JUNIPER NETWORKS

Internet of Things INSTITUTE

# Prepare Your IoT Network Ready for At-Scale Challenge

## Survey Insights Revealed by IoT Adopters

# Table of Contents

# Survey Objective

The purpose of this survey is to collect insights from technology decision-makers and influencers from organizations that have implemented IoT projects and to advise on how organizations should get their network infrastructure ready as they plan to implement IoT at scale.

Therefore, in this survey, we focused on companies that had already implemented at least one IoT project (as illustrated in Figure 1). In other words, respondents who were not already involved in IoT projects were not included in this research. For more details, see the Methodology section.

This white paper presents the key findings from the survey and our analysis. Our hope is that for organizations currently planning IoT initiatives, these insights from real world project experiences, will increase the odds of success.

Most respondents report that IoT Network Infrastructure is one of their areas of responsibility. One in five report it is their primary responsibility.

**Involvement with IoT network infrastructure.**

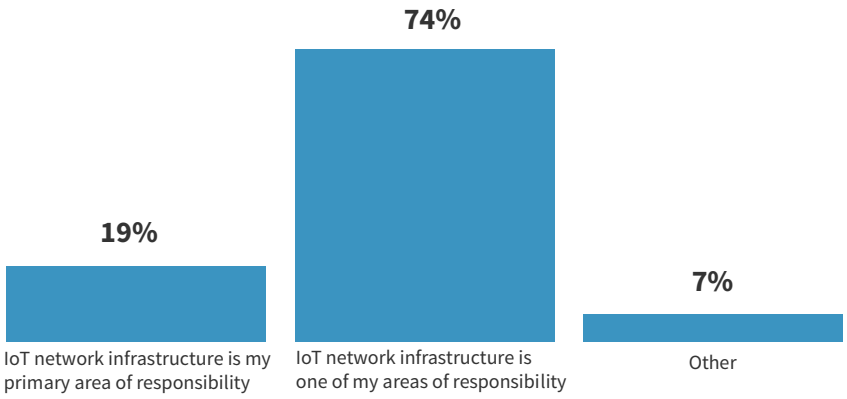


**Figure 1**

*Base=Respondents with direct involvement in IoT Network Infrastructure (n-160)*

# Methodology

On March 19, 2018, Informa Engage emailed invitations to participate in an online survey to a net 89,804 users of IoT Institute and/or IT Pro Today. By April 3, 2018, we had received 926 completed surveys, for an overall response rate of 1.0%. Of those 926 respondents, 160 were qualified for inclusion in the analysis by meeting both of the following criteria.

a. Organization has implemented IoT, or completed a Proof of Concept (PoC) project;
b. Respondent report personal involvement with IoT Network Infrastructure.

About half of all respondents represent organizations that have implemented multiple IoT projects. The most common types of respondent involvement with IoT are Technology/Solutions Decision Maker and Technology/Solutions Influencer, followed by Project/Initiative Influencer, and Implementer.

## Organizational Involvement with IoT

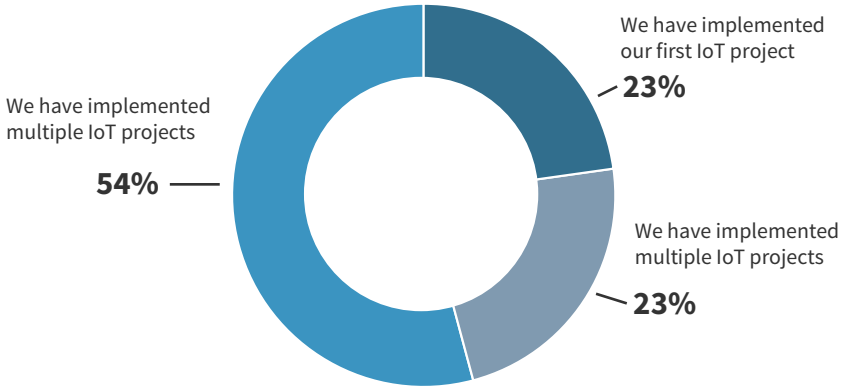


**Figure 2**

*Base=Respondents with direct involvement in IoT Network Infrastructure (n-160)*

## Respondent Involvement with IoT

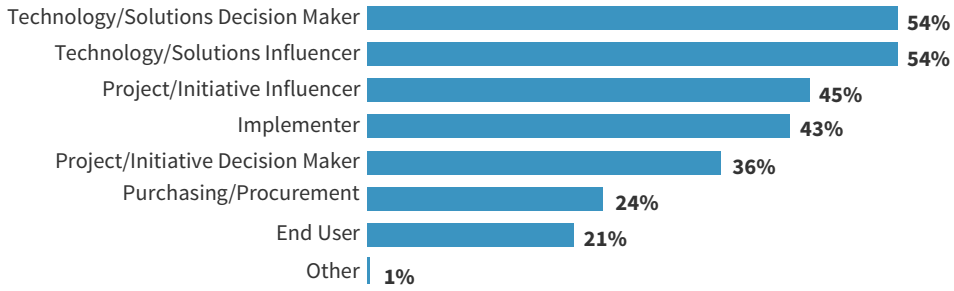


**Figure 3**

*Base=Respondents with direct involvement in IoT Network Infrastructure (n-160)*

## Organization Size–Number of Employees

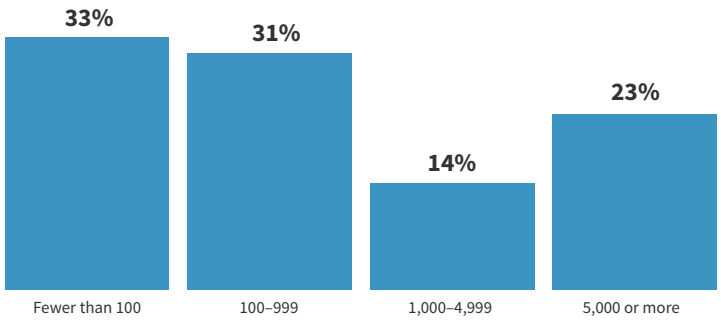


**Figure 4**

*Base=Respondents with direct involvement in IoT Network Infrastructure (n-160)*

## Organization Type

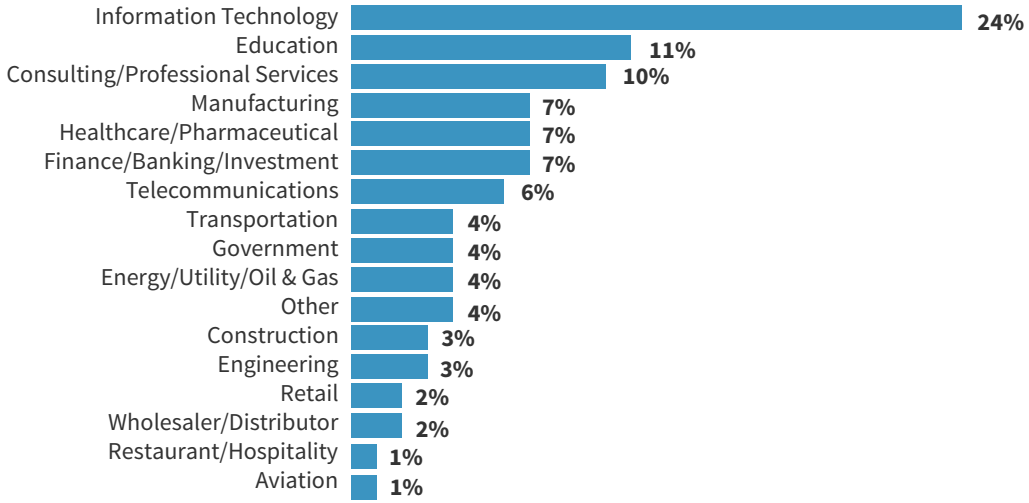


**Figure 5**

*Base=Respondents with direct involvement in IoT Network Infrastructure (n-160)*

# Top Takeaways

**IT Preparedness for IoT at Scale:** Respondents do not appear very confident in their organization's readiness to effectively operate and manage an IoT environment at scale. Just 31% consider themselves "very" or "totally prepared."

**Top IoT Challenges:** Respondents report their primary IoT-related challenges are ensuring security and privacy (56%), followed by architecture design and deployment (42%), IT/OT convergence (42%) and managing the complexity from integration and multi-vendor management (38%).

**Diverse IoT Application Workload Locations:** IoT application workloads are run in a variety of locations, most commonly their own private data center or control center (50%), at the network edge (35%), or in the public cloud. Twenty-nine percent of respondents have run their IoT application workloads in two or more clouds, which indicates that many IoT workloads are in a multi-cloud environment.

**Preferred Architecture Approach for IoT Network Design:** The most common approach for IoT network design is to use a shared physical underlay and use virtual overlay for segmentation (47%). The additional 20% who currently use separate physical networks plan to converge them in the future.

**Partnering With a 3rd Party Service Providers:** Currently, only four percent of respondents said they already partnered with IoT service providers. However, a clear majority (75%) plan to do so for future IoT implementations.

**Rising Demand of Managed IoT Network Services:** Thirty-two percent of respondents report their organizations use managed IoT network services today. However, when asked about their plans within the next 18 months, the percentage increases to 65%, more than a 100% increase. This indicates significant need for leveraging outsourced managed services to ease operations challenges.

**Importance of Network Automation Capabilities:** A majority of respondents (52%) believe network automation capabilities are either critical or very important for their IoT deployments. And companies that have already implemented multiple IoT projects are much more likely to rate network automation as critical than those that have only deployed one project.

# Top Challenges for IoT Deployments

For many organizations, the Internet of Things (IoT) will be a key enabler for their digital transformation. Data collected from connected machines can be used to increase operational efficiencies, enhance product designs, improve customer experiences, and even transform business models. Enterprise IoT adoption typically starts small and simple, but proliferates fast. Then these pilot projects often expand into more complex ones that are much more challenging. The complexity of implementing IoT at full production scale has led Gartner to predict that many expanded IoT deployments will fail at achieving their intended business outcomes.[1] Therefore, we asked survey respondents about the primary IoT-related challenges that they faced.

## What are your company's primary IoT-related challenges?

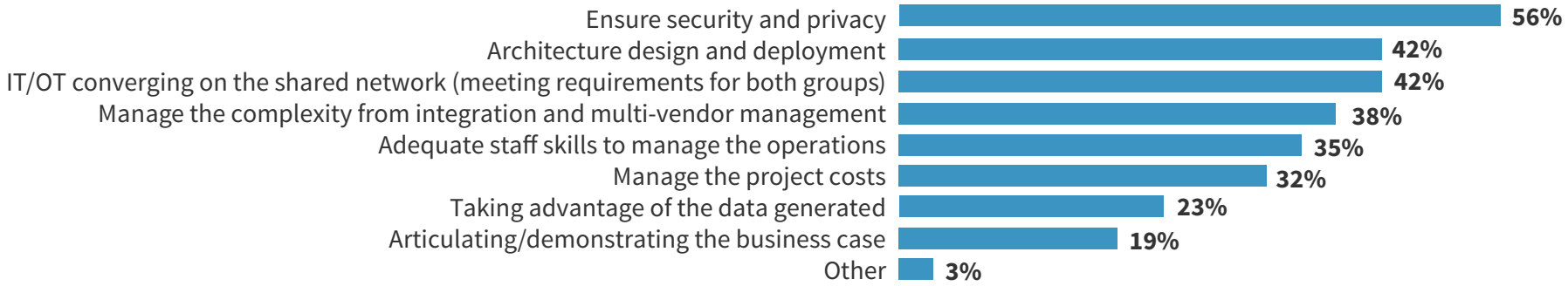


**Figure 6**

*Base=Respondents with direct involvement in IoT Network Infrastructure (n-160)*

1 Gartner Research Note: "Predicts 2018: Expanding Internet of Things Scale Will Drive Project Failures and ROI Focus"

Respondents report their primary IoT-related challenges are ensuring security and privacy (56%), followed by architecture design and deployment (42%), IT/OT converging on the shared network (42%), and managing the complexity from integration and multi-vendor management.

In the early days of IoT adoption, security was merely an afterthought. But several high impact IoT security incidents have made global news headlines, such as the Mirai DDoS attack in 2016. As a result, organizations have realized the importance of having built-in security to protect against IoT threats. In fact, security and privacy concern have been consistently rated as the number one barrier to IoT project success according to according to several other recent research studies.

Designing and deploying architecture for IoT is challenging because typically there are many components to consider - devices, networks, platforms, applications, and more. Dealing with one single use case is relatively easy, especially when experimenting with small scale deployments. However, when expanding to multiple IoT use cases at scale, the process becomes much more complex, involving different types of operating systems, protocols and communications requirements. Lacking a stable architecture that ensures the scalability, reliability and

agility needed to accommodate various IoT use cases, organizations will have a difficult time achieving the desired ROI.

Historically, the information technology (IT) and operational technology (OT) departments in asset-intensive industries such as manufacturing, energy, transportation and healthcare function fairly independently, running their networks separately based on different priorities and requirements. Over time, these two approaches have gradually combined to become IT/OT convergence. IT/OT convergence gives administrators a single view of their organization's information and offers tremendous benefits, such as improved visibility, higher operational efficiency and economic savings.

Coupled with the adoption of IoT technology, this convergence has been accelerated and become known as Industrial IoT (IIoT). Converging OT applications onto the same network that supports IT applications is not easy because the two teams have different priorities. For IT, their typical top security priority is protecting data so they tend to follow the traditional CIA hierarchy for security: confidentiality, integrity, and availability.

OT, on the other hand, uses an inverted CIA model, where availability comes first. OT teams need to ensure that things like control processes and production yields are not put at risk due to network changes. Traditional IT best practices, such as patching and updating, can potentially cause an industrial system to stop working. Unplanned downtime for these industrial machines can end up costing millions of dollars per minute.

When scaling IoT deployments from early pilot to production environment, enterprises need to integrate with existing systems, processes and infrastructure. IoT projects involve many different components and in many cases these components are supplied by different vendors. As a result, interoperability can be a big challenge. Without interoperability, integration becomes very complex and costly. It's been estimated that half of an IoT project's implementation costs are spent on integration alone.[2]

## IoT Workloads Running at the Edge and in Multicloud Environment Adds Additional Complexity

The business value of IoT comes from the data that these connected devices generate. According to ABI Research, by 2020, the data captured from IoT devices will reach 1.6 zettabytes.[3] Data alone does not generate much value. It's through the analytic process: extracting insights from the data and applying those insights to improve business processes that brings value. With such large volumes of data coming from IoT, it is worth exploring where organizations run their IoT application workloads today.

[2] https://www.gartner.com/smarterwithgartner/iot-integration-questions/
[3] https://www.abiresearch.com/press/data-captured-by-iot-connections-to-top-16-zettaby/

## Where do your IoT application workloads run today?

IoT application workloads are run in a variety of locations and/or platforms, most commonly in private data centers or control centers exclusively, followed by the network edge and public cloud.

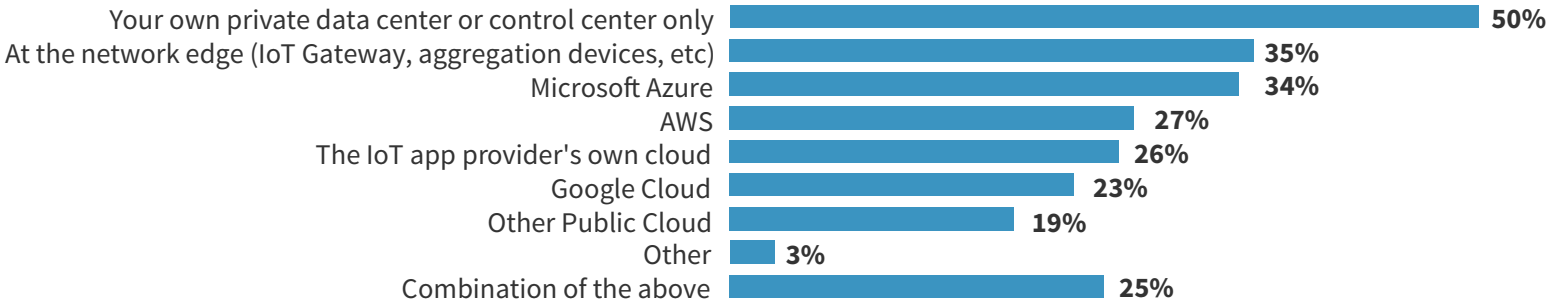


**Figure 7**

*Base=Respondents with direct involvement in IoT Network Infrastructure (n-160)*

Fifty percent of the survey respondents report that they run their IoT application workloads at their own private data center or control center. Thirty-five percent report running deployments at the network edge and the remaining run their application workloads at different public clouds. Moreover, 25% report that they use a combination of the above.

The percentage (50%) of workloads that run on premises is relatively consistent with the overall enterprise applications workload distribution trend today. What stands out in this survey's results is the fact that the network edge is the second most popular location where IoT applications are running today. This indicates a paradigm shift. Traditionally, the majority of analytics processes are run in a central location, whether it's in the data center or in the cloud.

The sheer volume of data being generated by IoT has led to the notion of edge computing and edge analytics, in which processing occurs closer to where the data is generated. With edge analytics, organizations move some analytics functions from the cloud to an edge analytics-enabled gateway. This dramatically reduces the amount of device data traffic to the cloud, thus saving costs attributed to network transport and cloud storage. It also dramatically improves availability, latency and the ability to perform real-time actions.

It's interesting to note over 29% of respondents have run their IoT application workloads in two or more public clouds or in third-party app providers' clouds.

### Where Do Your IoT Application Workloads Run Today?

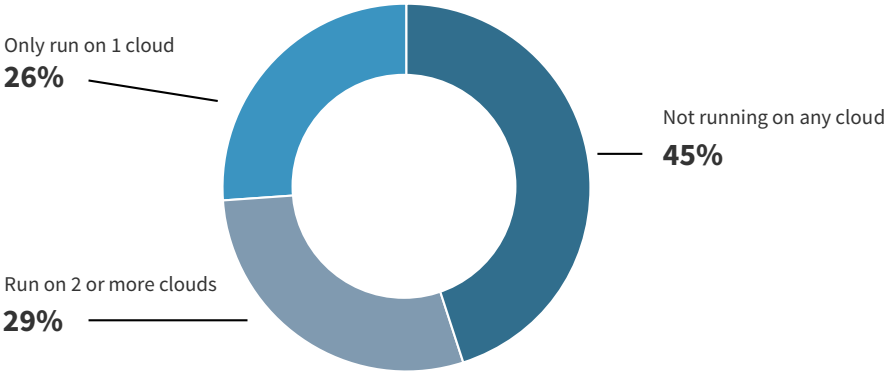


**Figure 8**

*Base=Respondents with direct involvement in IoT Network Infrastructure (n-160)*

This indicates that for many organizations, their IoT applications are already running in a multi-cloud environment. These multi-cloud environments add additional complexity, especially in terms of connectivity, security and operations, which enterprises need to consider when planning to scale IoT deployments to the next stage.


## Preferred Approach for IoT Network Architecture Design and Implementation

Selecting the right network architecture is critically important to the overall long-term success of IoT projects at scale. The choice of network architecture has direct impact on the connectivity, scalability, performance, security, availability and reliability for meeting IoT application requirements.

## Which of the following best reflects your company's approach to IoT network architecture?

The most common current organizational approach to IoT network architecture is shared physical underlay (47%). An additional 20% currently using separate physical networks plan to converge them in the future.

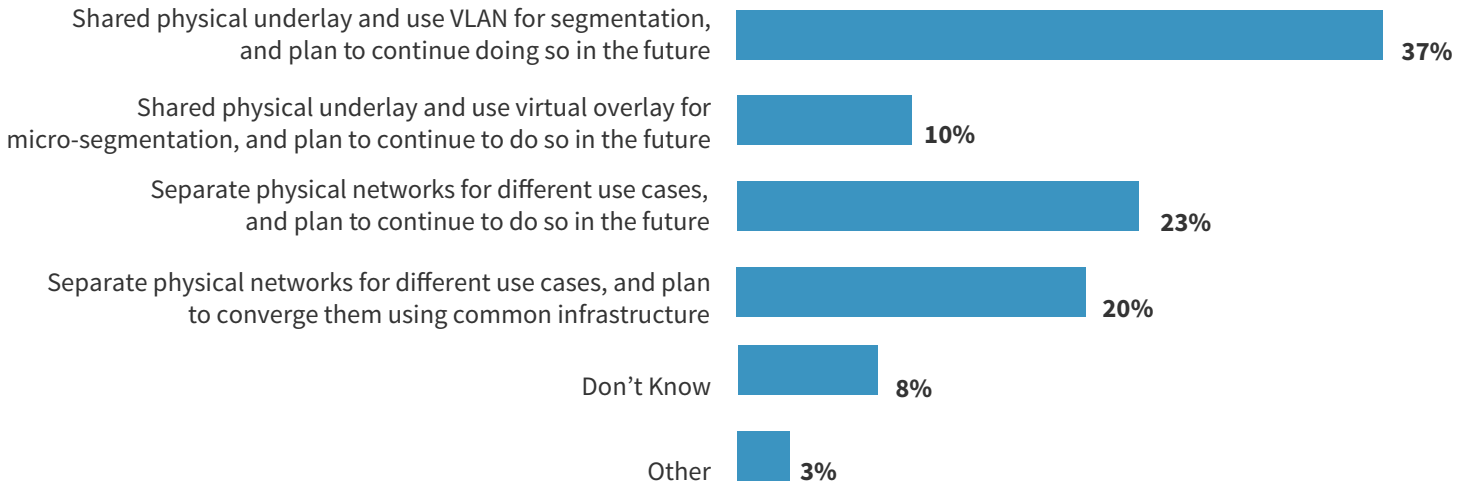


**Figure 9**

*Base=Respondents with direct involvement in IoT Network Infrastructure (n-160)*

According to our survey results, the most common or preferred approach to IoT network architecture today is shared physical underlay while using VLAN or virtual overlay for segmentation. Forty-seven percent report that they're already doing so and plan to continue in the future. Twenty percent of respondents report they're currently using separate physical networks for different use cases. However, in the future they plan to converge them using common infrastructure. Only 23% of respondents indicated that they're currently using separate physical networks for different use cases and plan to continue doing so in the future.

As different IoT devices are added to the same physical network infrastructure, there's a need to segment the IoT traffic for better security and policy control. When choosing segmentation approaches, organizations should make sure the selected approach will support not only layer 2 but also layer 3, so that IoT resources can communicate with the application, whether it's in the enterprise data center or in the cloud. Virtual network segmentation allows organizations to have greater flexibility to choose and prioritize virtual traffic based on application needs and to allocate network resources accordingly.

# Likelihood to Partner with 3rd Party Service Providers

In the past few years, various types of IoT service providers from different sectors continue to enter the market and build out their IoT practices team.

While only four percent of respondents report they already partner with service providers for their IoT implementation needs, 75% indicate that they're likely to do so in the future. This propensity implies a significant market opportunity for companies that offer IoT professional services.

Moving IoT deployments from early pilots to at-scale production is complex and many organizations do not have the expertise to do this by themselves. Therefore, it makes sense for them to partner with third-party IoT service providers to increase their project success rates and achieve better business outcomes.

While only four percent of respondents report they already partner with service providers for their IoT implementation needs, 75% indicate that they're likely to do so in the future.

## How Likely is Your Company to Partner with a 3rd Party for its IoT Implementation Needs?

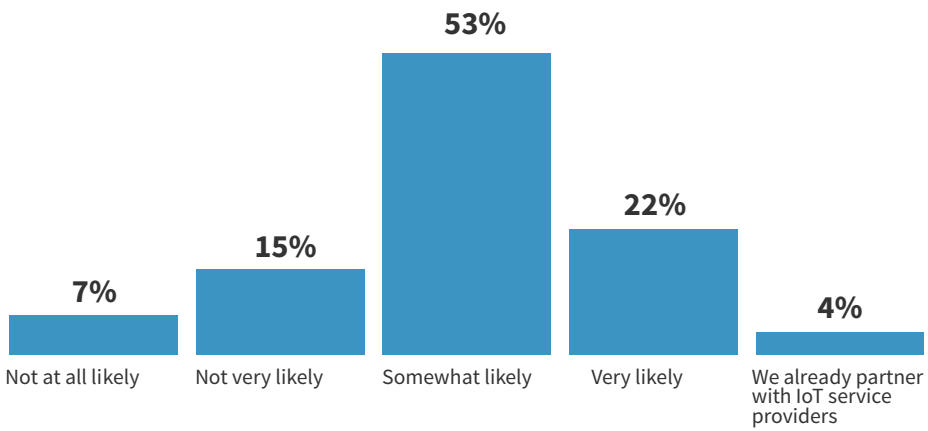


**Figure 10**

*Base=Respondents with direct involvement in IoT Network Infrastructure (n-160)*

## Who do you prefer to partner with to address your IoT-related challenges?

When partnering with outside companies to address their IoT-related challenges, respondents are equally likely to indicate a preference for Cloud Providers, System Integrators, and Managed Service Providers, followed by Network OEMs and OT Professional Service Providers. This lack of differentiation suggests a significant marketing opportunity.

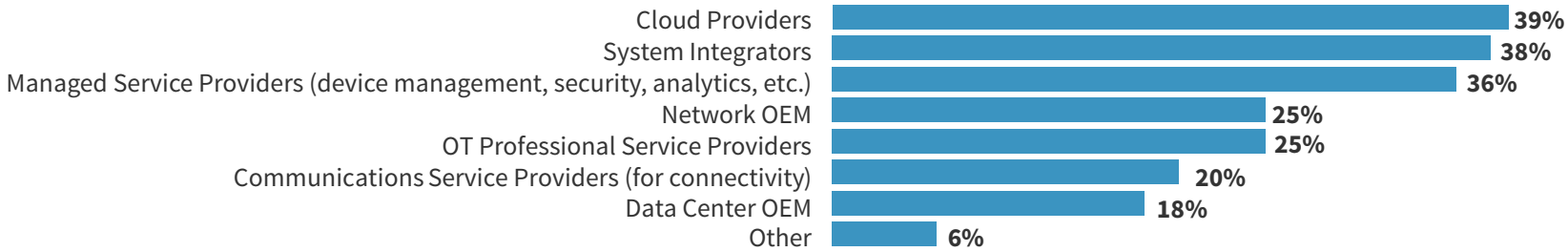


**Figure 11**

*Base=Respondents with direct involvement in IoT Network Infrastructure (n-160)*

# Network Operations Ready for IoT at Scale: Now and in the Future

Gartner predicts that by 2020, there'll be more than 20 billion connected IoT devices[4] and 250,000 new devices will be attempting to connect to enterprise networks per hour.[5] In the past, the adoption and growth of BYOD created tremendous challenges for IT teams to adapt and operationalize. Now, with IoT adoption at scale, the number of devices that will be connected to the network will increase exponentially. IoT leaders need to make sure their IT department is well equipped and prepared for the upcoming network operations challenge brought by IoT at scale.

[4] https://www.gartner.com/newsroom/id/3598917
[5] https://www.gartner.com/document/3587517

## How prepared is your IT department to operate and manage an IoT environment at scale?

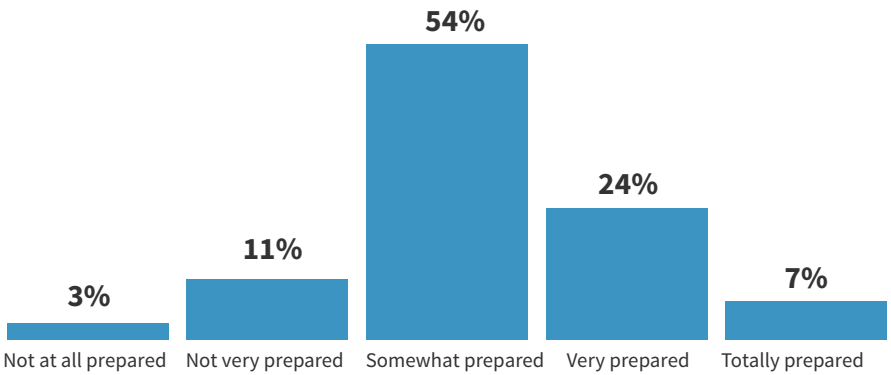


**Figure 12**

*Base=Respondents with direct involvement in IoT Network Infrastructure (n-160)*

When asked “How prepared is your IT department to operate and manage an IoT environment at scale and take advantage of insights to be gained from the data generated from IoT devices?”, only 31% of respondents indicate that they feel very prepared or totally prepared.

In general, two common ways to solve operations challenges are using outsourcing and/or automation. Essentially, this requires getting help from external parties to offload certain operations tasks and/or to change how tasks are performed to increase efficiency. We asked respondents to indicate their current and future preferences for using managed services to augment in-house IT as well as for adopting network automation.

# The Role of Managed Services to Augment In-house IT

When asked “Who operates the IoT networks at your company?”, a majority of respondents (68%) report in-house IT is currently operating their IoT networks at their organizations. However, within the next 18 months, operations responsibility will largely transition to a hybrid model, increasing from 27% to 54%. In addition, more IoT networks will be operated by managed service providers in the next 18 months. This shift is likely driven in part by the increasing complexity and operations burden associated with broadening scale of IoT implementations.

## Who Operates the IoT Network at Your Company Today?

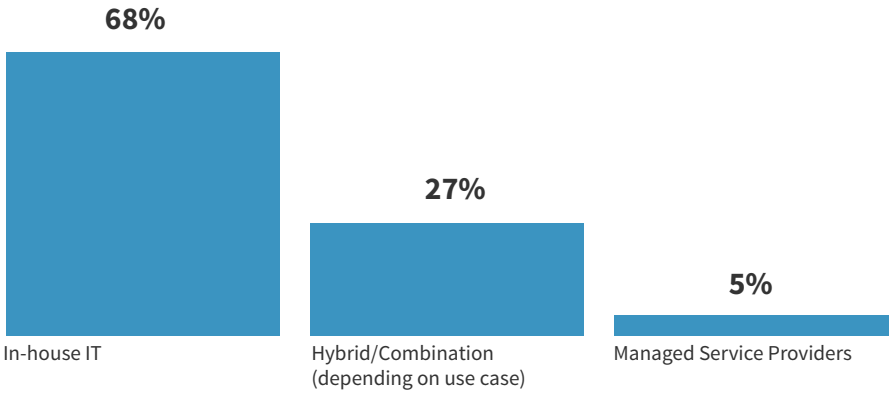


**Figure 13**

*Base=Respondents with direct involvement in IoT Network Infrastructure (n-160)*

## Who will Operate the IoT Network at Your Company in the Next 18 Months?

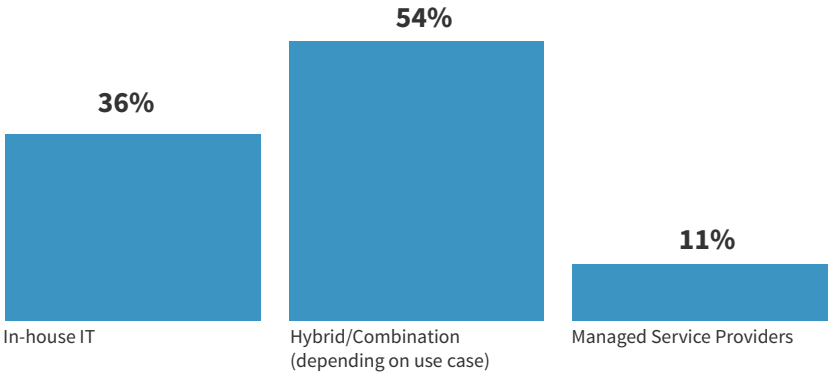


**Figure 14**

*Base=Respondents with direct involvement in IoT Network Infrastructure (n-160)*

## Importance of Network Automation Capabilities with IoT Adoption

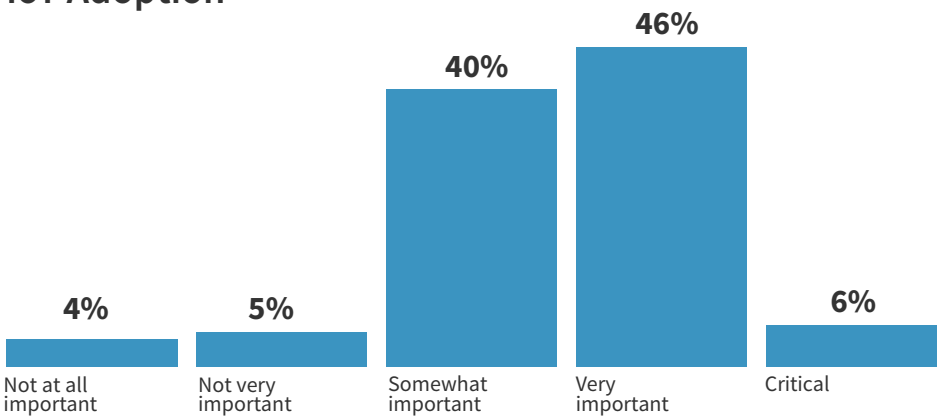


Figure 15

*Base=Respondents with direct involvement in IoT Network Infrastructure (n-160)*

When asked "How important is it for your company to have network automation capabilities with the adoption of IoT now and in the future?", a majority of respondents (52%) believe network automation capabilities are either critical or very important for their IoT deployments. And companies that have already implemented multiple IoT projects are much more likely to rate network automation as critical than those that have only implemented one project. This implies that the more IoT projects an organization implements, the greater the complexity. Therefore, it's critical for these organizations to have network automation capabilities in place, especially given the fact that most organizations lack the additional IT budget and dedicated resources necessary for successful IoT deployments.

Organizations that have implemented multiple IoT projects are more likely to rate the importance of network automation to be "critical".

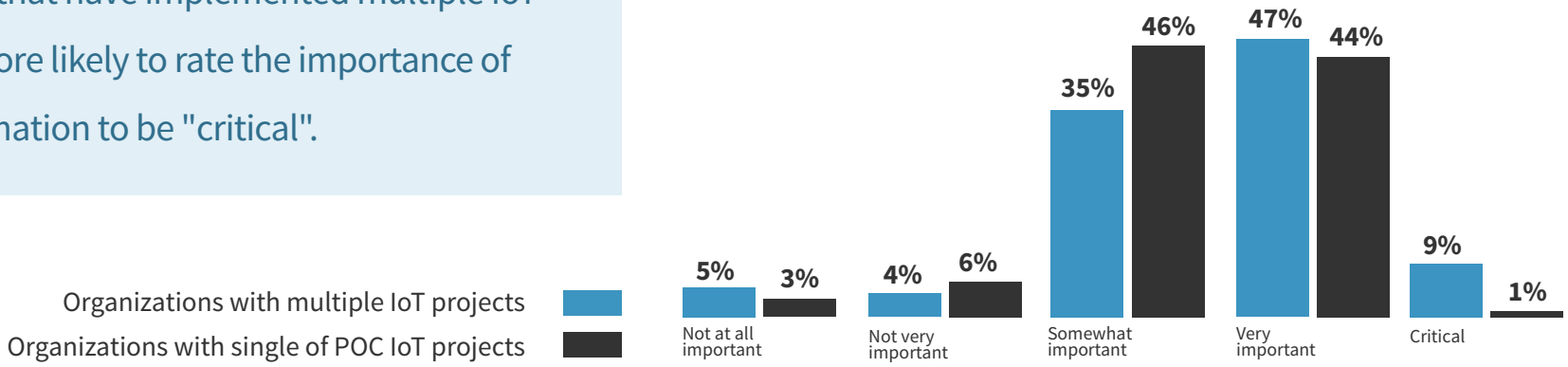


Figure 16

# Conclusion and Recommendations

As organizations are moving IoT deployments from early pilots to at-scale production, it's important to assess whether their existing network infrastructure is ready for the upcoming challenges of security, architecture design for IT/OT convergence and management complexity.

Due to the huge volume of IoT data that's generated, and the diversity of IoT use cases, application workloads are already starting to be distributed across data center, edge, and multi-cloud environments and this trend will continue. Therefore, IoT leaders need to consider and plan for how to ensure seamless connectivity, security and orchestration across multi-cloud environments.

When planning for converging multiple IoT applications onto the same enterprise network, IT leaders should and consider leveraging virtual overlay segmentation or micro-segmentation technologies to isolate the IoT traffic for better security and policy control.

Due to the huge volume of IoT data that's generated, and the diversity of IoT use cases, application workloads are already starting to be distributed across data center, edge, and multi-cloud environments and this trend will continue. Therefore, IoT leaders need to consider and plan for how to ensure seamless connectivity, security and orchestration across multi-cloud environments.

Operating IoT at scale will pose significant challenges for many IT departments who are not yet fully prepared. The increase in connected devices and applications simply adds more complexity. Network automation will be a critical must-have capability to address the upcoming massive IoT network operations challenge.

We exist to solve the world's most difficult problems in networking technology. Juniper Networks brings simplicity to networking with products, solutions, and services that connect the world.

A company of innovators, we believe that creating simplicity through engineering is the highest form of innovation. From our first release, the ground-breaking M40 router, to today's end-to-end advancements in network security, automation, performance, and scale, our drive to move beyond the constraints of complexity has expanded the reach of networks everywhere. We've enabled our customers to connect to everything and empower everyone in ways that have literally changed the world.

In the profusion of new technologies such as IoT, big data, and multicloud, complexity is the new hard problem. And complexity is on the wrong side of progress. With the strength of our resolve, we'll once again change the world.

Simple is our obsession.

Simple is powerful.

And simple always starts with engineering.

The IoT Institute connects IoT decision-makers and implementers, including those in the C-suite, IT and line-of-business managers. We inspire them by providing the latest news and analysis and case studies about technologies used in the Internet of Things, such as infrastructure, security, analytics and development tools. We capture the stories of IoT leaders imbuing intelligence across vertical industries.

The IoT Institute also conducts original research to provide unique insight into the state of IoT implementation and challenges and opportunities for key players.

In addition, we are the exclusive content outlet for the IoT World trade show and conference series -- the world's largest IoT events -- and feature advice and best practices from the subject matter experts who drive those events.