Report Summary – The Internet of Things and Enterprise Networks

Planning, Engineering, and Operational Strategies

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

April 2017

Report Summary – The Internet of Things and Enterprise Networks: Planning, Engineering, and Operational Strategies

Table of Contents

Executive Summary 1

Introduction 1

Key Findings 1

Research Participants: Directly Involved in Enterprise Networks and IoT Initiatives 2

IoT and the Network Infrastructure Team 3

- The Network Team Usually Leads IoT Projects 3
- The Network Team's Essential IoT Partners 3

IoT Network Planning and Engineering 5

- IoT Connectivity Strategies 5
- IoT Challenges to Network Planning and Engineering 7
- IoT Architectural Considerations: Edge Analytics 9
  - IoT Edge Analytics 9

Managing and Monitoring IoT Networks and "Things" 10

- IoT Monitoring Blind Spots 11
- Monitoring IoT Networks: Tool Choices 12
- Meeting the Challenge of IoT Monitoring and Management 13
- The Network Infrastructure Team and IoT Devices 16

Conclusion: How Network Teams Successfully Lead IoT Projects 17

- IoT Architectural Best Practices 18
- IoT Management and Service Assurance Best Practices 18

Demographics 19

Report Summary – The Internet of Things and Enterprise Networks: Planning, Engineering, and Operational Strategies

Executive Summary

This research summary highlights the results of an end-user research study that examined how enterprise network infrastructure teams contribute to the Internet of Things (IoT) strategies at their organizations. It reveals the planning and engineering challenges they encounter and the architectural choices they make to deliver connectivity to IoT devices. The research also examines how network infrastructure teams manage, monitor, and troubleshoot IoT networks and, in some cases, the IoT devices themselves. Finally, the research examines some of the organizational impacts experienced by network teams when they implement IoT projects.

Introduction

While the phrase Internet of Things (IoT) is relatively new, the idea of connecting "things" to the network is not. Enterprises have been connecting medical scanners, manufacturing systems, vehicles, and other devices to networks for years. Only recently, however, with industry leaders articulating the idea of IoT, have enterprises become strategic about how they connect this mishmash of things to networks and extract value from the data and control that connectivity affords them.

IoT often requires a partnership among IT organizations, operational technology organizations, and lines of business. When planning and implementing an IoT ecosystem, many IT organizations find themselves in unexplored territory, lacking a roadmap for success. With that in mind, EMA conducted research on how network infrastructure teams are supporting IoT. EMA surveyed 100 IT professionals who were (1) directly involved in planning, implementing, and/or operating networks and (2) directly involved in their organization's IoT initiatives.

This research summary explores how network infrastructure teams execute IoT projects. It identifies the technologies they adopt, the challenges they encounter, and the partnerships they form. EMA's intention is to offer some early guidance and suggestions on best practices that network infrastructure professionals can adopt when tasked with supporting IoT.

Key Findings

Network teams lead IoT projects. Nearly 90% of research participants said that the network team plays a leading role in at least some of their organization's IoT initiatives. The research also showed that the network team is most successful with IoT when it leads all of its organization's initiatives.

The network team relies on critical IoT partners. The network team's top internal partners on IoT projects are the IT service management group and the security team. Its most critical external partners are network operations software vendors.

Distributed edge analytics is a common feature of IoT architecture. 73% of organizations have implemented analytics at the edge of their IoT ecosystem. They have implemented this capability primarily to (1) improve system reliability, (2) expand real-time analysis of data, and (3) reduce security risk.

IoT security concerns are pervasive. Networking professionals identified security as a challenge in all aspects of IoT planning, engineering, and operations. Concerns included modeling of unique IoT threats, a lack of support for channel-based security techniques on IoT devices, scalability concerns in existing network security infrastructure, and more.

IoT security breaches have occurred. 52% of respondents reported that IoT has created or worsened blind spots in their network monitoring architecture. Among those reporting blind spots, 40% have experienced a security breach.

IoT scale challenges network monitoring tools. The primary challenge to effective IoT network monitoring is scale. There are simply too many devices connecting to the network. Enterprises are most often responding by (1) upgrading the network data processing capacity of their monitoring tools, (2) upgrading their monitoring tool licenses to account for device growth, and (3) installing network visibility controllers (also called "network packet brokers").

Real-time analysis of network data is essential. 72% of organizations say IoT has created a need for faster, real-time analysis of network data, primarily to help with detection of IoT security incidents and threats and to help with monitoring of IoT services.

Network teams are managing IoT devices. 68% of network teams have extended their monitoring tools to monitor and manage IoT devices.

Research Participants: Directly Involved in Enterprise Networks and IoT Initiatives

Forty-two percent (42%) of research participants were part of the "IT executive suite," while the rest held various staff-level positions. More than half (54%) worked in midmarket organizations (1,000 to 9,999 global employees) with the rest working for larger enterprises (10,000 or more employees). Twenty vertical industries are represented in this study. The most prominently represented industries were "banking/finance/insurance" (15%), "application/cloud/managed service provider" (10%), "education" (9%), and "manufacturing – not computer hardware or networking" (9%).

To qualify for participation in this research, survey respondents had to be directly involved in the networks supporting their organization's IoT initiatives. **Figure 1** shows the majority of respondents are playing multiple roles in these IoT projects, most frequently in monitoring IoT-related network availability and performance. Most of them are also helping to research and evaluate IoT-related network solutions and to plan and deploy IoT-related networks. Many are also working to identify new opportunities for the network infrastructure team to support IoT, which suggests a strategic role in IoT initiatives.

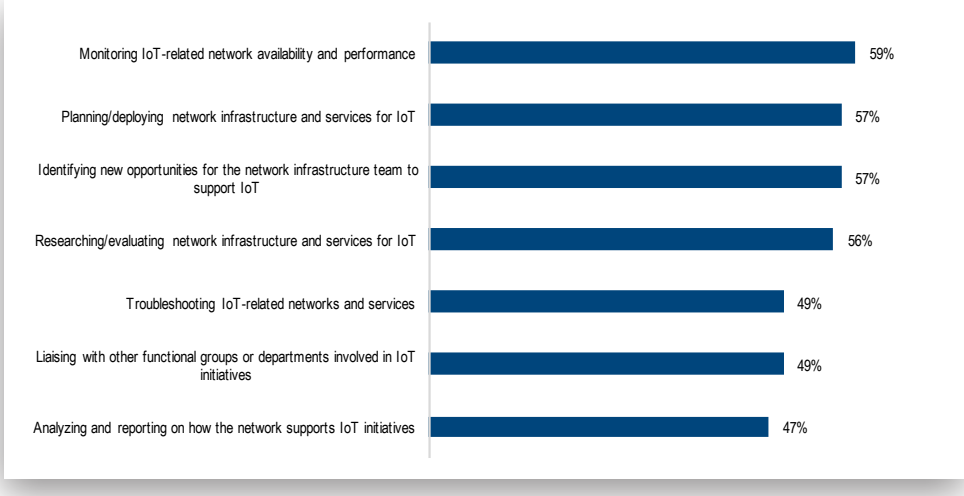

Figure 1. Research participants' involvement in their company's IoT initiative(s)

IoT and the Network Infrastructure Team

The Network Team Usually Leads IoT Projects

EMA asked research participants to describe the organizational role that the network infrastructure team plays in IoT. In 89% of enterprises, the network team plays a leading role in IoT initiatives at least some of the time. As **Figure 2** shows, the majority of network infrastructure teams (52%) play a leading in role in some IoT initiatives and a supporting role in others. Another 37% play a leading role in all IoT initiatives. Just 11% play a supporting role in all IoT activity.

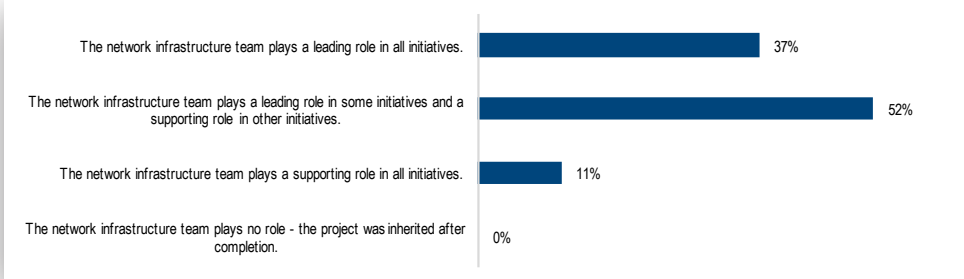

Figure 2. The role of the network infrastructure team in the overall planning, implementation, and operation of an organization's IoT initiatives

The Network Team's Essential IoT Partners

Figure 3 shows that the ITSM group was the most prominent internal partner for the network team. This finding demonstrates that the network team believes IoT requires a framework of standardized, industry-best practices for IT services. EMA suspects that enterprises are exploring ways to help the ITSM group map IoT ecosystems to service maps and industry best practices.

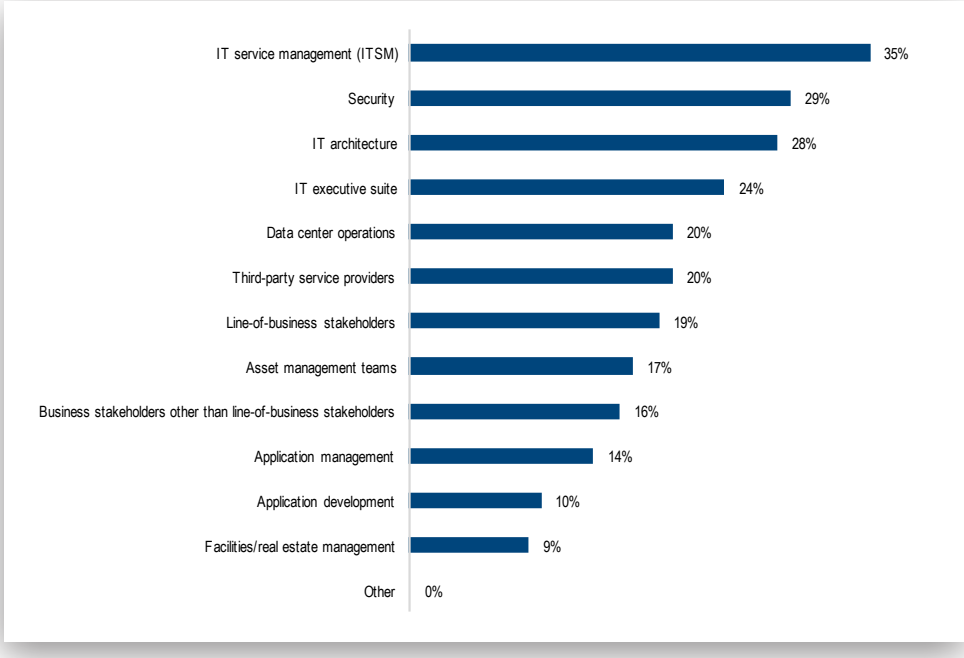

Figure 3. Internal stakeholders that collaborate most closely with the network infrastructure team on IoT initiatives

The security group and the IT architecture group were the chief secondary partners of the network team. And support from the IT executive suite is also important. Business stakeholders and application developers and managers are not prominent partners for the network team, however.

Figure 4 examines the external partners that the network team leans on for IoT. The network team clearly identified network operations software vendors as its most important external partners for IoT success. Later in this report we will explore this issue in depth, but for now it's clear that network management and monitoring software is a special area of focus for any network team that is involved in IoT.

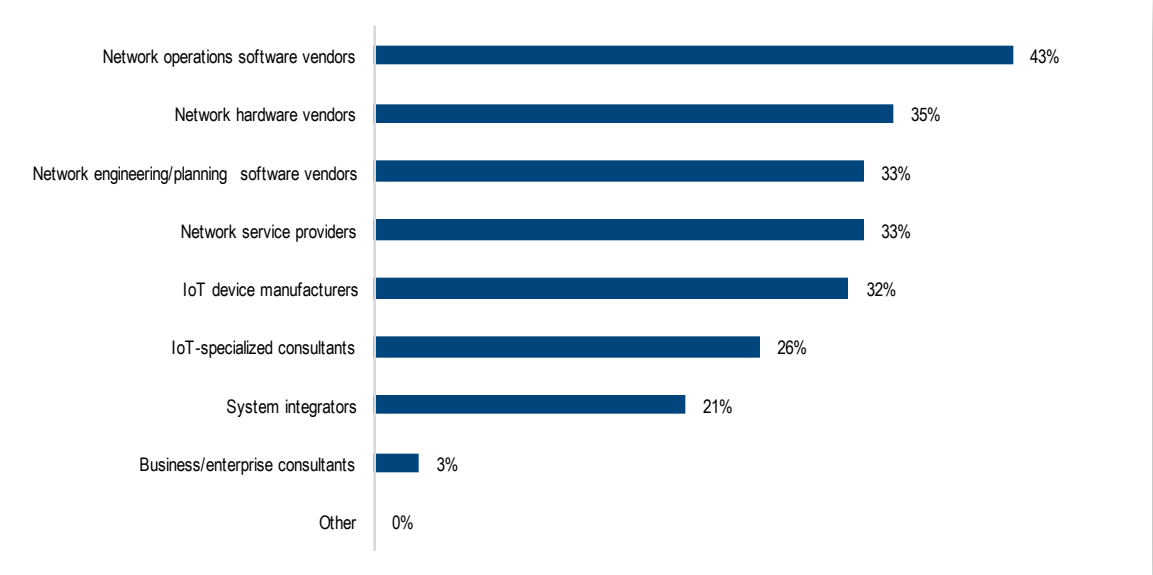

Figure 4. From the perspective of the network infrastructure team, these external partners are most critical to IoT success.

Network hardware vendors, network engineering/planning software vendors, network service providers and IoT device manufacturers are all clear secondary external partners that play important roles in helping network teams execute IoT projects. Network hardware vendors appear to be more important external partners to organizations that lean heavily on the network team for IoT. Of organizations with network teams that play a leading role in all IoT initiatives 57% identify their network hardware vendors as essential partners, versus only 25% of organizations where the network team plays a leading role in only some IoT initiatives.

Individuals outside the network infrastructure team will obviously feel differently about this list of external partners, but for the network team, this data should serve as a guide to establishing internal and external partnerships for IoT initiatives.

IoT Network Planning and Engineering

IoT Connectivity Strategies

When tasked with connecting IoT devices, a networking team will need to determine if it can support those devices with existing infrastructure. In most cases, an IoT initiative will involve devices that are deployed both within and without existing network footprints. Also, as we established earlier, nearly 90% of enterprises in this study have multiple IoT initiatives. While one project might fall mostly within the scope of the existing network, a second initiative might require connectivity in places where no network exists.

In this research, EMA sought to understand how network infrastructure teams address this connectivity puzzle. We established five general approaches to how an organization might deliver IoT connectivity.

- Existing LAN infrastructure – This term covers all local wired and wireless networks that an enterprise had in place prior to an IoT initiative.
- New LAN infrastructure for IoT – This category covers all new local wired and wireless network infrastructure an enterprise installed specifically to address gaps in coverage for IoT.
- Existing WAN services – This category includes pre-existing wide-area networks, including MPLS, broadband internet, and 4G/LTE wireless.
- New IoT-specialized WAN services – This category includes new wide-area technologies that an enterprise deployed specifically to provide connectivity to IoT, such as low-power WANs.
- Connectivity packaged by an IoT solution provider – In interactions with enterprises and service providers, EMA has determined that many providers of IoT-specific networks based on low-power WAN technologies rarely interact directly with enterprises. Instead they sell network connectivity to commercial and consumer IoT vendors that package connectivity with their devices and solutions. With that in mind, this last category covers all connectivity that enterprises acquire indirectly through IoT solution providers and vendors.

Three of these approaches to IoT connectivity emerged as fairly common, as **Figure 5** indicates. Nearly half of enterprises are using existing LAN infrastructure, new IoT-specific LAN infrastructure, and existing WAN services. IoT-specific WAN technologies and connectivity packaged by an IoT provider were less commonly used.

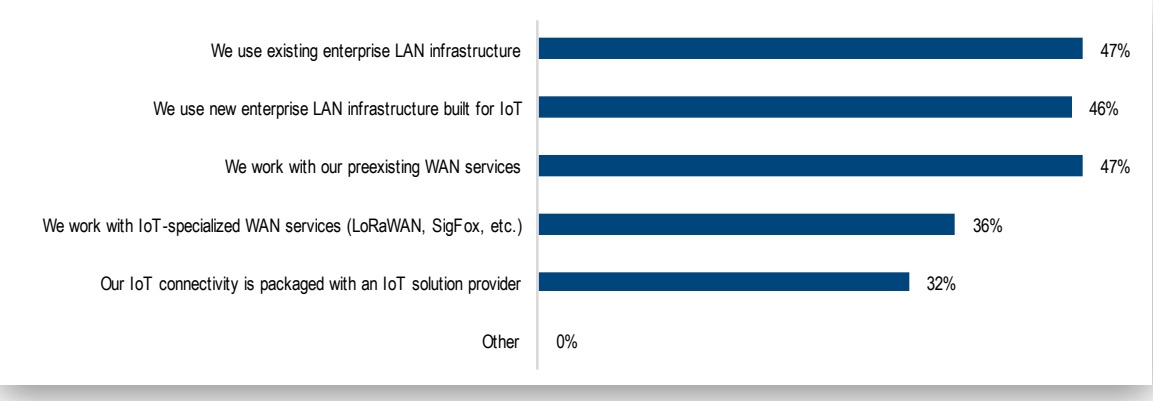

Figure 5. How enterprises deliver network connectivity to IoT devices

The data suggests that network teams are primarily working with familiar LAN and WAN technology to support IoT. Even those that are building new LAN infrastructure for IoT are likely to be using familiar Ethernet and Wi-Fi solutions since IoT devices connected to local networks don't face the power constraints that drive adoption of low-power technologies like LoRaWAN and SigFox.

Delving into the specific network technologies that enterprises use within their IoT-related networks also reveals just how important existing LAN and WAN technologies are to these IoT projects. **Figure 6** shows all of the network technologies that research participants are using in their IoT networks. The majority uses wireless LAN and Ethernet LANs, and many are also using wireline WAN and 4G wireless. Bluetooth is also a very important form of connectivity for these IoT projects, which suggests that many enterprises are pursuing IoT use cases based on location-based services, which often rely on Bluetooth beacons.

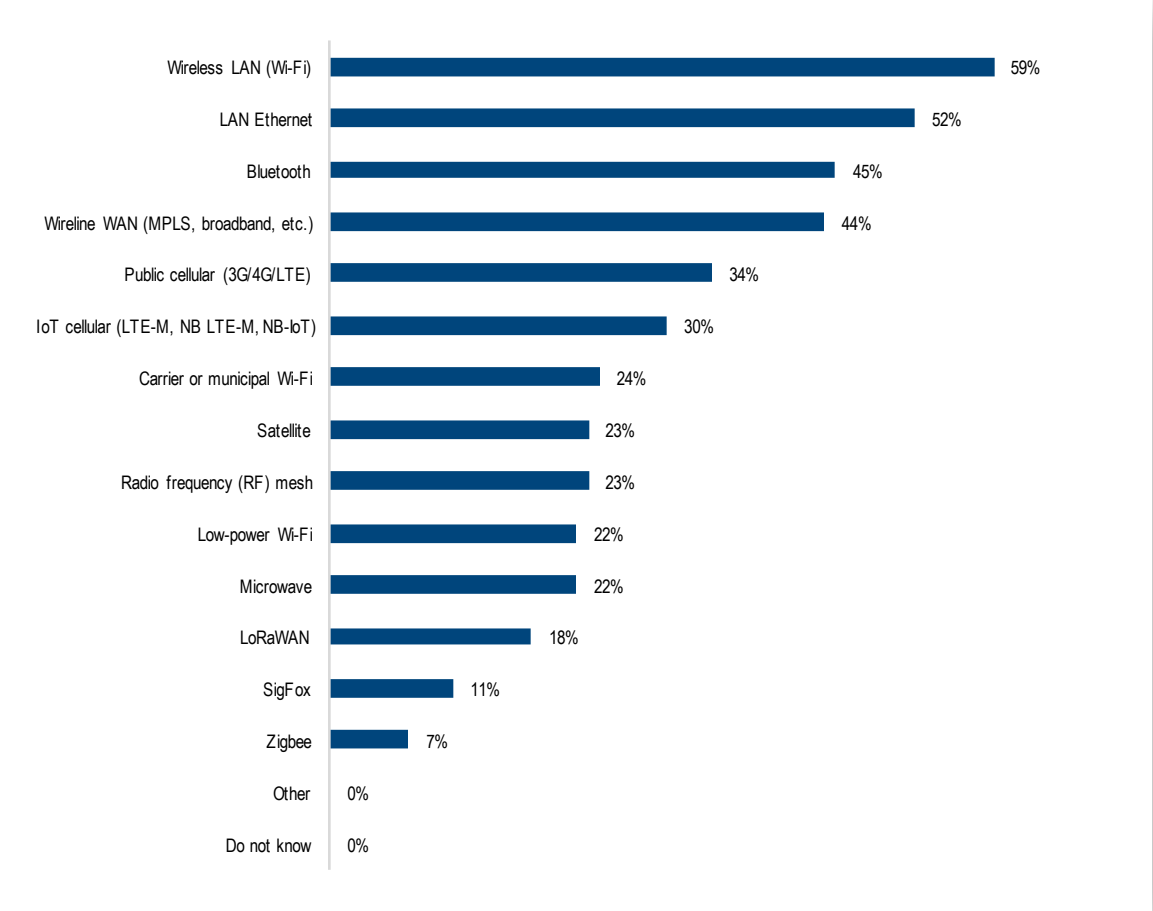

Figure 6. Network technology used to supply connectivity to IoT devices

IoT Challenges to Network Planning and Engineering

EMA asked research participants to identify the aspects of IoT network planning and engineering that they find most challenging. These IT organizations have a broad set of concerns, as **Figure 10** illustrates. Network address management tops the list of problems. Industry prognosticators have warned for years that IoT will add billions of new devices to networks. And each device will need an IP address and MAC address. If an organization manages IP addresses with an open source tool or a spreadsheet, they will struggle to scale these tools for IoT.

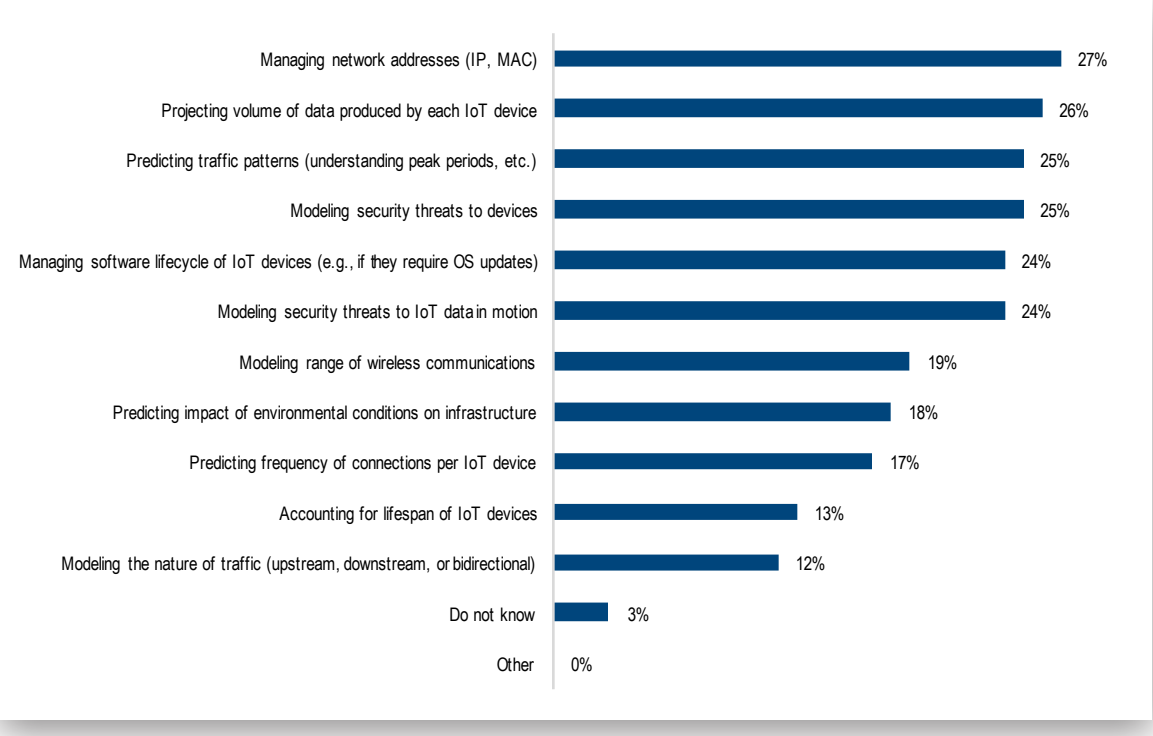

Figure 7. IT organizations identify top challenges to IoT network planning and engineering

These organizations are also struggling with how to predict the volume of data produced by IoT devices and the resulting traffic patterns. They need to understand if a device will essentially be sharing the occasional heartbeat or sending large volumes of data to the cloud for analysis. They also need to know if there will be peak periods when a device at a remote site will generate large packet flows that will compete with other critical applications. The network team will need to collaborate with line of business and/or operational technology groups to understand how much data these devices will send and receive, and when it will happen.

Security is also a top planning and engineering challenge. Respondents told us they struggle with modeling threats to IoT devices and to IoT data in motion. These concerns speak to two major issues. IoT devices are typically not produced by organizations with a long history of developing secure operating systems. Also, many of these devices have constraints that limit their ability to encrypt or decrypt data. Given these conditions, the network team must understand the threats to IoT data and devices and build a network that can address those threats. IT staff are especially concerned about this issue. They identified "modeling security threats to IoT data in motion" as a top concern (33%) at nearly three times the rate as respondents from the IT executive suite (12%).

As mentioned above, IoT devices often have power and computing constraints that limit the network team's ability to manage and secure IoT device connectivity. **Figure 8** reveals the problems these limited resources create for the network team. Only 12% of respondents claimed to suffer no adverse effects from such constraints.

Security is the top issue, with 36% of respondents saying that a lack of support for channel-based security techniques like Transport Layer Security (TLS) is challenging them. Resource discovery is the number two problem. Lacking compute resources, many IoT devices do not support the technologies that IT organizations use to discover devices, like Simple Network Management Protocol (SNMP).

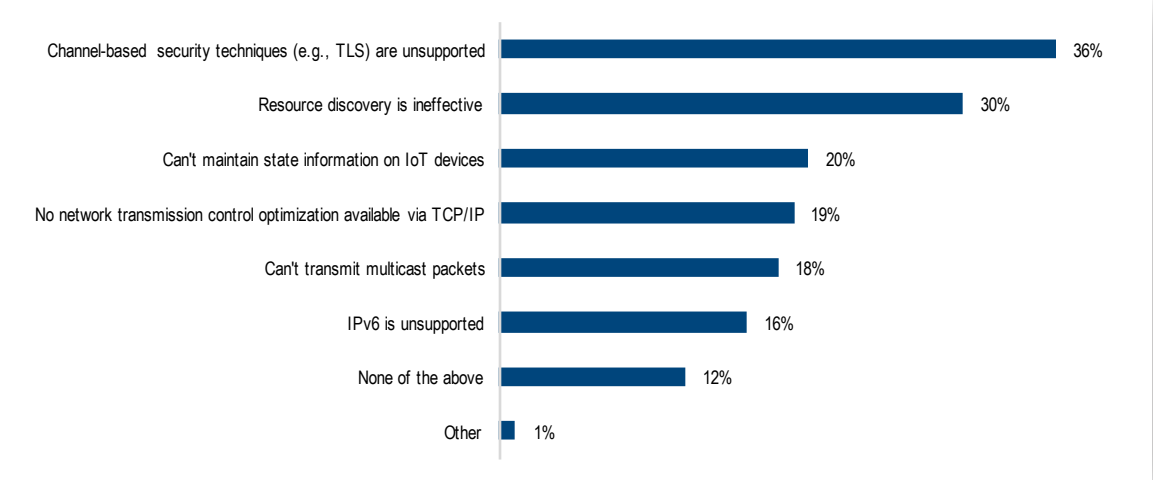

Figure 8. The top networking challenges associated with the power and computing constraints of IoT devices

EMA also asked research participants to identify the network resources that are most affected by the scale of their overall IoT ecosystem, given the number of devices they must connect and the traffic those devices generate. As seen in **Figure 9**, overwhelmed network security infrastructure is the biggest scale-induced headache for IoT. As traffic explodes, firewalls, intrusion protection systems, and other security devices will struggle to keep up. This is a clear sign that IoT will require security system upgrades in many enterprises.

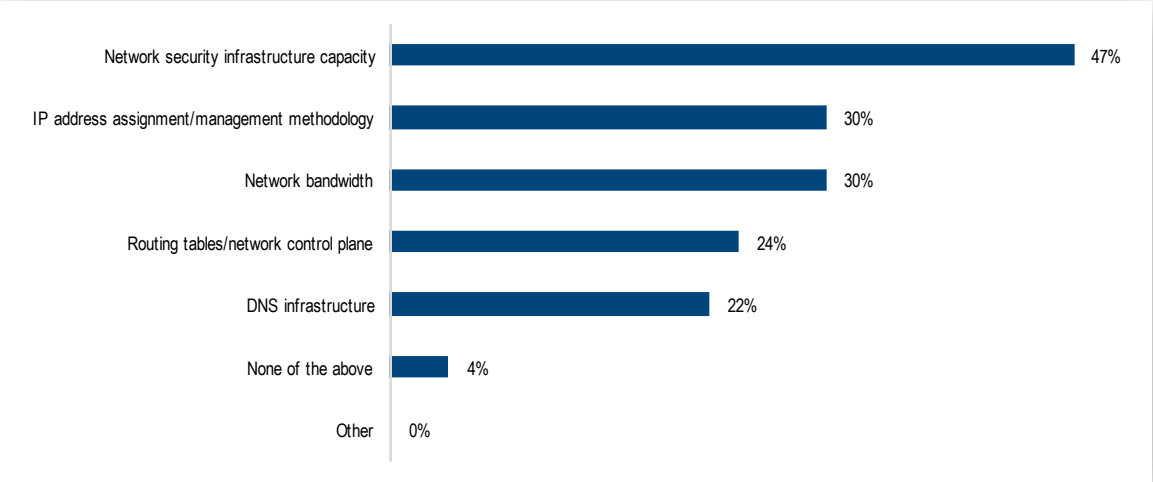

Figure 9. Network-related resources most challenged by the large scale of IoT initiatives

Security is a recurring theme throughout this section. These enterprises are struggling to model security threats. Device constraints are preventing them from using channel-based security controls. And the scale of IoT ecosystems is straining network security infrastructure. From top to bottom, IoT security is a challenge, and it appears that the network infrastructure team will bear the responsibility for fixing these problems. Already we've seen reports of massive distributed-denial-of-service (DDoS) attacks generated by compromised IoT devices. As IoT adoption grows, the security problem will worsen. Network infrastructure teams need to lead on this issue and find creative solutions to address it.

IoT Architectural Considerations: Edge Analytics

We are still in the early days of establishing best practices for IoT architecture, but some common themes have emerged that point to IoT success. One example is the use of analytics technologies at the edge of the network, closer to where IoT devices are located.

IoT Edge Analytics

IoT is all about data. Enterprises are pulling data from devices to discover valuable insights, support new business models, optimize operations, and improve customer experiences. All of these use cases will require some kind of data analysis.

Enterprises may be tempted to centralize their analysis of data, but centralization poses a variety of problems. For one, effective analytics initiatives create an enormous appetite for data, and that rising demand for data will ultimately strain network capacity. Also, centralized analytics introduces latency in data-driven decision-making. Some IoT initiatives will require analytical insights to be delivered at a speed that is only achievable by performing analysis closer to the devices themselves. Finally, centralized analytics introduces a single point of failure for IoT systems, a condition that is unacceptable for analytical functions that orchestrate or inform the delivery of critical local services and functions.

Thus, many enterprises are implementing IoT analytics at the edge of their network. In this study, 73% of enterprises reported using some form of edge analytics for IoT. Organizations with four or more IoT projects were much more likely to use edge analytics (88%) than those with one to three initiatives (60%), suggesting that enterprises may incorporate this architecture as they mature their approach to IoT and introduce more IoT traffic to the network.

Improved system reliability is the top driver for adoption of IoT edge analytics, as **Figure 10** reveals. Many IoT devices will be performing critical functions in the field. If they rely at least in part on analytics to perform those functions, an enterprise can't allow those IoT devices to be cut off from the analytics functions. Edge analytics architecture can back up cloud-based analytics or serve as the primary source of analysis of operational IoT data.

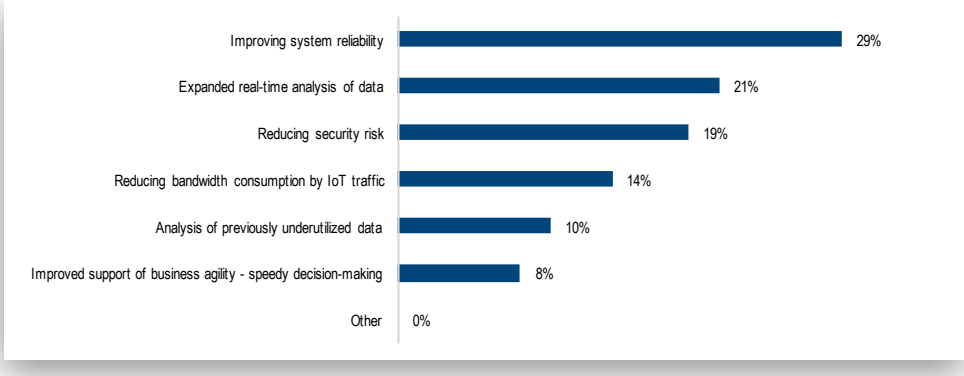

Figure 10. Top drivers for use of edge analytics in an IoT ecosystem

Expanded real-time analysis of data and reduced security risk are the secondary drivers of edge analytics adoption. As covered above, the distribution of analytics at the edge allows for more effective real-time analysis of IoT data. Thus, it is unsurprising that expanded real-time analysis is a secondary driver. Also, this research has already revealed that network infrastructure teams struggle with modeling security threats to IoT data in motion. Edge analytics reduces the amount of data that transits the network, which reduces the risk associated with IoT data in motion.

Reducing bandwidth consumed by IoT traffic is a relatively unimportant driver for edge analytics, despite the traffic growth enterprises are experiencing with IoT. But EMA observed some patterns that suggest enterprises are looking at how distributed IoT analytics can reduce IoT traffic. For instance, the QoS priority that an enterprise assigns to IoT traffic correlates with edge analytics adoption. Users of distributed IoT analytics are four times more likely (33%) than non-users of edge analytics (8%) to assign a high QoS priority to IoT traffic. Also, non-users of edge analytics are 20 times more likely (21%) than edge analytics users (1%) to assign a low QoS priority to IoT traffic. EMA suspects that users of edge analytics can afford to give such a high bandwidth preference to IoT traffic if they reduce the amount of data they have to backhaul to the cloud, which in turn limits the impact IoT traffic has on other applications. Moreover, non-users of edge analytics may be assigning a low QoS priority to IoT traffic because they want to minimize the impact that traffic has on other applications.

The adoption of edge analytics also correlates with growth of IoT-related network traffic.

- Adopters of edge analytics
  - Most describe today's IoT-related traffic growth as "significant" (44%) or "very significant" (33%)
  - 59% anticipate IoT-related traffic growth to be "very significant" in 24 months
- Non-users of edge analytics
  - Most describe today's IoT-related traffic growth as "somewhat significant" (46%) or see no growth at all (25%)
  - In 24 months, 38% still expect just "somewhat significant" traffic growth

Adopters of distributed IoT analytics will have an opportunity to mitigate the traffic growth that they are anticipating. In fact, two years from now enterprises might have a different set of priorities for edge analytics if IoT data continues to flood their networks.

Managing and Monitoring IoT Networks and "Things"

This research has explored the various ways that network infrastructure teams provide connectivity to IoT initiatives. Primarily they use existing LAN and WAN infrastructure for these projects, but supplement with new network infrastructure and new types of IoT-specialized connectivity such as LoRaWAN. This combination of new and existing networks will present some monitoring and management challenges. Also, many network managers will be tasked with monitoring and managing IoT devices, which adds to the burdens these teams bear. In this section we explore how network infrastructure teams are adapting their management approach for IoT networks and IoT devices.

IoT Monitoring Blind Spots

An IoT initiative can be disruptive. Multiple IoT initiatives can be revolutionary. The devices themselves vary widely, as do the use cases. With the network team playing a leading role in some, if not all, of these initiatives, they need to be ready to deliver highly available and high-performing networks. This means they must make sure their monitoring tools have adequate visibility.

Unfortunately, 52% of respondents said that their IoT initiatives had introduced or worsened blind spots in their network monitoring and service assurance architecture. In the following sections, EMA will explore how network infrastructure teams are addressing this issue. But before we proceed, it's important to consider the consequences of not doing anything about the problem. **Figure 11** reveals those consequences.

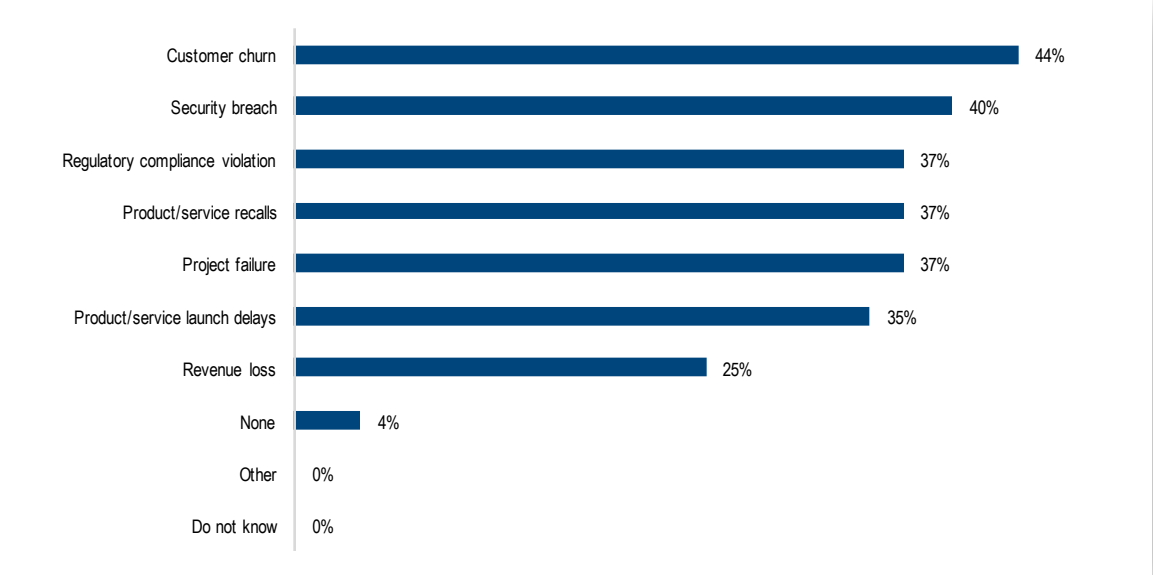

Figure 11. Business problems experienced as a consequence of blind spots in IoT-related network monitoring and service assurance architecture

Customer churn was the number one consequence of insufficient monitoring, which suggests that many of these enterprises are deploying IoT solutions that are critical to customer interactions and product and/or service delivery. The second most common result was a security breach, which is of particular concern considering recent news reports of compromised IoT devices being used in DDoS attacks. As we have observed throughout this research, IoT security is a major focus for network infrastructure teams. This finding simply confirms the necessity for vigilance and demonstrates that network monitoring is consequential to IoT security.

Monitoring IoT Networks: Tool Choices

Network infrastructure teams use a wide variety of tools to monitor the performance of IoT networking. As **Figure 12** reveals, four tools are most prominent. Network flow monitoring was the most popular. Device metric monitoring and log analysis tools weren't far behind, and "reports and metrics supplied by IoT solution providers" were also an important secondary approach.

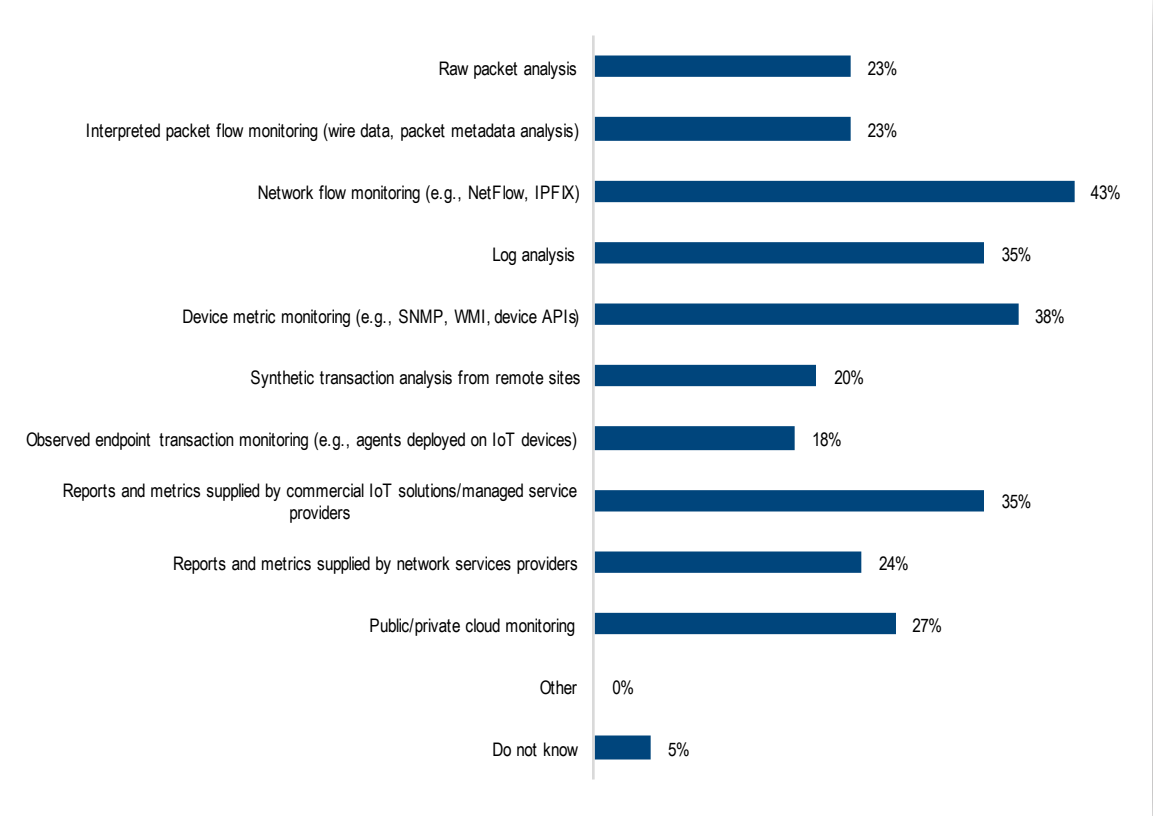

Figure 12. Network monitoring tools used for IoT performance monitoring

Packet-based monitoring, either raw packet analysis or interpreted packet flows are less common for IoT monitoring, and synthetic transaction analysis and observed endpoint monitoring are the least popular. Large enterprises use log analysis (46%) and device metric monitoring (50%) more often than midmarket companies (26% and 28%, respectively).

Meeting the Challenge of IoT Monitoring and Management

Figure 13 identifies the leading challenges that these organizations face when trying to monitor IoT networks. The sheer volume of devices connecting is the biggest problem, with the scale of IoT devices connecting to the network cited as the top challenge. But these organizations are clearly struggling with a handful other issues. Rogue device detection, monitoring for bursty traffic, high rates of change, and issues with monitoring profile configuration are all nearly as challenging as scalability.

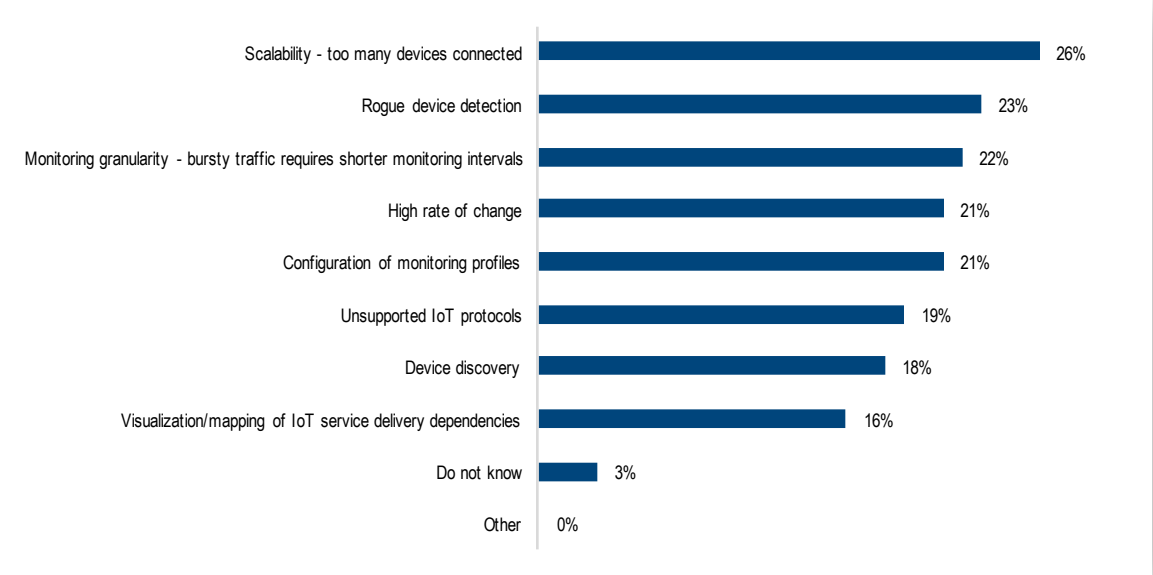

Figure 13. Leading challenges to effective IoT networking monitoring

"Unsupported IoT protocols" and "device discovery" were less common challenges, but each still affects nearly one in five organizations. The least common challenge was visualization and mapping of IoT service delivery dependencies, which suggests that network teams are doing a good job of evolving their tools in this area. This research has already established that the ITSM organization is an important internal partner to network infrastructure teams on IoT projects. Such collaboration would go a long way toward mitigating any visualization and mapping challenges associated with IoT service delivery dependencies.

Next, EMA asked respondents to describe what actions they are taking to improve visibility into IoT networking. They clearly have scalability in mind. As shown in **Figure 14,** the most common action that network managers reported taking was upgrading the data processing capacity of their network monitoring tools**.** The research has already established that IoT initiatives are causing significant network traffic growth, which in turn will increase the amount of network data collected by monitoring tools. Data processing upgrades will be essential for accommodating this increase in network data.

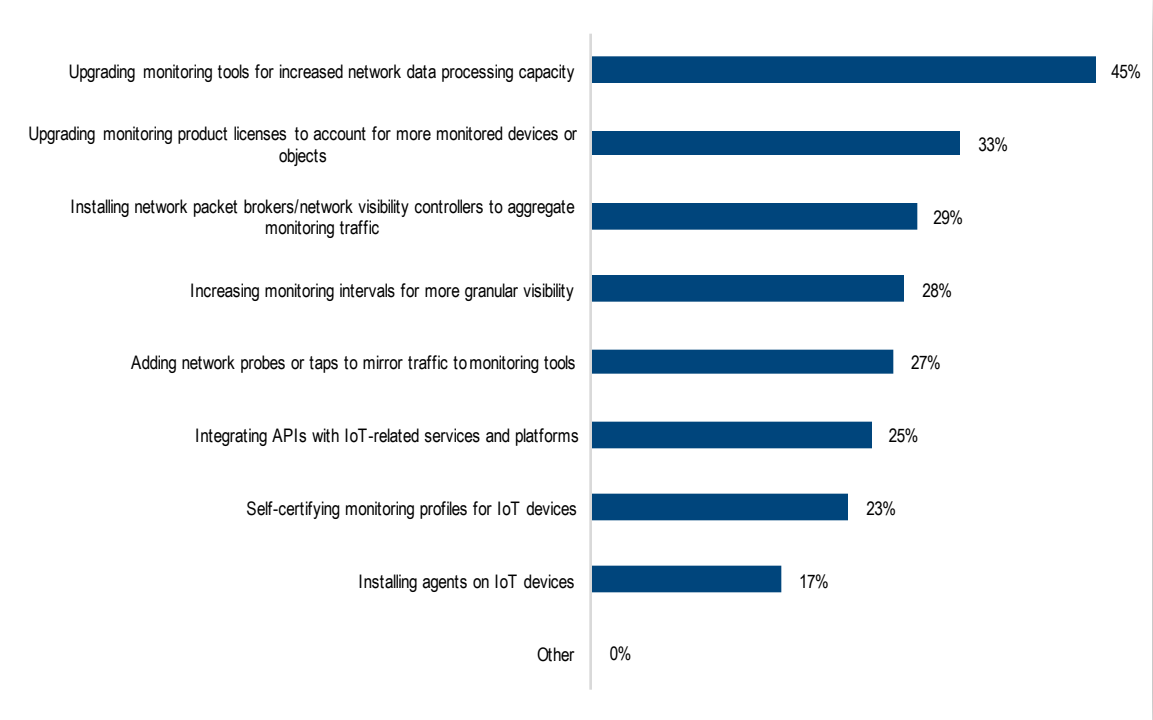

Figure 14. The most important steps network managers take to improve visibility into IoT networks

One-third of enterprises are also upgrading their monitoring tool product licenses to accommodate for growth in the number of devices and objects they must monitor in an IoT ecosystem. This can indicate that they have expanded their network for IoT and they need to monitor more network devices. But it could also mean that they are monitoring IoT devices directly and need to adjust their licensing for that growth in number of devices.

Twenty-nine percent (29%) of these organizations are installing network visibility controllers to aggregate monitoring traffic, and 27% are adding network probes or taps to mirror traffic to monitoring tools. Both of these findings suggest that IoT initiatives increase the need for a network monitoring fabric based on network visibility controllers and taps. It also suggests that IoT prompts enterprises to increase the number of network segments they monitor. Furthermore, the many features of network visibility controllers, such as packet filtering and load balancing, can help enterprises reduce the amount of data that hits an individual monitoring tool, thus mitigating the scalability challenges that many enterprises face with IoT monitoring.

Monitoring granularity is an issue for more than one-quarter of these organizations. They are modifying monitoring intervals to capture activity that might be missed otherwise, which suggests that many enterprises see an increase in bursty traffic with IoT. Without visibility into these traffic bursts, they will struggle to provide effective service assurance and to understand capacity utilization.

EMA suspects that effective IoT service assurance will lean heavily on real-time analysis of network data. Forensic network data analysis just won't get the job done in such a complex environment, especially when IoT technology drives mission-critical functions like patient care in hospitals and manufacturing systems in factories. Seventy-two percent (72%) of research participants said IoT initiatives have created a need for monitoring systems that can provide faster, real-time analysis of network data. Tools that can analyze large volumes of data quickly are able to detect and respond to events more quickly.

Figure 15 reveals how that faster analysis of network data will help with IoT projects. The majority of organizations will rely on it to detect IoT security incidents and threats and to monitor overall IoT services. Throughout this research, security has emerged over and over as a challenge for network teams, making this focus on real-time analytics for security rather unsurprising. And given the criticality of IoT services, it makes sense that network managers would want faster, real-time analysis for monitoring of those services. Troubleshooting is also a focus for nearly half of these organizations (46%), and 42% are using this analysis for optimization of IoT services.

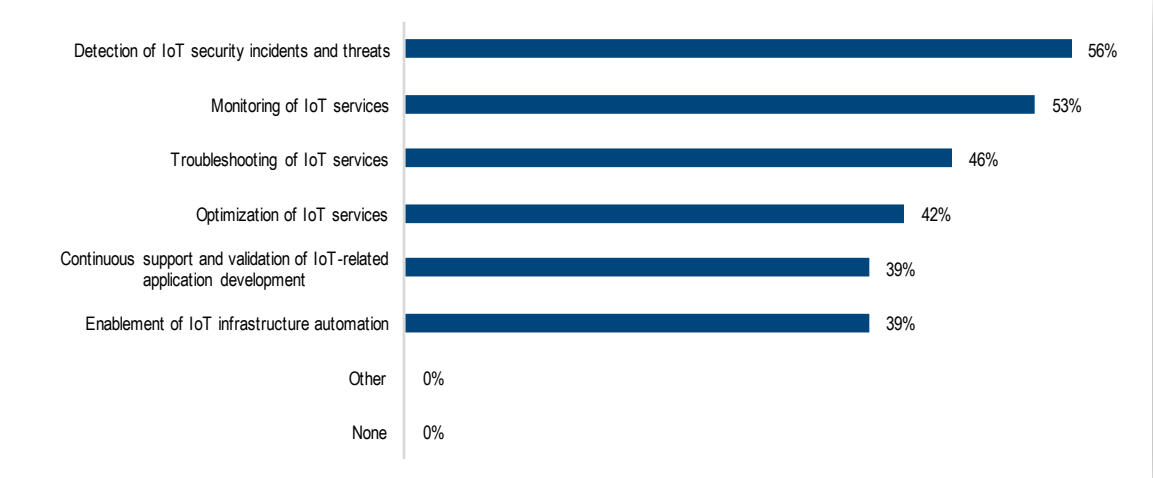

Figure 15. The aspects of an IoT ecosystem supported by faster real-time analysis of network data

The Network Infrastructure Team and IoT Devices

In industry interactions, EMA has observed that some early adopters of IoT are using their network monitoring tools to directly monitor and manage IoT devices. While some tools are inherently extensible to support IoT devices, others require the vendors to provide custom integrations.

Sixty-eight percent (68%) of the participants in this research have extended their IT or network management tools to monitor and manage IoT devices. **Figure 16** reveals how they do it.

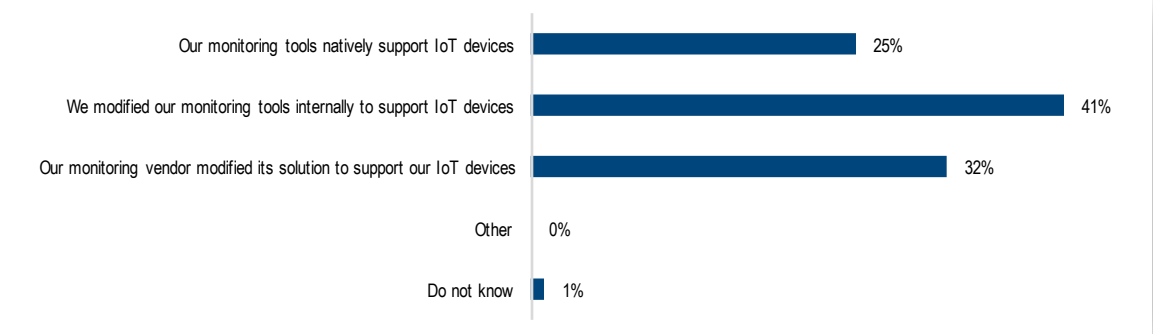

Figure 16. Primary approach to extending IT and network management tools to monitor and manage IoT devices

Only one-quarter of enterprises had management tools that could natively support IoT devices. The rest had tools that required some form of modification, most often modifications that the IT organization did internally. However, nearly one-third received custom modifications from their monitoring vendors.

Conclusion:
How Network Teams Successfully Lead IoT Projects

In this final section, EMA will identify some indicators of success, specifically aspects of projects captured in this research that were most often associated with a network team's successful support of IoT projects.

Figure 17 reveals that a network infrastructure team's success with IoT correlates with whether they have a leading role in the implementation of IoT initiatives. The pattern is impossible to ignore. Network teams that lead all IoT initiatives reported higher levels of success, and those exclusively playing a supporting role were the least successful. Network teams need to assert themselves. The network is the foundation of any IoT project, and there is little reason to sideline the experts.

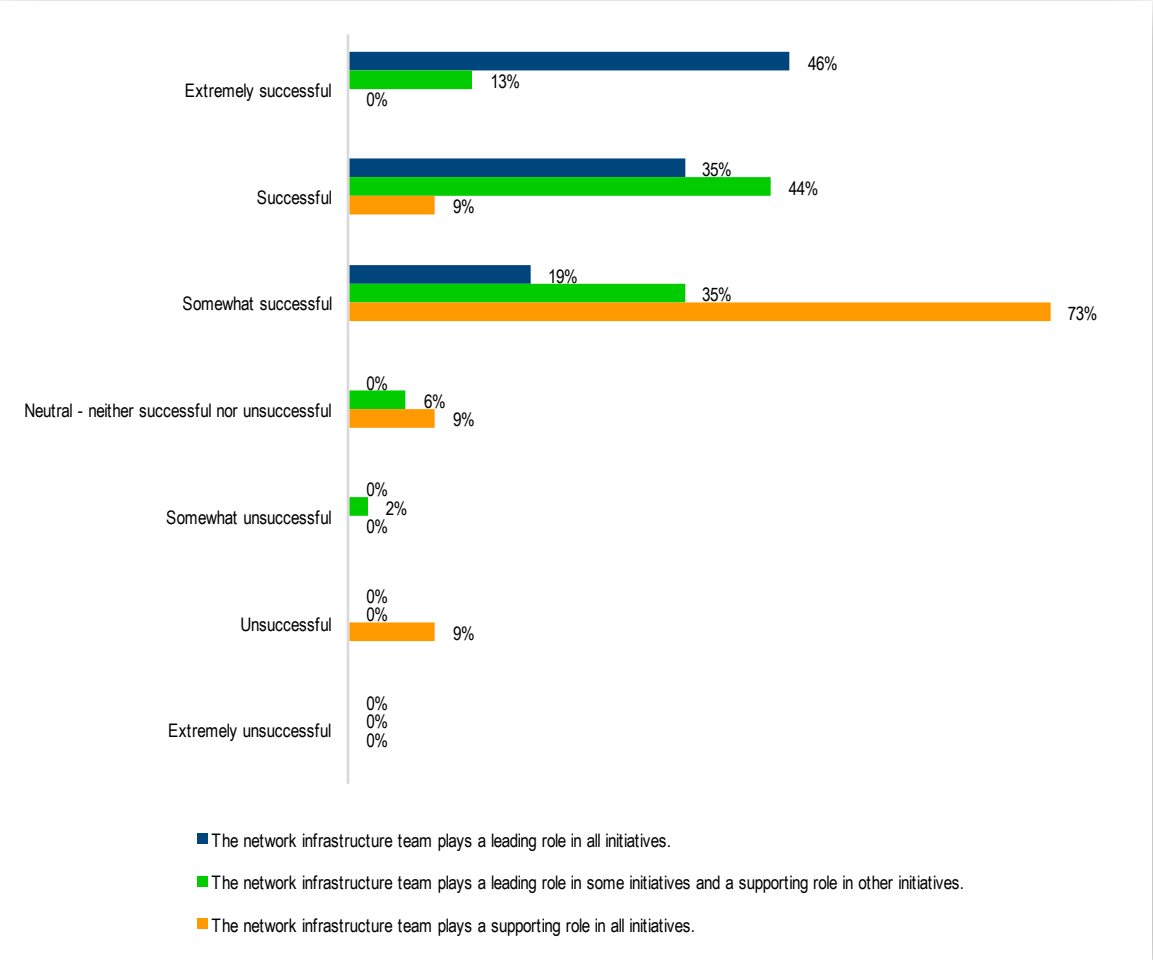

Figure 17. Network teams are most successful when they are allowed to lead IoT initiatives.

To identify some potential best practices, EMA analyzed the data from the perspective of two cohorts; we combined the "successful" and "extremely successful" groups into a "successful" cohort and the rest into the "somewhat successful to unsuccessful" cohort. In the following pages, we highlight areas in which successful organizations seem to do things differently than their less successful peers.

IoT Architectural Best Practices

EMA has identified the following best practices for IoT network engineering and architecture:

Use IoT analytics at the edge. Network teams that reported use of distributed analytics at the edge of their IoT ecosystem were 2.5 times more likely to be successful with IoT.

Prioritize IoT traffic. Successful network teams assign a high QoS priority to IoT traffic at 4.5 times the rate of other organizations.

Use diverse connectivity strategies. Successful organizations were almost three times more likely to use IoT connectivity that is packaged by an IoT solution provider. By no means does this suggest that enterprises should use packaged connectivity exclusively. They should continue to leverage their own LAN and WAN infrastructure and build out new capacity where it makes strategic sense. However, they shouldn't be afraid to outsource connectivity to an IoT solution provider when appropriate.

IoT Management and Service Assurance Best Practices

EMA has identified the following best practices for network teams that are managing and monitoring IoT:

Take ownership of IoT device monitoring. 77% of successful organizations extend network monitoring tools to monitor and manage IoT devices, versus 54% of less successful organizations. .

Make sure network monitoring can scale for IoT. Less successful organizations were twice as likely to say their network monitoring tools struggle with the scale of their IoT ecosystems. They simply can't handle the number of devices connecting to the network.

Upgrade network analytics and automate IoT infrastructure. 80% of successful organizations recognize that they need faster, real-time analysis of network data for IoT, versus just 59% of less successful network teams. Successful organizations were twice as likely to use this enhanced network data analysis to enable IoT infrastructure automation.

Integrate network management with data center operations and IT orchestration. Successful organizations were twice as likely to integrate network management tools with data center operations and IT orchestration systems.

Network infrastructure professionals may view IoT as a steep mountain to climb, and throughout this research, EMA has observed countless challenges. Security is a major threat that network teams must deal with as they adapt existing infrastructure while also building out new infrastructure. They must adapt and upgrade their management systems to account for IoT. They are taking ownership of IoT device monitoring and management to a greater extent than they may be comfortable with.

Network professionals also need to lead these initiatives if they are going to succeed. They can't sit back and let others take the wheel. This means they must forge partnerships with internal and external stakeholders and make sure that each of several ongoing IoT initiatives stays on course and succeeds.

No matter how daunting IoT may appear, network professionals should seize the opportunity and lead the way.

About Enterprise Management Associates, Inc.

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

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

3562-SUMMARY.050217