Starfleet RESEARCH

paloalto NETWORKS

The 2024 Benchmark Report on

IoT Security

How top-performing organizations use advanced Internet of Things (IoT) security to safeguard their network-connected devices

According to Best Practices IT Market Research

Table of Contents

Introduction
Overview of IoT Security

Today, billions of Internet of Things (IoT) devices are not just connecting us but revolutionizing the way businesses, government entities, and other organizations operate, from slashing costs to sparking innovation. The global number of connected IoT devices is expected to surpass 29 billion by 2027, a big jump from the estimated 16.7 billion devices today. Global spending on IoT technologies is expected to rise from $280 billion this year to $721 billion by 2030. From optimizing supply chains to enabling predictive maintenance, IoT is rapidly becoming a cornerstone of modern business strategy and operational success.

The following are brief descriptions of how just a few different business sectors are utilizing these IoT technologies:

Hospitality

In the hospitality sector, IoT devices have elevated the guest experience through personalized services, such as mobile-controlled environments and AI-driven interactions. The convergence of IoT with big data analytics has enabled hotels to optimize energy consumption and operational workflows, crafting a sustainable and responsive guest experience.

With the rapid proliferation of IoT devices comes an ever-growing challenge for businesses of all types and sizes: security.

Hotels, resorts and other lodging properties are increasingly implementing a variety of IoT devices to enhance the quality of the guest experience. Examples include sensor-based lighting that automatically adjusts to the time of day and guests' needs, as well as energy management systems designed to reduce energy consumption. Additionally, many hotels now employ smart locks that enable guests to use their phones as room keys. The adoption of AI-powered chatbots and even robots for food delivery and other services is also on the rise, providing more efficient and personalized guest experiences while allowing staff members to focus on other tasks. IoT technology is further being utilized to bolster safety and security within hotels. For instance, some establishments employ facial recognition software to identify potential threats. Moreover, IoT devices are used to monitor housekeeping and maintenance tasks, ensuring that rooms are both clean and well-maintained.

Restaurants are increasingly using IoT devices to enhance efficiency and customer service. These devices include connected thermostats, point-of-sale (POS) systems, and customer Wi-Fi hotspots. By connecting these devices to the internet, restaurants can remotely monitor and manage them, as well as gather data to refine operations. For instance, POS systems can deliver real-time sales

data, while customer Wi-Fi hotspots can track customer behavior and preferences. Many IoT devices can also be integrated with mobile apps, further augmenting their utility. Additionally, more restaurants are adopting robots to perform tasks such as cooking, cleaning, and delivering orders.

Retail

IoT devices are also transforming the retail industry by connecting devices and data, enabling retailers to create a more efficient and personalized shopping experience for their customers. In-store IoT applications include beacons, interactive displays, and connected fitting rooms. Beacons, small battery-powered devices that use Bluetooth Low Energy (BLE), send signals to nearby smartphones, allowing retailers to send targeted, location-based messages to shoppers, such as special offers or product recommendations. Interactive displays are another way retailers use IoT to enhance the in-store experience, providing product information, facilitating order placement, and enabling payments.

Hotels, resorts and other lodging properties are increasingly implementing a variety of IoT devices to enhance the quality of the guest experience.

Connected fitting rooms are becoming increasingly popular as well. These rooms use sensors to track which clothing items have been tried on, allowing store associates to quickly retrieve them for customers. Additionally, digital loyalty cards enable retailers to track customer purchase histories and tailor rewards based on individual shopper behavior, further personalizing the shopping experience.

Outside the store, retailers are employing IoT applications such as connected packaging and digital loyalty cards to provide a more seamless shopping experience. Connected packaging, which uses sensors and RFID tags, tracks products throughout the supply chain—from production to the retail shelf—ensuring timely delivery and meeting quality standards. By leveraging the power of IoT, retailers are able to offer a more convenient and personalized shopping experience for their customers.

Financial Services

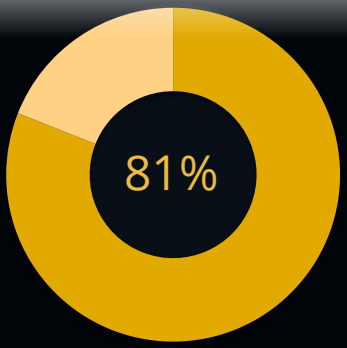
The use of IoT devices in the financial services industry has been gaining increased momentum. One of the most popular applications for IoT devices in this sector is fraud detection. By installing sensors in ATMs, banks can quickly identify when machines have been tampered with and take steps to prevent fraudulent withdrawals. Additionally, credit card companies are using IoT devices to monitor customer spending patterns and detect potential fraudulent activity.

IoT-powered payment devices can be categorized into two broad groups: those that facilitate payments (mobile phones, smartwatches, and contactless cards) and those that accept payments (point-of-sale terminals and appliances). Some banks are now utilizing chatbots to answer customer inquiries and provide account information. These devices are capable of handling a wide range of tasks, from providing account balances to transferring funds between accounts. Furthermore, beacons—small Bluetooth-based transmitters that connect with nearby smart devices—have enabled branches to personalize their customer services and obtain instant feedback from clients. When a customer enters a branch, banks can tailor their service approach based on the customer's profile and needs.

IoT-powered payment devices can be categorized into two broad groups: those that facilitate payments and those that accept payments.

Government

IoT enables government agencies to collect data and insights, enhancing the efficiency of their operations and services. For instance, the U.S. Department of Transportation utilizes IoT devices to monitor traffic patterns and identify congestion hotspots. Streetlights equipped with IoT technology can monitor air quality and the presence of pedestrians and cyclists, aiding decisions related to pollution control and traffic safety. Additionally, IoT-enabled trash cans can notify sanitation workers when they need emptying, and intelligent water meters can detect leaks, helping utilities optimize resource usage. The Department of Homeland Security employs IoT security cameras and sensors to detect illegal border crossings. Furthermore, IoT devices are used for various security purposes, such as detecting unauthorized intrusions or facilitating communication with first responders in emergencies.



Percentage of security leaders (and other qualified respondents) who say that their organizations have experienced an IoT-focused attack within the past year

Source: Starfleet Research; research findings are derived from the Q1 2024 survey on IoT Security

Healthcare

In the healthcare sector, the global IoT market is expected to reach $188 billion by 2028, more than quadrupling its value compared to 2020. The rapid proliferation of Internet of Medical Things (IoMT) technology is transformative, affecting medical professionals and patients alike. IoT devices such as ultrasounds, thermometers, glucose monitors, and electrocardiograms are increasingly becoming connected, enabling patients to monitor their health more effectively. Wearables and implantable devices now offer real-time health status updates, crucial for managing chronic conditions and preemptive healthcare measures.

Hospitals are using a variety of IoT devices to improve patient care, streamline operations, and reduce costs. These include wearable devices that can be worn on the body or even implanted underneath the skin, allow doctors to monitor patients' vital signs in real-time. This information can then be used to diagnose and treat conditions more quickly and effectively. These also include medical devices, such as pacemakers and blood pressure monitors, and hospital equipment, such as MRI machines and X-ray machines. By collecting data from these devices, hospitals can gain insights into patient health, hospital workflow, and much more.

IoT enables government agencies to collect data and insights, enhancing the efficiency of their operations and services.

Manufacturing

In manufacturing, IoT devices enhance traceability and operational efficiency and effectiveness. In fact, the integration of IoT technology in manufacturing has led to a 20% increase in Overall Equipment Effectiveness (OEE), according to a 2024 Siemens report, demonstrating the operational advantages of IoT in industrial settings. Innovations in sensor technology and machine learning have led to predictive maintenance capabilities, minimizing downtime. The integration of IoT with robotics has further streamlined production lines, reinforcing the symbiosis between human and machine intelligence. By connecting devices and machines to the internet, manufacturers can collect data and gain insights that can improve efficiency and quality. Some common IoT devices used in manufacturing include:

- **RFID tags:** RFID tags are often used to track inventory. They can be attached to products or pallets, and they transmit data that can be used to track the location of the tagged item.
- **IoT sensors:** Sensors can be used to monitor conditions in the factory, such as temperature, humidity, and machine vibration. This data can be used to improve operating conditions and identify potential problems.

- **IoT cameras:** Cameras can be used for quality control or security purposes. For example, they can be used to check for defects in products or to deter and detect theft.
- **IoT controllers:** Controllers are used to automate processes in the factory. For example, they can be used to operate conveyor belts or robotic arms. By using controllers, manufacturers can reduce human error and improve efficiency.

A Double-Edged Sword

While the benefits of an increasing number of businesses, government entities, and other organizations embracing IoT technology are abundantly clear, so too is the heightened potential for attacks. This exposes a growing battlefield of security challenges for organizations of all types and sizes. As headlines regularly remind us, an IoT security breach typically involves more than just data loss. It often leads to substantial financial damage, reputational harm, and operational disruptions.

In manufacturing, IoT devices enhance traceability and operational efficiency and effectiveness.

Exploits targeting vulnerabilities in IoT devices can be used to gain access to sensitive data, launch denial-of-service attacks, or take complete control of the devices. Additionally, IoT devices are susceptible to IoT worms, which can rapidly spread across networks of connected devices, disrupting critical business functions and causing serious damage. For many organizations, the sheer number of IoT devices now connected to their networks presents a vast attack surface for malicious actors to exploit.

According to a 2024 study by Forrester, 34% of companies that experienced a breach targeting IoT devices were more likely to report cumulative breach costs between $5 million and $10 million, compared to those that experienced cyberattacks on non-IoT devices. Today, more than ever, companies, government entities, and nonprofit organizations alike need to adopt advanced IoT security practices and cutting-edge technologies to protect against evolving threats.

Standard cybersecurity measures are woefully inadequate in preventing hackers and criminals from accessing IoT devices. The next chapter will explore the need for purpose-built IoT security solutions that can effectively protect businesses, governments, organizations, and individuals from these ever-growing threats.

Chapter 1

Exploring the Need for IoT Security

In the race to connect everything, IoT devices often cross the finish line with vulnerabilities in tow, thanks to designs that prioritize speed over security. These devices remain some of the most vulnerable endpoints due to their design, which prioritizes low latencies for real-time data capture. Historically, integration has been considered more important than security in the design of IoT products, making them challenging to defend.

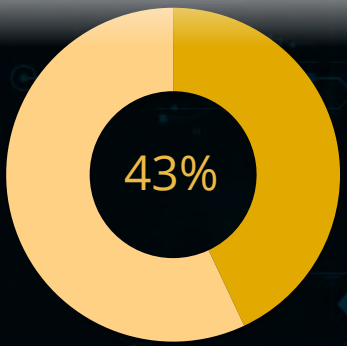
In fact, most IT leaders regard IoT as the most vulnerable component of their security frameworks. This vulnerability arises because many organizations rely solely on IP scanning or API-based integrations for asset inventory, methods that do not support real-time tracking of IoT devices on their networks. Although many IoT devices are equipped with basic security features to guard against potential threats, these measures are typically insufficient to withstand sophisticated cyberattacks. As a result, the vulnerabilities in IoT devices can become entry points for malicious actors to infiltrate enterprise networks, leading to potentially far-reaching and severe consequences.

Historically, integration has been considered more important than security in the design of IoT products.

Examples of IoT Security Failures

There is no shortage of reported incidents illustrating the Pandora's box of security challenges that continually catch businesses off guard. The following examples highlight just a few of the security failures that have made headlines in recent years due to common vulnerabilities in IoT devices:

- In 2021, it was revealed that many popular fitness trackers were vulnerable to hacking due to weak security protocols, allowing hackers to access personal data such as heart rate, location, and sleep patterns.
- In 2022, a ransomware attack against a healthcare system in the UK resulted in the release of confidential patient data. The attackers used a variant of the



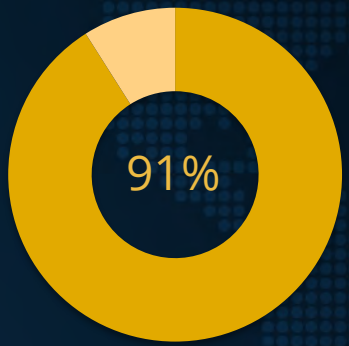
Percentage of security leaders (and other qualified respondents) who view stolen or compromised data as their “top concern” with potential IoT attacks

Source: Starfleet Research; research findings are derived from the Q1 2024 survey on IoT Security

- That same year, a Mirai malware-infected IoT botnet was used in an attempted DDoS attack against several banks in the United States.
- Earlier in the year, attackers using a Mirai botnet had taken down much of the internet in the US by targeting routers and other internet-connected devices.
- Also in 2022, a ransomware attack on a major educational institution led to the breach of sensitive research data. The attackers exploited vulnerabilities in the institution's IoT-connected heating and cooling system to infiltrate the network.
- Additionally, a series of espionage and eavesdropping cases involving IoT devices in corporate boardrooms were reported, where unsecured video conferencing systems were manipulated to gain unauthorized access to confidential meetings.
- In 2023, a popular home IoT device designed for energy management was compromised, leading to widespread access to consumers' usage data and potential manipulation of household energy consumption.
- Also in 2023, an IoT attack involving a botnet of home appliances caused a significant distributed denial of service (DDoS) attack on a national telecommunication provider's network, disrupting services for millions of users.

The manufacturers of IoT devices have not always done everything possible to safeguard them.

These examples underscore the vulnerabilities of IoT devices. Research conducted for this benchmark report reveals that 43% of security leaders, along with other qualified survey respondents, rank stolen or compromised customer or other data as their primary concern in relation to IoT attacks. This is followed by reputational damage at 31%, stolen intellectual property at 17%, and operational downtime at 14%. For healthcare organizations, patient safety is also



Percentage of security leaders (and other qualified respondents) who say that manufacturers do a "poor " or "very poor“ job of securing their IoT devices from attacks

Source: Starfleet Research; research findings are derived from the Q1 2024 survey on IoT Security

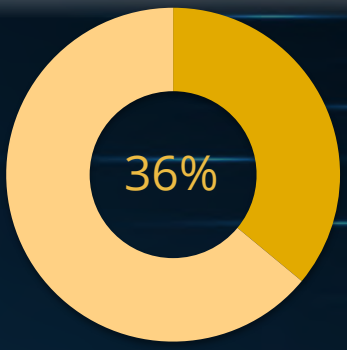
a top concern, especially in scenarios where a malicious actor could gain unauthorized network access via a medical or other IoT device.

Manufacturers of IoT devices have not always taken all possible measures to safeguard them. Two key concepts to consider in this context are "privacy by design" and "security by design." Privacy by design means that privacy considerations are integrated into the design of IoT devices from the outset. Similarly, security by design involves incorporating security features into the design of IoT devices from the beginning. These approaches often fail for various reasons. First, IoT devices are frequently designed with convenience in mind, which can sometimes compromise security. For instance, many devices come with default passwords that are easy to guess or transmit data without encryption. Second, IoT devices are often updated remotely, creating vulnerabilities if the update process is not properly secured.

IoT devices are frequently designed with convenience in mind, which can sometimes compromise security.

Simply put, IoT devices are often shipped with vulnerabilities, run unsupported operating systems, are difficult to patch, and lack encryption in communication. These devices are susceptible to medium or high severity attacks. According to research conducted for this benchmark report, almost half (46%) of survey respondents indicate that their organizations are "still struggling to gain IoT device visibility" on their networks.

In response to these IoT security concerns, governments in the United States, Europe and elsewhere have passed a series of mandates and laws, including the Internet of Things Cybersecurity Improvement Act in the US and the EU Cybersecurity Act. These laws require that manufacturers of IoT devices take measures to help to protect against malicious attacks and data breaches.



Percentage of security leaders (and other qualified respondents) who say that their organizations plan to upgrade their IoT security measures within the next year

Source: Starfleet Research; research findings are derived from the Q1 2024 survey on IoT Security

One notable development took place in April 2024, when the UK became the first country to legally mandate cybersecurity standards for IoT devices. The new regulations are designed to protect consumers from cyber threats and enhance the nation's defense against escalating cyber-crime. Under the Product Security and Telecommunications Infrastructure (PSTI) regime, it is now a legal requirement for manufacturers to incorporate security protections into any product that connects to the internet.

And while the enactment of regulatory laws designed to safeguard IoT devices is imperative, it hardly suffices. To effectively protect their data and systems from potential attacks, business, government agencies and other organizations must also implement IoT security technology and adopt best practices for securing connected IoT devices on their networks. They need to actively monitor their networks for suspicious activity and install security patches as soon as they become available.

In a Zero Trust system, all devices and users must be verified and authenticated before they are granted access to resources.

A key concept that comes into play is the so-called *Zero Trust security model.* The model is based on the premise that no devices or users should be automatically trusted, regardless of whether they are inside or outside of a network. In a Zero Trust system, all devices and users must be verified and authenticated before they are granted access to resources. This verification process can happen through a variety of methods, such as two-factor authentication or biometric identification. Only then can businesses, government agencies and other organizations have confidence that their data and assets are safe from the constantly evolving threat landscape, no matter what IoT devices are connected to their network.

Unfortunately, most existing IoT security solutions lack any inbuilt prevention or enforcement, employ dated signature-based discovery methods focused on known devices, and have slow and complex deployments relying on integrations to provide any form of security. Hence the need for an advanced and comprehensive solution that can deliver real-time visibility, control and protection. The reality of the situation, however, is that most technology solution providers fail to come even close to offering this level of security, given the scope and limitations of their platform capabilities and the inherent challenges posed by IoT devices. Exploring the nature of these challenges is the focus of the next chapter.

Chapter 2

Understanding the Challenges of IoT Security

As cyber adversaries harness AI to craft stealthier malware and more devastating botnets, the slew of challenges related to IoT security have grown increasingly complex. These botnets are specifically engineered to hijack personal IoT devices and broaden the scope of distributed attacks. The healthcare and manufacturing sectors are particularly at risk, grappling with the rapid proliferation of new IoT devices that compound the vulnerabilities of existing ones.

Given these escalating threats, IoT security has surged to the forefront of priorities for businesses, government agencies, and other organizations. In fact, research conducted for this benchmark report reveals that 91% of qualified respondents now rank the implementation of new or upgraded IoT security measures among their top three business initiatives for the next 12 months, compared to 80% last year.

It is important to understand the myriad challenges associated with protecting IoT devices against hackers.

However, before taking action, it is important to understand the myriad challenges involved in protecting IoT devices from hackers. This knowledge will guide the development of the necessary technology capabilities to prevent unauthorized access and safeguard data, which may be dispersed across multiple devices and various network locations.

The following are brief descriptions of some of the biggest challenges:

- **Complexity:** As IoT device types, uses, and numbers grow, so does the complexity of managing them all. Organizations must now manage a variety of different types of IoT devices, from different manufacturers, running different operating systems (some of which may be proprietary), with disparate management tools. Closing the numerous security gaps between IoT sensors, systems, and legacy infrastructure is becoming increasingly challenging. Complexity creates operational challenges and increases the chances that something will be missed, leading to increased risk.
- **Lack of visibility:** With numerous devices constantly linking to the corporate network, blind spots and gaps in visibility pose serious security vulnerabilities. Without comprehensive network visibility, businesses maybe be unaware of all the connected devices or the activities they are engaged in. Monitoring devices on a network continuously is the only way to detect attacks or suspicious activity. The absence of visibility can become a security nightmare for businesses, given that hackers can effortlessly exploit unmonitored devices to gather sensitive data or launch attacks on other systems.

- **Varied security levels:** IoT devices often have different levels of security, which can make it difficult to ensure that all devices are properly protected. For example, a consumer device might have basic security features, while an industrial machine might have more robust security measures in place.
- **Inadequate protections:** Many IoT devices have inadequate security features, leaving them open to attack. Hackers can exploit these vulnerabilities to gain access to sensitive data, disable critical infrastructure, or even take control of the devices themselves.
- **Poorly designed networks:** The way in which IoT devices are interconnected can create security vulnerabilities. Poorly designed networks can create "islands" of devices that can be used by attackers to launch attacks on other parts of the network.
- **Unencrypted data:** In many cases, data collected by IoT devices is not encrypted, making it easier for attackers to access and use it. There are a few reasons why data might not be encrypted. In some cases, encryption adds complexity and cost to the device. In other cases, the device may not have the necessary processing power to encrypt the data.
- **Lack of standards:** There are no universally accepted standards for IoT security, making it difficult for many organizations to know what specific measures they should be taking to protect their devices.
- **Regulation:** In some industries, such as healthcare and financial services, there are now specific regulations around the use of IoT devices. These regulations add another layer of complexity and can create additional challenges around compliance. In some cases, the regulations may conflict with each other, adding yet another level of complexity.
- **Insufficient resources:** Implementing effective IoT security measures requires significant time and financial resources, including costs related to IT staffing and technology deployment. which may present a challenge for smaller organizations as well as highly decentralized organizations.
- **Limited understanding:** Even today, there tends to be a lack of understanding among some organizations about the risks posed by IoT devices and how to effectively mitigate them.

Closing the numerous security gaps between IoT sensors, systems, and legacy infrastructure is becoming increasingly challenging.

Taken together, these challenges explain why so many businesses, government entities, and other organizations remain vulnerable to attacks via IoT devices. They also underscore the urgent need for implementing advanced IoT security measures. The specific measures that organizations should take to address these challenges will be the focus of the next chapter.

Chapter 3

Implementing the Right IoT Security Measures

When it comes to the dollars and cents of IoT security, the numbers speak louder than words. Discussions about implementing new IoT security measures, or upgrading existing ones, invariably begin with an examination of return on investment. So, what is the ROI on IoT security? A recent study by Gartner revealed that the average return on investment for enterprises implementing IoT security exceeded 30%. Conversely, those who neglected to invest in IoT security experienced an average negative return of -5.6%.

Undoubtedly, a data breach can lead to catastrophic financial damage and harm to reputation. In 2023, the average cost of a data breach was estimated at $9.5 million. The healthcare industry bore the brunt, with the highest average cost of a data breach at $11 million. These costs can escalate further if the breach results in the loss of customer data or sensitive information.

To say that the business case for investing in IoT security is compelling, particularly for organizations dealing with sensitive data or subject to stringent compliance regulations, is an understatement. For instance, many security threats in healthcare organizations involve imaging devices, which are integral to the clinical workflow. These devices, connected to hospital networks, are often inadequately protected. Hackers gaining access can potentially disrupt the quality of care, causing harm to patients. They could also extract patient data, leading to privacy breaches.

To say that the business case for investing in IoT security is compelling is an under-statement.

By now, most healthcare organizations, regardless of size, have recognized the risks posed by these devices and have taken steps to protect their networks, such as implementing authentication measures and encrypting data in transit. However, these measures are merely the beginning. IoT security also necessitates the deployment of purpose-built technology capabilities.

Regrettably, most cybersecurity solutions available today do not adequately address the unique risks posed by IoT devices. For instance, endpoint protection platforms, designed to safeguard traditional computing devices, are generally ineffective against IoT devices due to a lack of visibility. Similarly, solutions enabling network segmentation and firewall policy can be ineffective against IoT threats, as many attacks involve lateral movement within a network.

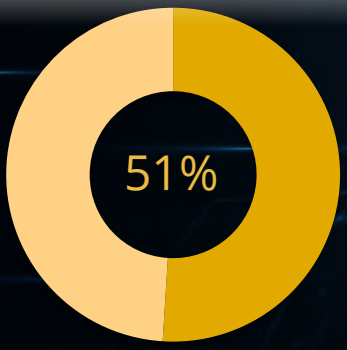
While some solutions can provide accurate device visibility, most fail to identify new, unknown devices, creating blind spots that leave organizations vulnerable

to attack. Even those cybersecurity solutions marketed as IoT security solutions often lack native enforcement capabilities and require users to manually create security policies, which prolongs the time to value. These solutions may also fall short in adopting Zero Trust principles and integrating with existing systems. Without the capability to see and contextualize IoT devices on a network, protecting them adequately becomes nearly impossible. In contrast, a state-of-the-art solution is designed to offer visibility into all IoT devices on the network, automatically assess risks, and provide robust protection against both known and unknown threats.

Unknown IoT security threats are those that have not been previously identified and are challenging to anticipate or guard against. Conversely, known IoT security threats are those that have been recognized and for which protective measures are established. As expected, unknown threats are often more challenging to defend against because they exploit vulnerabilities that have not yet been identified. For instance, a hacker might develop a malicious software program intended to infect devices and spread malware through a previously unknown security flaw. Once the vulnerability is identified, it can be patched, but until that point, devices and data remain at risk. This type of threat, known as a zero-day threat, exploits these previously unknown vulnerabilities.

Unknown threats are often more challenging to defend against because they exploit vulnerabilities that have not yet been identified.

Only by recognizing the limitations of existing cybersecurity solutions in the context of IoT vulnerabilities, and by committing to enhance visibility into all devices on a network, can organizations advance in implementing serious IoT security measures. Such measures must focus on deploying a purpose-built solution that provides comprehensive visibility, surfaces unmanaged device data across the network, conducts device risk analysis, and enables the enforcement of recommended device risk-based policies.



Percentage of security leaders (and other qualified respondents) who view their existing technologies as “inadequate” for securing IoT devices on their networks

Source: Starfleet Research; research findings are derived from the Q1 2024 survey on IoT Security

device data across the network, providing device risk analysis, and enabling the enforcement of recommended device risk-based policies.

The following are some of the key features and functionality that should be enabled by such a solution:

- **Discover IoT devices in, say, the first 48 hours.** The solution should expand visibility to all IoT devices, even those never seen before on the network.
- **Enable one-click compliance assessment.** The solution should be able to score and track risk based on vulnerability information, anomalous device behavior, vendor advisories, crowdsourced device data and more.
- **Lock all evasions.** The solution should prevent 100% of all known, unknown, and zero-day threats for all IoT devices on a network.
- **Facilitate Zero Trust adoption.** The solution should provide prescriptive least-privileged access policy recommendations and one-click enforcement.
- **Integrate with top IT and security technologies.** The solution should enhance existing technologies with playbook-driven native integrations.

A purpose-built solution provides comprehensive visibility, surfaces unmanaged device data across the network, and conducts device risk analysis.

By implementing a solution with these features and functionality, organizations can minimize the risks posed by internet-connected devices, ensuring that they continue to reap the benefits of these devices while keeping their networks as safe as possible. Unfortunately, according to research conducted for this benchmark report, more than half (51%) of security leaders (and other qualified survey respondents) view their existing technologies as “inadequate” for securing IoT devices on their networks. It is no wonder, then, that more than one-third (36%) of respondents also say that their organizations plan to upgrade their IoT security measures within the next year.

The next chapter will focus on a large regional healthcare organization that has already undertaken such an upgrade, yielding impressive results by any measure.

Chapter 4
Success Story

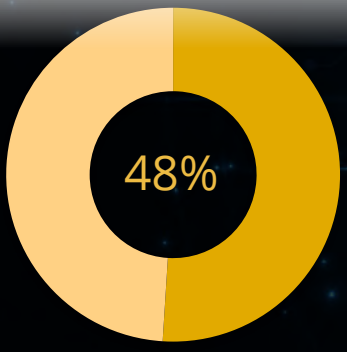
WAUBONSEE
COMMUNITY COLLEGE

For over 50 years, Waubonsee Community College has been a leading provider of high-quality academic programs, equipping lifelong learners with the skills necessary to succeed in an ever-changing economy. With a commitment to offering cutting-edge resources and fostering exploration across a wide range of subject areas, Waubonsee serves over 30,000 students through its four campuses in Illinois and robust online community. However, the college faced significant security risks due to its open, digitally enabled campuses, where hundreds of IoT devices, including smart TVs, security cameras, and credit card machines, must be protected. Inadequate security measures not only put students' educational, employment, health, and financial records at risk but also compromise their personal safety.

As the Information Security Manager at Waubonsee, Tarun Trivedi is responsible for ensuring a streamlined and secure educational experience for students across the entire Waubonsee system. However, as the sole member of the department at the time, Trivedi faced the daunting task of securing the entire Waubonsee network and all its devices without deep visibility into their communication and risk levels.

Trivedi sought a platform that would provide clear visibility and risk assessment for every device.

"We encountered numerous unknowns," Trivedi explains. "I had no way of knowing where these devices were communicating." During regular check-in meetings with the college's CIO, Trivedi realized that he couldn't provide a comprehensive report on each device's risk status or an overall assessment of network security. Recognizing the need for a robust solution to monitor and manage Waubonsee's IoT security risks, Trivedi sought a platform that would provide clear visibility and risk assessment for every device, seamless implementation, an intuitive user interface, and reliable customer support. Additionally, he aimed to find a solution that would not impact the existing system or require modifications to hardware or software.



Percentage of security leaders (and other qualified respondents) who view the "complexity of [their] IoT ecosystem" as the biggest challenge in protecting against potential threats

Trivedi and his network team had specific requirements in mind for their IoT security solution:

- Complete visibility into the entire IoT network, including the categorization of approximately 1,000 devices and their risk levels.
- Phased implementation that seamlessly integrates with existing systems without disruption or modification.
- Real-time monitoring capabilities to ensure device protection while enabling collaborative student engagement.

To address the challenges faced by Waubonsee, Trivedi implemented an IoT security solution that specifically focuses on the unique threats posed by IoT devices. Traditional cybersecurity tools often fail to detect the malicious activities that target IoT devices, making a dedicated IoT security solution essential. The chosen solution provides full visibility into all network-connected IoT devices, enabling effective identification and countermeasures against IoT-focused threats. It leverages machine learning to detect vulnerabilities and suspicious activities, ensuring comprehensive protection. The solution operates continuously, providing automated Zero Trust security and integrated workflows. It also utilizes edge computing to reduce latency and improve real-time analysis.

The solution provides full visibility into all network-connected IoT devices, enabling effective identification and counter-measures against IoT-focused threats.

With the implemented IoT security solution, Trivedi now has full visibility into the types of devices present on Waubonsee's network. He can monitor all traffic originating from these devices, ensuring comprehensive security. The solution revealed that the network consists of approximately 1,000 devices, categorized into 40 different types, including five varieties of security cameras.

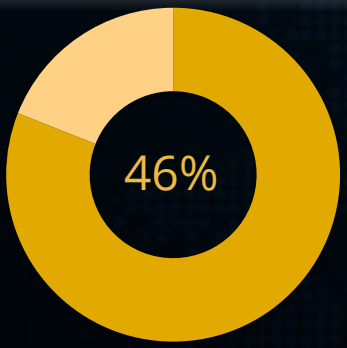
The IoT security solution employs machine learning and three-tier profiling technology to create a unique profile for each device. This enables Trivedi and his team to receive alerts whenever a device deviates from its normal behavior.

Shortly after deployment, the solution detected that a printer was communicating with its manufacturer to receive software updates, violating Waubonsee's security policy. Trivedi was promptly alerted to this high-risk behavior, allowing his team to adjust the printer's settings and mitigate the risk of a breach. He can now provide comprehensive status reports to the CIO, showcasing a detailed list of all devices at Waubonsee and their respective risk levels. The visibility provided by the IoT security solution clarifies any previously unknown risks, ensuring Trivedi has an accurate understanding of the college's entire IoT security posture.

As an educational institution handling sensitive user data, Waubonsee must adhere to strict security standards. Vulnerabilities in IoT devices, such as smart building devices, cameras, payment machines, and computers, can expose critical student data to hackers. However, strong security measures should not hinder open and collaborative learning. To support students pursuing programming careers in game development, Trivedi's team assisted gaming clubs on campus in creating their own secure file networks. The implemented IoT security solution allows Trivedi to monitor student devices without disrupting their academic or recreational activities. He emphasizes the importance of addressing risks from all perspectives, not just one dimension. As technology continues to advance, maintaining visibility and control over multidimensional IoT security risks becomes increasingly critical.

Waubonsee has greatly enhanced its ability to protect sensitive data while fostering an open and collaborative learning environment.

By implementing a robust IoT security solution, Waubonsee Community College has greatly enhanced its ability to protect sensitive data while fostering an open and collaborative learning environment. The solution's comprehensive visibility and control over IoT devices enable the college to navigate the complexities of modern educational technology with confidence, ensuring the safety and success of its students and faculty.



Percentage of security leaders (and other qualified respondents) who say that their organizations are still “struggling” to gain IoT device visibility”

Source: Starfleet Research; research findings are derived from the Q1 2024 survey on IoT Security

Chapter 5
Maximizing Success with IoT Security

In the shadowy world of cyber threats, IoT devices often act as unwitting accomplices, hiding dangers from traditional security measures. To uncover and combat these hidden threats, businesses, government agencies, and other organizations need to arm themselves with a purpose-built, state-of-the-art IoT security solution. This solution must provide full visibility into all network-connected IoT devices, any of which could serve as gateways for attacks.

Endpoint protection platforms and intrusion detection and response systems are designed to protect networked computers and servers but are not equipped to handle the unique challenges posed by IoT devices. Similarly, network segmentation and firewall policies are ineffective against IoT-focused attacks.

Only a purpose-built IoT security solution that utilizes machine learning to identify vulnerabilities and suspicious activities, even those never seen before, can offer the necessary level of protection. This solution should operate continuously, providing automated Zero Trust security and integrated workflows. To ensure it is future-proof, it should run on a highly scalable cloud architecture.

In the shadowy world of cyber threats, IoT devices often act as unwitting accomplices.

Peopleware

Maximizing success with IoT security extends beyond deploying the right technology solution. It also involves determining who within the organization is responsible for overseeing IoT security on a daily basis. In some instances, this responsibility falls to the IT department. Some organizations may establish a specialized cybersecurity team within the IT department. In other cases, new leadership positions may be created for this purpose, although generally, chief information security officers (CISOs) are responsible for developing and implementing the security strategy for an organization. This includes everything from creating policies and procedures to training employees on security best practices.

One might think that, given the complex nature of IoT devices and networks, it could be advisable to create a dedicated IoT security team, especially for large organizations that handle sensitive data. However, with a fully integrated, high-performance IoT solution, it is generally possible for existing security and operations teams to secure all network-connected IoT devices without having to make changes to existing practices, policies, or procedures.

Enterprises and other large organizations may also utilize a security operations center, or SOC, which is a central location from which it can monitor and manage security events. An SOC can serve as a central point of contact for responding to security incidents. By coordinating the response of security personnel, a SOC can help to minimize the impact of an IoT security breach. The role of the SOC is likely to become increasingly important with the continued proliferation and adoption of network-connected IoT technology.

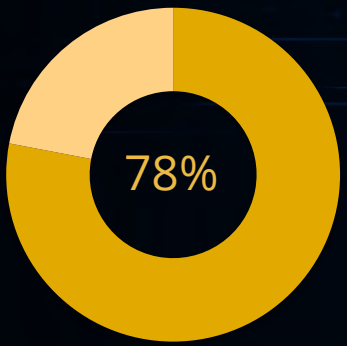
Metrics

Any business, government agency, or other organization serious about IoT security must establish useful performance metrics to track and measure progress over time. These metrics should be employed continuously, with data analyzed to identify trends and patterns. By doing so, organizations can pinpoint areas for improvement, make necessary changes, and drive continuous performance enhancement as new threats inevitably emerge.

Useful performance metrics help organizations track and measure progress over time.

The following are five metrics that can be used to track and measure performance with respect to IoT security:

- Percentage of devices that have been patched within a specified period of time (e.g., 7 days) of a security update being released. (Often, companies have been criticized for taking too long to patch vulnerabilities.)
- Percentage of devices that are using two-factor authentication. Two-factor authentication is important because it adds an extra layer of security to devices that are connected to the internet.



Percentage of security leaders (and other qualified respondents) who say that their organizations track and measure IoT security performance using relevant metrics, such as CVSS scores

Source: Starfleet Research; research findings are derived from the Q1 2024 survey on IoT Security

- Number of reported security incidents during a specified period of time (say, per month).
- Total cost of all security breaches over a specified period of time (e.g., the past year).
- Average Common Vulnerability Scoring System (CVSS) score for all devices.

The CVSS score is an industry-accepted system that takes into account a number of factors, including the severity of the vulnerability and its reach. As such, it provides a more comprehensive picture of risk than other measures, such as the number of Common Vulnerabilities and Exposures (CVEs), which are a list of publicly known cybersecurity vulnerabilities (maintained by the nonprofit organization Mitre and commonly used by security professionals to track risk).

The CVSS score is updated in real-time, which means that it can be used to track trends over time. This is important because IoT security is an evolving field, and what may have been considered secure a year ago may no longer be adequate today. The score is calculated based on three factors: attack vector, attack complexity, and privileges required. It assigns a numerical score to IoT device vulnerabilities to indicate their severity. CVSS scores range from 0 to 10, with 10 being the most severe, and can be translated to a risk level as follows:

The future of IoT holds enormous promise, but it also presents enormous risks.

0.1 - 1.0 : Low Risk
1.1 - 3.0 : Moderate Risk
3.1 - 5.0 : High Risk
5.1 - 7.0 : Very High Risk
7.1 - 9.0 : Critical Risk
9.1 - 10 : Catastrophic Risk

CVSS scores can be used to prioritize vulnerability management processes. For example, an organization may choose to patch all vulnerabilities with a score of 7 or higher within 24 hours, while patching all vulnerabilities with a score of 9 or higher within 12 hours. CVSS provides an effective way to prioritize results, quickly exposing any behavioral anomalies and threat details for security teams to initiate a response. When paired with the right technologies, organizational resources and processes, CVSS can help ensure that the most critical vulnerabilities are addressed in a timely manner, reducing the chances of a malicious attack and the likelihood of data breaches—which, after all, is the name of the game when it comes to IoT security.

Conclusion

The expansion of IoT technologies continues to drive innovation across multiple industries. The convergence of IoT with AI and machine learning is leading to the creation of devices capable of more complex decisions and more personalized interactions than one could have imagined only a few years ago.

The integration of edge computing with AI and the expansion of 5G networks is making it feasible for more applications to process data locally, enhancing responsiveness and reducing data transmission costs. This integration is driving a surge in innovative applications and broader adoption. Digital twins, which are virtual models of physical systems, are being increasingly enhanced by IoT data. These models are crucial for simulating and testing scenarios rapidly and cost-effectively, with applications expanding across various sectors.

The future of IoT holds enormous promise, but it also presents enormous risks. According to research conducted for this benchmark report, 46% of businesses, government agencies, and other organizations are still struggling to gain visibility into the ever-growing number of IoT devices on their networks. Additionally, 54% of them view their existing cybersecurity solutions as inadequate for protecting against the potential threats posed by IoT devices, highlighting that many IT and security teams still have considerable work to do in this area.

Organizations can be assured of adequate protection only by implementing purpose-built technology capabilities.

Confidence in IoT security can be built only by prioritizing vulnerabilities based on their potential impact and exploitability and adopting a zero-trust approach. Organizations can be assured of adequate protection only by implementing purpose-built technology capabilities. Traditional cybersecurity solutions are insufficient on their own for protecting networks from the constant threat posed by unsecured IoT devices. Legacy solutions, even those that claim to offer protection for internet-connected devices, invariably leave organizations vulnerable to attacks.

IT and security decision-makers need to recognize the shortcomings of products that misleadingly present themselves as comprehensive IoT security solutions. More importantly, they need to prioritize the implementation of purpose-built tools specifically designed to actively scan networks, quickly identify and mitigate IoT threats, and prevent potential attacks. As the IoT landscape continues to evolve, it is imperative for organizations to adopt advanced, tailored security measures to effectively mitigate risks and safeguard their digital ecosystems.

Palo Alto Networks is the world's cybersecurity leader. We innovate to outpace cyberthreats, so organizations can embrace technology with confidence. We provide next-gen cybersecurity to thousands of customers globally, across all sectors.

Our best-in-class cybersecurity platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art automation. Whether deploying our products to enable the Zero Trust Enterprise, responding to a security incident, or partnering to deliver better security outcomes through a world-class partner ecosystem, we're committed to helping ensure each day is safer than the one before. It's what makes us the cybersecurity partner of choice.

This benchmark report is the result of primary and secondary research conducted by subject matter experts at Starfleet Research, which is the IT market research arm of Starfleet Media. Starfleet Research is a world leader in benchmarking best practices in technology-enabled business initiatives. Our benchmark reports, focusing on how companies can maximize performance and achieve their desired objectives with respect to specific technology-enabled business initiatives, are read by thousands of industry practitioners and others around the world. Our digital content assets, including our Smart Decision Guides, are widely considered to be the most authoritative industry resources for IT decision makers charged with evaluating and making technology purchases.

Contact Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054

www.paltoaltonetworks.com
(866) 320-4788

Contact Starfleet Research
219 W. Chicago Ave. Suite 400
Chicago, IL 60654

www.starfleetresearch.com
research@starfleetmedia.com

Research notes: In Q1 2024, Starfleet Research conducted an online survey to capture the perspectives of IT and cybersecurity leaders, IT staff and other industry practitioners with firsthand experience with IoT security in their organizations. 342 qualified respondents participated, from industries that include Consumer Goods and Retail (16%), Healthcare (14%), Financial Services (12%), Hospitality (11%), Manufacturing (7%), and Transportation (5%). Representatives from government agencies and other public sector entities (6%) as well as nonprofit organizations (4%) also participated. Qualified respondents were comprised primarily of security and IT managers and directors (31%); security and IT staff (22%); and CISOs and other senior leaders (14%). Geographic location of survey respondents: North America (54%); Europe (25%); Asia (13%); Other (8%). Size of survey respondents' employers, by revenue: Very small and small companies – i.e., less than $10M in revenue (27%); Midsize companies – i.e., $10M to $100M in revenue (31%); Large and very large companies – i.e., more than $100M in revenue (28%).