A Forrester Consulting
Thought Leadership Paper
Commissioned By ForeScout

November 2017

Fail To Plan, Plan To Fail

Understanding The Roles Of LoB Practitioners And SOCs In Securing IoT Environments

FORRESTER®

Table Of Contents

Project Director:
Chris Taylor,
Senior Market Impact Consultant

Contributing Research:
Forrester's Security and Risk research group

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

Executive Summary

Technological advancements have given rise to a deluge of new types of connected devices — i.e., internet of things (IoT) — which, in turn, introduce new security threats that enterprises are ill-equipped to combat and even recognize. Many enterprises are not adequately prepared to deliver on these security needs, applying dated strategies and policies to a new breed of threats. Furthermore, individual lines of business (LOBs) — who often work with operational technology (OT) — and traditional security teams, such as a security operations center (SOC), often don't see eye to eye on how IoT connected devices should be managed.

In August 2017, ForeScout commissioned Forrester Consulting to determine if organizations can adequately and accurately secure their networks due to the explosion of connected, IoT devices on the network whether they are used throughout the enterprise or support specific areas of the business. Individual lines of business who work with the operational technology within companies often implement these new devices or applications without the necessary security oversight, thus creating security vulnerabilities within their networks. Security teams cannot defend what they cannot "see." Therefore, total device knowledge is key to secure operations. Our survey found that companies are indeed concerned about the security of their networks in this new connected age, and they are scrambling to find the right tools, resources, and processes to meet these rising security concerns.

Forrester defines the internet of things as the technologies that enable objects and infrastructure to interact with monitoring, analytics, and control systems over internet-style networks. This includes both the specific devices — i.e. things — as well as the processes and functions — i.e. operational technology (OT) — that this technology enables. For this study, we have grouped connected "things" (i.e. devices) and OT together under the broad category of IoT.

KEY FINDINGS

- IoT is forcing security leaders to re-assess how they secure their networks.
- Risk tolerance with IoT security is shockingly high, forcing security teams to evolve their security strategies.
- IoT security gives over 50% of security leaders anxiety.
- There is little consensus between individual lines of business and IT about who is responsible for IoT management and security.
- Auditing based on visible devices can satisfy compliance, but knowledge of all devices — known and unknown — is crucial for security.
- Device knowledge and better compliance are key steps forward for improving IoT security.

Internet Of Things (IoT) Demands A New Security Approach

The world is in the midst of the connected product (internet of things) revolution with 90% of businesses expecting to see their volume of connected devices increase over the next few years. Businesses can already see the benefits of connecting devices to the network that were not traditionally connected to improve their business processes and functions. However, businesses recognize that these new devices bring the burden of added security requirements: 77% of companies admit that increased usage of IoT devices creates significant security challenges.

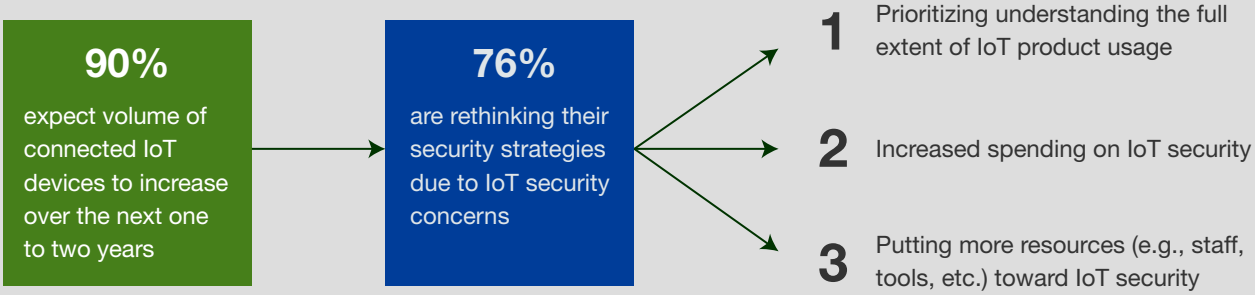
The problem with these security challenges is that most organizations are not properly prepared to manage them. Security teams are deeply ingrained in doing security the way it has always been done, but they are aware that those technologies and processes don't provide the needed security. As a result, 76% of companies claim that IoT security concerns are forcing them to rethink IT and line-of-business security strategies (see Figure 1). This strategy revamp includes:

- Prioritizing understanding the full extent of IoT product usage.
- Increasing spending on IoT security.
- Putting more resources (e.g., staff, tools, etc.) toward IoT security.

77% of companies agree that increased usage of IoT devices creates significant security challenges.

Figure 1

IoT growth is forcing companies to adjust security strategies



Base: 603 IT and business decision makers with involvement in their organization's network and data security processes
Source: A commissioned study conducted by Forrester Consulting on behalf of ForeScout, August 2017

RISK TOLERANCE IS FAR TOO HIGH

Fifty-nine percent of companies said they were willing to tolerate medium to high risk in relation to IoT security compliance — an alarming testament to how ill-informed companies are in the face of IoT security threats (see Figure 2). The fact that businesses are willing to accept this level of risk for IoT shows a staggering lack of understanding of the problem and sets the stage for a variety of future cyberattacks. Tolerating a high risk with IoT is like a freight company acknowledging most of its fleet has mechanical issues but choosing to hope for the best.

The response about the level of risk is striking, which suggests there might be more to this than meets the eye. When putting this risk tolerance into the context of the 77% of companies saying that IoT creates significant security challenges, it suggests that companies' "tolerance" seems to be less about what they are comfortable with and more about what they are powerless to control. Part of the issue is that 44% of companies see budget constraints as top barriers for improving IoT security. As companies struggle to handle the surge in IoT devices and associated compliance requirements, security budgets must increase at a matched pace, or it will force companies to accept a higher level of risk because they are not prepared to do otherwise.

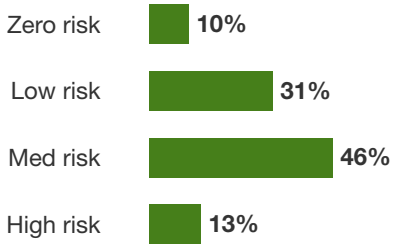
IOT SECURITY GIVES SECURITY PROFESSIONALS ANXIETY

Given the risk many security leaders are forced to accept, it's not surprising that 54% percent say that IoT security gives them anxiety. But with the challenges companies face, we expected this number would be higher — perhaps the reason it wasn't higher is because security leaders don't see a need to be anxious about something they can't control. We found that a higher percentage of line-of-business security decision makers were anxious (58%) about IoT security compared to their IT counterparts (51%). This indicates either a disconnect in how they approach IoT security or a fail point; if IT teams, who have to technically address the issues, don't exhibit the same concerns over IoT, it might be hard for LoB leaders to get the assurances they need that their devices are secure. Anxiety over IoT is driven by three main causes (see Figure 3):

- **Cost and time needed to manage.** IoT exponentially increases the surface area of a network and thus requires substantially more time for security professionals to properly manage it. It's also relatively new: Knowing exactly how it should be managed isn't as straightforward as other security procedures.
- **Potential negative impacts of a security breach.** Security failure of one device on a network can compromise the entire network.
- **Lack of security skills.** If IoT is difficult to manage, it will also be difficult to secure. New technology introduces new security requirements that many security teams are not properly trained to address.

Figure 2

"How much security risk is your company willing to tolerate in relation to compliance requirements for IoT security?"

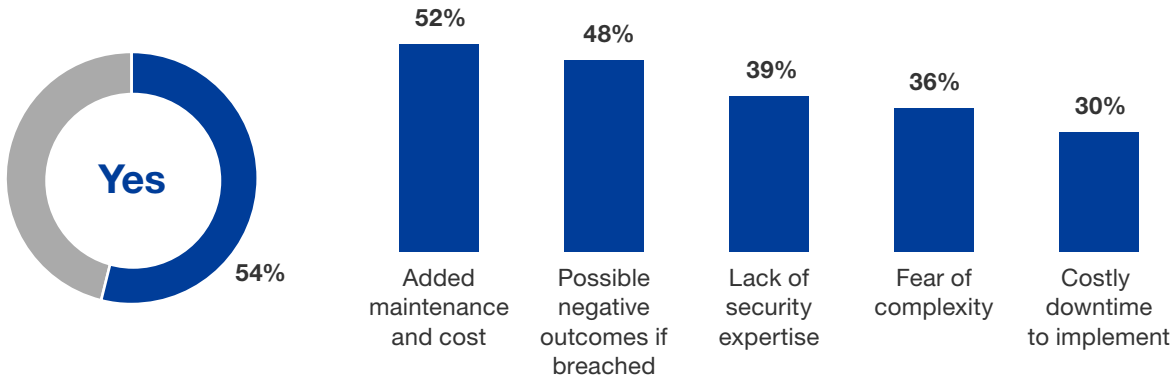


Base: 603 IT and business decision makers with involvement in their organization's network and data security processes
Source: A commissioned study conducted by Forrester Consulting on behalf of ForeScout, August 2017

Tolerating a high risk with IoT is like a freight company acknowledging most of its fleet has mechanical issues but choosing to hope for the best.

Figure 3

"Does IoT security give you anxiety? And why?*"



Base: 603 IT and business decision makers with involvement in their organization's network and data security processes
*Base: 327 IT and business decision makers who indicated that IoT security gives them anxiety.
Source: A commissioned study conducted by Forrester Consulting on behalf of ForeScout, August 2017

IT And Business Leaders Are Not Aligned On IoT Security Management

IT and line of business have different perceptions about how IoT devices and security should be configured and managed. Some feel like individual lines of business should own their own security and others feel like somebody else should be in charge. When asked who is primarily responsible for securing IoT devices on an enterprise IT network, 44% of IT respondents said the SOC, whereas LoBs more commonly identified themselves as the primary party responsible. Conversely, 45% of IT respondents believe that LoBs should be responsible for default devices configurations, and 46% of LoB respondents think IT should be in charge. This creates two possible scenarios: 1) an environment in which IoT security is managed in silos (IT for IT and LoBs for LoBs) with limited availability across the company, or 2) an environment in which everyone is expecting someone else to take responsibility (see Figure 4). Regardless of which outcome your company faces, it can result in security lapses if devices are left unaccounted for or improperly configured.

As enterprises consider how to manage IoT security, most companies stick with what they know and keep security under the purview of IT, such as a security operations center. Typically, this approach works in general, but only if organizations already have visibility into what devices exist. Any SOC can manage or support devices, but it's also critical that they coordinate and collaborate with the asset managers, LoB teams, and network teams that are plugging devices in. This is important for two reasons:

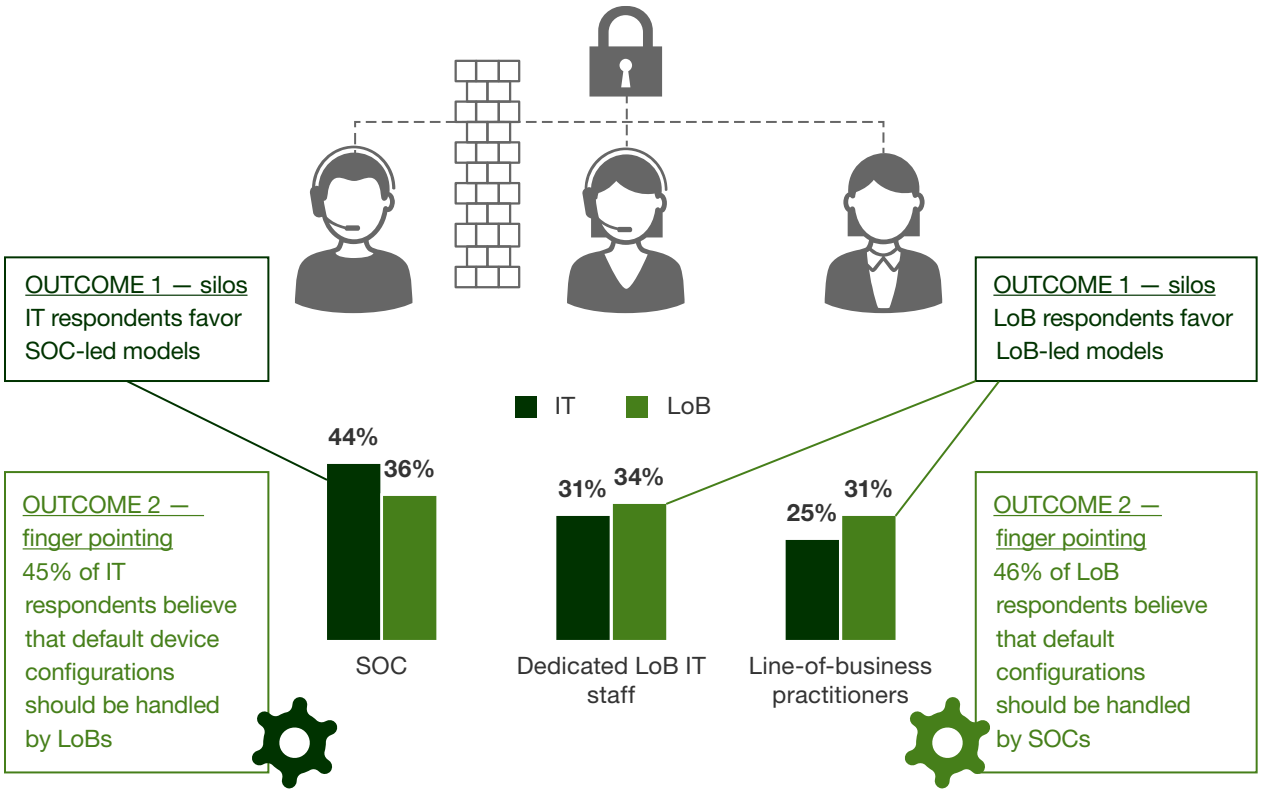
- **Managing default security configurations.** Fifty percent of companies say that default configurations for IoT devices should be handled by the SOC. However, when broken out by job titles, 54% of LoB respondents think that default configurations should be managed by the LoB staff or device manufacturers. This finding indicates that LoB users are deploying devices with the assumption that all the proper controls are in place without even needing to utilize a SOC as a command and control point for their IoT security needs. Further, 45% of the IT respondents think LOBs own this — therefore giving them less motivation to work together.
- **Getting proper visibility of devices on the network.** Unless SOCs are actively involved with the asset managers and LoB teams during device setup, it's difficult for them to get a fully accurate count of what devices are connected. SOCs need 100% visibility as security failure of one device on a network can compromise the entire network.

Ask yourself:

Who would your company's SOC or line-of-business teams say is responsible for IoT configuration and security management?

Figure 4

Confusion of who is responsible for securing IoT devices on the network leads to two outcomes



Base: 603 IT and business decision makers with involvement in their organization's network and data security processes
Source: A commissioned study conducted by Forrester Consulting on behalf of ForeScout, August 2017

Security Complacency Can Lead To Problems

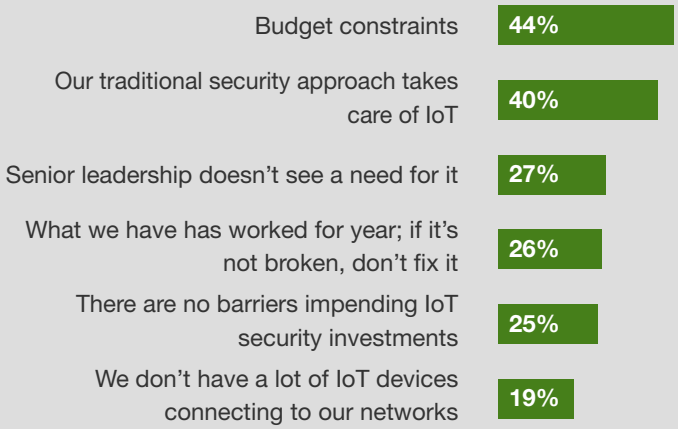
Knowing that IoT security is a major challenge and concern, we asked respondents to identify key barriers that were impeding improvements to IoT security. IT and LOB respondents reported similar challenges, indicating parallel — if ineffective — approaches to IoT security. It short, both groups appear to struggle in the same ways at the same time. The top responses were (see Figure 5):

- **Belief that traditional security approaches take care of IoT.** Security teams have been securing legacy systems for years. The myth is that it's easy for them to apply those same practices to IoT. However, the idea of "if it's not broken, don't fix it" doesn't apply when working with new technologies that have been relatively untested or unidentified.
- **Lack of support from senior leaders.** Building on the belief that current methods are good enough, many senior leaders might find it hard to justify investing in new tools or personnel. Unfortunately, it will likely take a breach to get their attention, at which point it's too late.
- **Budget constraints.** Forty-four percent of companies cited budget as a key barrier. Lack of budget impacts a company's ability to hire for the right technical skills and purchase the proper tools to manage IoT security properly (reported as a challenge for 31% and 25% of companies respectively). This also helps explain why maintenance and costs are the most common causes of anxiety around IoT security. Even in cases where budgets are increasing, organizations need to ensure that the budgets for IoT security increase in proportion to the growth of IoT devices. Between debunking beliefs that current security is adequate and struggling for executive support, finding the needed budget can be an uphill battle.

Unfortunately, it will likely take a breach to get the attention of some senior leaders. At that point, it's too late.

Figure 5

"What has been the biggest barrier keeping your company from investing more in IoT security?"



Base: 603 IT and business decision makers with involvement in their organization's network and data security processes
Source: A commissioned study conducted by Forrester Consulting on behalf of ForeScout, August 2017

Even in cases where budgets are increasing, organizations need to ensure that the budgets for IoT security increase in proportion to the growth of IoT devices.

COMPANIES LACK TOTAL SECURITY CONFIDENCE WITH IOT

As many companies hold the belief that current security policies are adequate for covering IoT, we asked them to rate their confidence in their current IoT security. On a scale from 1 to 10, with 10 being full confidence, most responses were positive, with 70% in the 8 to 10 range. However, that left 30% of companies with medium to low confidence in the security of their IoT networks. In particular, only 13% rated themselves a 10 (full confidence). Considering what's at stake and the potential ramifications of a security breach, it is a little concerning to see that 87% of companies do not have full confidence in their IoT security.

87% of companies do not have full confidence in their current IoT security.

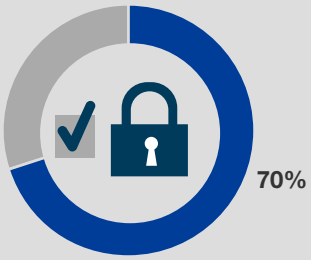
Taking this point further, we posed the following hypothetical question:

"If your company was audited and was required to identify all IoT connected devices and solutions it uses, how confident would you be in your ability to accurately identify 100% of the IoT connected devices and solutions your company is using?"

Like the results about security confidence, we saw most respondents in the 8 or 9 range, but only 18% had full confidence. That is a major issue if 82% of companies are not fully confident that they know all devices that are on their network (see Figure 6). The network and security world that our businesses now find themselves in is compliance-driven and audit-focused. Our study indicates that while most organizations feel they would be able to adequately pass a compliance audit focused on IoT controls, in truth, they knowingly acknowledge they aren't 100% sure. This highlights a potential fail point for many companies that could likely become a serious avenue for a network breach.

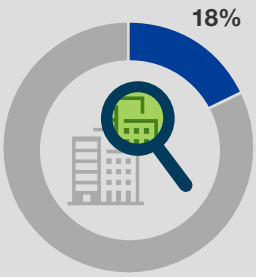
Figure 6

"How confident are you that your IoT network is secure?"



70% Highly confident

"If audited, how confident are you that your could identify 100% of the IoT connected devices or solutions being used?"



18% Fully confident

Base: 603 IT and business decision makers with involvement in their organization's network and data security processes
Source: A commissioned study conducted by Forrester Consulting on behalf of ForeScout, August 2017

Satisfaction with current IoT security is high, but doesn't hold up when truly tested.

FORRESTER®

IoT Security Begins With IoT Visibility

We identified four key steps that businesses are taking to meet growing challenges as they begin to redefine their network security strategies to accommodate the growth of IoT (see Figure 7):

- **Improving awareness and visibility into IoT devices.** Understanding what devices are on the network is a critical first step in being able to secure it. You can't protect what you can't see: that is why this was the most commonly identified next step (48%).
- **Putting greater emphasis on compliance.** While many companies currently tolerate medium to high risk with IoT security compliance, it's not necessarily by choice. A renewed focus on compliance, coupled with efforts to increase network visibility, will enable security leaders to be more confident if audited and lower their forced tolerance of risk.
- **Centralizing management and implementation of IoT devices.** While most companies currently manage devices centrally under a SOC or IT control, there still exists a disconnect in who is responsible for initial configuration and implementation. By centralizing both the implementation and management of IoT devices, companies will have more consistent configurations, better awareness of new devices, and less confusion between IT and LoB teams about security ownership.
- **Finding IoT security partners to provide tools and expertise.** As companies invest more in IoT security, they'll need partners that can help fill their skills gaps and enable them with the proper tools. When asked for the most important criteria when considering a next-generation IoT security solution, the top responses were: 1) solutions must integrate with existing security systems, and 2) ease of implementation. Companies want partners that can work with them seamlessly to augment their security without needing to completely revamp their entire security solution.

In support of these next steps, 82% of enterprises expect their spending on IoT security to increase over the next one to two years. In theory, the relative spend going toward IoT should be reflective of the growth seen in IoT devices versus traditional security improvements. However, this can be a tough sell, given that 40% of respondents feel traditional security measures are sufficient for IoT. As such, it becomes more critical than ever that security teams demonstrate to executive teams the importance of securing their IoT environments — and the risks of not doing so. By showcasing to senior leadership the importance and value of IoT security, security teams can earn the funding and resource allocations required to adequately protect their IoT environments. With increased funding and a new security strategy focused on visibility and compliance, companies can begin taking strides forward to reduce their anxiety about IoT and regain confidence that their networks are secure.

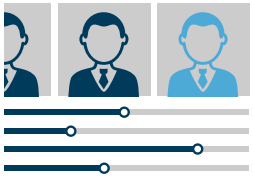
Figure 7

"What steps is your organization taking to improve your IoT security?"

Improving awareness and visibility

Greater emphasis on compliance

Centralizing management of IoT security



Finding partners with the right tools and expertise

Base: 603 IT and business decision makers with involvement in their organization's network and data security processes
Source: A commissioned study conducted by Forrester Consulting on behalf of ForeScout, August 2017

48% of companies see improved awareness and visibility of IoT devices as a critical next step to improving IoT security.

Key Recommendations

Today's companies face a world of constant and ever-expanding connectivity. Each day, new devices and capabilities come online that can offer decisive advantages for businesses to grow and thrive. However, those same devices and technologies, if left unattended and unaccounted for, can be the very origin point for a network breach and ultimately an organization's demise. To better defend IoT-enabled systems, we suggest that businesses do the following:

Know thyself. Without a clear security strategy, your company will continue to face security anxiety and challenges. Ask yourself the following questions and be honest with yourself on your answers:

- **Do I truly have full visibility into my network? What level of risk am I willing to accept?** If there is not comprehensive knowledge and control of every device that touches the network, then that network is not secure — even if you can pass an audit based on the devices you do know about.
- **Who owns the configuration and implementation of new devices?** It is imperative that your security team and network team collaborate and coordinate their IoT implementations and security protocols to enable total device oversight.
- **Can you? Should you?** Ask these questions whenever a new device or technology is offered as a solution or "need" for your team. Can you use a wirelessly enabled toaster? Sure. Should you introduce an unnecessary threat vector into your network for the comfort of your personnel? Probably not.

Rise above the standard. Meeting a compliance standard or audit mandate is simply achieving the very bottom layer of capability: It is literally one step above likely failure. Your team must strive to rise above those baselines and move forward with planning and strategies that drive innovation and optimization while safely adopting new technologies that benefit the business.

Fight tech with tech. It is impossible for humans to keep up with the growth and diversity of network-connected devices that are prevalent today. To have any chance of addressing the issues around IoT security and accounting, your team needs to leverage dedicated technical solutions focused on the specifics of IoT security controls. Use technology to combat technical failures and empower your security and LoB teams as they work to address IoT sprawl.

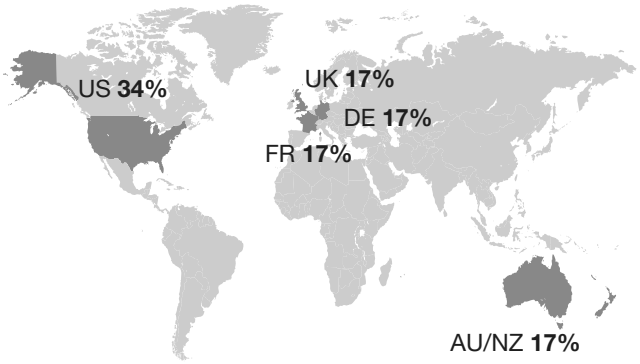
FORRESTER®

Appendix A: Methodology

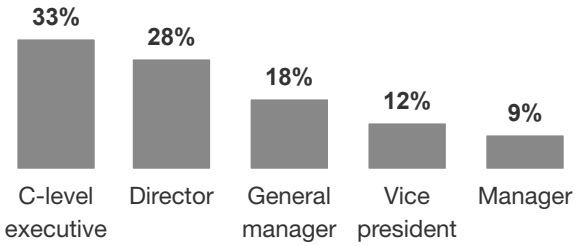
In this study, Forrester interviewed 603 IT and business decision makers with involvement in their organization's network and data security/endpoint security processes. Questions provided to the participants asked about challenges with IoT security and overall awareness of devices on their network. Companies surveyed were from the US, UK, Germany, France, and Australia/New Zealand and had employee counts of 2,500 or more. Respondents were offered a small incentive as a thank you for time spent on the survey. The study was completed in August 2017.

Appendix B: Demographics/Data

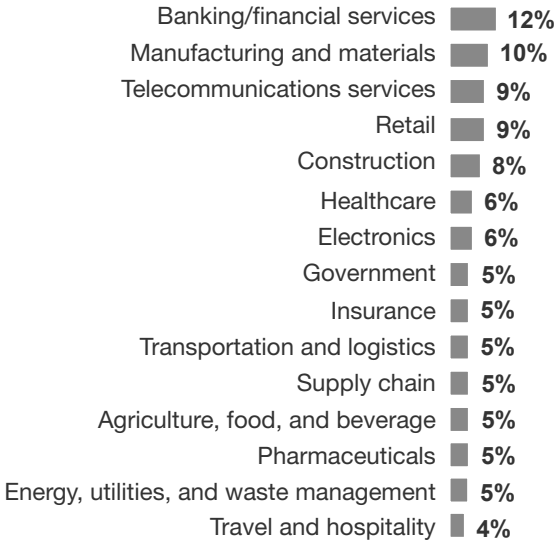
RESPONDENT DEMOGRAPHICS:



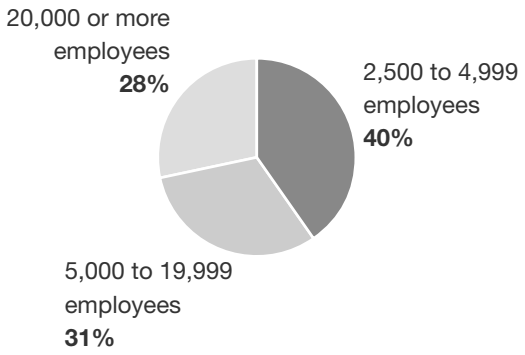
RESPONDENT LEVEL



INDUSTRY



COMPANY SIZE



Base: 603 IT and business decision-makers with involvement in their organization's network and data security / endpoint security processes.
Source: A commissioned study conducted by Forrester Consulting on behalf of ForeScout, August 2017

FORRESTER®