


Monitoring Optimization 2010

Trends and Issues Surrounding Network and Security Monitoring

Sponsored by: 

Introduction

Monitoring is an essential practice for operating today's networks in an efficient and secure manner. Every organization recognizes this fact and many have made significant investments in monitoring tools and technology, yet significant challenges are faced in successfully deploying and optimizing their use. ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) analysts conducted a research project involving network and security operations professionals during September 2009 to study the challenges and best practices for optimizing monitoring. The primary goal was to understand the barriers organizations face in successfully deploying their monitoring products and practices, and how those issues are being addressed.

The Need for Visibility

The primary purpose of monitoring technologies is to provide visibility into the ongoing operations of an IT infrastructure, for assuring reliable availability and performance of applications and services as well as protecting their integrity while meeting compliance requirements. Network and security operations teams make significant investments in monitoring tools and technologies, many of which rely on direct access to network traffic packet streams in order to provide their function. A key challenge to optimizing monitoring coverage lies in the use and sharing of traffic access points such as SPANs and TAPs.

A Lack of Coverage

One key finding in our research is that most organizations are falling short in monitoring their network segments. Only 19.3% believe they have achieved sufficient monitoring coverage, and EMA found three key reasons why the rest were not able to meet their goals:

Only 19.3% believe they have achieved sufficient monitoring coverage.

1. Lack of Network Access – 43% of respondents reported they lack sufficient SPANs/TAPs to which they could attach monitoring tools. This results in part from a lack of access to network segments of interest and also in part due to the lack of ability to share what access points do exist.
2. Sub-optimal Monitoring Tool Deployments – two thirds of participants (66%), indicated they lack enough tools or the budget to buy them. Despite this, we also found that nearly half of participants (47%) were not fully utilizing the tools they had in place. Add to that the 25% who reported tools which were overloaded and dropping packets, and it becomes clear there is a great opportunity for optimization.
3. Lack of Staff or Staff Skills – nearly a quarter of our research group (24%) reported they either lack the staff to keep up with monitoring tasks or the training within existing staff to keep up with administration or interpretation. This situation results from both current and ongoing budgetary pressures as well as a trend (identified by 62%) of staff moving towards more generalist roles, reducing the availability of technical specialists.

Packet Filtering – Opportunities and Challenges

One of the ways to provide broader coverage as well as to keep monitoring tools running at optimal capacity is to implement filtering and sharing of network traffic packet streams. If done properly, this can extend the scope of existing tools as well as reduce the administrative (and hence training) load on overburdened staff. Key findings in this area include:

1. Most companies (67%) use some form of filtering to manage utilization of their monitoring tools.

Monitoring Optimization 2010

Trends and Issues Surrounding Network and Security Monitoring

2. Ongoing administration of filters for tuning and to prevent packet loss is a constant challenge, with nearly half (46%) of respondents indicating they need to change filter configurations on a weekly or more frequent basis.
3. Filter administration itself is perceived to be difficult by the vast majority (80%), and nearly half (46%) characterize it as either “very hard” or “nearly impossible.”
4. A lack of command line interfaces (CLI) skills for administering filters on both network and security teams is cited as an aggravating factor, raising the need for graphical, intuitive alternatives.

The 10 Gigabit Ethernet Factor

Monitoring tools which can handle 10Gb Ethernet environments are plentiful, but costly, driving many to question whether or not existing 1Gb-rated tools can meet the interim needs for monitoring 10Gb environments. We found that while a minority of participants indicated they have already converted or upgraded their tools to 10Gb (20%), or that their existing mirroring solution was converting 10Gb to 1Gb for them (15%), the remaining 65% need to extend the life of their 1Gb tools by other means. Monitoring optimization solutions can provide this function, allowing both media conversion from 10Gb to 1Gb while also filtering non-essential traffic so that 1Gb tools don't get overloaded.

EMA Summary and Analysis

While companies have invested heavily in monitoring tools, the results of the survey indicate a variety of challenges in establishing and optimizing network traffic access, whether for security monitoring or network monitoring and troubleshooting. These issues translate into operational risks that will inevitably grow over time. Factors such as the move to 10Gb infrastructure and stricter compliance requirements are aggravated by staff growth limits and technical skill gaps. As a result, the majority of our survey participants are not able to achieve desired monitoring coverage and/or their tools are fully loaded and regularly dropping packets, compromising the integrity of their role and purpose.

Much of the difficulty comes down to the relationship between staff and their ability to make the most of the monitoring tools they have on hand. According to one senior network engineer at an Internet operations provider, “There's a tremendous amount of variability in the traffic we see coming from our various customers, and we don't have enough tools or people in place to baseline them all.” A HIPAA security consultant expressed similar concerns noting, “Many of the data center teams I work with don't realize what to use SPAN for, let alone how to set it up.” And a network director summed up his ideal answer as follows, “I need staff to be more general and broadly capable, so they can better collaborate – but they also need to specialize further to keep up with specific domain technologies.”

Many of these challenges can be met with the use of monitoring optimization solutions which provide flexible filtering and data sharing, reducing administrative hurdles and allowing operators to keep up with changes in the managed environment. With ongoing pressures to do more with less, technologies that facilitate better sharing and leveraging of management data for multiple functional purposes should find favor in terms of cost efficiencies, while also allowing monitoring tools to deliver their intended improvements of key IT metrics for uptime, security, and performance.

Many challenges can be met with the use of monitoring optimization solutions.

About EMA

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that specializes in going “beyond the surface” to provide deep insight across the full spectrum of IT 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 its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise IT professionals and IT vendors at www.enterprisemanagement.com or follow EMA on Twitter (http://twitter.com/ema_research).

1998.121109

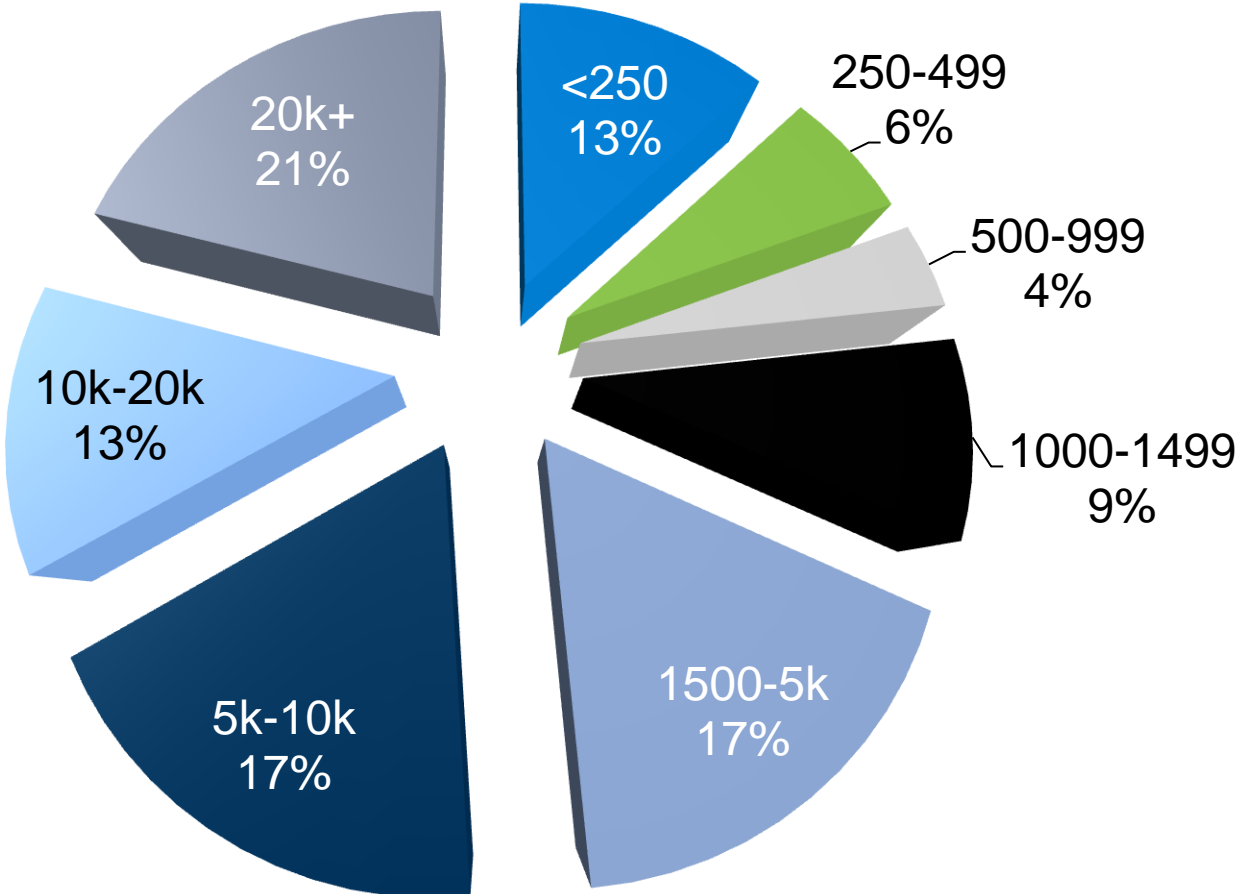
Monitoring Optimization 2010

Trends and Issues Surrounding Network and Security Monitoring

Research Results for Anue Systems

December 2009

Participants: Broad Range of Organizational Sizes (# Employees)



Sept 09: n=125

Participants: Rich Diversity in Industry Sectors Represented

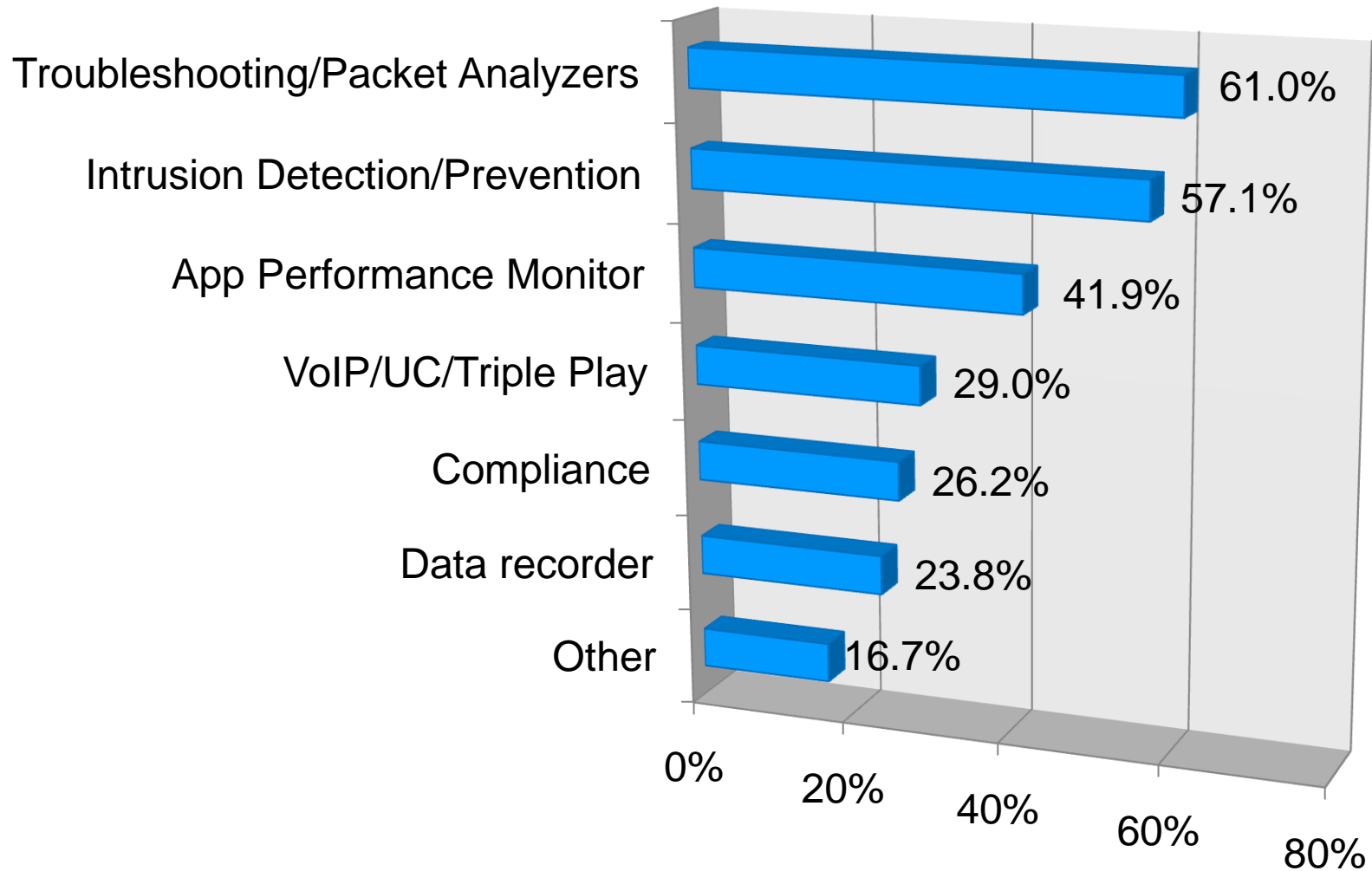


Top 10 Sectors	% Participants
Finance/Banking/Insurance	15.2
High Tech: ISV/VAR/SI	13.6
High Tech: App/ISP/Managed/NW Service Provider	9.6
Prof Services/Consulting	9.6
Healthcare/Medical/Pharma	8.8
Telecommunications	8.0
Manufacturing	7.2
Government	4
Aerospace/Defense	3.2
Education	3.2

Sept 09: n=125

Access Role: Monitoring Tools in Use Attached to SPANs and TAPs

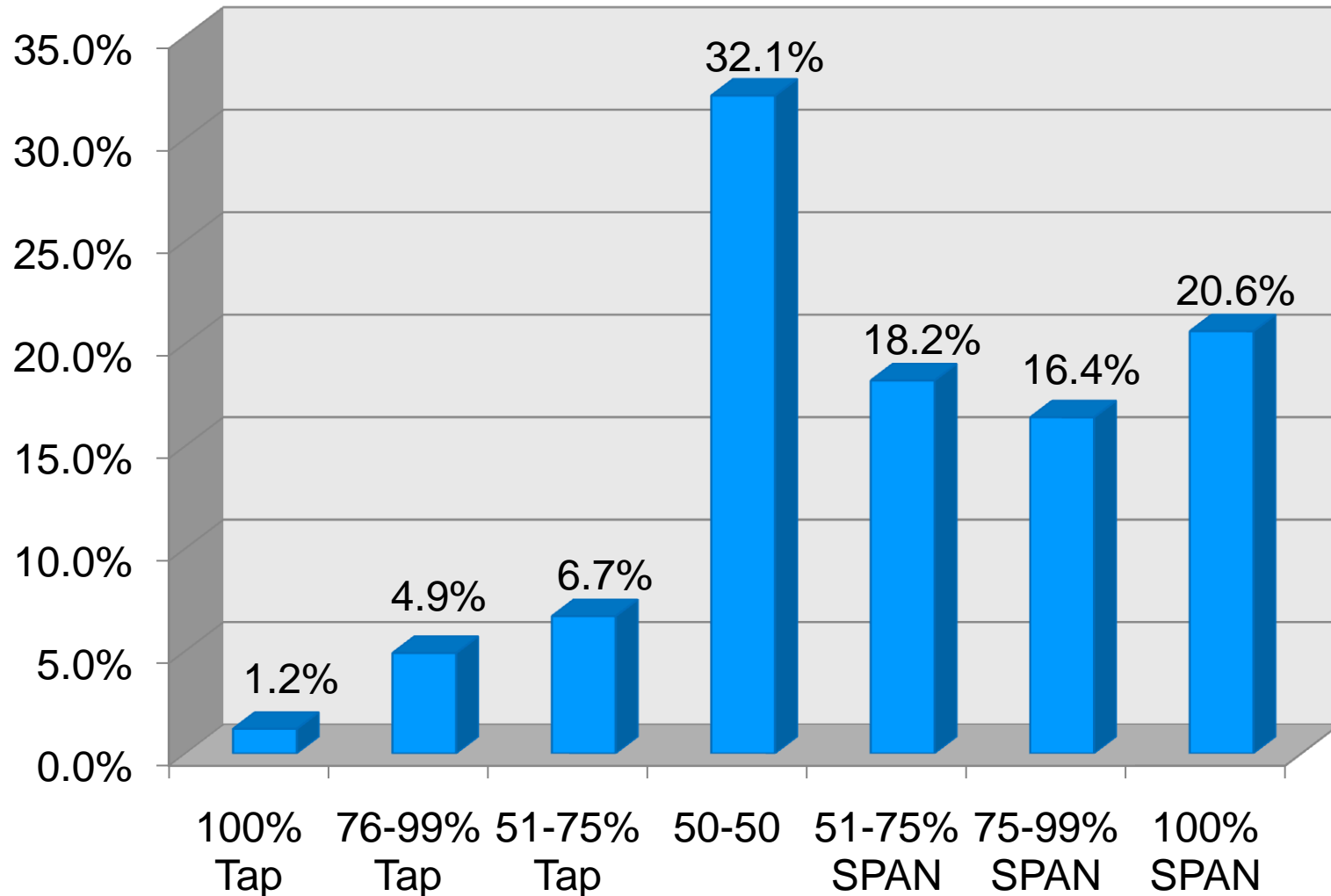
Broad diversity evidences high access demand



Sept 09: n=210

Access Types Deployed: SPAN vs. TAP

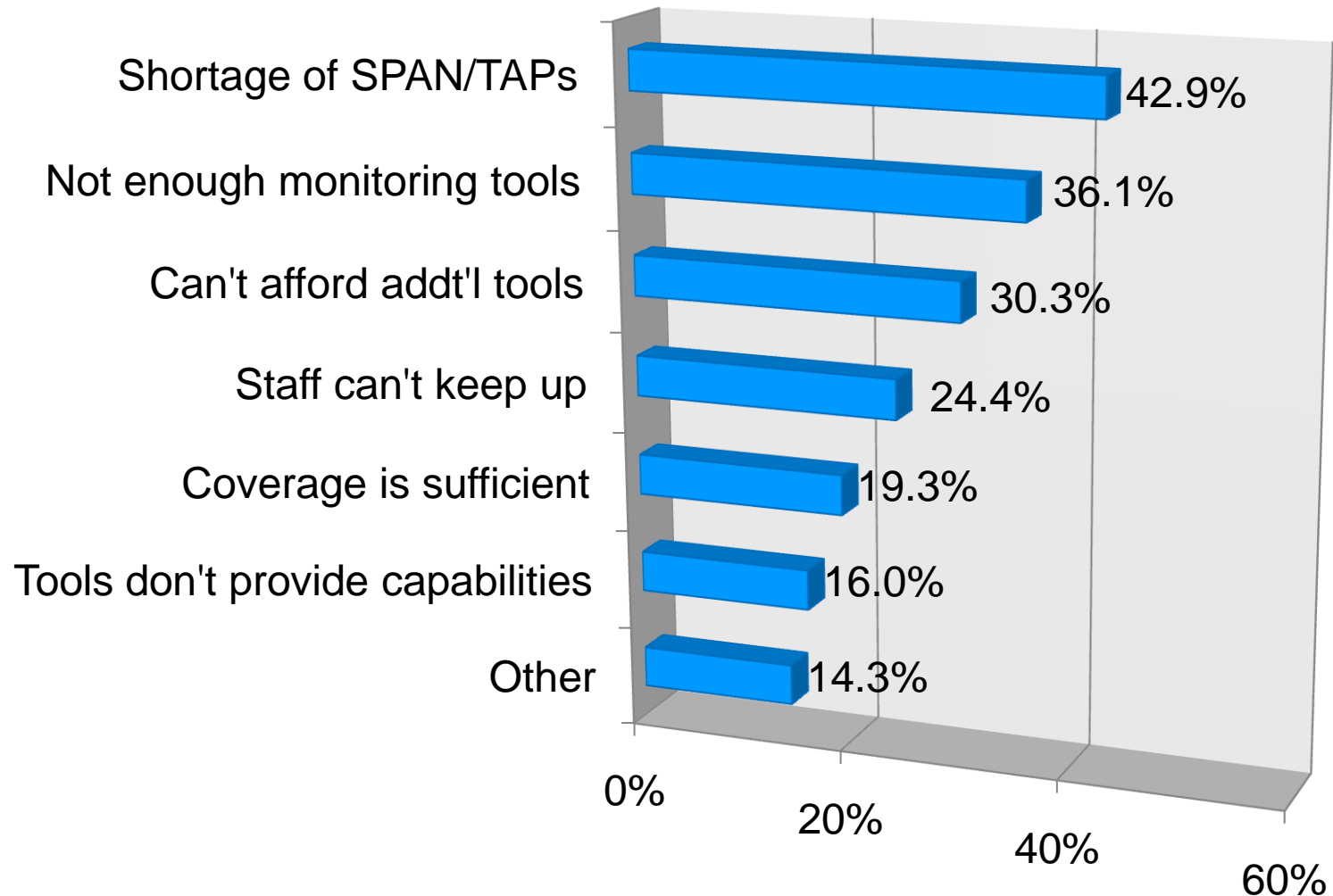
SPAN preferred, though a mix is most often used



Sept 09: n=165

Coverage: Why aren't 100% of network segments monitored?

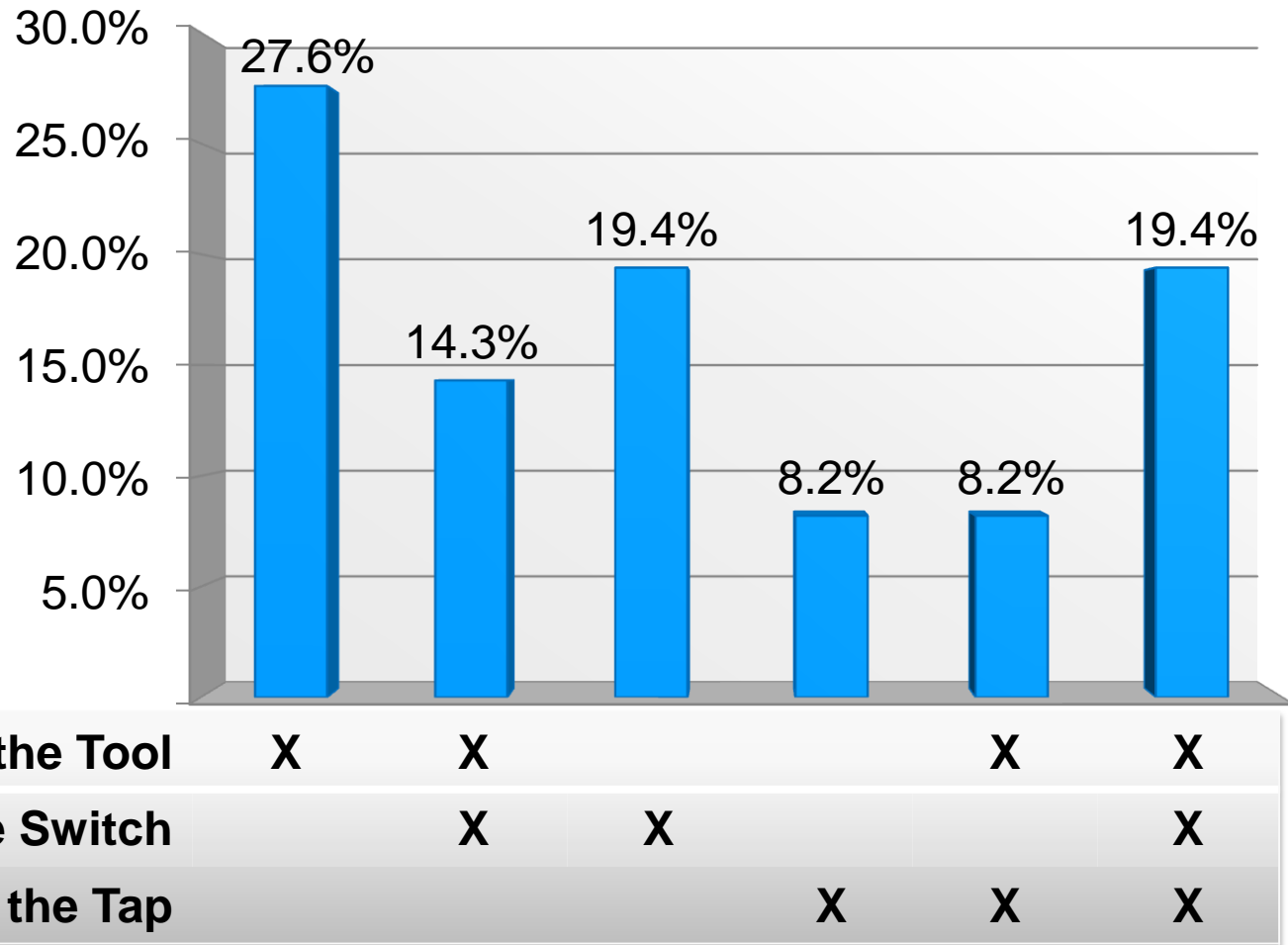
Lack of tools, available access, staff shortage all common



Sept 09: n=119

Where Filters are Implemented

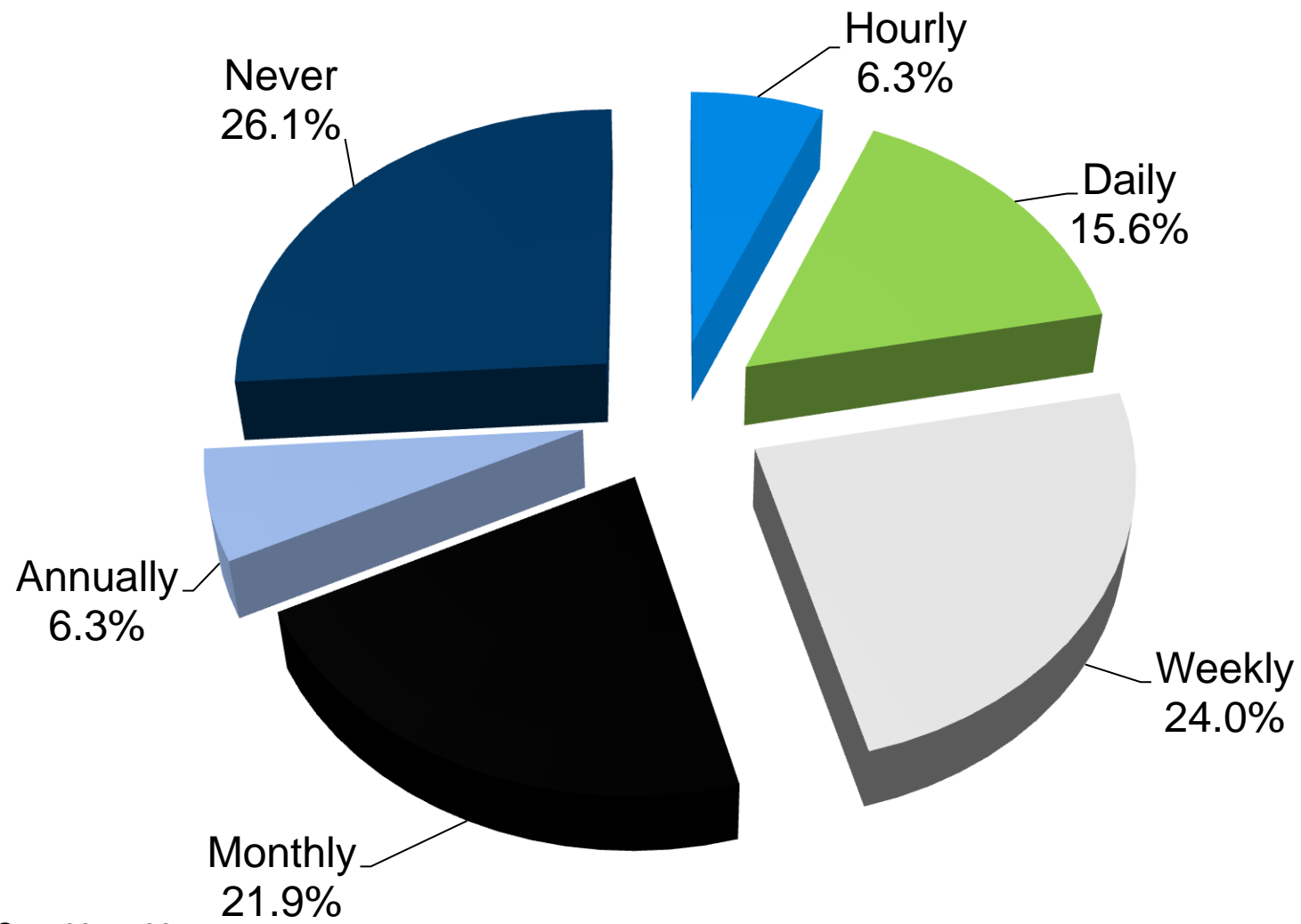
Tool and switch filters most common; Tap filters lag adoption



Sept 09: n=98

Correcting Filters for Dropped Packets – Frequency of Changes Required

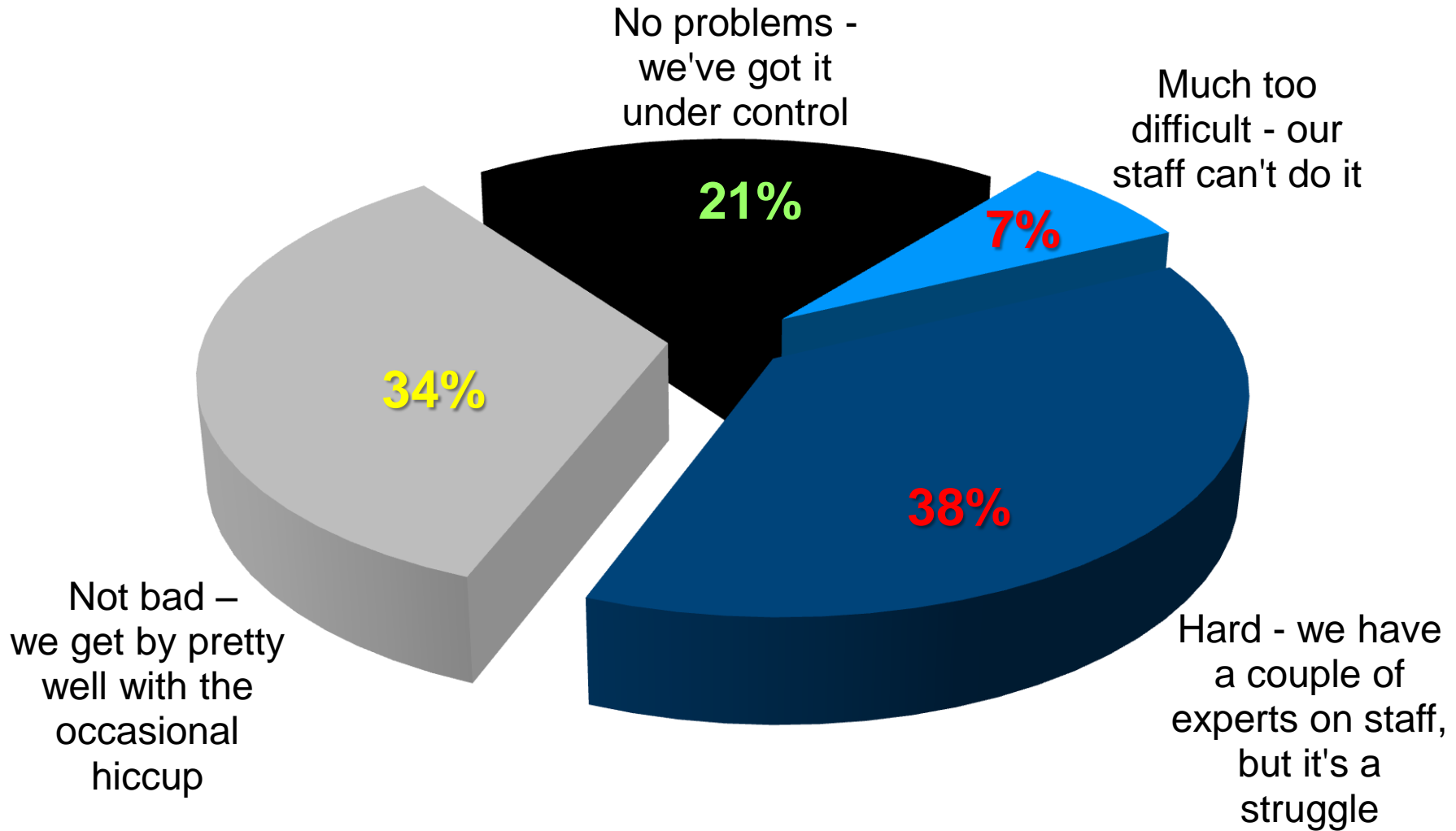
Nearly half make changes weekly or more often



Sept 09: n=96

Difficulty with CLI Filter Administration

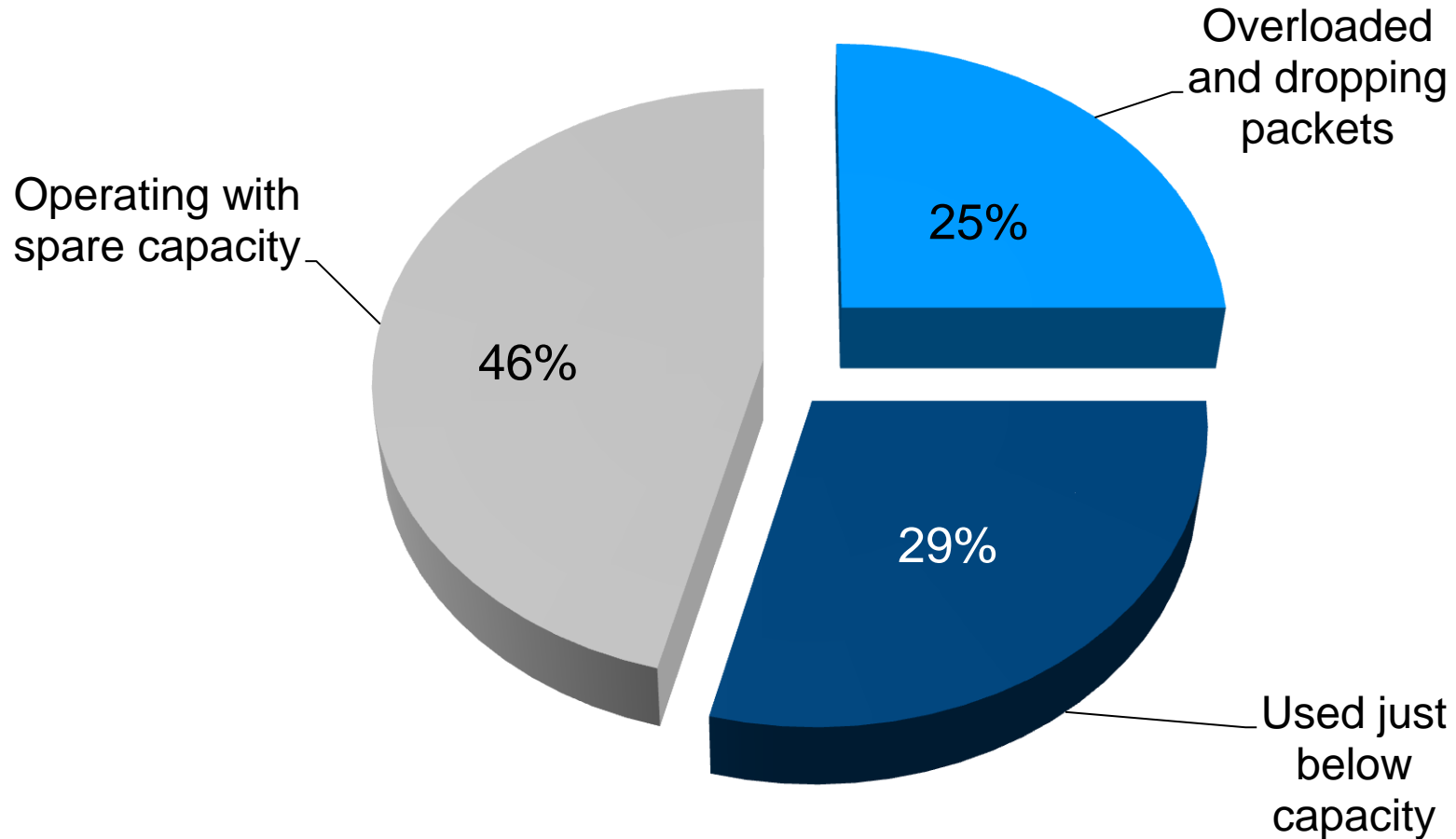
45% find this a major challenge



Sept 09: n=146

Problems with Monitoring Tool Utilization

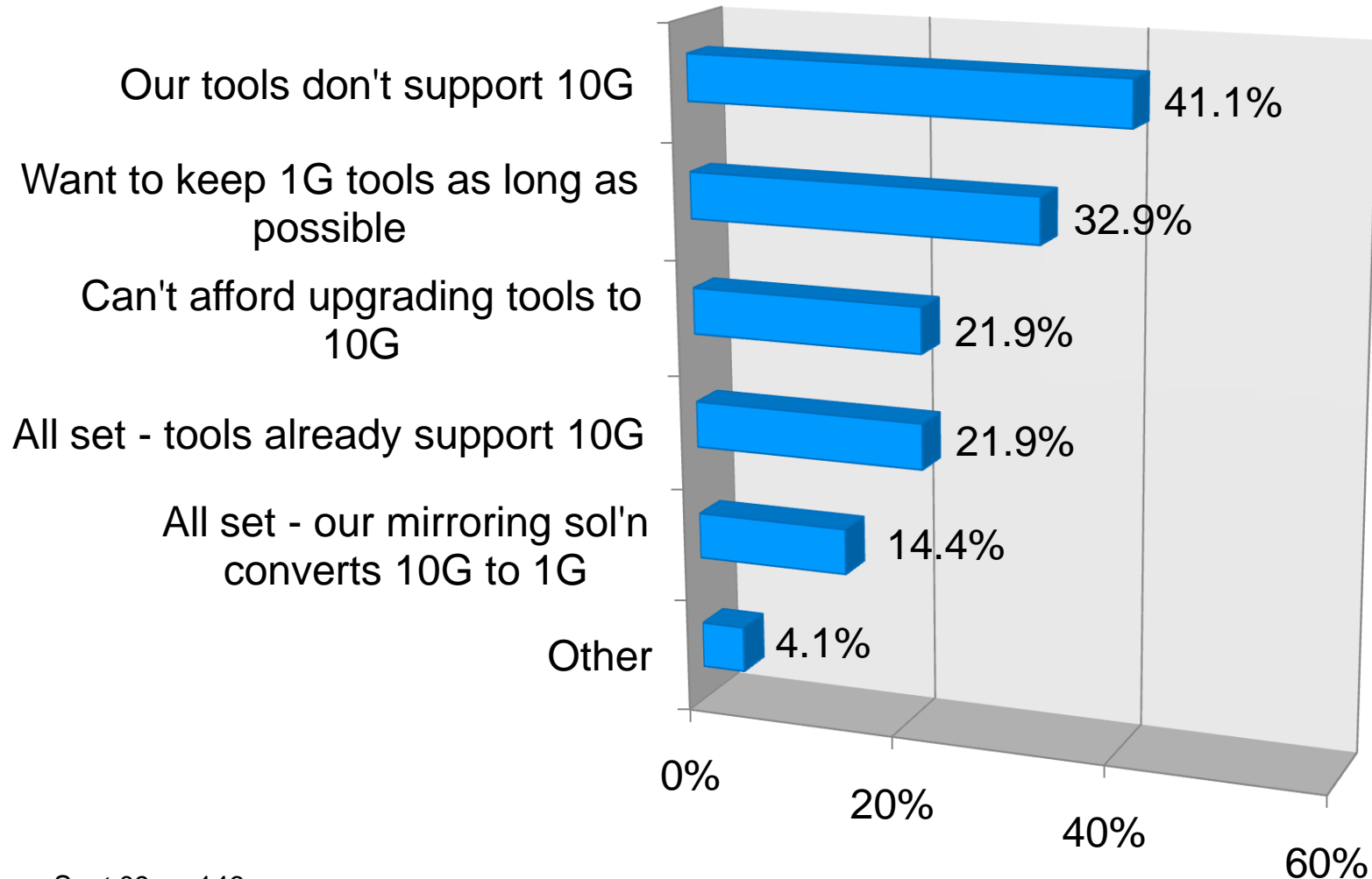
Less than one third optimally tuned; many are compromised due to overloading



Sept 09: n=146

Strategy for Monitoring 10Gb Ethernet

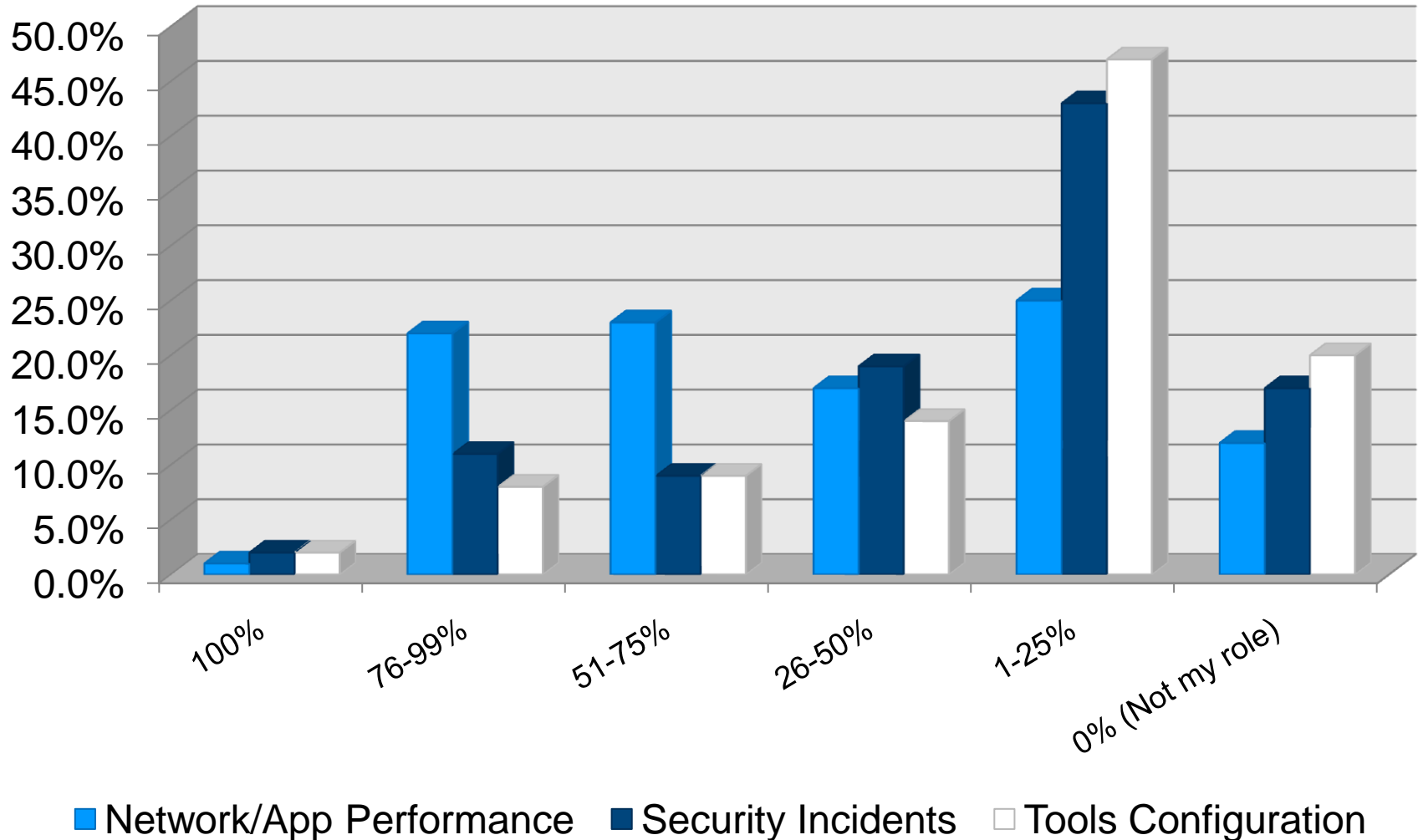
Majority need help extending life of 1Gb Tools



Sept 09: n=146

Overworked Staff: Time Spent Troubleshooting Network/Security/Config

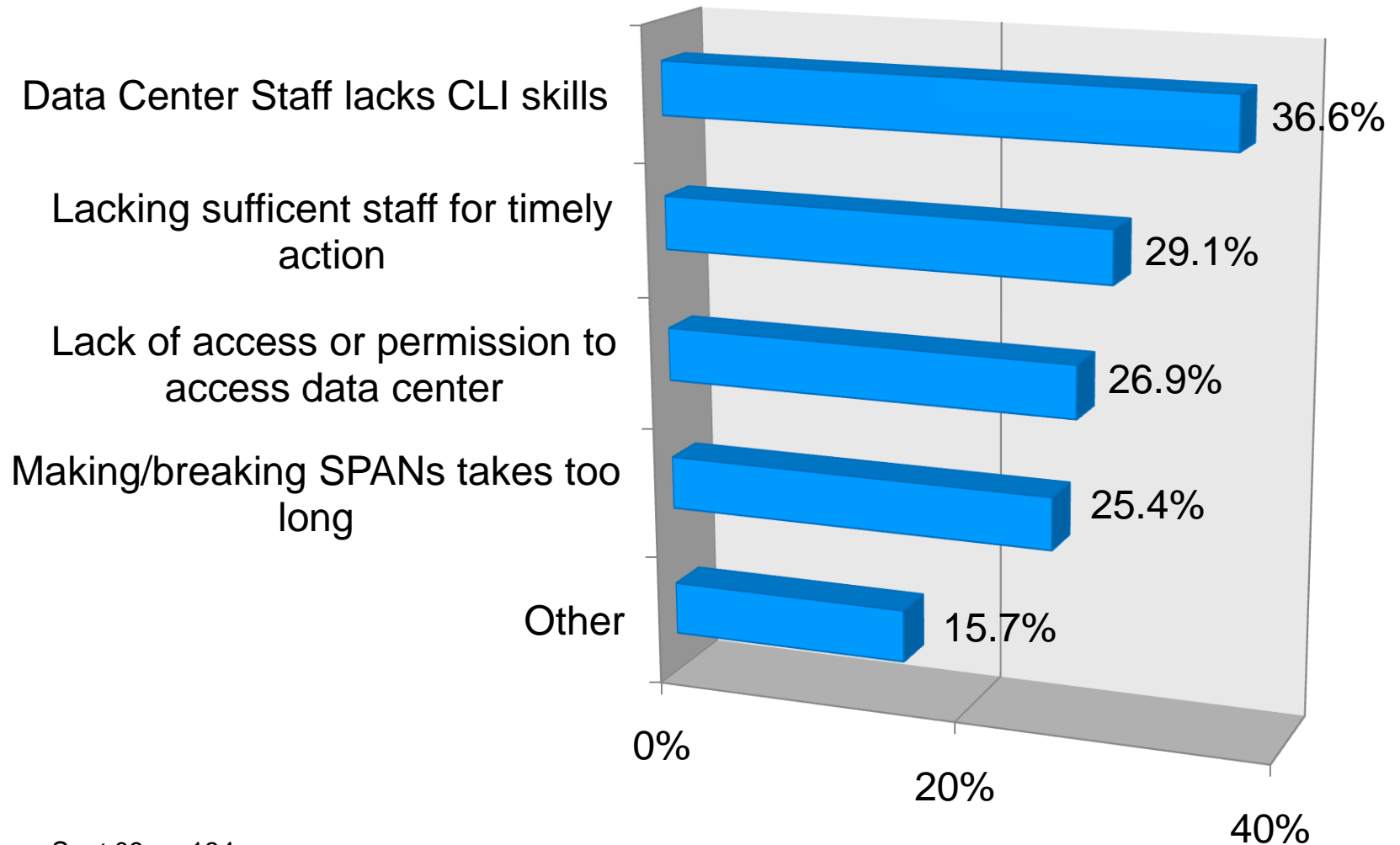
Network /App primary focus; security & tools add demand



Sept 09: n=133

Challenges in Establishing Access

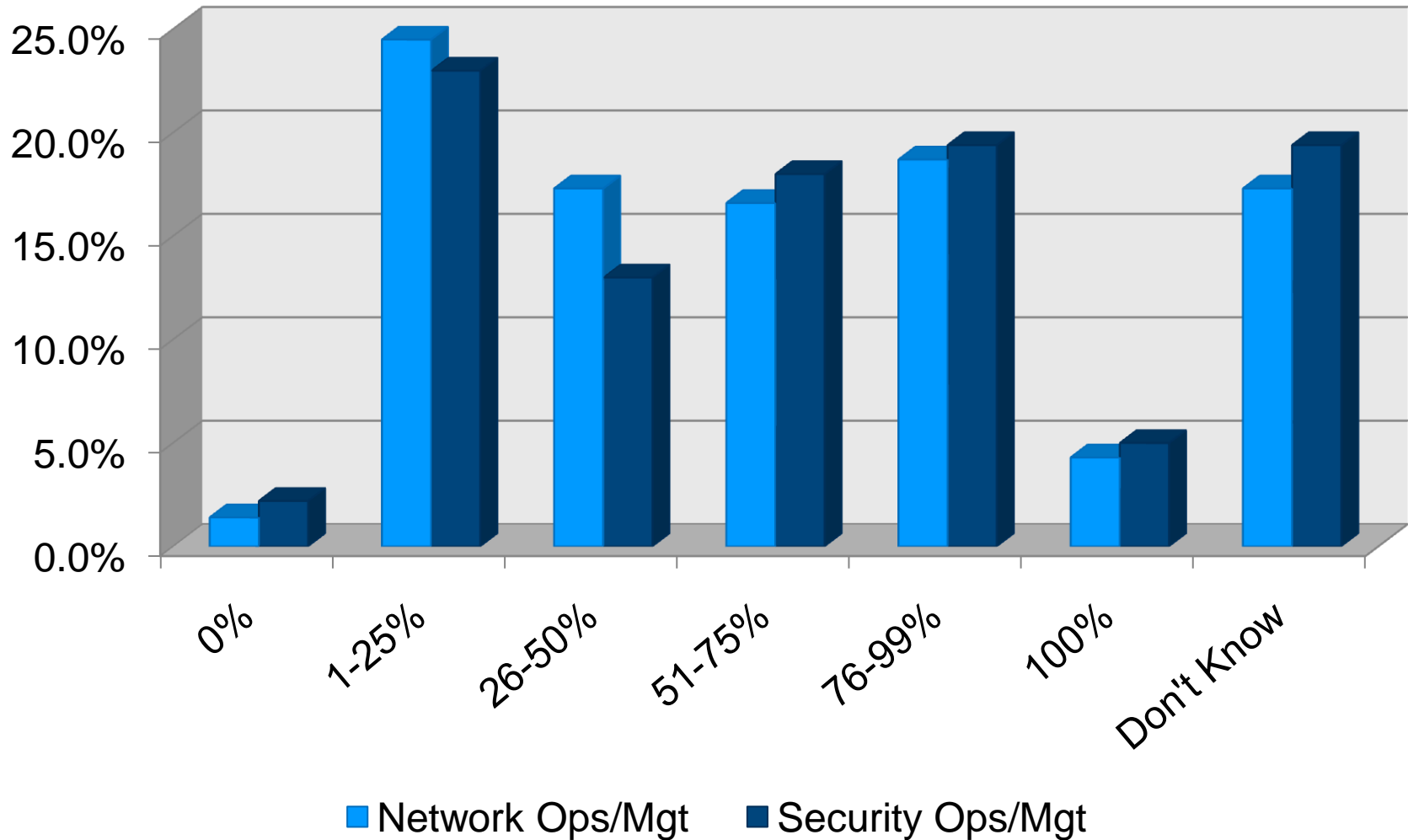
Skill gap is dominant barrier; staff, permissions and logistics also common aggravators



Sept 09: n=134

Filter Admin: Who is adept at CLI?

Few are fully trained; Network Ops less likely than Security



Sept 09: n=139

Participant Quotes



- “There is big gap right now, due to lack of tools and people trained to do the analysis to find relevant compliance information from the network.”
HIPAA Security Consultant
- “Many (data center personnel) don’t realize what to use SPAN for or how to set it up.” *HIPAA Security Consultant*
- “We’re very resource constrained, and there is such variation in the amount and type of traffic coming from our customers that we don’t have the tools or the people to properly baseline normal versus abnormal.” *Senior Network Engineer*
- “We want our employees to be broadly knowledgeable – via cross-training and building a more systemic view” *Senior Network Engineer*
- “I need staff to be more general and broadly capable, so they can better collaborate, but they also need to specialize further to keep up with specific domain technologies”, *Network Director*

Participant Quotes



- “We are looking for persistent sources of (security) data. Traffic monitoring for incident response is usually only done sporadically.” *Principal SOC Consultant*
- “There have been a lot of wins for sharing security data with network operations. Many are not security issues at all, but security monitoring recognizes things that are broken, and the rule of thumb is that it might be a compromised system, but it might also be just a bad application situation.” *Principal SOC Consultant*
- “Intelligent network taps are awesome – they solve the conflict between network operations and network security needs, which often create push-pull relationships.” *Principal SOC Consultant*
- “There are two SPANs per switch – network and security, and then you are done. If we need to monitor both inbound and outbound for network performance, then we give up security access.” *Network Performance Manager*
- “We filter in the tools, except for some applications such as DLP, where we don’t want things like NetBIOS or GLP getting scanned, so we filter those upstream.” *Network Performance Manager*