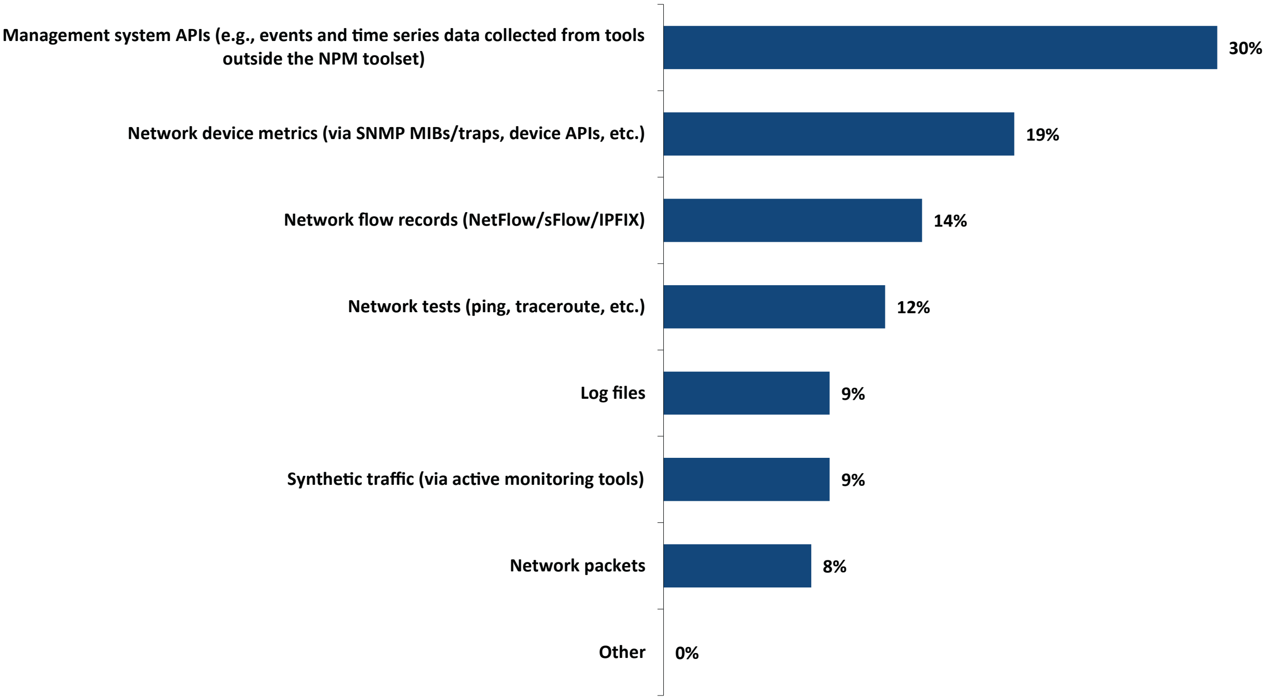

Figure 5. Enterprises identify the single most relevant and important source of data collected and analyzed by their NPM tools

Infrastructure metrics collected via SNMP MIBs and traps and network device APIs are the next-most important data source. This is the core network data source for performance monitoring. When a hiring manager is scanning resumes for job candidates with NPM tool experience, this is the type of tool the majority of them are going to highlight. Tools that specialize in SNMP-based metrics typically excel at discovering network devices and monitoring their health and performance.

"SNMP stats are most valuable. They provide more information about what kind of device I'm dealing with and where it is located," said an IT analyst with a very large North American government agency.

"For me, it's the packets running down the wire. You do need to complement it with other statistics, like CPU and memory utilization, but I'm not a fan of SNMP. I might revert to CLI interaction to troubleshoot," said the managing director of infrastructure at a very large North American financial company.

"Real packet capture is ideal. It allows us to send the raw performance metrics to some sort of analytics engine that crunches the data," said a senior network engineer with a large North American retail company.

Everything else in Figure 16 is essentially tied for third. Network flow records, such as NetFlow, have an edge on the rest. Many tools that support the two most popular data sources listed in the chart will also offer some rudimentary NetFlow analysis features to give insight into traffic. However, there is a robust market of specialist vendors that provide much deeper analysis of network flows.

Packets are at the bottom of this list. Packets provide an extremely granular view of network traffic. Ideally, they are the best source of data for an NPM tool, but packets are also the most resource intensive data to collect and analyze. As a result, many enterprises use other data sources for sustained, broad monitoring of the network and use packet-based monitoring in strategic places. In fact, enterprises with moderately-sized networks (1,000 to 4,999 devices) are more likely (13%) to select packets as their most critical data source, versus just 2% of enterprises with large networks (5,000 or more devices). IT management tool architectures and engineers are also more likely to select packets (16%).

> *"SNMP stats are most valuable. They provide MORE information about what kind of device I'm dealing with and where it is located."*
>
> - Senior principal IT tool engineer, large North American aeronautics company.

> *"It's the packets running down the wire. You do need to complement it with other statistics, like CPU and memory utilization, but I'm not a fan of SNMP. I might revert to CLI interaction to troubleshoot."*
>
> - Senior principal IT tool engineer, large North American aeronautics company.

Size of NPM Toolsets

Over the years, EMA's network management practice has found that enterprises rarely use only one tool for network performance management. Although this research found that the strategic priority is a fully-integrated, multifunction NPM platform, in practice, very few enterprises achieve this strategy. There will always be a handful of other tools the network team uses to answer questions the core tool can't answer.

In fact, some enterprises will use redundant tools to deal with product unreliability. "We use two different SNMP tools for redundancy. If the first tool missed something, it will be picked up by the other, whether it's a software issue or a polling issue. We do it to cover our bases," said a network operations analyst with a midsized North American transportation enterprise.

The managing director of infrastructure at a very large North American financial company told EMA that his team uses two core tools: a real-time packet analysis tool and an SNMP-based infrastructure monitoring tool with limited NetFlow monitoring capabilities. In addition, his team uses a handful of other tools that were developed in-house that pull various statistics from the network and compare findings with the data in the core toolset.

> *The typical enterprise has three to six tools installed, but only two to four are used regularly.*

Figure 6 reveals the state of NPM toolkits today. In the chart, the bars represent the number of NPM tools that enterprises have installed. The line reveals how many tools the IT organization uses regularly. There is a clear gap. The curves in the chart suggest that the typical enterprise has three to six tools installed, but only two to four are used regularly.

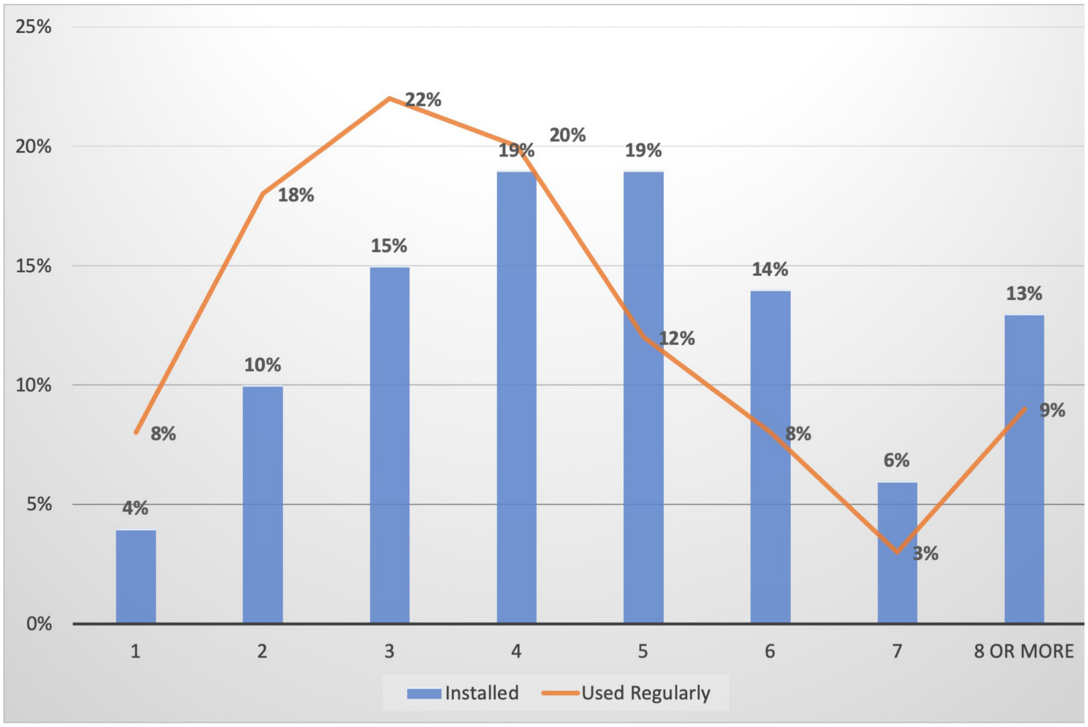

Figure 6. Number of individual NPM tools: installed versus used regularly

Correlating Insights Across Data and Tools

The research has established that enterprises use multiple tools and multiple source of data for network performance management. The key challenge with such a toolset is the ability to correlate insights across those data sources and those discrete tools. EMA zoomed in on this issue in a couple of ways. First, the survey asked participants if they have a tool that can correlate insights across multiple sources of network data, such as packets, flows, device metrics, logs, and management system APIs.

NPM Tools Correlating Multiple Data Sources

Figure 7 reveals that 98% of enterprises have at least one tool that can do this multi-data correlation. Clearly, this is a fundamental requirement of NPM tools. In fact, 50% of enterprises consider this correlative ability essential to IT operations. Criticality of this correlation is even higher among organizations that use five or more NPM tools (60%), versus just 39% of those that use one or two tools. This suggests that IT organizations have core NPM tools that can correlate insights while they use a number of secondary tools to complement them, much as the managing director of infrastructure at a very large North American financial services company noted earlier. Remember that he had a tool that correlated insights across SNMP and NetFlow data, a second tool that provided packet-based insights, and a handful of complementary tools.

98% of enterprises have at least one tool that can do multi-data correlation. 50% of enterprises consider this correlative ability essential to IT operations.

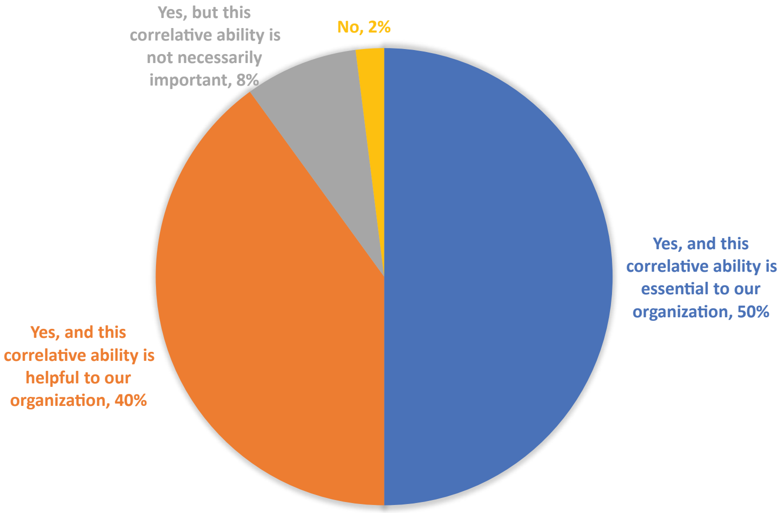

Figure 7. Question: Does your organization have at least one NPM tool that can correlate insights from two or more classes of network data?

Figure 8 identifies ways in which this correlation of data sources in a single tool helps the IT organization. For instance, nine in ten respondents said it enhances their ability to infer application performance insights and detect security events. Eight in ten can glean end-user experience insights, detect anomalous behavior, and proactively prevent problems from impacting users. Seven out of ten say this correlation reduces noise during event management.

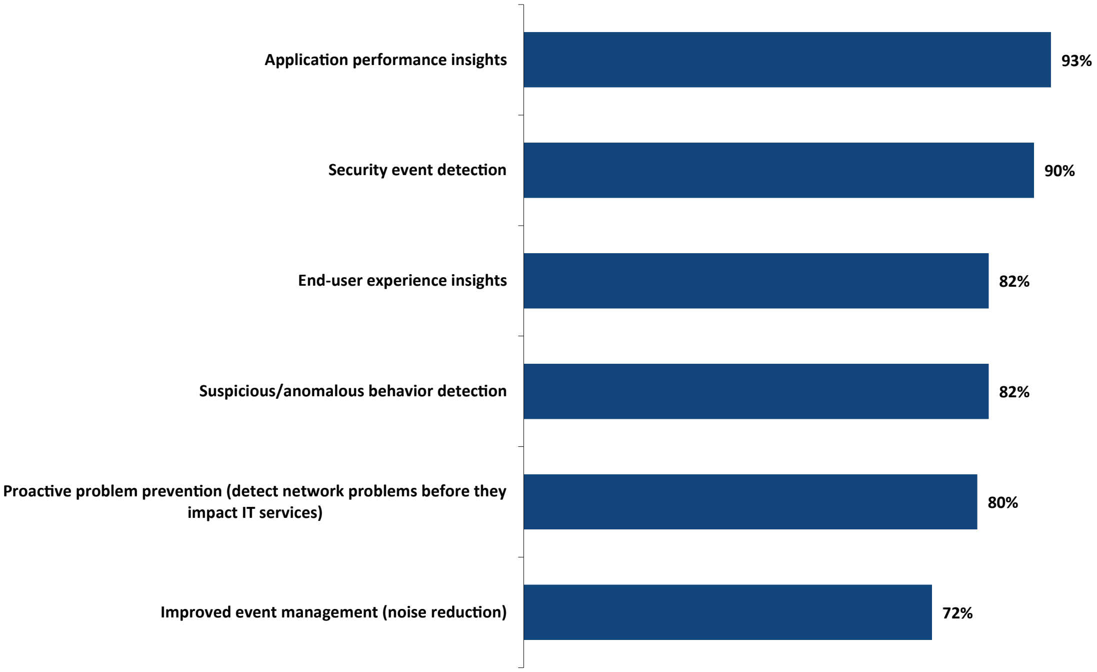

Figure 8. General operational tasks enhanced by correlation of multiple data sources in a single tool

Correlating Insights Across Multiple NPM Tools

EMA asked the 230 research participants who are using more than one NPM tool regularly to identify the primary method they use for correlating insights and integrating workflows across these tools. **Figure 9** reveals that 99% have established some kind of strategy, and most of them are taking a relatively sophisticated path to correlation and workflow integration. For instance, only 7% take an ad hoc, manual approach. Of course, the number of users who actually rely on ad hoc correlation is probably much higher, given that this is a strategic priority, not a description of current state. Also, organizations who identified network flow records (NetFlow) as the most important and valuable source of data for NPM tools were more likely to adopt an ad hoc, manual correlation strategy (11%).

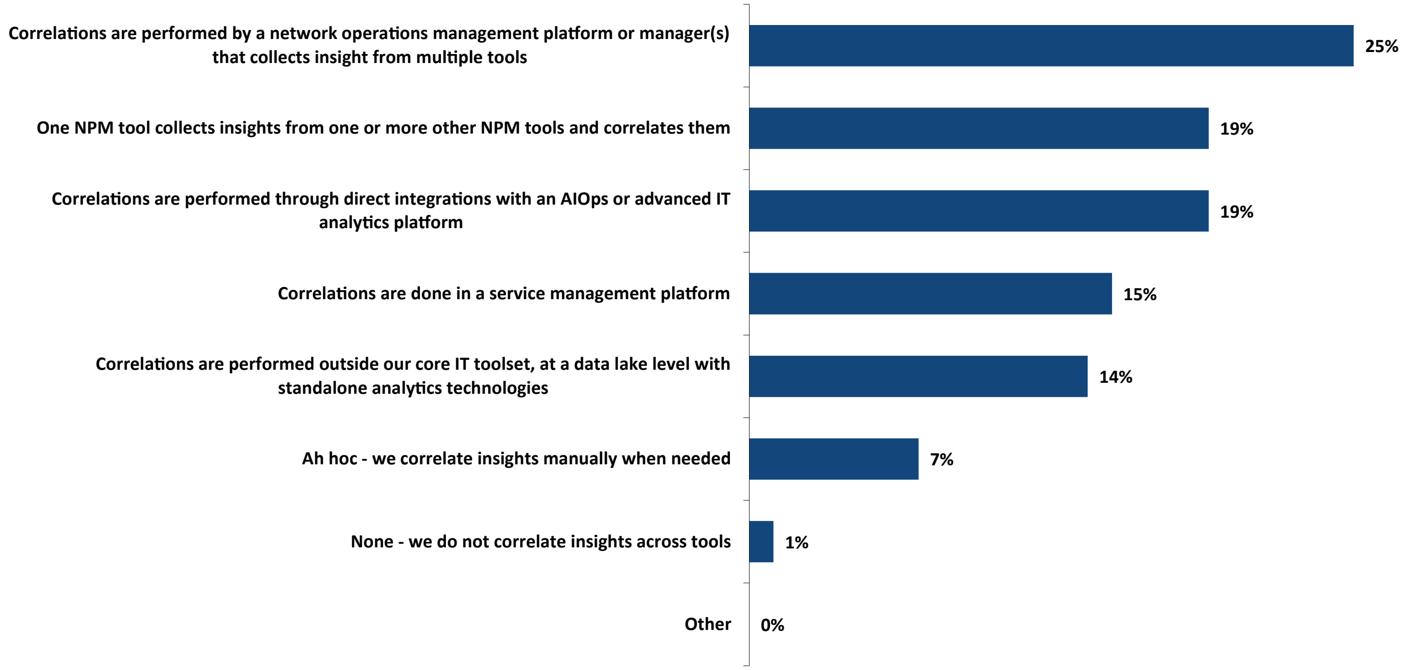

Figure 9. Primary approach to correlating insights and integrating workflows across multiple NPM tools

"Enterprises typically do not have a process for correlating [insights] across tools. I have never encountered a client that had a process for correlation across tools. It's one event at a time, or 'We didn't get an event at all. Why wasn't there an event in our tool?'" said a senior consultant for a medium-sized North American IT operations consultancy.

The most popular strategy is the integration of NPM tools with a network operations platform or manager of manager. "We've built a homegrown management console that pulls information together from multiple tools. It's an application-level view console. Sometimes, the application management team will want one specific [insight] that requires different [correlations], and they will offload data into other management tools," said the managing director of infrastructure for a very large North American financial company.

The other most common approaches to this correlation are the use of an NPM tool that can collect and correlate insights from other tools and the integration of NPM tools with an AIOps or advanced IT analytics platform, where correlation can be done with NPM tools and also other IT operations platforms. The former is more popular in Europe (28%) than North America (16%).

Correlations in a NOC platform or manager of managers was a popular response among application management professionals (47%). Correlation done within a data lake with analytics tools was popular among organizations with 500 or more remote sites (23%) and among people who work within a cross-domain support team (50%) or a NOC (35%). Members of the network architecture group (50%) emphasized integration with AIOps.

EMA asked respondents to characterize their success with correlating insights and integrating workflows across multiple NPM tools. Just over one-quarter rated themselves as very successful, as **Figure 10** details. About half were successful, but not quite as effusive. The rest saw room for improvement.

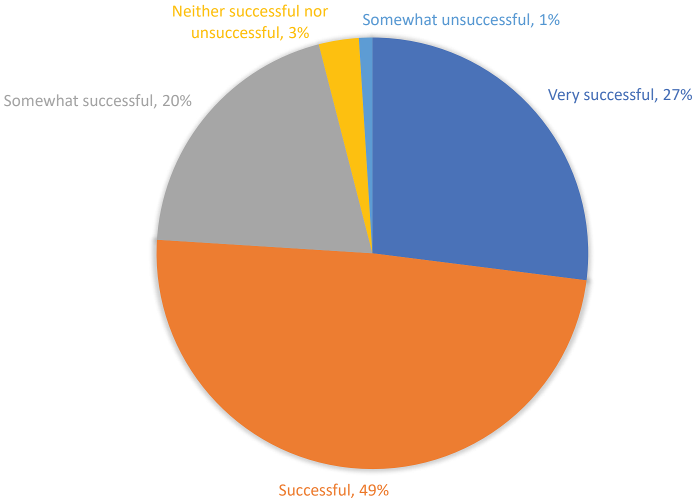

Figure 10. Success with correlating insights across multiple NPM tools

EMA observed some statistically significant affinities between correlation strategies and success. AIOps platform integration was associated with the highest levels of success. Correlation at the data lake-level or within a service management platform was likely to be successful, but not *very* successful. Ad hoc, manual correlation strategies were typically only somewhat successful.

"[Correlation is] difficult to do because we have lots of manual processing and things are highly dynamic with virtualization and vMotion. So, we rely on the experience of the actual operational engineer and their knowledge. We attempted to use a manager of managers using CMDB integration, but that project went nowhere because it means we had to make sure our CMDB was up to date. It just shifted the manual processes burden to the person managing the CMDB," said the senior principal tools engineer at a large North American aeronautics enterprise.

Priorities for NPM Tool Features and Functionality

Overview of Technical Functions

EMA asked respondents to identify their top functionality requirements of NPM tools. **Figure 11** reveals a diverse set of opinions. No single feature was selected by one-third or more of people. Two features stood out from the rest: traffic volume analysis and network traffic visualization. These features help enterprises answer two key questions: How much traffic is on my network? Who is communicating on my network? Correlating the answers to these two questions can give a network manager a good overview of the health and performance of a network.

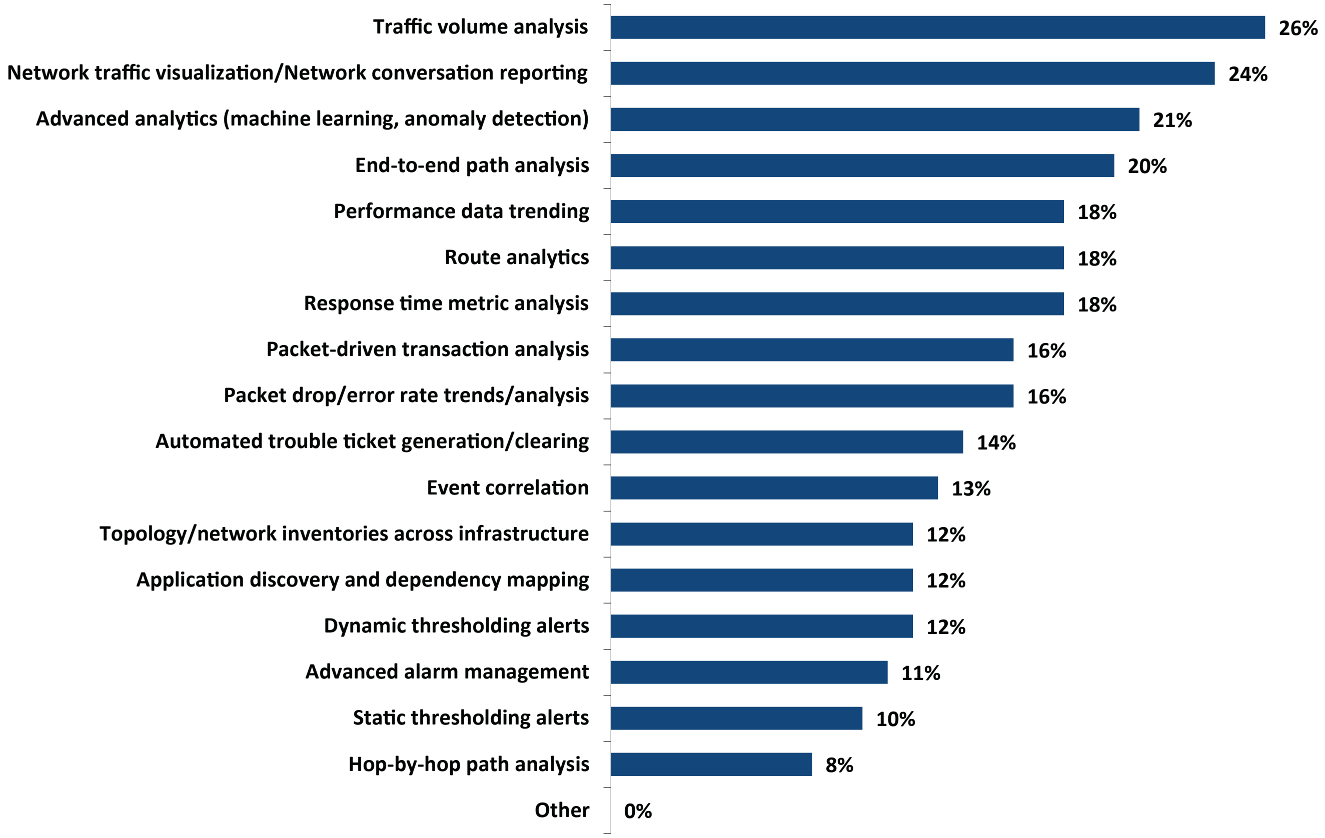

Figure 11. Enterprises rank the most important technical functions of NPM tools

However, these top features are also relatively basic functions. In fact, traffic volume analysis is favored by more organizations with simpler networks. Thirty-four percent of enterprises with fewer than 50 remote sites on the network prioritize this kind of analysis, versus only 18% of those with 50 to 499 sites. Enterprises with fewer than 50 sites are also more likely (25%) to value performance data trending. Those with fewer than 1,000 network devices also favor this trending more than others (25%).

Advanced analytics features are a high priority. NPM vendors are increasingly investing in algorithms that draw on concepts like machine learning and artificial intelligence to add more value and insight to users. Large enterprises (5,000 to 19,999 employees) are especially interested in this capability (32%).

End-to-end path analysis is also prominent, but respondents who describe NPM tools as critical to their job function are less sanguine about it (14%). The same goes for route analytics (only 12% of critically engaged users).

Packet-driven transaction analysis is a moderately important feature, but it is more often important to individuals who identify packets as their top data source for NPM tools (35%). Large enterprises are also more focused on this analysis (23%).

Dynamic threshold alerting, which might also be described as alerting based on observed baselines, is relatively less popular in this context, but one focal interviewee saw tremendous value from it. “Baselining and alerting technology can address business hour timeframes and time zone differences to reduce false positives. These baselines [should be calculated] in intervals of minutes, [but] most legacy products can only calculate baselines hourly. Tighter intervals will provide more proactive monitoring and analysis,” said an IT analyst with a very large North American government agency.

NPM vendors are increasingly investing in algorithms that draw on concepts like machine learning and artificial intelligence to add more value and insight to users. Large enterprises are especially interested.

Advanced Analytics Functionality

This research found that advanced analytics based on machine learning and AIOps concepts are one of the most valuable features of current NPM tools. The majority of vendors today either offer some kind of advanced analytics, or they're investing in such technology for future releases. **Figure 12** reveals that 60% of enterprises are already using advanced analytics embedded in NPM tools, and nearly half of that group consider such features critical to their organization. Another third is planning to use such features in the future.

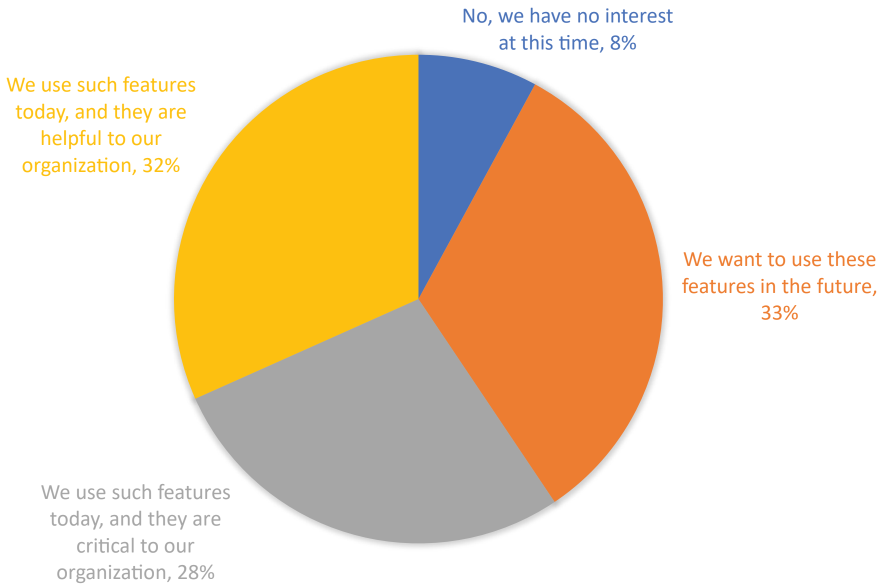

Figure 12: Using advanced analytics features embedded in NPM solutions

"It's a concept that we would like to explore at some point. I'm interested in seeing whether it's a viable technology or just another buzzword," said the senior principal tool engineer at a large North American aeronautics enterprise.

"We're just starting to use it. One challenge is how to do the analysis. Our vendor has a public cloud analysis engine, and we're very sensitive to data exposure. On the other hand, in-house analysis can be cost-prohibitive," said the managing director of infrastructure at a very large North American financial company.

Some analytics capabilities require significant compute resources, which prompts some vendors to offer such features as a cloud-based offering. This inhibits enterprises from adopting the technology. "Our vendor has a public cloud-based analysis engine and we're very sensitive to data exposure. In-house can be cost-prohibitive, and cloud-based is risky," said the managing director of infrastructure at a very large North American financial services company.

60% of enterprises are already using advanced analytics embedded in NPM tools, and nearly half of that group consider such features critical to their organization.

Figure 13 identifies some of the use cases enterprises are most interested in tackling with these analytics capabilities. The chart shows broad interest in a number of scenarios. The most popular use case for analytics, by a narrow margin, is automated traffic analysis—for example, rule-based anomaly detection. Respondents who identified network flow records (50%) were the most likely to consider this use case valuable, while those focused on device metrics (SNMP) were the least likely to be interested (18%).

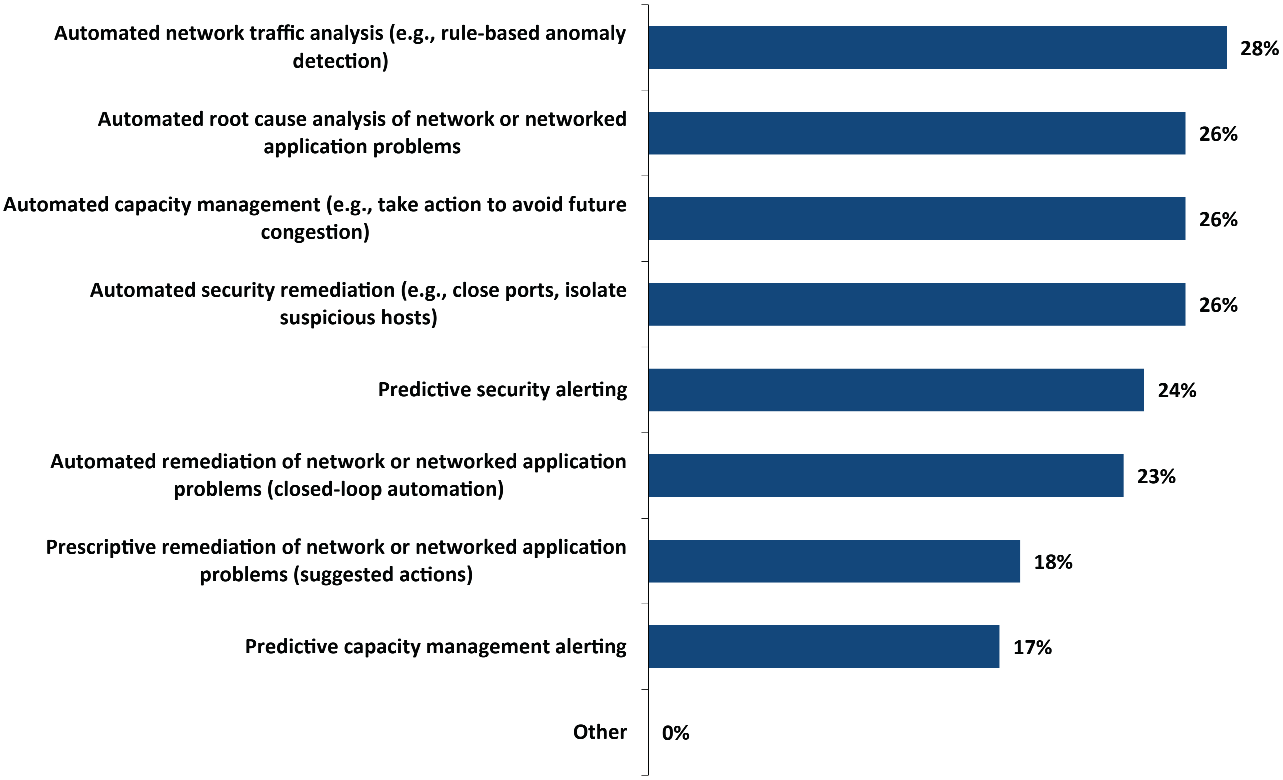

Figure 13. Most important use cases for advanced analytics features embedded in NPM tools

When it comes to service performance issues, enterprises are more interested in automating root-cause analysis of such trouble, rather than actual remediation. However, they do appear more open to closed-loop operations than prescriptive, suggested remediation actions. Automated root-cause analysis was less important to organizations with moderate-sized NPM toolsets and smaller networks. Organizations that use three or four NPM tools (17%) or that have fewer than 1,000 network devices (18%) selected it the least often. Individuals from the IT analytics group (60%) and application management (47%) were more interested in root-cause analysis.

Enterprises are also showing significant interest in automating changes related to capacity management. Respondents who are constantly engaged with NPM tools are more open to automated remediation (29%) than those who are only often engaged (16%). Organizations that use five or more NPM tools are also more interested in automated remediation (30%) than those that use only one or two (13%).

Automated security remediation (closing ports, isolating suspicious hosts) is also a popular use case. Predictive security alerting, which is moderately important, drew more interest from enterprises that connect fewer than 50 sites to the WAN (37%).

Of lease interest are prescriptive remediation of network and application trouble (suggested actions) and predictive capacity management alerting. However, respondents working in a NOC were very interested in predictive capacity management alerting (40%).

Ninety-nine percent of enterprises claim to have some ability to analyze network packets in their NPM toolset, and 70% have the ability to perform both real-time and forensic packet analysis.

Packet-Based Monitoring: Real-Time Versus Forensic Analysis

Ninety-nine percent of enterprises claim to have some ability to analyze network packets in their NPM toolset, and 70% have the ability to perform both real-time and forensic packet analysis, as shown in **Figure 14.** Forensic analysis allows an enterprise to look at packet data after an event has taken place, while real-time analysis can reveal insight as events happen. Some NPM tools can perform both of these tasks, while others specialize in one or the other. In fact, of the 70% of enterprises that have both real-time and forensic packet analysis capabilities, only 36% have a tool that can do both. The rest are using two separate platforms. North Americans are more likely (41%) to use two tools than Europeans (20%).

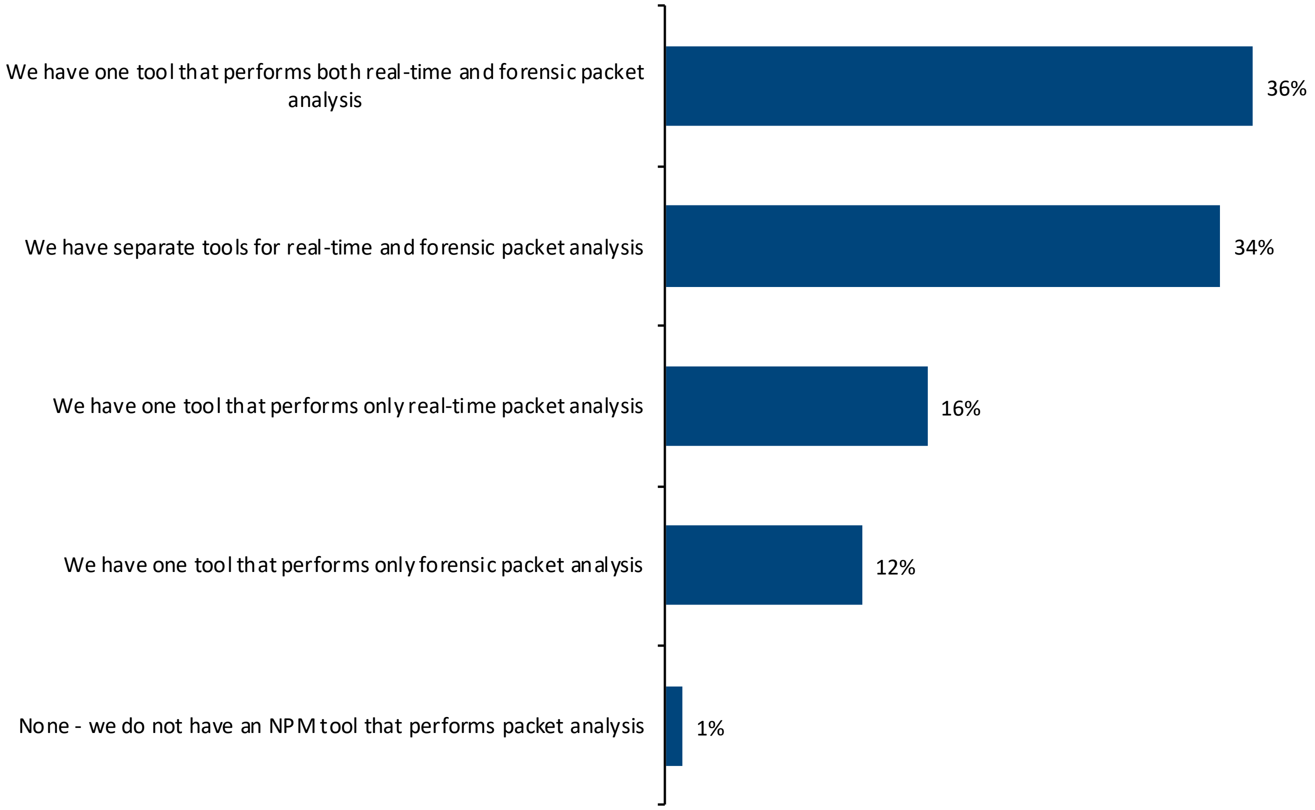

Figure 14. The packet-based monitoring capabilities of enterprises

Enterprises that consider network flow records to be their most important source of NPM data are more likely to have one packet analysis capability or the other, but not both. For instance, 21% say they have only a forensic packet analysis tool, and 32% say they have only a real-time packet analysis tool. This suggests that enterprises who invest in both real-time and forensic packet analysis are less likely to need network flow records. Those who have one or the other type of visibility turn to network flows to fill their visibility gap.

Due to limitations in the length of EMA's survey questionnaire, respondents were not asked (in this context) how deep their visibility into packets goes. For instance, some real-time packet analysis tools are limited to Layer 2 through Layer 4 analysis. They can reveal insight into TCP sessions, but not application layer (Layer 7). Layer 7 analysis can be more resource-intensive. Also, some NPM users leave application performance to the application management team, meaning separate teams have their own tools for their own areas of responsibility and never the twain shall meet.

"We entertained the idea [of a Layer 7 packet analysis tool] but we asked ourselves as a network team, are we in the business of troubleshooting application transactions and sessions, or do we terminate our responsibility at the TCP layer? We decided that as long as the TCP handshake is done in a reasonable timeframe, then we are done. Everything else is an application issue. That has to do with how our IT organization works," said the senior principal tool engineer with a large North American aeronautics organization.

Enterprises with smaller networks (fewer than 1,000 devices), are the most likely to have a single tool for forensic analysis only (16%).

Real-Time Packet Analysis Tool Performance

The amount of traffic a real-time packet analysis tool has to process often exceeds the maximum line-rate performance of the tool, so enterprises will often cluster several instances of the tools together and load balance packet flows across them using a network packet broker. **Figure 15** reveals how enterprises have to do this today. Only 33% say a single instance of their tool meets their needs. The rest are either using a clustered deployment, or they need to upgrade their tools. European respondents were less likely (3%) to need a tool upgrade, versus 14% of North Americans.

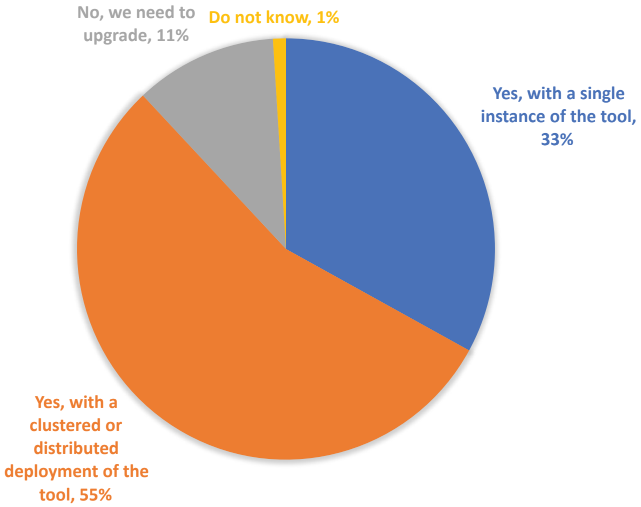

Figure 15. Question: Does the real-time packet processing rate of your NPM tool meet your organization's needs?

"I'm fine with the performance, but the price for performance is too high. We won't even look at the highest-end version [of our tool] because it's just too expensive. It's priced for people whose primary business is the network, and that's not us. If we had one giant device that could collect everything, that would be great. Instead, I have nine devices collecting [and analyzing] packets," said the managing director of infrastructure at a very large North American financial company.

Finally, EMA asked these enterprises if their tool performance is impacted when packet flows push them toward maximum line-rate performance. Sixty-six percent see some degradation in the tool's ability to decode or decrypt application layer protocols, as **Figure 16** reveals.

> *"The price for performance is too high. We won't even look at the highest-end version [of our tool] because it's just too expensive. It's priced for people whose primary business is the network, and that's not us."*
>
> - Managing director of infrastructure at a very large North American financial company.

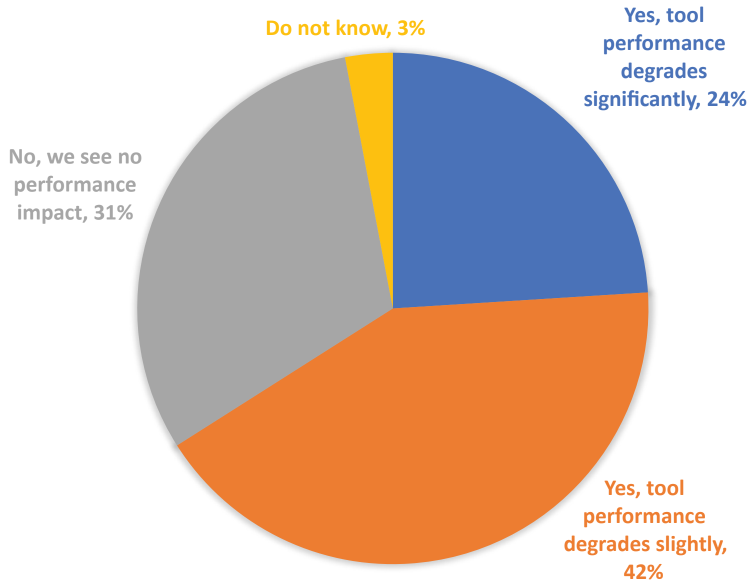

Figure 16. Question: As your real-time, packet-based NPM tool approaches maximum line rate, is the tool's ability to decode or decrypt application layer protocols affected?

NPM Use Cases

Through its ongoing research, EMA has defined five core use cases for NPM toolsets.

- Monitoring health and performance of networks and networked applications
- Troubleshooting network and networked application service problems
- Network capacity planning and management
- Cloud application assessments and migration planning
- Security monitoring and incident response

Security monitoring and response is the most popular use case for NPM tools, followed by capacity management and network and networked application health and performance monitoring.

In this section, EMA will identify which use cases are a priority for enterprises and the network data that is most valuable to these individual use cases.

NPM Use Case Priorities

Figure 17 reveals that security monitoring and response is the most popular use case for NPM tools, followed by capacity management and network and networked application health and performance monitoring which, for brevity's sake, EMA will refer to as network operations monitoring. Cloud application assessments and troubleshooting are the least popular.

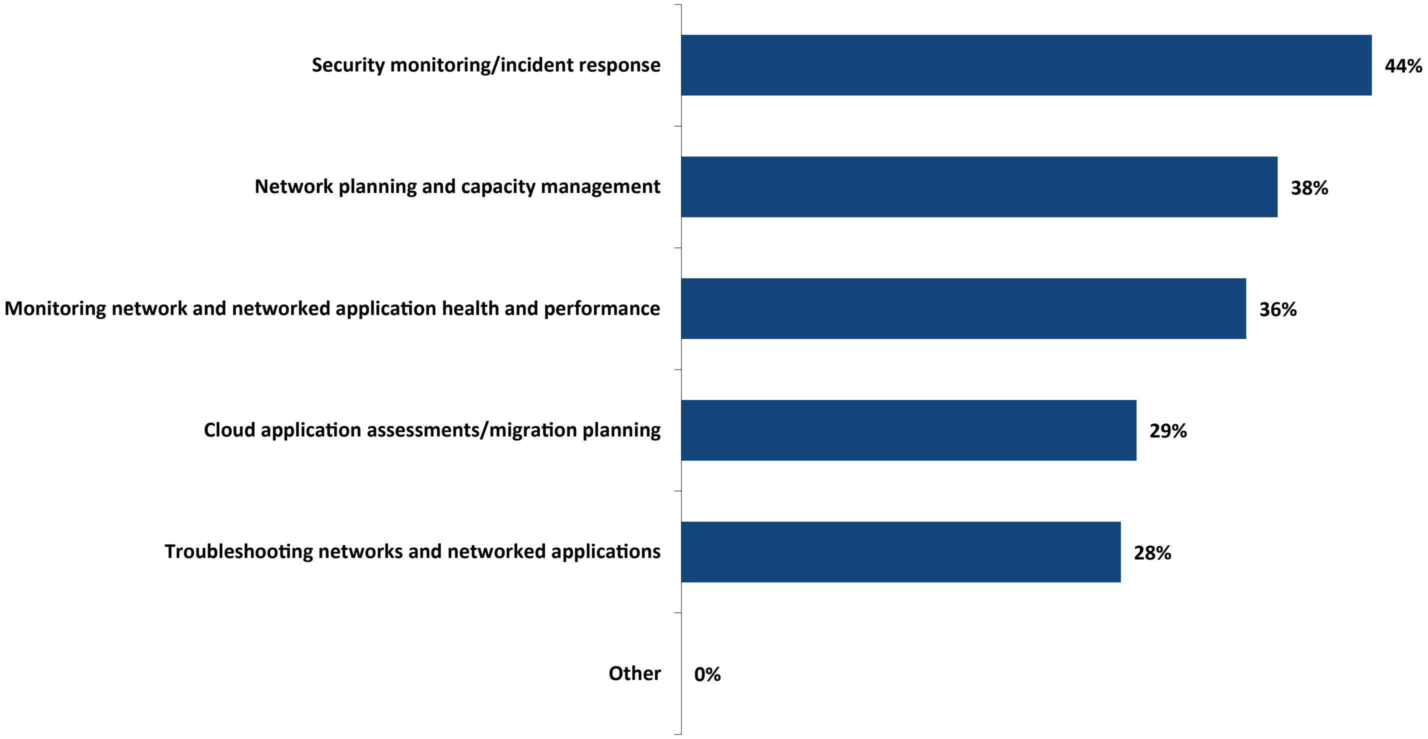

Figure 17. Enterprises identify their top two NPM use cases

At first glance, the prominence of the security use case is surprising. However, past EMA research found that more than 90% of network operations teams have established formal collaboration or partnerships with their organization's security team.[3] These enterprises also identified NPM as the most valuable network management tool for facilitating this collaboration. It is also worth noting that respondents were allowed to select two use cases in answer to this question, and 190 of the 250 participants did so. EMA suspects that many of those individuals consider one of the other four use cases on this list as their primary choice and security as their secondary use case. In other words, network professionals up and down the organizations, from those who monitor performance to those who plan capacity, also consider security as part of their remit. Figure 2 supports this hypothesis. When asked to identify their two primary modes of engagement with NPM tools, survey participants chose network operations monitoring and network capacity planning most often. Network security monitoring was a distant third-place finisher on that list.

In another research study from 2019, EMA found that 99% of network teams involved with integrating the network with their organization's cloud strategy use their tools to assess the network requirements of applications that are migrating to the public cloud.[4] This use case is clearly important, but NPM tools are not necessarily the only class of tool used for such assessments.

[3] EMA, "Network Management Megatrends 2018: Exploring NetSecOps Convergence, Network Automation, and Cloud Networking," April 2018.
[4] EMA, "Network Engineering and Operations in the Multi-Cloud Era," March 2019.

"Capacity planning is for sure something we do with NPM tools. When we're deploying a new technology that will be dependent on how much traffic it can ingest, we have to look at traffic trends and determine growth over the next five years to make sure the technology will be viable. But we think about security, too. We're identifying issues on the perimeter and we notify security about it, telling them about the number of sessions on the firewall and so on," said a senior principal tool engineer with a large North American aeronautics enterprise.

Mapping Network Data to NPM Use Cases

EMA asked respondents to identify the data currently collected by their NPM tools that is most valuable to the five use cases this research investigated. Their responses are not necessarily a consensus on which classes of data are ideally suited to supporting these cases, because the research participants were biased by the tools they have available to them. Instead, the results are about practicality, a reflection of how IT organizations balance their use case requirements with the realities of budget, complexity, skill level, and more.

NPM Data and Network Operations Monitoring

Figure 18 reveals the network data IT organizations are most successfully applying to network operations monitoring. In the experience of these respondents, management system APIs, network flows, and network device metrics are the most valuable sources of data applied to network operations monitoring. This research previously found that management system APIs are the most valuable source of data for NPM tools in general. In the following pages, readers will see that these APIs are prominently valuable for every use case.

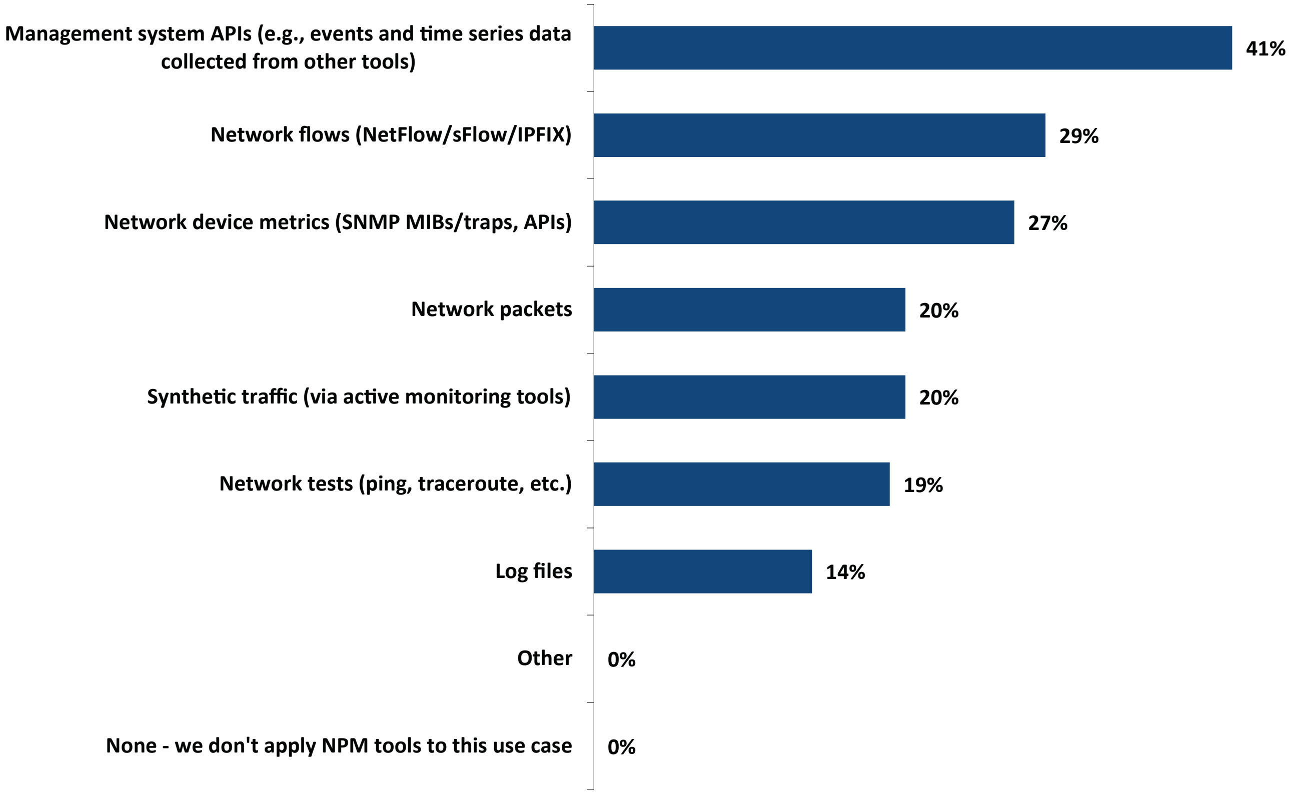

Figure 18. Data most valuable for network operations monitoring with NPM tools

Network operations monitoring typically requires real-time analysis of data. Network flows are generally the easiest source of traffic data to collect, from cost and complexity perspectives. Thus, it's not surprising to see network operations monitoring as a secondarily important data source. Network device metrics, which provide real-time insight into the health of individual network nodes, are the third-most popular data source.

Packets, which can provide a more complete picture of performance than flows, are less favored for network operations monitoring. However, Europeans (28%) had a stronger affinity for it. Also, streamlined NPM toolsets correlate with a higher focus on network packets. Organizations that use only one or two NPM tools were much more likely (32%) to identify packets as a valuable data source, versus only 12% of those who use three or four tools. On the other hand, enterprises that use five or more NPM tools are much more likely to favor management system APIs (49%) than those that use only one or two (27%).

Enterprises with 500 or more remote sites rely more on device metrics (39%) than those with fewer than 50 sites (20%) or 50 to 499 (24%). The larger and more complex a network, the more difficult it is to collect traffic data comprehensively. There will be many sites where polling switches and routers are the best way to get answers about performance.

"We use [SNMP] quite a bit when trying to monitor remote sites. When a connection goes down, [SNMP rules out our devices as the root cause], and we look at [our WAN provider] to do the troubleshooting. We ask them to tell us why the connection is down," said a network operations analyst at a medium-sized North American transportation company.

NPM Data and Network Troubleshooting

Figure 19 reveals less consensus about the value of NPM data for network troubleshooting. Management system APIs are only slightly more valued than network flows, and packets aren't far behind. Network tests rise in prominence here, which is unsurprising. Enterprises have used ping and traceroute for decades to get a quick understanding of potential root causes of trouble. Overall, while management system APIs are the clear favorite for troubleshooting, flows, tests, and packets are all virtually tied as the top secondary data source.

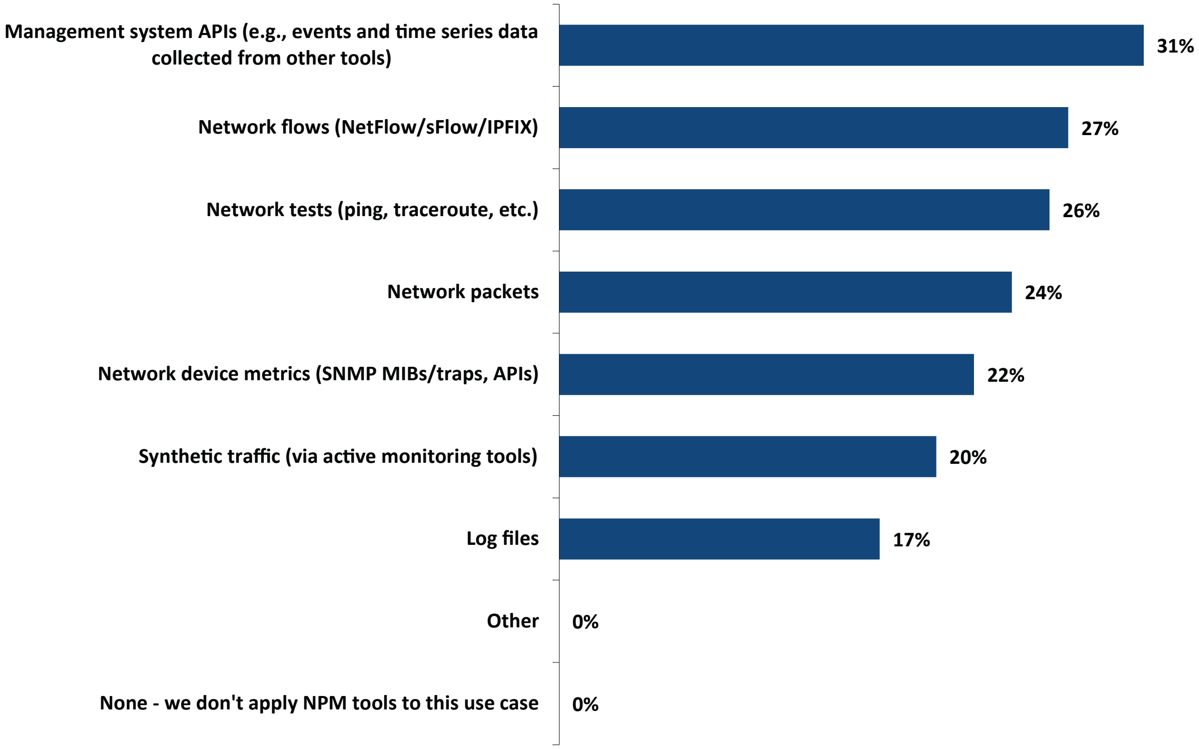

Figure 19. Data most valuable for network troubleshooting with NPM tools

Troubleshooting with packets is particularly important to enterprises that manage larger networks (5,000 or more devices). Thirty-three percent of such enterprises emphasize packets, versus only 18% of enterprises with 1,000 to 4,999 devices.

NPM Data and Network Capacity Planning/Management

Management system APIs emerged as the preferred data source for capacity planning and management, and the consensus is stronger here than it was with troubleshooting, but not quite as prominent as it was for network operations monitoring. North Americans (37%) favored these APIs more than Europeans (23%). **Figure 20** shows that no other source of data is particularly differentiated from the others. Network tests and network device metrics are slightly favored over others, but the margin is small.

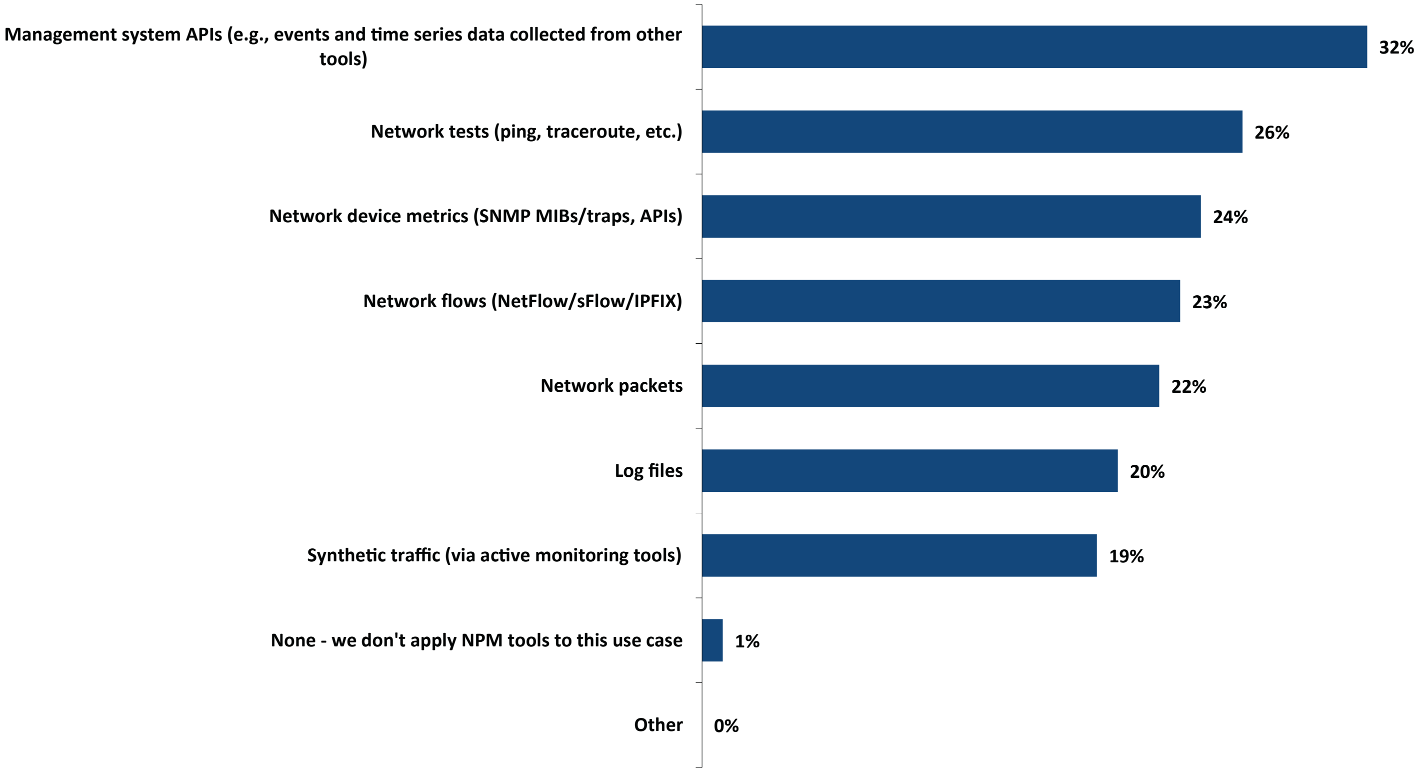

Figure 20. Data most valuable for planning/managing network capacity with NPM tools

"SNMP is useful for capacity planning. I can see bandwidth and make decisions for upgrading equipment or switching a different type of equipment, like broadband versus MPLS. So, we use SNMP for that," said a network operations analyst with a midsized North American transportation enterprise.

Packets are more valuable to operators of large networks of 5,000 or more devices (33%), but less valuable to those with just 1,000 to 4,999 devices (16%).

NPM Data and Cloud Application Assessment

Figure 21 reveals that management system APIs are the most popular source of data for cloud application assessments, but the margin over other preferences is negligible. Device metrics, synthetic data, tests, and flows are all quite important, too. Packets are the least popular, probably because many network teams will collect data for such assessments over two weeks or more, which is an expensive proposition given the potential volume of packet data involved. However, packets are more popular with networks of 5,000 or more devices (27%).

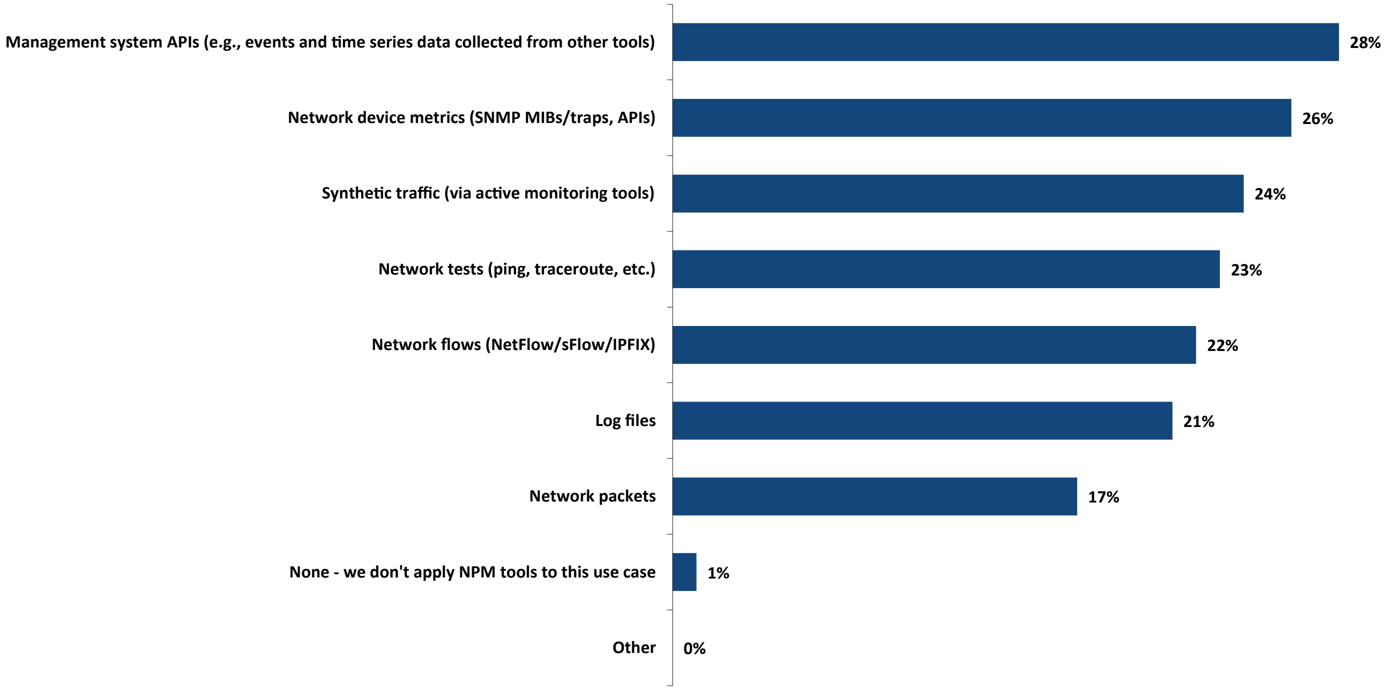

Figure 21. Data most valuable for assessing cloud application requirements with NPM tools

NPM Data and Security Monitoring and Management

Finally, EMA assessed the perceived value of data for security monitoring and management with NPM tools. **Figure 22** shows a prominent top-four data sources, with management system APIs and network flows in a virtual tie at the top. Network tests, packets, and logs are all clearly secondary sources for this use case. However, Europeans (27%) saw more value in packets for security use cases than North Americans (15%).

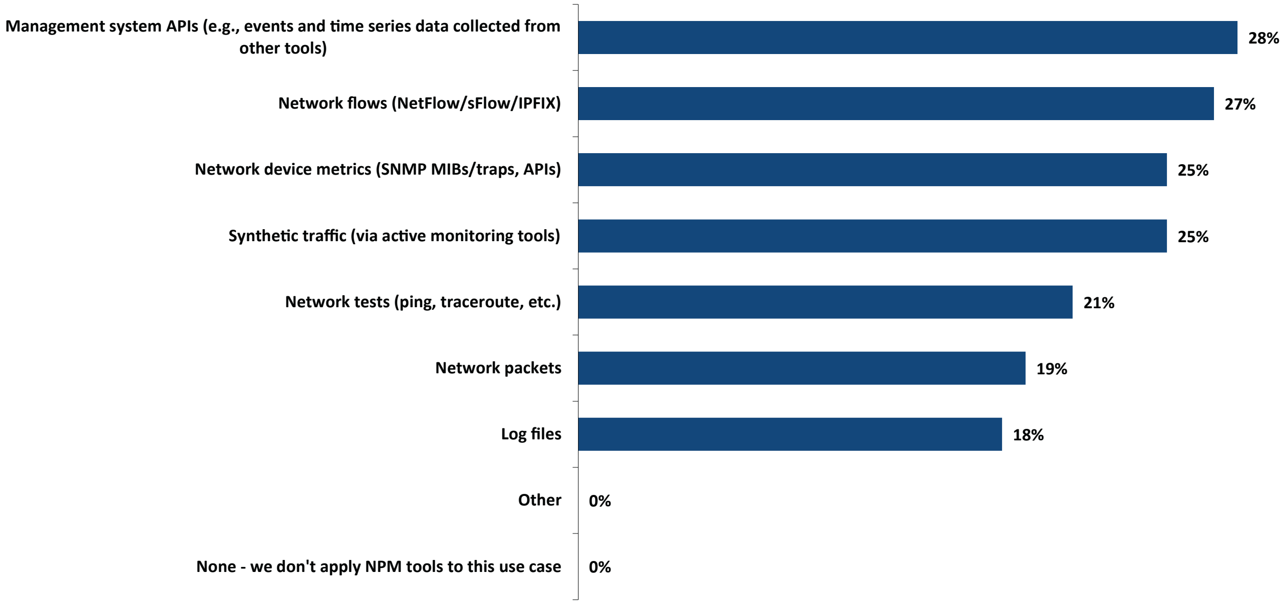

Figure 22. Data most valuable for monitoring and managing security with NPM tools

The Network and Beyond: Getting the Big Picture with NPM

NPM tools are rarely used in isolation. In other words, it's about more than the network. Already from this research, it's clear that enterprises pivoting their NPM tools toward security and cloud applications. Thus, it's important to consider how enterprises extend the value of tiered NPM tools beyond the network view. This segment looks at the issue from several angles.

Correlating NPM Insights with Application Performance, End-User Experience, and Security

Figure 23 reveals preferences for correlating NPM insights with application performance. This is a frontline issue for the network team, since the primary mission of a network is to connect users to high-performing applications.

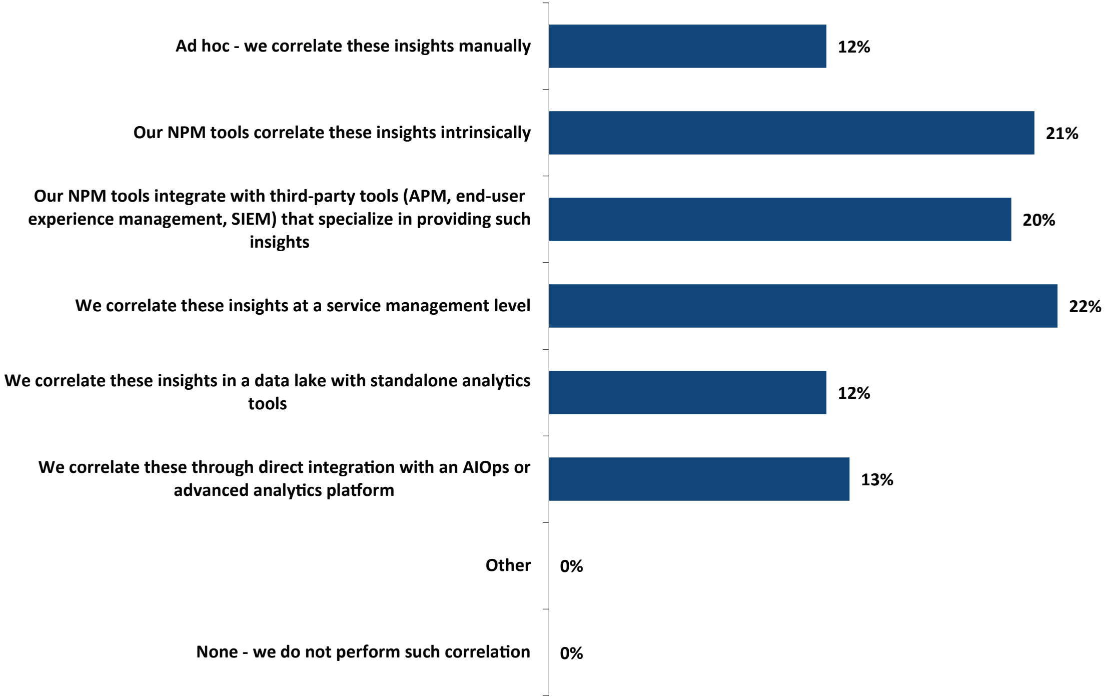

Figure 23. Primary approach to correlating NPM insights with application performance

There are three popular approaches to application performance correlation. First, enterprises conduct this correlation at the service management level, presumably by integrating NPM tools with a service management tool. This approach is more common among enterprises that identified either network flow records (35%) or synthetic data (36%) as their most strategic source of data for NPM. This approach was less popular with individuals who work in application management/support (11%) and IT analytics (12%).

Second, enterprises adopt NPM tools that correlate application performance intrinsically. There are several real-time packet analysis tools that offer this capability. Third, enterprises achieve correlation by integrating with a specialized tool—in this case, an application performance management platform.

One focal interviewee uses a packet-based monitoring tool with intrinsic application performance monitoring insights. "My mindset is, I don't manage the network. I manage the applications that run on it. I need to look down the stack into the network itself. We take a top-down approach, rather than a bottom-up approach. I don't start with the network and build my way up to the application. When I have a network with 4,000 ports going down, I don't care about them unless there is traffic running on them. Networks are unstable by their very nature. If something is broken but not affecting anything, it's not important," said the managing director of a very large North American financial company.

Figure 24 shows how enterprises prefer to correlate NPM insights with end-user experience. Unlike with application performance, there is a clear hierarchy of popular strategies. In this case, direct integration with a specialized end-user experience management tool is preferred. Intrinsic correlation is more common with enterprises that have fewer than 50 remote sites on the WAN (26%), versus 14% of those with 50 to 499 sites.

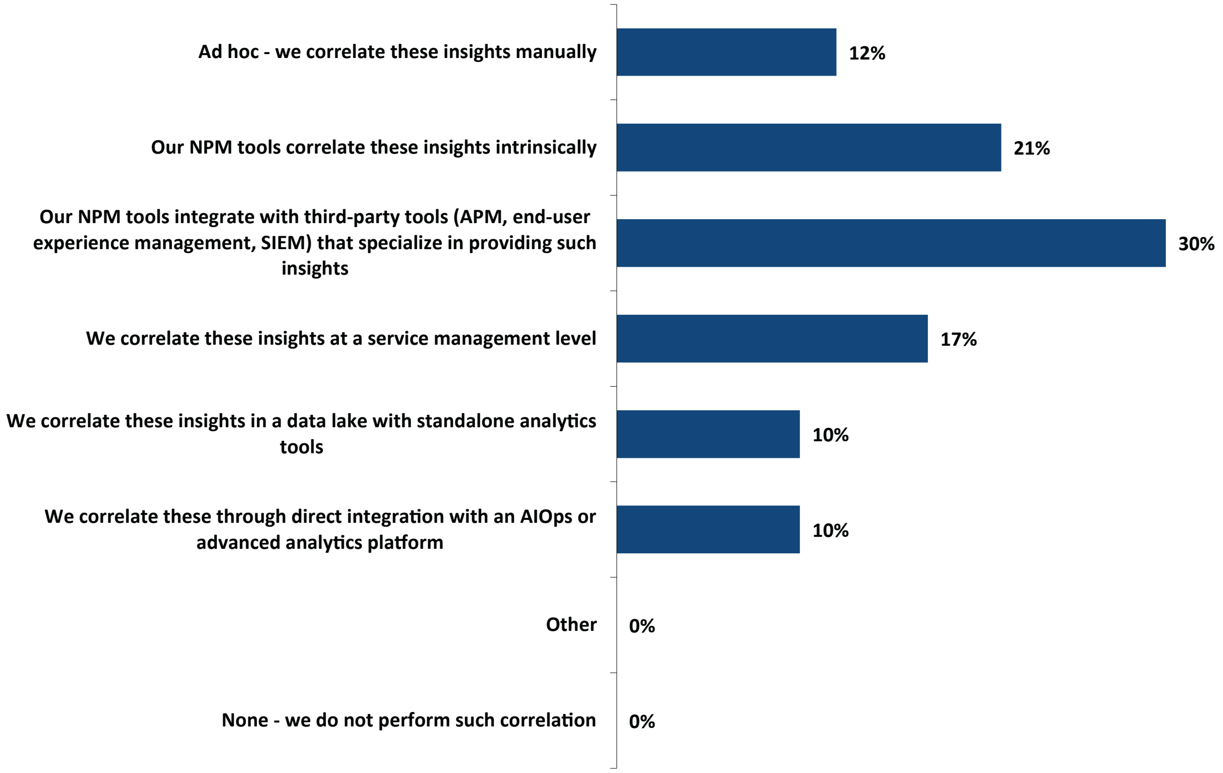

Figure 24. Primary approach to correlating NPM insights with end-user experience

The secondary approach is an NPM tool with an intrinsic ability to perform this correlation. Enterprises with 500 or more remote sites do this integration more often (36%) than those with fewer than 50 sites (18%).

Service management platform integration is the third choice. The other approaches are relatively rare. However, enterprises with 5,000 or more network devices in their network are more likely (18%) to take an ad hoc approach to end-user experience correlation, versus only 6% of enterprises with 1,000 to 4,999 devices.

Finally, **Figure 25** reveals preferred strategies for correlating NPM insights with network security monitoring. Again, the preferred approach is to integrate directly with a security monitoring solution. Direct integration is more common with operators of networks with 1,000 to 4,999 devices (34%), but less common among those with smaller networks (20%).

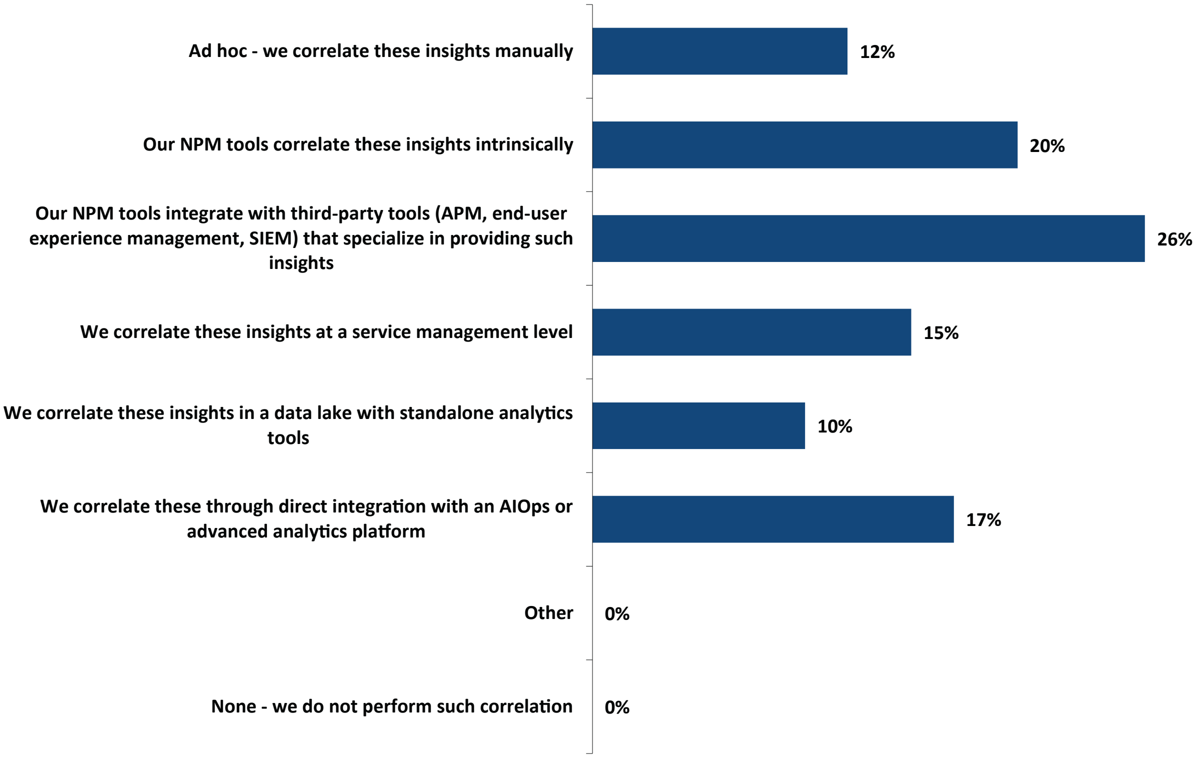

Figure 25. Primary approach to correlating NPM insights with network security monitoring

The secondary preference is using an NPM tool with intrinsic security correlation. This approach is more common with enterprises that consider network flow records to be their most strategic NPM data source (32%), but those with a focus on synthetic data are very unlikely to have intrinsic security correlation (5%). Individuals from the network engineering group (56%) are very likely to claim their tools correlate with security intrinsically, which may be a reflection of their technical expertise rather than anything their tool is able to do. On the other hand, individuals from the NOC (13%), application support (11%), and IT analytics (6%) all appear less inclined to look for this capability.

In the case of security, integration of NPM tools with AIOps or advanced analytics platforms emerges from relative obscurity as the third choice of enterprises. This appears to be an early opportunity for enterprises that are exploring AIOps solutions.

Direct polling of the cloud, logs, synthetic traffic, and cloud provider billing data are all less valuable in NPM tools.

NPM Tool APIs and Integrations

NPM vendors offer application programming interfaces (APIs) on their tools for a variety of reasons, from integration with third-party tools to customization of the product. This research found that 98% of enterprises are using these APIs, as **Figure 26** reveals. Nearly all of them find these APIs either helpful or essential to IT operations.

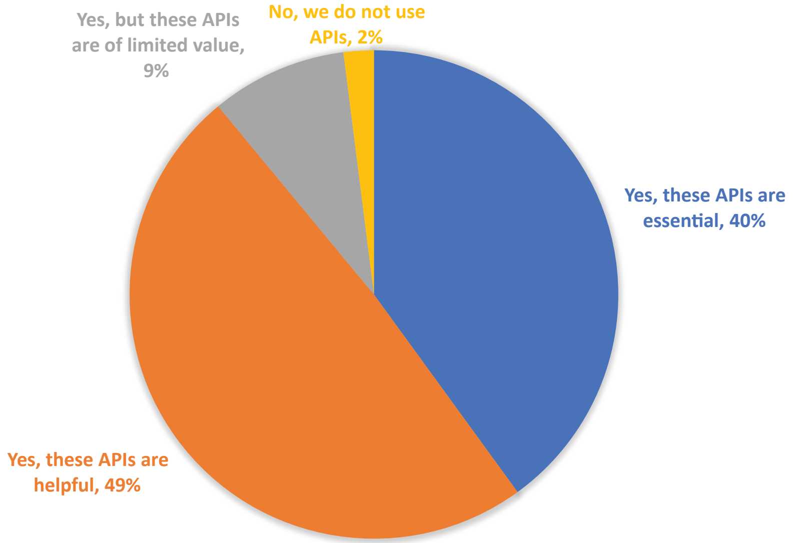

Figure 26. Question: Does your organization use the APIs provided by NPM tool vendors to enhance the functionality or value of those tools?

"We use APIs, and we struggle with them from some of the older vendors. The new vendors with REST APIs are better and easier to use. SOAP-based APIs are less useful. API quality is now a vendor evaluation criterion," said a senior principal tool engineer with a large North American aeronautics enterprise.

"I would like to use APIs more. My predecessor took [our current tool] out of the box and set it up to monitor things in isolation. I tend to like aggregating data together. There is a lot of valuable data out there, but I don't have time to deal with it. An API allows me to build out how an application runs across the network and how it performs. It will help with troubleshooting," said the managing director of infrastructure at a very large North American financial company.

Organizations that use five or more NPM tools are more likely (49%) to consider these APIs essential than those who use one or two tools (29%), which suggests that a key value of APIs is the integration a fragmented toolset. IT management tool architects and engineers, who do a lot of this custom work, are also more likely (48%) to place this much value on tool APIs, as are people who are constantly engaged with NPM tools (52%). APIs are also more often essential to operators of networks with 5,000 or more devices (63%) or with 500 or more remote sites (52%).

> *"We use APIs, and we struggle with them from some of the older vendors. The new vendors with REST APIs are better and easier to use. SOAP-based APIs are less useful. API quality is now a vendor evaluation criterion."*
>
> - Senior principal tool engineer with a large North American aeronautics enterprise.

Figure 27 reveals how enterprises use these APIs. The least-popular use case is the streaming of data to a data lake. Instead, enterprises are enhancing or automating the administration of NPM tools, they are implementing custom data collection, they are customizing the tool itself, or they are implementing integration with third-party systems.

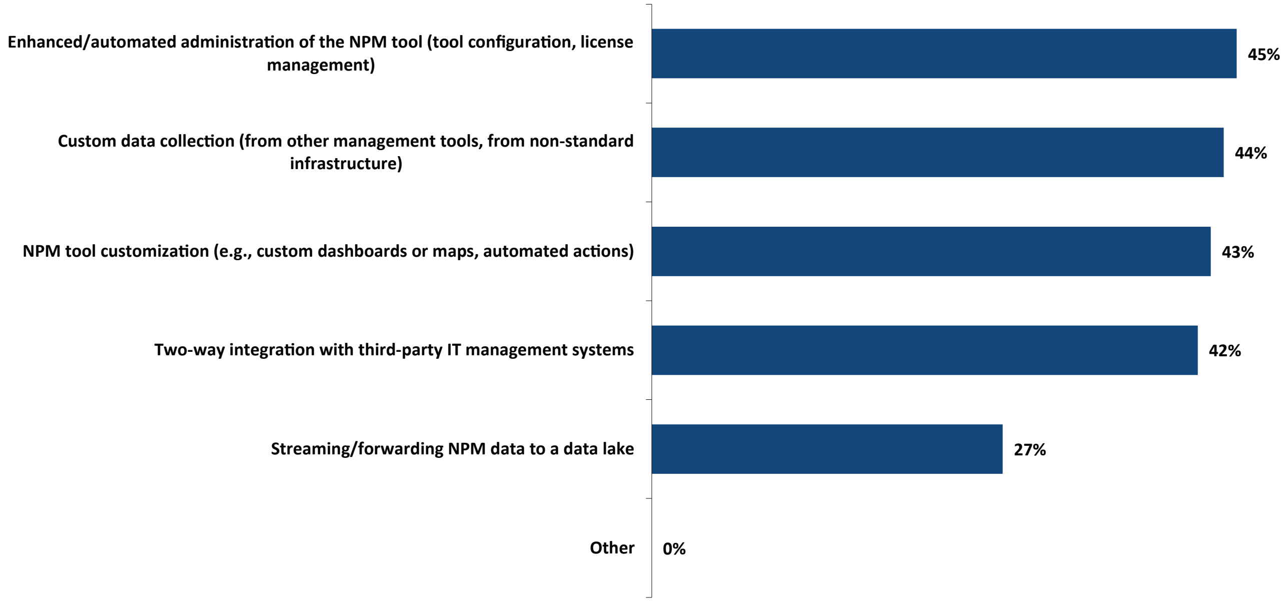

Figure 27. How organizations use the APIs provided by NPM tool vendors

Custom data collection is a higher priority for operators of networks with 5,000 or more devices (56%). It is also a priority for people in the application management group (65%) and project management (53%).

This research already established that management system APIs are the number-one source of data for NPM tools. In this section, EMA examines which management systems are the focus for this API-based data collection. **Figure 28** reveals the IT systems from which NPM tools collect data for combined analysis with network data. IT service management and security monitoring are the top priorities. IT/cloud orchestration, cloud monitoring, network configuration management, compliance management, and application performance management are all relatively popular, too.

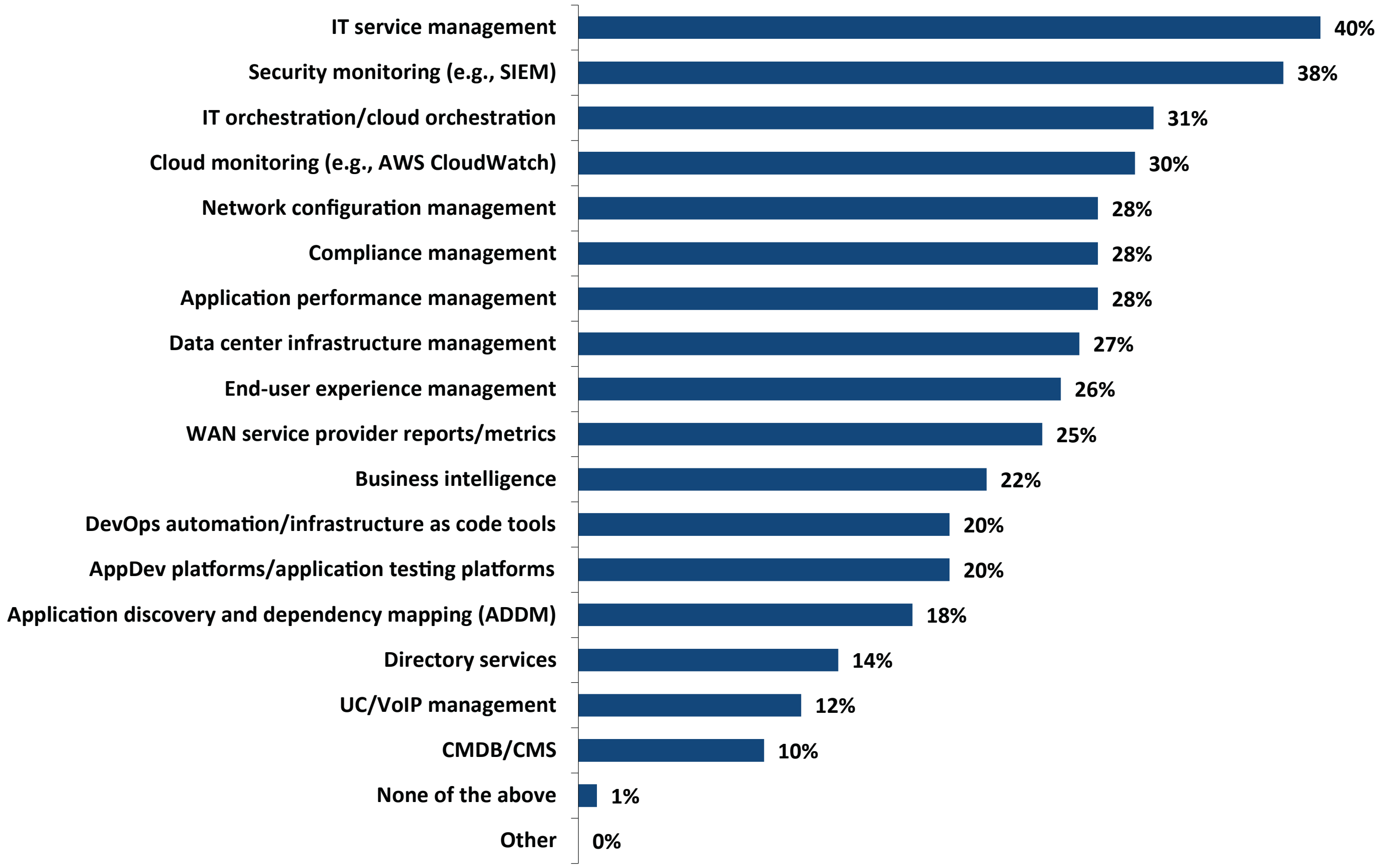

Figure 28. IT systems from which NPM tools collect data, events, metrics, etc. to combine with analysis of network data

"We have an initiative starting soon to tie NPM tools to IT service management. The business wants to have a service menu through which people make a request and it rolls out across the entire infrastructure, more like an AWS self-service model," said a senior network engineer with a large North American retail company.

Operators of networks with more than 5,000 devices are particularly interested in IT/cloud orchestration data (47%), versus just 21% of those with fewer than 1,000 devices. While CMDB/CMS are the least popular source of data in NPM tools, Europeans (17%) are more interested this kind of integration. Individuals who work in a NOC have stronger interest (29%) in pulling data from directory services. IT analytics professionals are more interested in pulling data from business intelligence (47%). IT executives (42%) and IT asset management professionals (50%) are more interested in data from cloud monitoring tools.

> *"We have an initiative starting soon to tie NPM tools to IT service management. The business wants to have a service menu through which people make a request and it rolls out across the entire infrastructure, more like an AWS self-service model."*
>
> - Senior network engineer with a large North American retail company.

EMA found several correlations between core NPM data preferences and IT systems that supply data through this integration, which suggests areas where enterprises are best able to combine data for analysis. For instance, enterprises who focus on log data with NPM tools are more likely to pull data from IT service management (59%) and end-user experience management (45%). Enterprises focused on synthetic traffic in NPM tools are more likely (36%) to pull data from business intelligence tools.

Figure 29 reveals which IT systems receive data from NPM tools to provide users of those third-party systems with insight into the network. IT service management stands out as the big opportunity for this kind of integration. Security monitoring, data center infrastructure management, IT/cloud orchestration, and network configuration management are secondary targets.

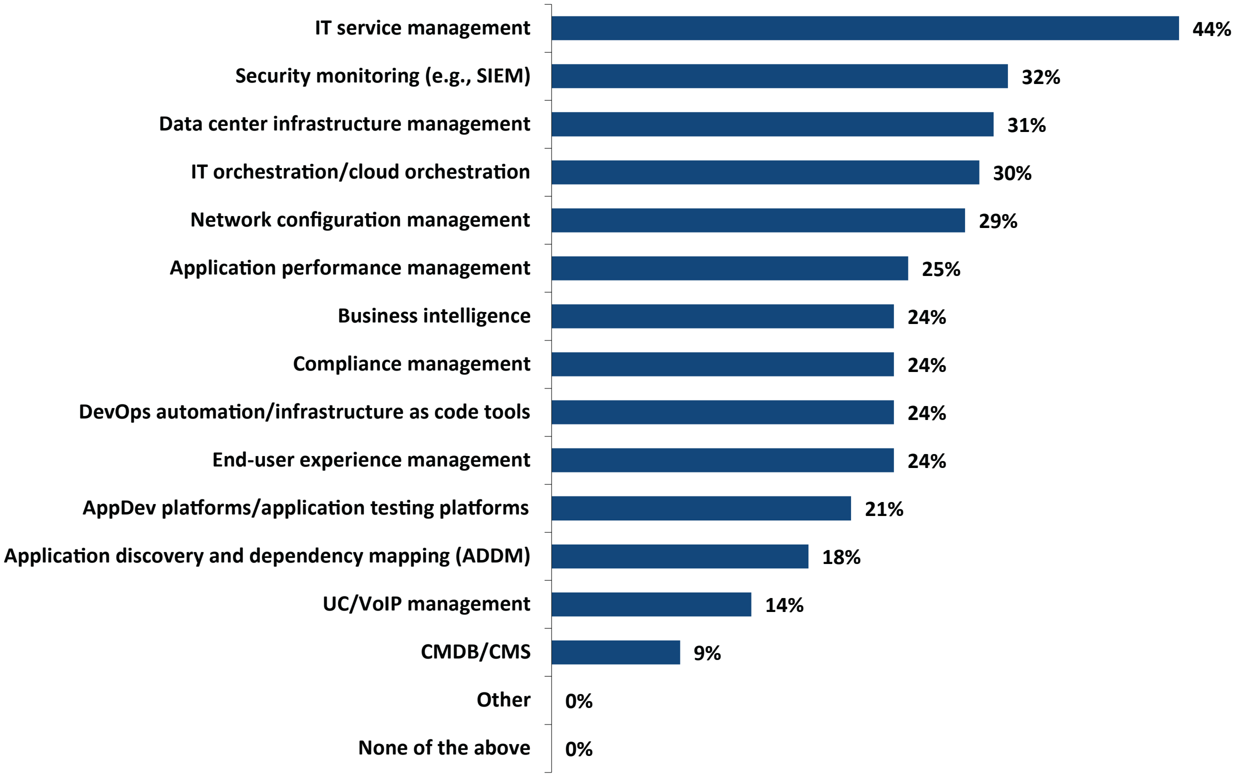

Figure 29. IT systems to which enterprises forward NPM data to provide their users with insight into the network

Again, CMDB/CMS are not big opportunities, but operators of networks with 1,000 to 4,9999 are more likely (14%) to send NPM data to these systems, versus just 5% of those with smaller networks. Enterprises that are constantly engaged with NPM tools were the most likely (42%) to send NPM data to security monitoring tools, versus only 24% of those who occasionally use such tools.

Enterprises that consider device metrics their most important NPM data source are the most likely (43%) to send NPM data to a network configuration management tool, versus only 21% of those who focus more on network flow data.

Challenges to Effective NPM Tool Strategies

This section explores some of the top challenges that enterprises face when implementing and using NPM tools. It looks at the issue from the perspective of both NPM platform problems and data challenges. It also looks at the places in the enterprise network that are most difficult to manage with these tools.

Platform Challenges

EMA asked respondents to identify the issues that most affect usability and effectiveness of NPM tools. Three key challenges emerged. First, more than one in five enterprises are struggling with the fact that their tools lack true real-time insights, as **Figure 30** reveals. For instance, their NPM platforms are primarily forensic in nature. In this case, they lack the depth of real-time analysis to prevent problems proactively. It is likely that these individuals have some real-time visibility, but the depth of that visibility is limited. For deeper analysis, they have to rely on forensic capabilities.

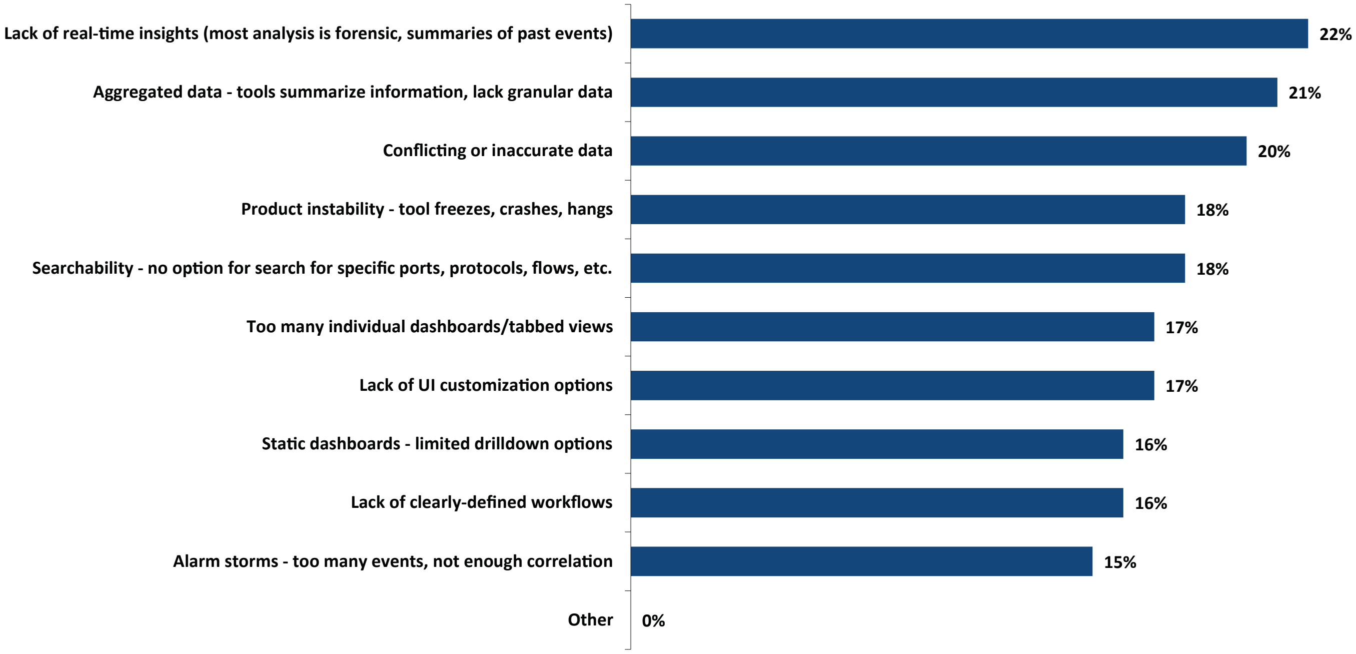

Figure 30. Issues that impact the usability and effectiveness of NPM tools

The next top challenge is the issue of aggregated data, where tools summarize information and lack granular insight. In this case, enterprises might be using a tool that records transactions and events, but it discards the underlying data it uses to create those transactions and events. By discarding the underlying network data, the tools limit a user's ability to dig deeper during certain tasks, like troubleshooting or capacity planning. North Americans (25%) complained of this issue more often than Europeans (13%).

"I would like more granularity out of my tool. When we open a ticket with our WAN provider, most of the time they come to us and say the site was up when they looked at it. In my tool, I can't see if it was our device or the network connection that caused the problem. I'd like to be able to log into a device and see logs that told me what caused the outage," said a network operations analyst with a midsized North American transportation enterprise.

“A lot of SNMP tools do rollups. As new technologies emerge, it would be awesome to collect data forever so I can go as far back as I want to look at trends. Also, a lot of vendors try to be everything to everyone, and they don’t do anything particularly well. I like tools that are very targeted,” said the managing director of infrastructure at a very large North American financial company.

Finally, 20% of survey respondents said their tools are collecting conflicting or inaccurate data. This can occur when they are collecting data from multiple vantage points with multiple tools, or when instrumentation of the network for data collection has been implemented improperly.

Product stability and searchability are the top secondary challenges. Searchability speaks to the issue of being able to run a search for specific ports, protocols, flows, or other variables. Users simply can’t find the information they need without scrolling through various dashboards, event lists, or reports. Stability refers to a tool that crashes, freezes, or lags.

> *“A lot of SNMP tools do rollups. As new technologies emerge, it would be awesome to collect data forever so I can go as far back as I want to look at trends. Also, a lot of vendors try to be everything to everyone, and they don’t do anything particularly well. I like tools that are very targeted.”*
>
> - Managing director of infrastructure at a very large North American financial company

“Our tool is quite slow. When you’re troubleshooting an issue, the web interface slows down and that becomes an issue for us,” said a senior network engineer with a very large North American retailer.

Product stability was less of a problem for operators of smaller networks, with fewer than 1,000 devices (11%), suggesting that some tools struggle with stability as the tool scales. In fact, 28% of enterprises with 1,000 to 4,999 devices complained about stability.

The least challenging issues are static dashboards, a lack of clearly-defined workflows, and alarm storms. However, one focal interviewee drew a connection between product instability and poorly-defined workflows, saying both issues are linked to the fact that some NPM vendors have poor product strategies.

“Product stability is the biggest one for me. I see a lot of bugs and a lot of inconsistency in the architecture and the algorithms that [vendors] use from one area of the product to another. I also see vendors who do not quite understand or research how the product is going to be used, whether it will be an engineering tool or an operations tool. How do I make this product fit into a workflow, and how do I make it flexible enough to support multiple organizations with diverse workflows? Some vendors do not think about that enough,” said the senior principal tool engineer with a North American aeronautics enterprise.

The scope of an organization’s WAN appears to affect the NPM platform challenges it most struggles with. For instance, organizations with fewer than 50 remote sites were less likely to struggle with alarm storms (10%) and user interface customization (11%), and more likely to struggle with conflicting or inaccurate data (27%) and a lack of real-time insights (27%). Enterprises with 500 or more sites were less likely to struggle with a lack of real-time insights (14%) and clearly-defined workflows (10%), and more likely to struggle with alarm storms (21%) and user interface customization (22%).

Data Challenges

There is no doubt that NPM tools are only as good as the data they collect. If data collection is problematic, tool effectiveness is doomed. EMA asked research participants to identify their top data challenges with their NPM tools. **Figure 31** shows that there are two major challenges that enterprises need to address: security risk and data quality.

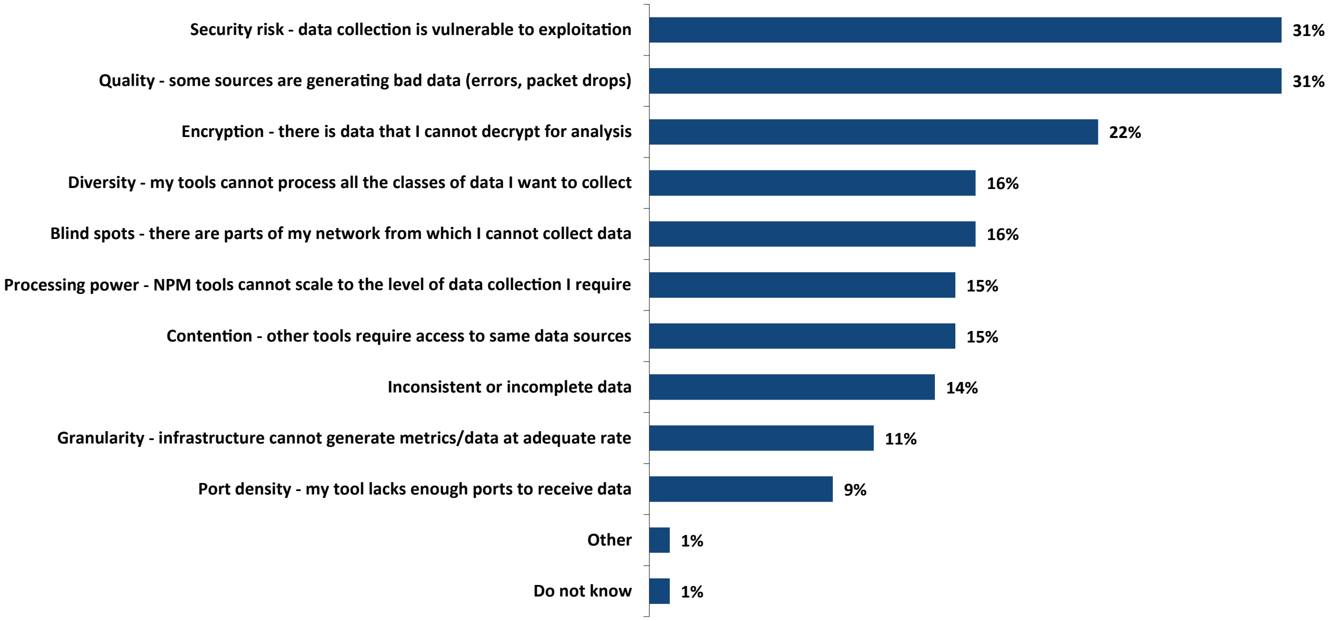

Figure 31. Data-related issues most challenging to success with NPM tools

Nearly one-third of enterprises are struggling significantly with securing and protecting the network data they collect with NPM tools. Packets are particularly sensitive in this context, but nearly any data pulled from the network is potentially compromising. Individuals who work with the application management and support team are particularly concerned about security (53%), but those who work in a NOC are not (21%).

Nearly one-third of enterprises are struggling significantly with securing and protecting the network data they collect with NPM tools.

Nearly one-third are also struggling with data quality. In this case, the data sources are generating bad data, such as errors and packet drops. Data quality is particularly challenging to enterprises with fewer than 50 remote sites (40%). Individuals who work in a NOC are also more likely (54%) to struggle with this issue, but IT management tool architects and engineers are not (21%), which suggests that there is a disconnect on this issue between users and implementers of tools.

“Data quality is the biggest issue. You don’t want the report to make the data; you want the data to make the report. You want to be able to solve the right problem. If your data model isn’t accurate, there is no point in reporting on it,” said a senior consultant with a medium-sized North American IT operations consultancy.

Encryption is another prominent challenge. Encryption ensures privacy, but it limits visibility into data, handicapping an NPM's tool to provide insight to users. All other challenges are less common, especially data granularity and port-density on individual tools.

While the processing power of tools was only a moderate challenge in EMA's survey, some focal interviewees considered it a top challenge. "Performance of the tools is one thing that is always on my mind, especially when it comes to application response time, whether the tool is capable of processing all the records the network is producing, rather than dropping 20% of them," said the senior principal tool engineer at a large North American aeronautics enterprise.

Conclusion

This research provides enterprises with insight into how peers are succeeding (and failing) with NPM tools. It illuminates how different NPM technologies are applied to different use cases, from a platform perspective and a data perspective. EMA suggests that enterprises use the insights in this report to build their own tool strategy based on the needs they have.

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.

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

3834.060219