JUNIPER NETWORKS

Internet of Things INSTITUTE™

Securing IoT at Scale Requires A Holistic Approach

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 Internet of Things (IoT) projects and to advise on how organizations should get their security posture 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 by sharing these insights from real world project experiences the odds of success will increase for organizations that are currently planning for IoT initiatives.

Involvement with IoT Security

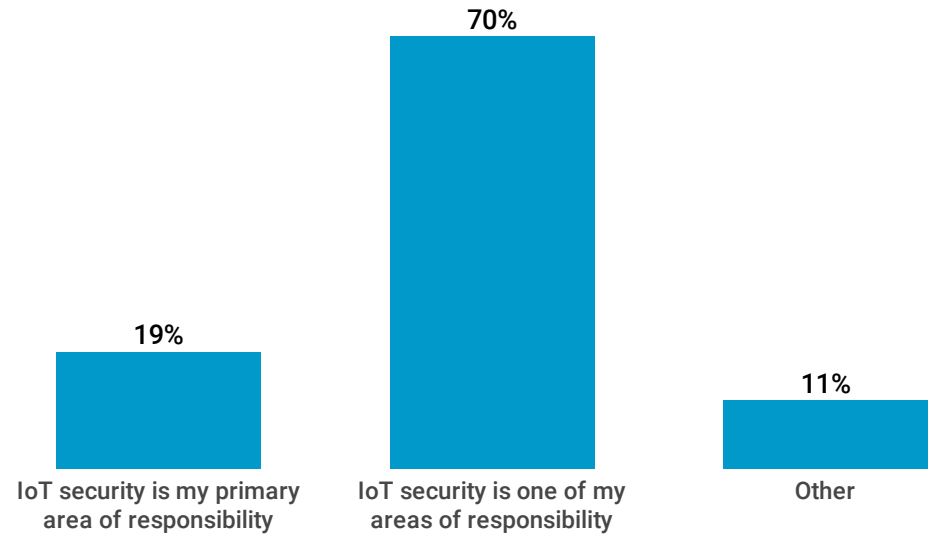


Figure 1

Base = Respondents with direct involvement in IoT Security (n=176).

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, 176 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 security.

Organizational Involvement with IoT

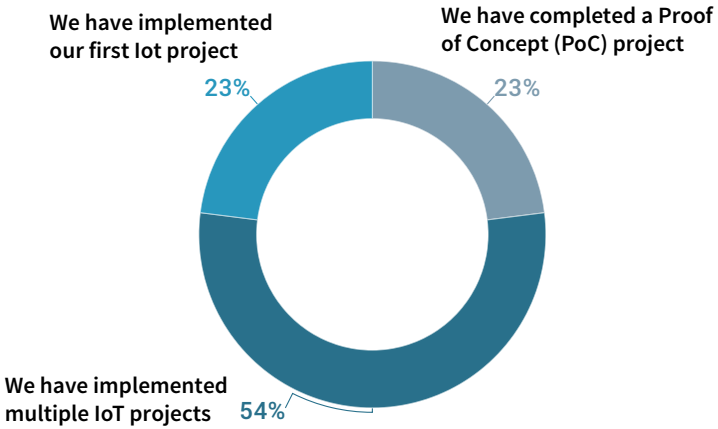


Figure 2

Base = Respondents with direct involvement in IoT Security (n=176).

Respondent Involvement with IoT

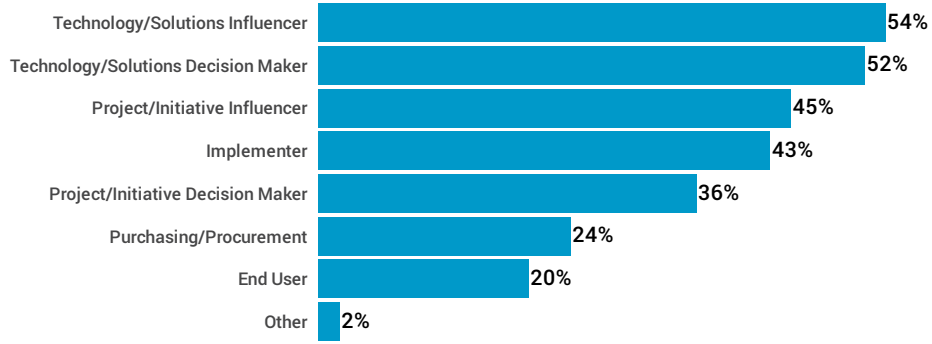


Figure 3

Base = Respondents with direct involvement in IoT Security (n=176).

Organization Size–Number of Employees

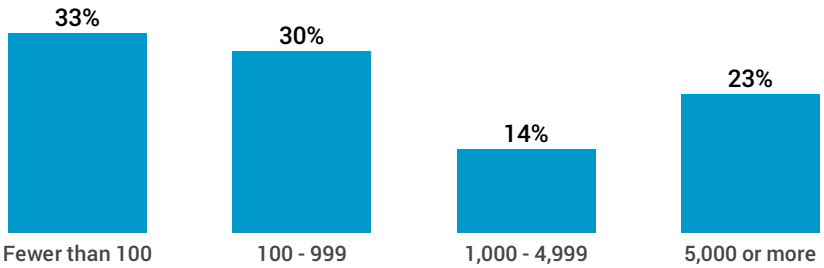


Figure 4

Base = Respondents with direct involvement in IoT Security (n=176).

Organization Type

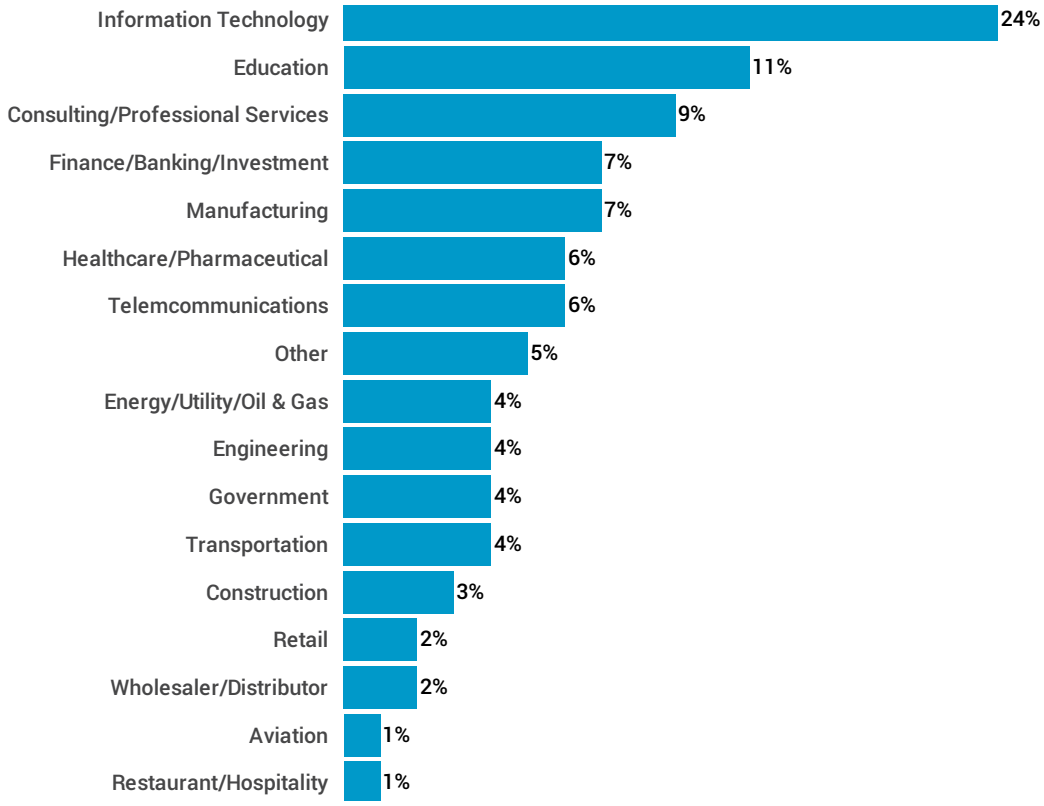


Figure 5

Base = Respondents with direct involvement in IoT Security (n=176).

Top Takeaways

Various Types of IoT Security Risks: Respondents expressed high levels of concern around diverse types of IoT security risks – privacy, critical business data breaches due to IoT device vulnerability, IoT malware proliferation, IoT equipment damage from remote hijack and service downtime.

Top IoT Challenges: Respondents reported their top challenges when it comes to IoT security are hard-to-detect sophisticated IoT threats (51%), followed by compliance (39%), inability of disparate security systems to work together (37%) and not enough staff to keep up (36%).

Diverse IoT Application Workload Locations: IoT application workloads are run in a variety of locations, most commonly in a private data center or control center (51%), at the network edge (36%), and 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.

Prioritized Investment Areas to Strengthen Security Posture: Strengthening an organization's security posture to protect against IoT threats requires investment in different areas. When it comes to priority, IoT Endpoint and Edge (IoT gateway / aggregation device) rank at the top, closely followed by network and cloud.

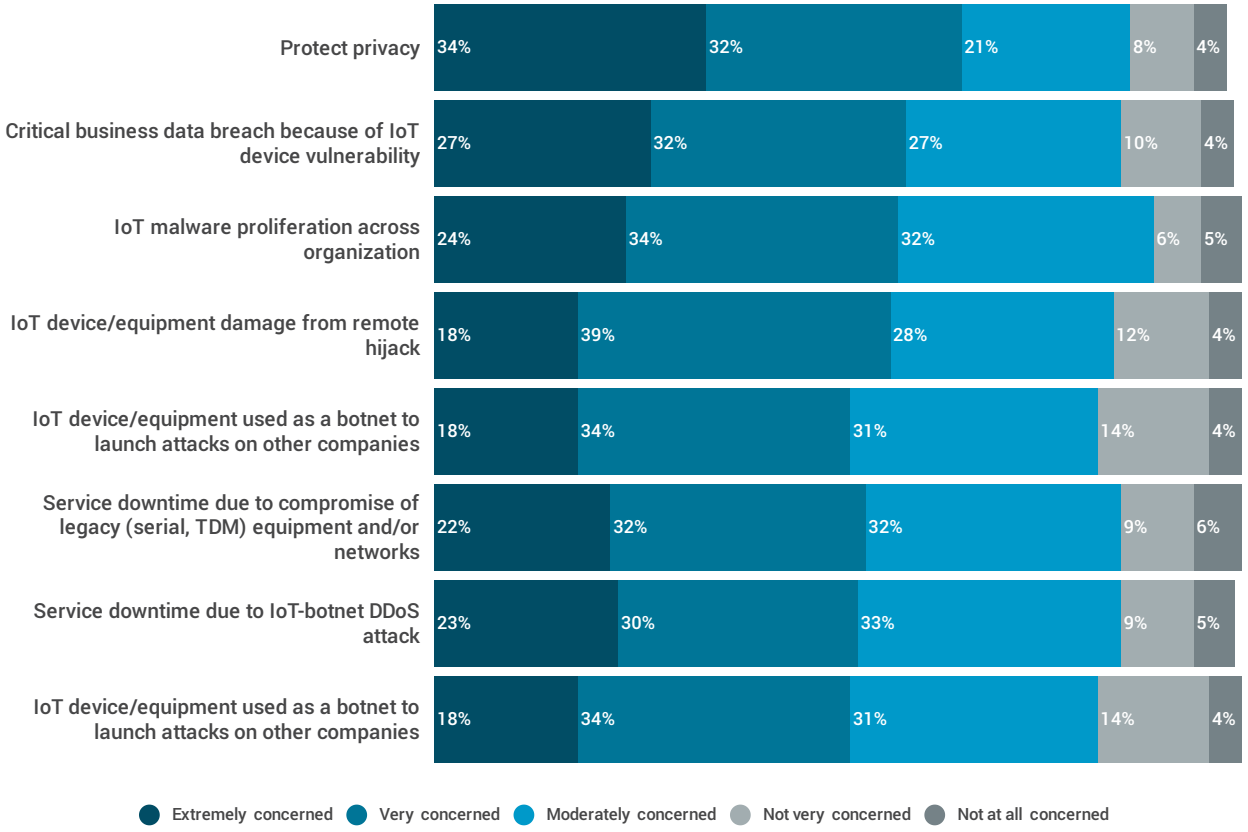
Battery-Powered IoT Devices: A majority of respondents (62%) report that more than half of their IoT devices are battery powered.

The Role of Network in Defending Against IoT-related Security Threats: A majority of respondents (72%) believe the role of the network is very important or even critical for their IoT security. And companies that have already implemented multiple IoT projects are much more likely (26%) to rate the importance as critical than those that have implemented only one project (9%).

Rising Demand of Managed IoT Security Services: 42% of respondents report their organization use managed security services today. And 34% said they are considering doing so in the next 18 months, indicating significant opportunities for managed security service providers to offer IoT-specific services to capture such market demand.

Enterprises Have Concerns Around Various Types of IoT Security Risks

How concerned is your company about each of the following types of security incidents?



Over the last several years, there have been numerous, well-publicized IoT security incidents. The Mirai botnet attack in which IoT devices were hijacked and used to create widespread distributed denial of service (DDoS) disruptions is one of the most well-known to date. Other attacks, such as Bashlite, effected tens of thousands of IoT devices. All of these incursions have helped raise awareness around the urgency of ensuring IoT security.

In an effort to know more about the security concerns of IoT leaders, we asked survey participants to rate their primary concerns and to identify areas where they feel the most vulnerable.

Figure 6

Base = Respondents with direct involvement in IoT Security (n=176).

Respondents expressed the greatest level of concern around privacy (66% indicated “very” or “extremely concerned”). In addition, high levels of concern were expressed regarding many other types of potential security risks. These included critical data breaches resulting from vulnerability of IoT devices (59%), IoT malware proliferation across the organization (58%) and IoT device/equipment damage from remote hijack (57%).

While privacy represents a key area in terms of IoT security, our survey results also point to significant levels of unease related to other aspects of IoT security. In essence, IoT security is not one-dimensional. Instead, our survey results indicate that IT leaders also see potential threats to business applications, which have become critically important productivity tools for lines of business users, customers and partners. In addition, unplanned downtime due to IoT-botnet DDoS attacks can have detrimental effects not only on a company’s brand value and reputation, but also incur millions of dollars in lost revenue. For example, in the case of the Mirai attack on Dyn, a range of large web service companies, such as Twitter, GitHub, Spotify and PayPal, were rendered inaccessible. It was projected that approximately $110 million in potential revenue was lost due to the attack.

Top IoT Security Challenges

With more than enough examples of IoT breaches and attacks, most IoT leaders are already well aware of the importance of having security in place for their deployments. But what exactly are the top challenges they face? The following question was designed to find out.

What are the top challenges that you face when it comes to IoT security?

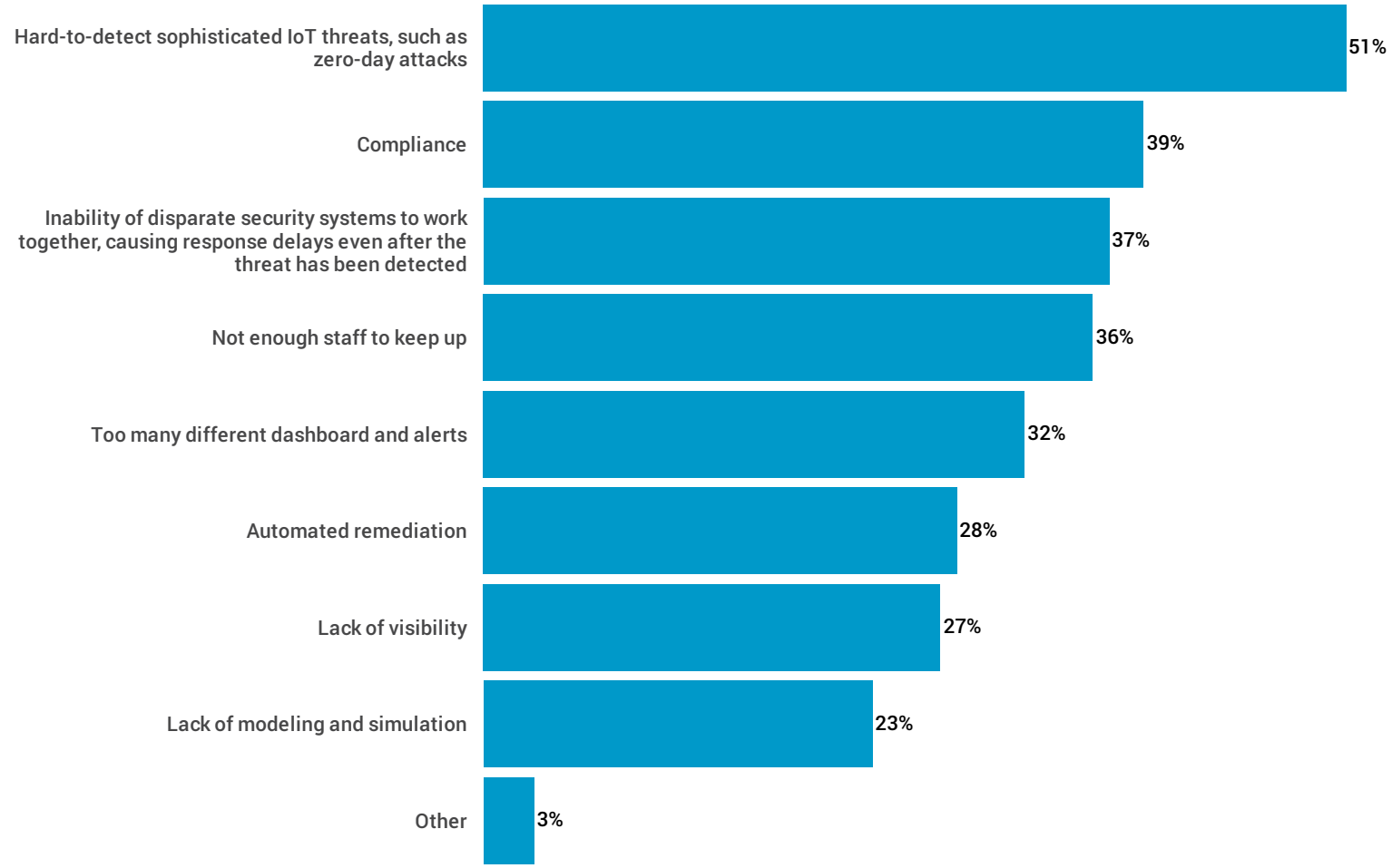


Figure 7

Base = Respondents with direct involvement in IoT Security; multiple answers permitted (n=176).

According to our survey results, more than half the respondents (51%) ranked "hard-to-detect sophisticated IoT threats such as zero-day attacks" as the number one IoT security challenge. Other top challenges included compliance (39%), inability of disparate security systems to work together causing response delays (37%), and not enough staff to keep up (36%).

For example, in 2017 Satori, a variant of Mirai, hijacked more than 100,000 DSL modems in Argentina. The attack quickly extended to other countries and doubled in size over the following week. Security researchers believe that Satori's author had used reverse engineering for discovering the vulnerabilities. Satori represented a classic zero-day approach: launching an attack against a previously unknown vulnerability for which no patch was then available. Researchers believe the variety of malware searching for IoT device vulnerability will increase. Since these are unknown, they're much harder to detect and prevent.

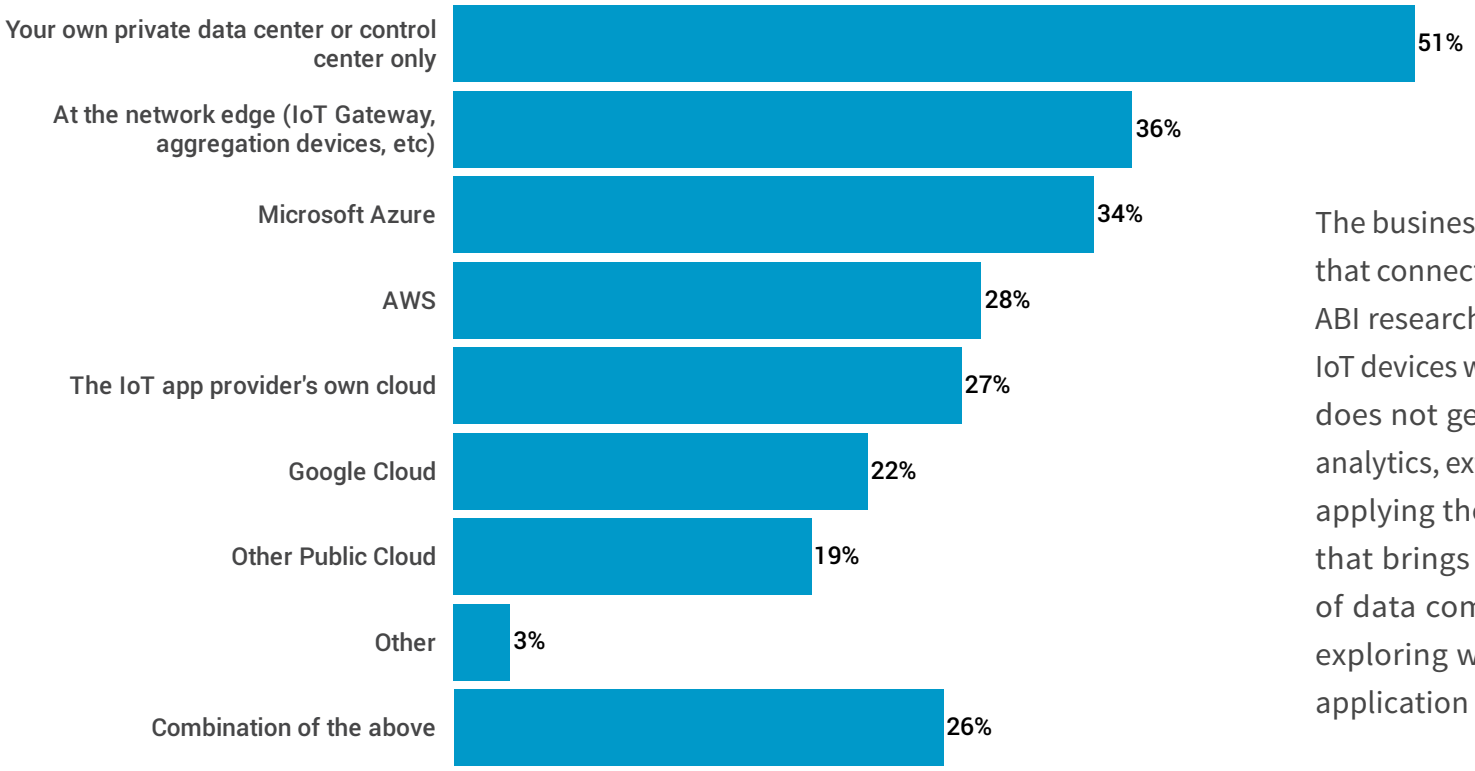
There is a rising trend of hackers searching for IoT device security flaws and creating malware that will exploit these zero-day vulnerabilities.

Industries such as utilities, oil and gas, transportation and manufacturing, must comply with regulatory guideline and mandates for critical infrastructure protection (CIP). As these industrial companies continue the deployment of intelligent connected sensors and devices to improve operational efficiency, they'd need to ensure they're able to continue meeting the compliance requirements. In fact, regulatory compliance is a key driver for the IoT security spending uptake. The challenge comes with IoT deployment at scale. The sheer volume and variety of sensors, devices and event data that need to be tracked and compiled into reports make security monitoring extremely difficult and labor intensive.

Most organizations already have multiple security hardware and software solutions in place, typically from different vendors. However, while each security product might perform an individual function, they don't cooperate with each other as a unified system. As a result, security teams have the time-consuming task of monitoring multiple dashboards across several disparate platforms. When you factor in IoT at scale, admins can end up confronting thousands of threat alerts per day or even per hour. They require the tools to keep up. Different security systems should act as one adaptive security architecture and support automated threat detection and remediation.

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

Where do your IoT application workloads run today?



The business value of IoT comes from the data that connected devices generate. According to ABI research, by 2020 the data captured from IoT devices will reach 1.6 zettabytes . Data alone does not generate much value. It is through analytics, extracting insights from the data, and applying those insights to improve business, that brings value. With such a large volume of data coming from IoT, it would be worth exploring where organizations run their IoT application workloads today.

Figure 8

Base = Respondents with direct involvement in IoT Security; multiple answers permitted (n=176).

[1] https://www.abiresearch.com/press/data-captured-by-iot-connections-to-top-16-zettaby/

Fifty-one percent of survey respondents reported that they run their IoT application workloads only in their private data centers or control centers. Thirty-six percent maintained deployments at the network edge and the remainder run their workloads in a public cloud. Moreover, 26% reported that they use a combination of the above.

In our survey, 51% of respondents deploy on-premise workloads. This is relatively consistent with the overall enterprise application workload distribution trend today. Our survey found that the network edge is the second most popular location where IoT applications run today and this indicates a paradigm shift. Traditionally, data analytics occurs at a central location, whether it's in a data center or in the cloud.

However, due to the sheer volume of data being generated by IoT, the notion of edge computing and edge analytics has emerged, which moves data processing closer to where the data is generated. Employing edge analytics, organizations can move analytics functions from the cloud to an edge analytics-enabled gateway. This change dramatically reduces the amount of device-based data traffic to the cloud. As a result, it offers savings related to the costs of network transport and cloud storage, as well as improves availability, latency and real-time actions.

It's also interesting to note that over 32% 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?

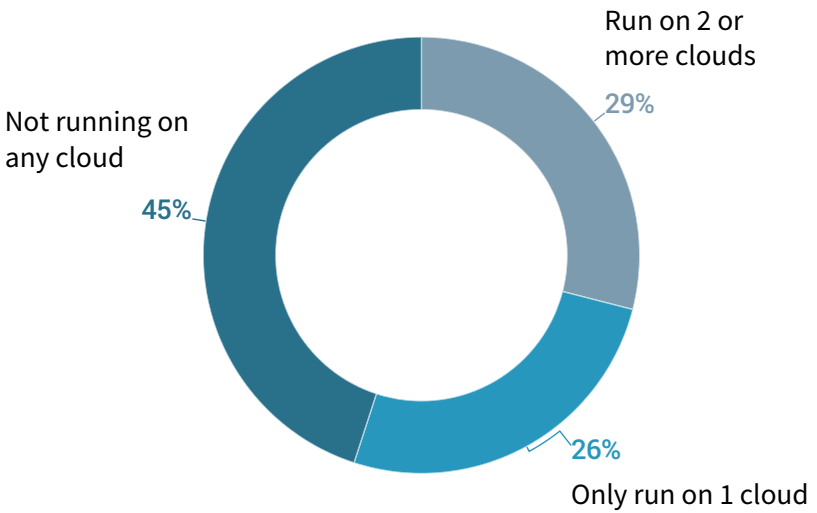


Figure 9

Base=Respondents with direct involvement in IoT Security (n-176)

This trend indicates that for many organizations, their IoT applications are already running in a multi-cloud environment. As enterprise leaders make plans to scale the IoT deployments, they should consider how to address the multi-cloud complexity, especially in terms of connectivity, security and operations.

With IoT Application Workload Being Distributed to Everywhere, Perimeter-based Firewall is Not Sufficient for Providing IoT Security

Do you consider a perimeter-based firewall to be sufficient for providing IoT security?

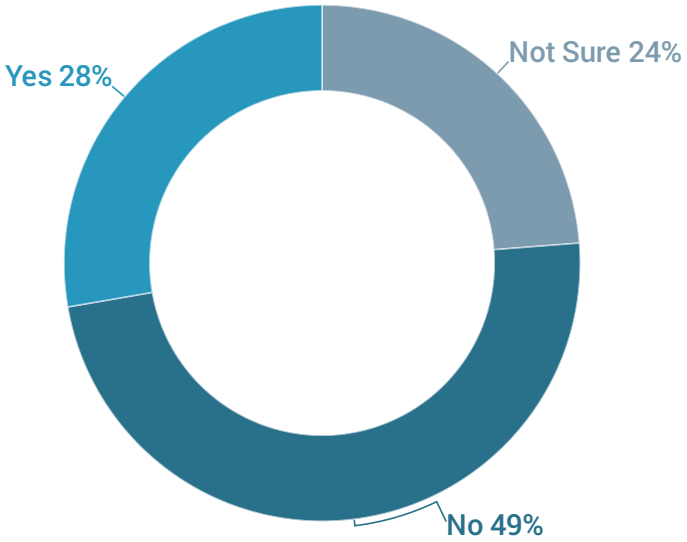


Figure 10

Base = Respondents with direct involvement in IoT Security (n=176).

Traditionally, IT professionals use firewalls to protect their private networks and applications. This is based on a model of fundamental trust in processes that run inside the network and a lack of trust in those that run outside the network wall. As a result, security controls are typically deployed at the perimeter.

This approach represents a flawed model in the current environment as threats can be introduced into a trusted network both knowingly or unknowingly. And since IoT application workloads are being deployed in an increasingly diverse number of external places, the notion of perimeter has become vague.

Half of our survey respondents (49%) considered a perimeter-based firewall as insufficient for providing IoT security. As IoT data and application workloads are spread into multiple clouds and across ubiquitous IoT networks, security detection and policy enforcement also need to be widespread with a zero-trust model.

Prioritized Investment Areas to Strengthen Security Posture for IoT Deployments

Based on the increased awareness of the importance of strengthening the security posture for IoT deployments, many security decision makers expect their firms to increase IoT security spending this year and in following years . Garter says worldwide IoT security spending will reach $1.5 billion in 2018 and $3.1 billion in 2021 . However, it's useful to consider where companies will choose to prioritize investments to strengthen their IoT security postures.

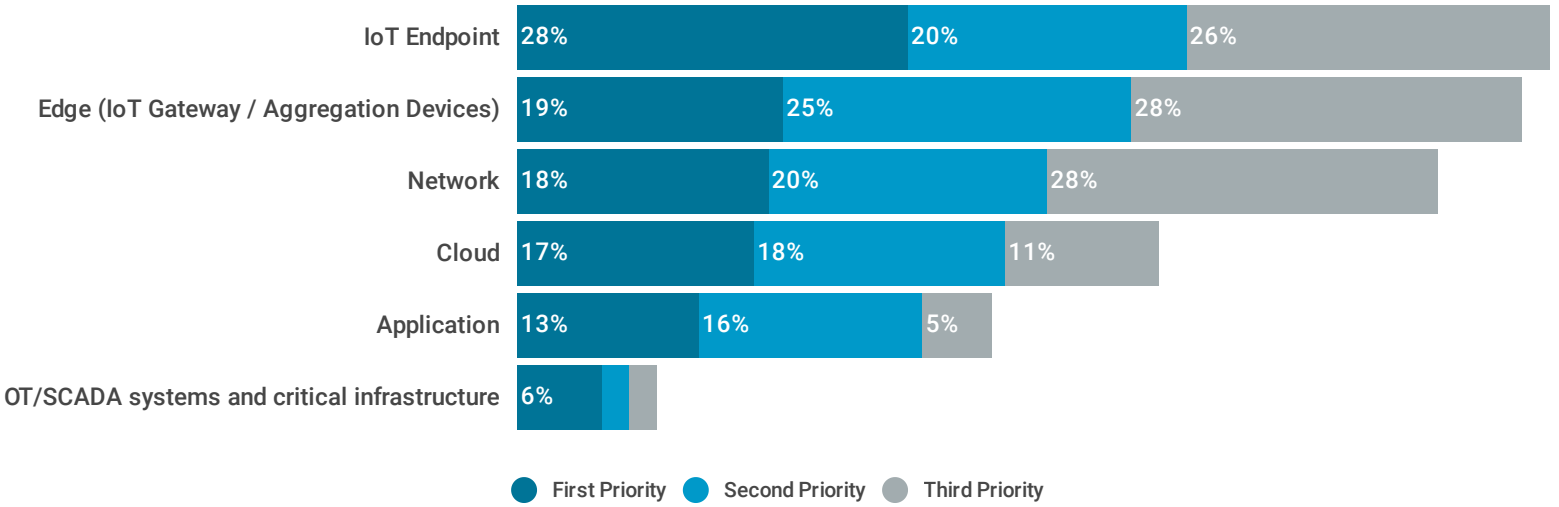


Figure 11

Base = Respondents with direct involvement in IoT Security (n=176).

Based on the survey responses it's not surprising that securing IoT endpoints ranks as the highest priority. However, what's worth paying more attention to here is that edge-, network- and cloud-based security also garnered a significant number of votes. This indicates that securing IoT deployments requires a holistic approach, one that extends to endpoints, edge, network, cloud, and applications.

[2] https://www.forrester.com/47+Of+Businesses+Say+They+Have+The+Tools+To+Support+IoT+Security+Policies/-/E-PRE10148
[3] https://www.gartner.com/newsroom/id/3869181

In terms of security capabilities that are the most effective in countering incursions against IoT devices and networks, threat intelligence and detection capabilities scored the highest percentage (37%), followed by edge-based intrusion detection and analytics-based anomaly detection. This correlates well with earlier indications that "hard-to-detect sophisticated IoT threats such as zero-day attacks" are the most pressing IoT security challenge. Moreover, a significant percentage of respondents (36%) indicated that their IoT application workloads currently run at the network edge.

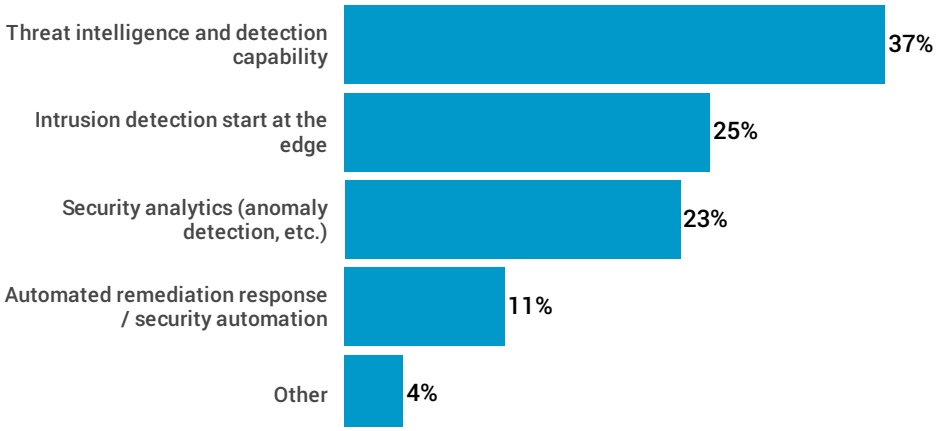


Figure 12

Base = Respondents with direct involvement in IoT Security (n=176).

Therefore, as organizational leaders plan their IoT security strategies, they should consider prioritizing investments in advanced threat prevention (ATP). When choosing a vendor solution, we recommend prioritizing those that include machine learning and behavior analytics capabilities for anomaly detection and which support both on-premise and cloud-based deployment models.

Are you currently using managed security services?

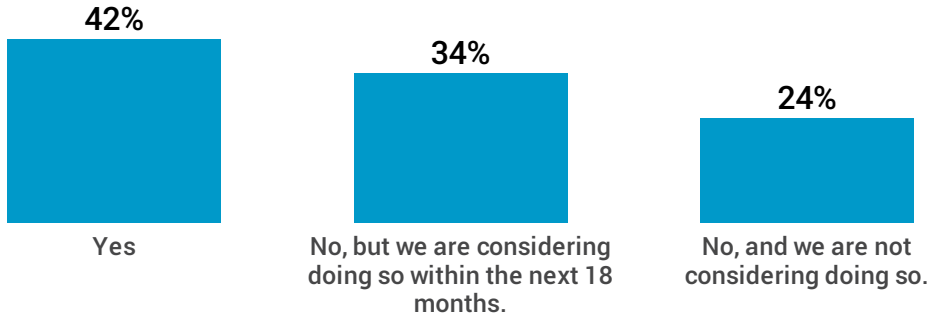


Figure 13

Base = Respondents with direct involvement in IoT Security (n=176).

Respondents from our survey recognized the importance of cloud-based managed security services. For example, 42% are currently using managed security services and an additional 34% are considering doing so in the next 18 months. That's partly due to the fact that IoT complexity often demands a more advanced security skills level.

According to research from IDG, 70% of cybersecurity professionals cite the cybersecurity skills shortage as having had an impact on their organizations.

Given the shortage of security personnel and the fast pace of IoT threat growth, it makes sense for organization to use managed security services to enhance their organization security posture against IoT risks.

These results also imply significant business opportunities for managed service providers. In fact, many are already establishing managed IoT security services to capture the enterprise customer demand. Some common service offerings include managing and monitoring security vulnerabilities of IoT-enabled assets, deployment and enforcement of corporate security policies, providing asset visibility, patching, incident alarm and response, and compliance reporting.

62% Report That More Than Half of Their IoT Devices Are Battery Powered

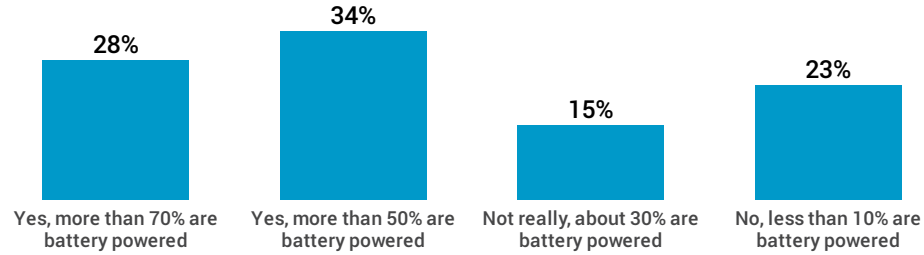


Figure 14

Base = Respondents with direct involvement in IoT Security (n=176).

Battery reliance is another common characteristic of IoT devices. Sixty-two percent of survey respondents reported that more than half of their IoT devices are battery powered. Even more significantly, almost a third (28%) indicated that 70% of their devices are battery powered. This situation creates a dilemma for security implementation. When you run security functions on devices, batteries are depleted much faster. And many of these IoT devices are supposed to live for five years or even longer without needing humans to manually change batteries.

In order to balance their ability to sustain the battery life of devices with the need to have active security in place, organizations are leveraging the edge and the network to deploy defense-in-depth solutions.

[4] The Life and Times of Cybersecurity Professionals
https://c.ymcdn.com/sites/www.issa.org/resource/resmgr/surveyes/ESG-ISSA-Research-Report-Lif.pdf

Rising Importance of Using Network in Protecting Organizations Against IoT-related Security Threats

The role of the network is considered particularly important with regard to better protecting against IoT-related security threats; 72% consider it either “critical” or “very important”.

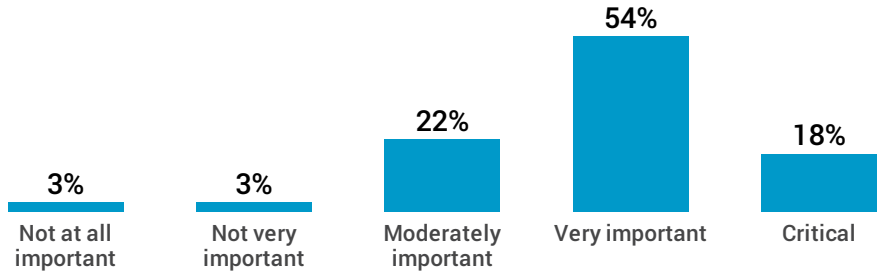


Figure 15

Base = Respondents with direct involvement in IoT Security (n=176).

The role of the network is considered particularly important when it comes to improving protection against IoT-related security threats. Seventy-two percent consider it either “critical” or “very important”. For those companies that have already implemented multiple IoT projects, 26% rated the importance of the network for IoT security as critical versus the percentage of organizations (9%) that have implemented only one project.

How important is the role of the network protecting your company against IoT-related security threats?

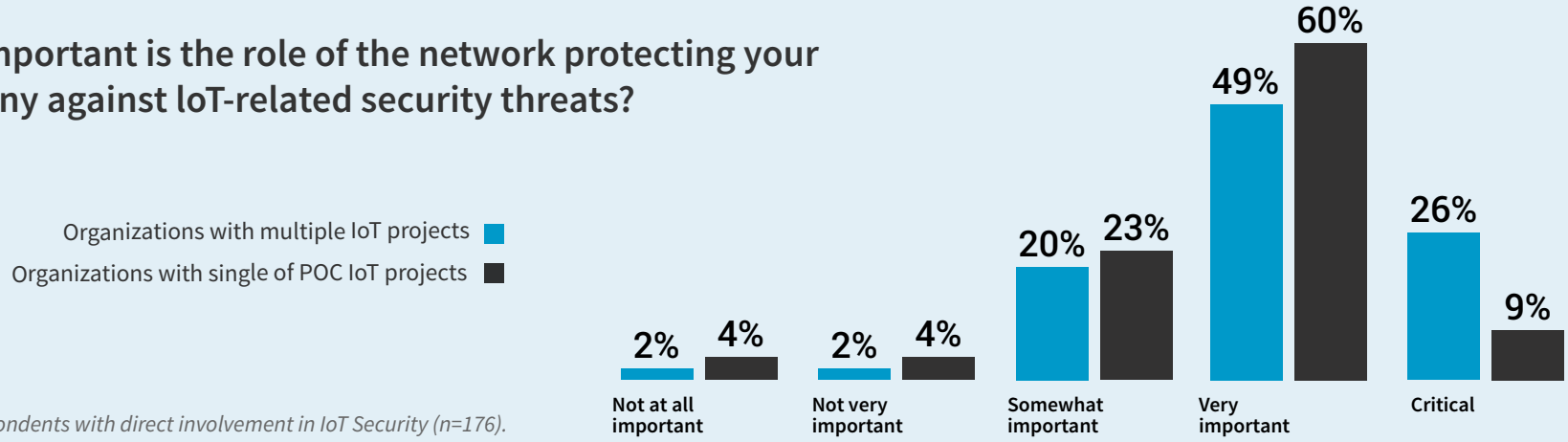


Figure 16

Base = Respondents with direct involvement in IoT Security (n=176).

Conclusion and Recommendations

Due to a number of well-publicized IoT security breaches and attacks, increased numbers of organizations are aware of the importance of security. They understand the importance of not treating security as an afterthought. This is particularly true as these organizations prepare to move from IoT deployment pilots to at-scale production.

Securing IoT at scale requires a holistic approach. It's about more than just securing the endpoints and must also include the edge, network, cloud and applications. Due to the huge volume of IoT data being generated, and the diversity of IoT use cases, application workloads are already starting to be distributed across data center, edge, and multi-cloud environments. This trend will only continue. Since IoT data is omnipresent, security also needs to be everywhere. Traditional perimeter-based firewalls are simply no longer sufficient.

When planning to strengthen an organization's security posture, IoT leaders should prioritize investing in advanced-threat-prevention (ATP) solutions with analytics capabilities that can address the challenge of detecting unknown threats. In addition, organizations should consider using managed IoT security services from third parties to cope with security personnel shortage and compliance needs.

> With a majority of battery-powered IoT devices, the role of edge and network in defending against IoT-related threats is increasingly critical.

Organizations need their networks to offload the security burden from the endpoints themselves to save battery life and to provide defense-in-depth protection. Deeper visibility into the network behavior of IoT devices can help detect anomalies and thus minimize the risk of zero-day attacks. Finally, leveraging the entire network to enforce security policy everywhere, from edge to core to cloud, improves the overall security posture.

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.

IoT World Today 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.

IoT World Today 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.