A Forrester Consulting
Thought Leadership Paper
Commissioned By Armis Inc.

September 2019

State Of Enterprise IoT Security In North America: Unmanaged And Unsecured

How Enterprise Security Professionals Are Responding To The Evolving Threat Of Unmanaged Devices

FORRESTER®

Table Of Contents

1 Executive Summary

3 Number And Variety Of Unmanaged And IoT Devices Is Growing Fast

4 Most Enterprises Remain Vulnerable

9 Investment In Enterprise IoT Security Solutions And Practices Is Insufficient And Need To Increase

11 Key Recommendations

12 Appendix

Project Director:
Line Larrivaud,
Market Impact Consultant

Contributing Research:
Forrester's Security and Risk research group

FORRESTER®

74% of enterprise security professionals feel their current security controls and practices are not adequate for unmanaged and IoT devices.

Executive Summary

The use of unmanaged and IoT devices in enterprises is growing every day across every industry. With an estimated compound annual growth rate (CAGR) of 30%, it is forecast that around 18 billion IoT devices will be in use by 2022.[1] Some of this growth is business-driven, being tied to business optimization initiatives, while some of it is unintentional and under the radar of IT security staff. As the proportion of unmanaged devices within enterprises grows and exceeds that of managed devices, so too does the organization's attack surface. Security professionals are now facing an unprecedented level of risk — the stream of cyberattacks has been unrelenting and hardly a month goes by without a major breach hitting mainstream headlines.

In July 2019, Armis commissioned Forrester Consulting to evaluate the current state of unmanaged and IoT device security in North America, as well as the future trends. To explore this topic, Forrester conducted an online survey with 403 technology decision makers responsible for IoT security in their organizations, and three interviews with CISOs and IT project managers across healthcare, manufacturing, and transportation industries. We found that the enterprise IoT environment has grown increasingly complex, creating exposures that security professionals struggle to address. To protect firms, security leaders need to increase the spending dedicated to unmanaged and IoT security to ensure that they have appropriate security measures in place.

KEY FINDINGS

- **The use of unmanaged and IoT devices within enterprise environments is already prevalent and growing rapidly, driven by a combination of business needs and unintentional factors.** Today, 69% of surveyed respondents estimate that at least half of all devices on their enterprise network are unmanaged or IoT, and 26% estimate that unmanaged devices outnumber managed devices on their network by three to one. This raises the concern of enterprise security professionals in terms of knowing how to secure these devices, with 79% being very-to-extremely concerned about device security.
- **Enterprise security professionals fail to understand and address the security risks brought by unmanaged and IoT devices.** Almost three quarters (74%) of respondents felt their current security controls and practices are not adequate for unmanaged and IoT devices. Just as worrying is the lack of understanding of what constitutes an IoT device. As a result, 67% of surveyed organizations have experienced a security incident related to unmanaged or IoT devices.
- **Investment in IoT security solutions is insufficient and needs to increase.** Sixty-eight percent of surveyed security professionals believe that their level of spending to secure unmanaged and IoT devices is inadequate, relative to the risks presented by these devices. To respond to evolving cyberthreats, budgets dedicated to unmanaged and IoT devices security will need to increase. Some security controls will be widely used and become standard practices, such as device risk assessment (96%) and new behavior monitoring (96%).

DEFINING AN UNMANAGED OR IOT DEVICE

For this study, we defined unmanaged and IoT devices as any system that can communicate with other devices and systems in your organization, process and transmit information, has an operating system (no matter how simple), but cannot be managed via traditional security tools. Such devices can include, but are not limited to:

Office devices and peripherals	Printers, VoIP phones, smart TV screens and monitors, Bluetooth keyboards, headsets, etc.
Building automation	HVAC systems, security systems, lighting systems, cameras, vending machines, etc.
Personal or consumer devices	Smartphone, smart watch, gaming consoles, Apple TV, Slingbox, digital assistants (Amazon Echo, Google Home, etc.), cars.
Industry-specific devices	Industrial control systems (PLCs, HMIs, robotic arms, etc.), medical devices (patient monitoring systems, mobile imaging systems, infusion pumps, communication badges, etc.), retail (barcode scanners, POS system, loss prevention, etc.), warehouse (inventory systems).
IT infrastructure	Access points, routers, switches, firewalls, baseboard management controllers of servers.

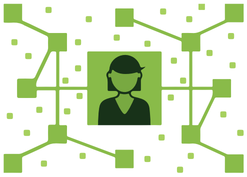
Number And Variety Of Unmanaged And IoT Devices Is Growing Fast

With around 18 billion IoT devices forecasted by 2022[2], technology leaders are dealing with an increasingly complex IT environment. In surveying 403 enterprise security professionals across various industries (see appendix B), we found that 87% of them have seen an increase in the number and use of unmanaged and IoT devices connecting to their organization's network in the last 24 months (see Figure 1). We also found that:

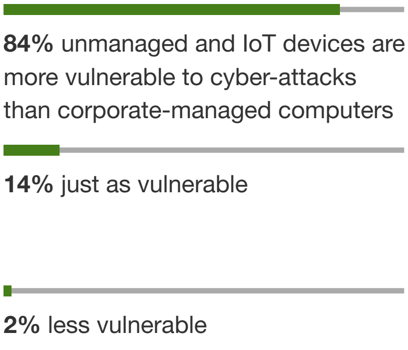
- **The increase in unmanaged and IoT devices connecting to enterprise networks has been rapid.** Over the last few years, enterprises have implemented a variety of IoT applications and solutions across a range of apps.[3] As a result, the enterprise IoT environment now makes up a significant portion of the larger IT ecosystem: 69% of surveyed organizations estimate that at least half of all devices on their enterprise network are unmanaged or IoT, and 26% of organizations estimate that unmanaged devices outnumber managed devices on their network by three to one. Respondents are expecting this rapid growth to continue over the next 24 months.
- **Exponential device growth is driven by business and other factors.** With the aim of improving business performance and collaboration, the use of data in business insights and even regulatory compliance, organizations have been introducing IoT devices to all areas of their operations. This is especially true in: 1) the manufacturing sector where we see IT converging with operational technology (OT) devices; 2) the healthcare sector where we see the introduction of connected medical devices for patient monitoring and healthcare delivery; and 3) in all sectors where we see the introduction of smart electronics, appliances, HVACs, and lighting in smart buildings. This growth is compounded by the unintended introduction of connected devices onto the enterprise network — with employees connecting their own devices to the network, and with manufacturers building connectivity into devices as diverse as speakers, security cameras, telecommunications devices, etc.
- **Enterprise security professionals are concerned with risk exposure.** The security of IoT deployments was among the top 10 concerns in 2017.[4] Two years later, 79% of surveyed respondents for this study are very-to-extremely concerned about the security risks posed by unmanaged and IoT devices, and 84% believe that unmanaged and IoT devices are more vulnerable to cyberattacks than corporate-managed computers (see side bar figure).

While unmanaged and IoT devices bring the promise of productivity, efficiency, and collaboration, they offer little in the form of security, creating new security exposures for organizations.

> "I think the number of devices touching the network that are not secure will continue to increase. As a consequence, we also believe the risk factor for those devices will increase,and the number of devices being hacked or manipulated will increase as well."
>
> *Medical device security project manager, US medical group*



"Compared to corporate-managed computers that are running enterprise security agents, how vulnerable do you believe unmanaged and IoT devices are to cyberattacks?"



84% unmanaged and IoT devices are more vulnerable to cyber-attacks than corporate-managed computers

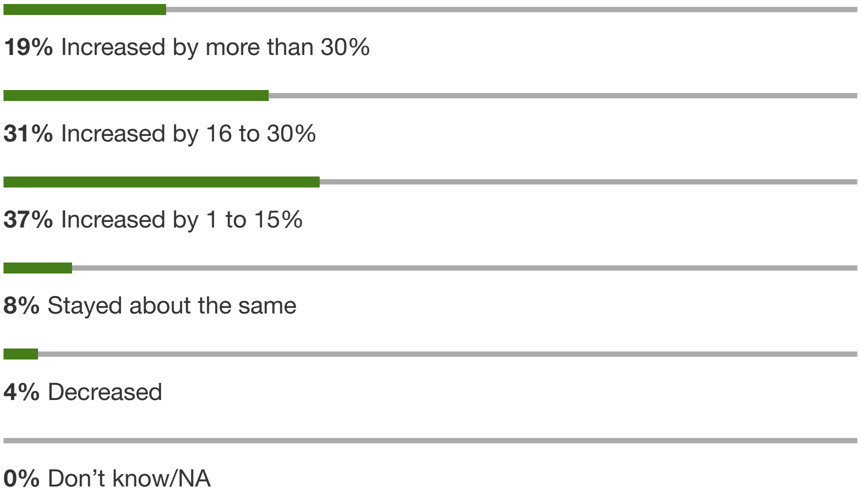
14% just as vulnerable

2% less vulnerable

Base: 403 technology decision makers with responsibility over IoT security at US and Canada firms
Source: A commissioned study conducted by Forrester Consulting on behalf of Armis, July 2019

Figure 1

"How has the use of unmanaged and IoT devices evolved in your organization in the last 24 months?"



Base: 403 technology decision makers with responsibility over IoT security at US and Canada firms
Source: A commissioned study conducted by Forrester Consulting on behalf of Armis, July 2019

- Unmanaged and IoT devices outnumber managed devices in 69% of the organizations surveyed
- 84% of respondents believe that unmanaged and IoT devices are more vulnerable to cyber-attacks than corporate-managed devices

Most Enterprises Remain Vulnerable

Unmanaged and IoT devices pose a real security risk to organizations, but many IT managers are not fully aware of these risks, nor are they equipped with the knowledge, skills, and resources to sufficiently manage them. As a result, enterprise security professionals fail to address the security threats brought by unmanaged and IoT devices:

› **Most enterprise security professionals lack a thorough understanding of IoT-related risks.** They are not clear on the extent of the risks, and how best to address them, leading to a lack of confidence in their ability to manage IoT security risks. Seventy-four percent feel their current security controls and practices are not adequate for unmanaged and IoT devices, 51% say they do not fully understand the risks associated with unmanaged and IoT devices, and 80% are just not sure where to start (see Figures 2 and 3). In addition, some miss out on securing certain types of devices as there are misconceptions on what classifies as an IoT device.

› **Traditional security tools and in-house skills are not adequate to protect unmanaged and IoT devices.** Fifty-three percent of respondents feel they don't have effective tools to protect unmanaged and IoT devices from attacks. Many struggle to identify, classify, and locate the devices connecting to their network — 41% say they do not have full visibility of unmanaged and IoT devices connected to their network and in their airspace. They are also facing challenges in bringing expertise in-house — 47% say they feel their IT team lacks the right skills to keep their business safe, and 31% say there is an unavailability of security employees with the right skill set on the market.

"Visibility is number one for me, if you can't see it, you can't protect it. Then only are you able to make some smart decisions about what you should and shouldn't allow the device to do, apply policy to that, and make it more intelligent."

CISO, US Airline

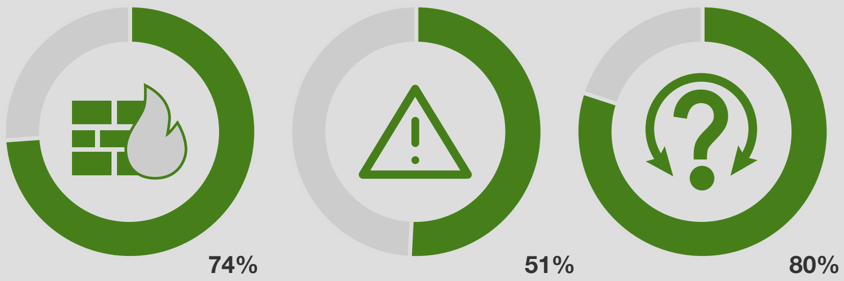
- **Recommended security frameworks are not effectively followed for unmanaged and IoT devices.** Security frameworks such as those recommended by the United States' National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS) are being used by 75% of the surveyed organizations, with 64% of them applying these guidelines to their population of unmanaged and IoT devices. However, 88% of respondents still feel their existing security controls do not fully meet the requirements of these security frameworks for unmanaged and IoT devices (see Figures 4).
- **IoT security budgets are not keeping up with exponential growth of devices.** Technology leaders have to prioritize their security investments across a wide range of areas, not always providing the full priority to unmanaged and IoT devices. As a result, IoT security spending is not proportionate to the growth in devices and complexity of the environment, with 71% of respondents allocating less than 20% of their IT security budget towards unmanaged and IoT device security. In turn, this is making it challenging for them when trying to implement IoT security best practices and solutions. Most of the respondents (68%) admit their current security spending is inadequate, relative to the risks presented by unmanaged and IoT devices. And, despite the growing use of these devices in the last two years, spending has stayed the same or decreased for 32% of those firms.
- **As a result, most organizations fail to secure unmanaged and IoT devices, and thereby suffer from security incidents.** Beyond the Mirai incident, more security breaches are impacting unmanaged and IoT devices.[5] There has been a spike in ransomware attacks on manufacturing and healthcare organizations.[6, 7] Medical devices have been identified as being exposed to hacking.[8] Microsoft recently identified that enterprise IoT devices were being actively targeted by nation states.[9] Each of these reveal the growing risks and difficulties organizations are facing when protecting IoT devices that are connecting to their network. Sixty-seven percent of surveyed organizations have experienced some sort of security incident from unmanaged or IoT devices (up to 75% in the financial services industry). Consequences from these incidents have affected companies in multiple ways, including data leakage in 64% of the cases, raised customer or patient privacy concerns for 56% of the organizations, and reduced revenue for 45% of them (see Figure 5).

The extent of security exposure for unmanaged and IoT devices is often not well understood or addressed by enterprise security managers. Security incidents are now forcing them to look at how to better mitigate those risks.

67% of organizations surveyed have experienced a security incident related to unmanaged or IoT devices.

> "The sheer propagation of these devices is just astonishing. I actually struggle to find devices that are not internet connect versus those that are."
>
> *CISO, Global Food Manufacturer*

Figure 2



Feel their current **security controls and practices are not adequate** for unmanaged and IoT devices.

Do not fully understand the risks associated with unmanaged and IoT devices

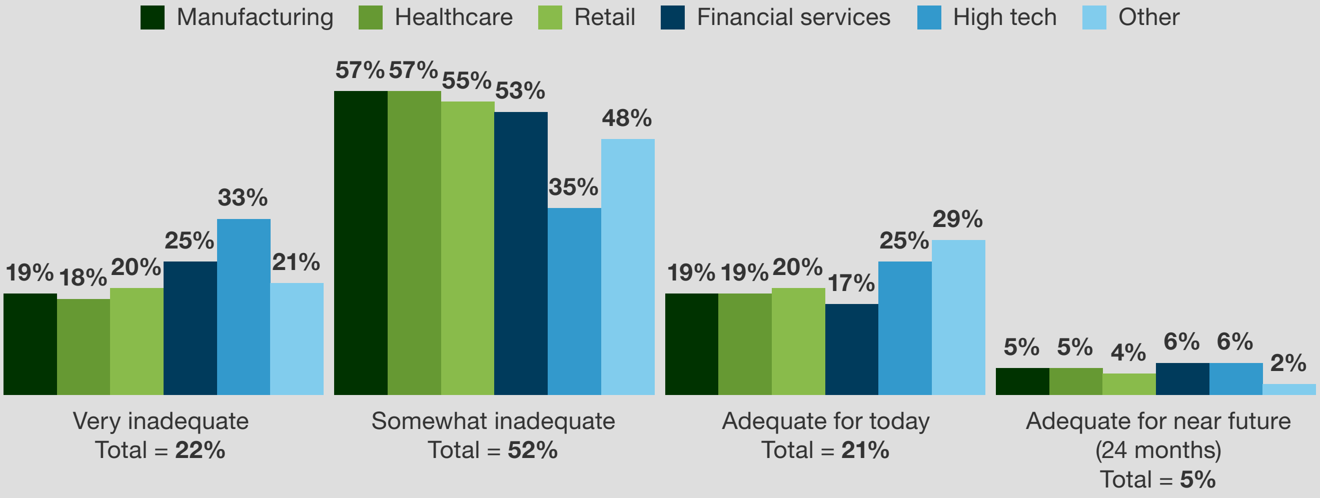
Know they need to address unmanaged and IoT security policies, but **aren't sure where to start**

Enterprise security professionals do not fully understand the extent of the security risks and how best to address them.

Base: 403 technology decision makers with responsibility over IoT security at US and Canada firms
Source: A commissioned study conducted by Forrester Consulting on behalf of Armis, July 2019

Figure 3

"How adequate do you think your current security controls and practices are for unmanaged and IoT devices?"

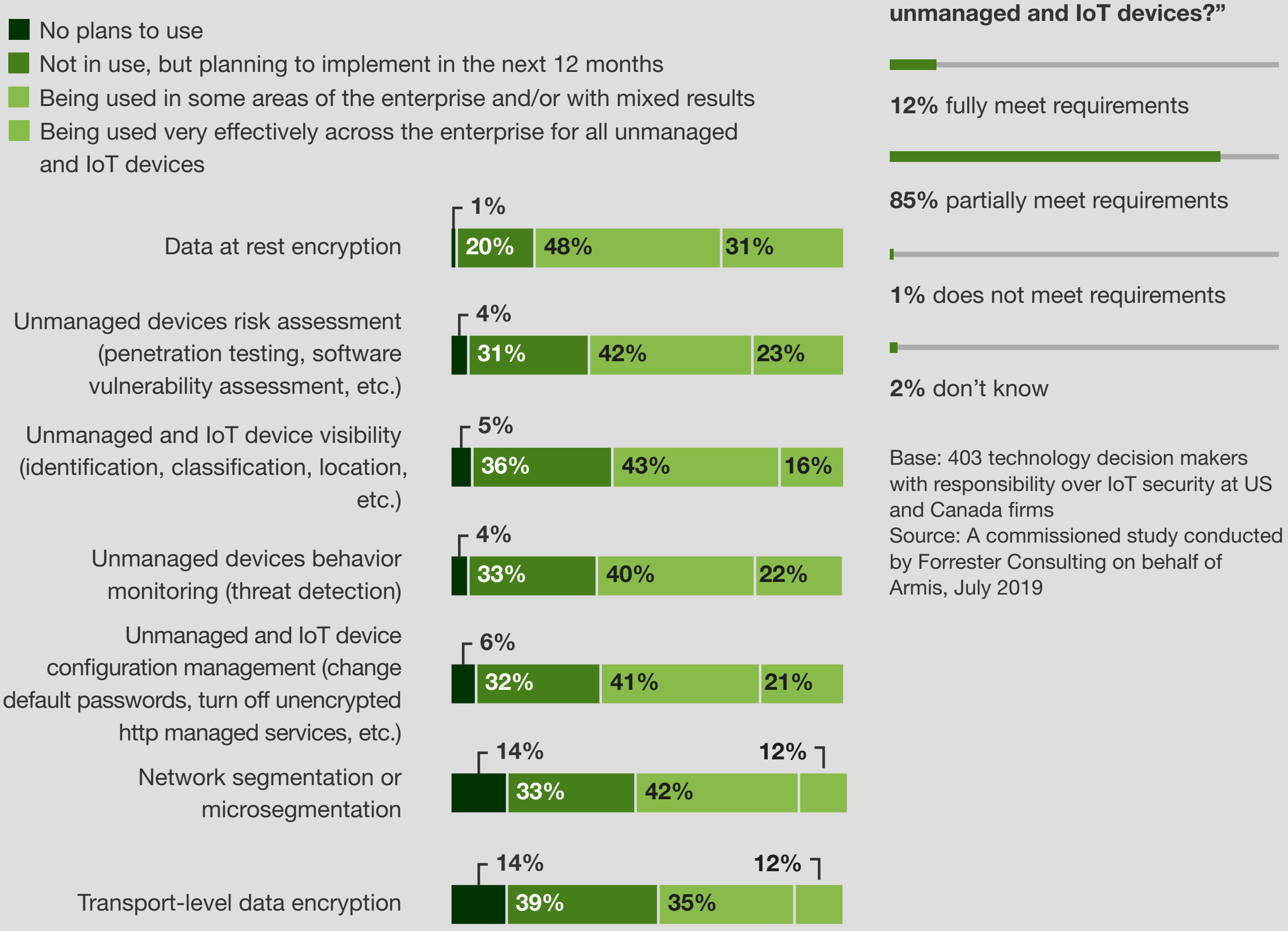


Base: 403 technology decision makers with responsibility over IoT security at US and Canada firms
Source: A commissioned study conducted by Forrester Consulting on behalf of Armis, July 2019

Figure 4

"Which of the following security controls and practices are being used for unmanaged and IoT devices throughout your enterprise, and how effective is each?"

"How well do your existing security controls meet the requirements of that security framework for unmanaged and IoT devices?"

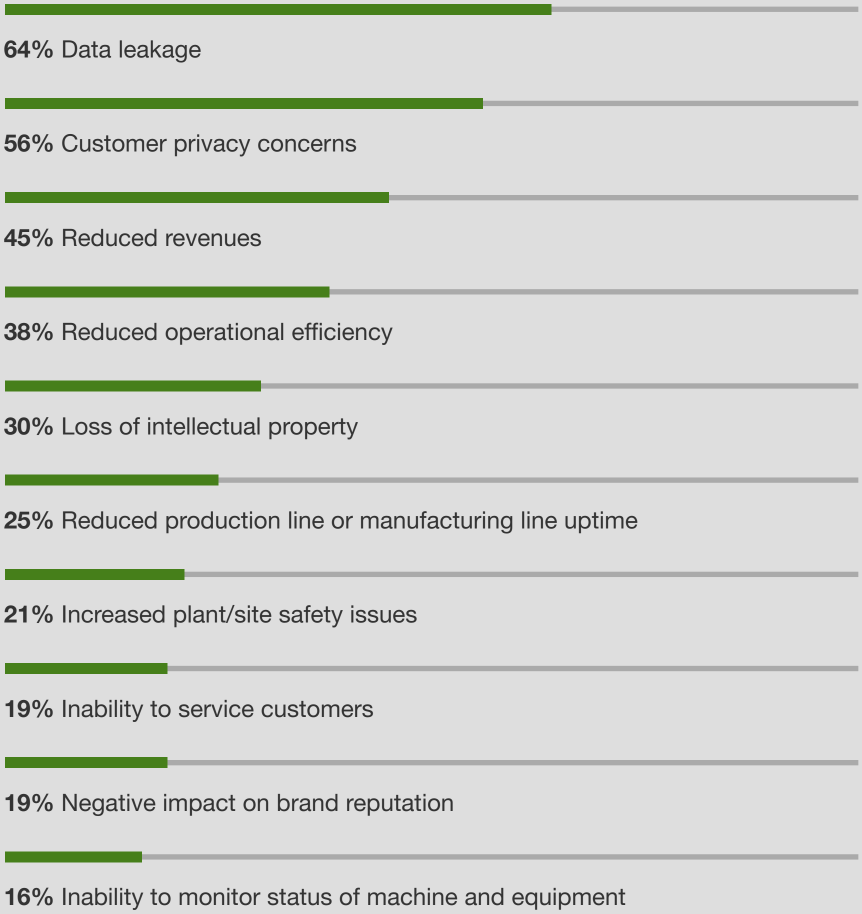


Base: 403 technology decision makers with responsibility over IoT security at US and Canada firms
Source: A commissioned study conducted by Forrester Consulting on behalf of Armis, July 2019

Base: 403 technology decision makers with responsibility over IoT security at US and Canada firms
Source: A commissioned study conducted by Forrester Consulting on behalf of Armis, July 2019

Figure 5

“What consequences has your organization experienced due to security incident(s) associated with unmanaged or IoT devices?”



Base: 403 technology decision makers with responsibility over IoT security at US and Canada firms
Source: A commissioned study conducted by Forrester Consulting on behalf of Armis, July 2019

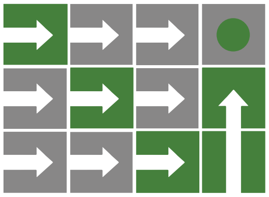
Investment In Enterprise IoT Security Solutions And Practices Is Insufficient And Need To Increase

Enterprises must be prepared to address the exposure and vulnerability related to unmanaged and IoT devices. As suggested by security frameworks from organizations such as NIST and CIS, a broad spectrum of security functions are required to properly secure unmanaged and IoT devices. In response, we found that enterprises are planning to increase spending on IoT security and to deploy a broad range of controls.

- **To respond to increasing risks, budgets dedicated to unmanaged and IoT device security must increase.** Findings from 2017 showed that about half of IoT security budgets were expected to increase in the following year globally.[10]
- **However, budgets appear to still be too low.** This will intensify as enterprise security professionals realize the extent of security exposure related to unmanaged and IoT devices is broader than they think. Ninety-three percent of them say they will increase their security spending dedicated to those devices over the next 24 months. About half of them (47%) plan to increase their spending significantly, by 10% or more.
- **In alignment with popular security frameworks, a broad spectrum of security functions will be deployed.** The top priority of large companies[11] is to direct their IoT security spending toward deploying an agentless solution (55%), since agents can't be used to monitor or protect unmanaged or IoT devices. Other companies will equally prioritize improving data classification and encryption (51%) and the deployment of agentless solutions (50%) (see Figure 6). Organizations will be looking to partner with solution providers that help them overcome their main challenges of navigating the complexity of their IT environment (52%) and being ready to respond to changing/evolving nature of internal and external IT threats (47%).

Deploying an agentless solution in the next 12 months is a top priority for half of the surveyed organizations.

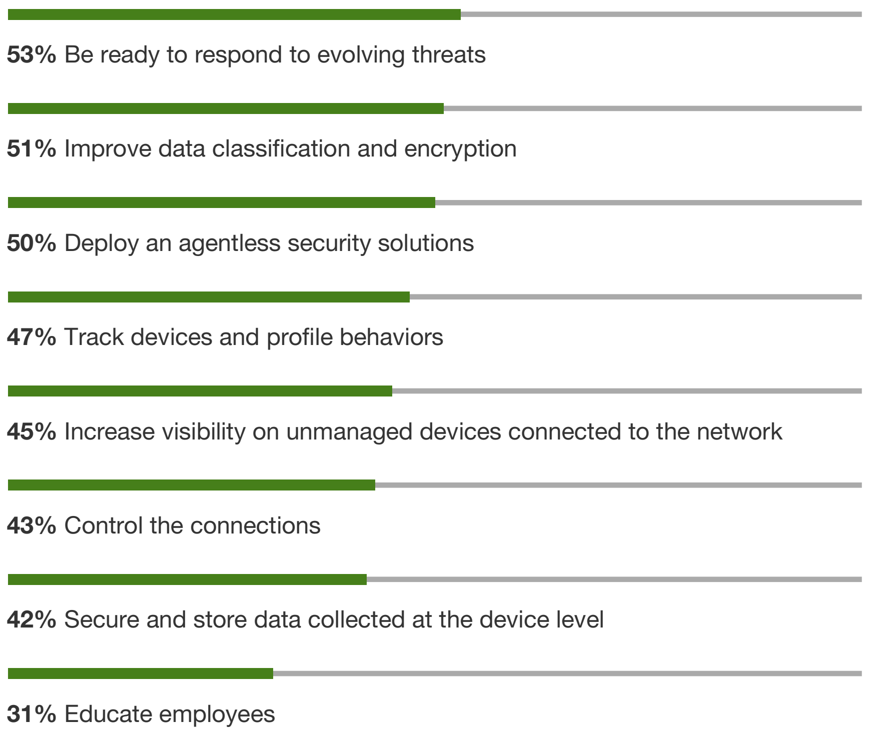
> "This isn't going to eliminate any risk or threat out there but solutions that allow us to dive into the details of a potential threat gives us confidence that we're proactive in tackling those risks ahead of time as opposed to responding reactively to what could happen to us."
>
> *Medical device security project manager, US medical group*



> "Where I would like to go is to apply behavioral analytics to the IoT devices to help determine what normal looks like. So it can also then help me determine what abnormal looks like."
>
> *CISO, US Airline*

Figure 6

“What are your organization’s top priorities when it comes to IoT security for the next 12 months?”



Base: 403 technology decision makers with responsibility over IoT security at US and Canada firms
Source: A commissioned study conducted by Forrester Consulting on behalf of Armis, July 2019

Key Recommendations

As the number of unmanaged and IoT devices in enterprise environments continues to grow, so does the importance of implementing security solutions, practices, and controls that can identify and protect these devices. While business leaders are excited about the business insights they will garner from deploying IoT devices, improper and inadequate security controls on these devices leaves organizations and customers at higher risk of data loss, physical damage, and revenue loss. Organizations need to adopt an aggressive cybersecurity posture to defend against the myriad of new threats that these new devices introduce. Without such security protections, organizations are likely to be victimized by cyberattacks.

Forrester's in-depth survey and interviews of enterprise security professionals about unmanaged and IoT devices yielded several important recommendations:

Assess and inventory your enterprise IoT devices. You cannot secure things if you don't know they exist. This demands completing an inventory of all devices connected to your network, and then using that information to build policies and implement controls to ensure devices are appropriately monitored and secured. This will minimize the risk of unintended data breaches or other related security incidents.

Prioritize device classification and protection, and use it to build the appropriate controls. Leverage the inventory of devices to understand how and where they are used, how they drive the business, what critical data they have or activities they perform, and how they may be exploited or manipulated. This will help ensure your security policies are effectively applied, and security frameworks such as NIST and CIS properly enforced for unmanaged and IoT devices.

Raise awareness on the growing IoT security risks. As an enterprise security professional, you need to demonstrate to stakeholders that unmanaged devices are more vulnerable than managed computers and at the same time not as well protected as managed computers, since they can't accommodate standard security agents and be easily patched. This will help you build the business case to secure additional budget allocation to acquire the necessary technologies and resources to properly secure unmanaged and IoT devices and mitigate risks.

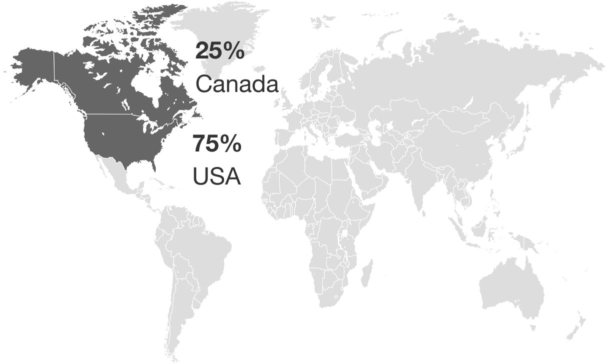
Anticipate future threats by implementing the appropriate solution(s), providing device visibility, risk assessment, threat detection, and protection specific to unmanaged and IoT devices. As you identify your needs, create a comprehensive IoT security architecture that addresses your organization's specific IoT use cases and security requirements. The challenge here is that many existing security solutions were built for traditional computers and don't work for unmanaged and IoT devices. New, purpose-built solutions are now available, and should be looked at carefully. However, ensure they address the strategic security need, deliver the appropriate security measures for the devices in question, and integrate with existing security and management tools.

Appendix A: Methodology

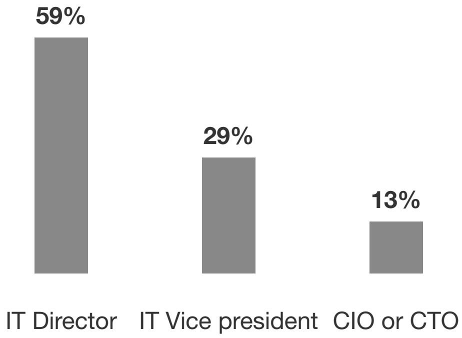
This spotlight is based on a wider Thought Leadership study that looked at the state of IoT security at North American enterprises. In the original study, Forrester conducted an online survey of 403 technology decision makers responsible for IoT security in their organizations, and three interviews with CISOs and IT project managers across various industries. Questions provided to the participants asked about their challenges and priorities, budgets and planning, and use of unmanaged and IoT devices security solutions. The study was conducted in July 2019.

Appendix B: Demographics/Data

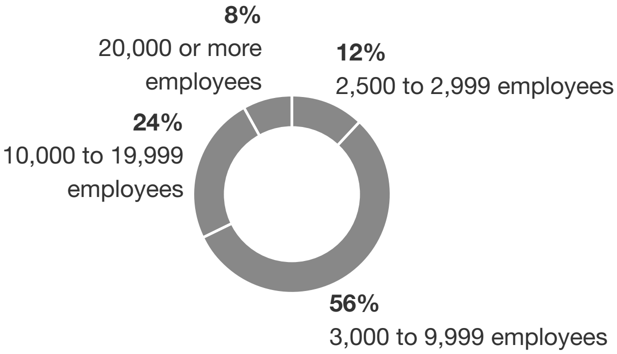
"In which country do you work?"



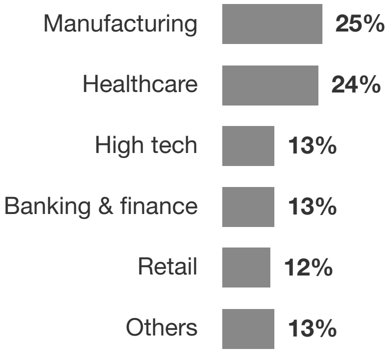
"Which title best describes your position at your organization?"



"Using your best estimate, how many employees work for your firm/organization worldwide?"



"Which of the following best describes the industry to which your company belongs?"



Base: 403 technology decision makers with responsibility over IoT security at US and Canada firms
Source: A commissioned study conducted by Forrester Consulting on behalf of Armis, July 2019

Appendix C: Supplemental Material

RELATED FORRESTER RESEARCH

"The State Of IoT Security 2018," Forrester Research, Inc., January 9, 2018.

"The Top Security Technology Trends To Watch, 2019," Forrester Research, Inc., August 1, 2019.

"Best Practices: Securing IoT Deployments", Forrester Research Inc., October 11, 2017.

"Protecting Industrial Control Systems And Critical Infrastructure From Attack," Forrester Research, Inc., April 19, 2018.

"Best Practices: Medical Device Security", Forrester Research, Inc., May 21, 2019.

Appendix D: Endnotes

[1] Source: "Internet of Things forecast," Ericsson, (https://www.ericsson.com/en/mobility-report/internet-of-things-forecast).

[2] Source: Ibid.

[3] Source: "The State Of IoT Security 2018," Forrester Research Inc., January 9, 2018.

[4] Source: Ibid. Base: 1,802 global telecommunications decision makers at firms with 1,000+ employees.

[5] Source: John E Dunn, "Pacemaker controllers still vulnerable 18 months after flaws reported," Naked Security by Sophos, August 14, 2018 (https://nakedsecurity.sophos.com/2018/08/14/pacemaker-controllers-still-vulnerable-18-months-after-flaws-reported/).

[6] Source: Andy Greenberg, "A Guide to LockerGoga, the Ransomware Crippling Industrial Firms," Wired, March 25, 2019 (https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms/).

[7] Source: Scott Pelley, "How cybercriminals hold data hostage... and why the best solution is often paying a ransom," 60 Minutes, May 5, 2019 (https://www.cbsnews.com/news/ransomware-how-cybercriminals-hold-data-hostage-and-why-the-best-solution-is-often-paying-a-ransom-60-minutes-2019-05-05/?ftag=CNM-00-10aab7d&linkId=66981137).

[8] Source: "Cyber Actors Use Internet Of Things Devices As Proxies For Anonymity And Pursuit Of Malicious Cyber Activities," Federal Bureau of Investigation Public Service Announcement, August 2, 2018 (https://www.ic3.gov/media/2018/180802.aspx).

[9] Source: Zak Doffman, "Microsoft Warns Russian Hackers Can Breach Secure Networks Through Simple IoT Devices," Forbes, August 5, 2019 (https://www.forbes.com/sites/zakdoffman/2019/08/05/microsoft-warns-russian-hackers-can-breach-companies-through-millions-of-simple-iot-devices/?ss=cybersecurity#7c81bc93617f).

[10] Source: "The State Of IoT Security 2018," Forrester Research, Inc., January 9, 2018.

[11] Large companies refers to companies with 20,000 or more employees.