ARMIS®

# Guide to Securing your Complex IoT Environments

# Table of Contents

# A Complete A-Z of IoT Asset Security

Year on year, Internet of Things (IoT) assets are becoming more present in our traditional enterprise and OT infrastructure. Whether it's a hospital setting or car manufacturer, IoT is transforming and automating our industrial spaces. At Armis, we see firsthand how this surge in IoT adoption is creating incredible opportunities—but also significant security challenges for our customers. Many organizations struggle to secure their connected devices, leaving critical systems vulnerable. That's why we've developed this buyer's guide—to share key insights and help you make informed decisions to protect your organization as it digitalizes and grows.

# The IoT Security Landscape

## Understanding IoT Market Trends

The IoT market is growing exponentially, projected to exceed 30 billion devices by 2030. Sectors such as manufacturing, healthcare, energy, critical infrastructure, retail, and logistics are leading this growth, driven by the need for real-time monitoring, automation, and operational efficiency. IoT enhances everything from improving patient care with connected medical devices to optimizing supply chains using smart sensors.

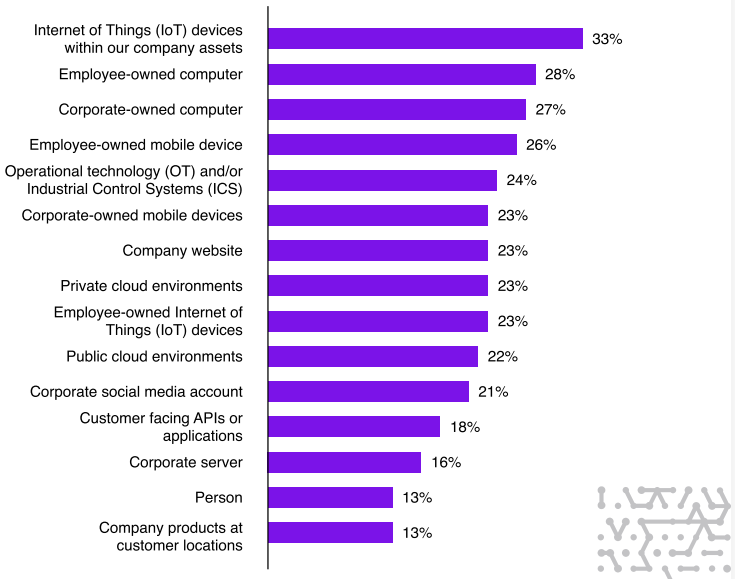
However, this explosion of connected devices significantly increases the attack surface, creating new vulnerabilities and challenges that require robust security measures.

### Which of the following was targeted as a part of this external attack?

Source: Forrester's Security Survey, 2024

Base: 1240 Security decision-makers who experienced an external attack when their company was breached

Not all responses shown



## What Sets IoT Apart?

IoT security focuses on protecting devices and networks to ensure the integrity and accuracy of data flow. Unlike traditional IT systems, IoT assets are often lightweight, lack advanced built-in security, and rely on continuous connectivity, making them unique targets for cyberattacks. Operational Technology (OT), which powers industrial systems such as manufacturing lines, intersects with IoT, further complicating the security landscape.

**What counts as IoT?**

Check out our Appendix of IoT assets here.

# Key Security Challenges and How to Address Them

Securing IoT devices is a complex task due to their unique characteristics. Below are some of the biggest challenges and actionable tips to help organizations tackle them effectively:

| | Challenge | Top Tip |
|---|---|---|
| **Lack of Situational Awareness and Asset Inventory** | Organizations don't know where to begin and are often still drowning in a sea of spreadsheets. | Prioritize implementing a comprehensive asset inventory system and leverage automation tools to triage and rank alarms by severity. This will help reduce lateral creep and address critical threats first. |
| **Lack of Traditional Security Support** | Many IoT devices cannot run traditional antivirus or firewalls, leaving systems exposed to exploitation. | Implement network segmentation to isolate IoT devices from critical systems and limit potential damage from attacks. Use products like Armis Centrix™ for Asset Management and Security and Intelligence Center to monitor traffic to and from IoT devices for suspicious activity. Additionally, ensure all IoT devices are operating behind a secure gateway or VPN for added protection. |

| | Challenge | Top Tip |
|---|---|---|
| **Default Credentials** | IoT devices often ship with hardcoded or easily guessable credentials, which are rarely updated by users, greatly increasing attack vulnerabilities. | Upon deployment, enforce a policy requiring the immediate change of all default usernames and passwords. Use strong, unique credentials for every device and consider implementing Passwordless MFA that is FIDO Certified wherever possible. Password managers can help organize and secure these credentials. |
| **Outdated Legacy Devices** | Older IoT devices often lack modern security updates or compatible patches, creating critical security risks. | Regularly audit all IoT devices on your network to identify outdated models. For unsupported devices, consider replacing them with newer models that receive regular updates. Where replacement isn't feasible, isolate legacy devices on a separate network segment to limit their exposure and monitor their activity closely. |
| **Unclear Accountability/ Organizational Accountability** | IoT devices are frequently managed by operational technology (OT) teams rather than IT teams, causing gaps in oversight and security enforcement. | Establish clear collaboration between OT and IT teams by defining shared responsibilities for IoT security. Develop unified policies and provide cross-departmental training to ensure consistent security practices. Designate an IoT security coordinator to oversee and bridge the gap between teams. |
| **Always-Connected Nature** | With constant internet connections, IoT devices are more prone to remote attacks, especially if left unpatched or unmanaged. | Use monitoring tools to track device connections and disconnect any suspicious or unauthorized devices immediately. Consider deploying a zero-trust security model to restrict access based on the principle of least privilege.<br><br>By addressing these challenges with proactive strategies, organizations can significantly reduce the risks associated with IoT devices and build a more secure infrastructure. |

# Questions to Ask Before Investing in IoT Security

When evaluating an IoT security solution, clarity and strategy are essential. Ask yourself:

## 1 What's the difference between IT and IoT security?

IT security protects traditional computing systems (servers, desktops, etc.), while IoT security focuses on safeguarding connected devices like smart appliances, sensors, and industrial equipment. IoT devices are often more vulnerable due to limited processing power and fewer built-in security features.

## 2 How should I start securing IoT devices?

Begin by identifying all connected IoT devices and assessing their vulnerabilities. Use strong, unique passwords for each device, ensure they're running the latest firmware, and implement encryption for data transmission. It's also important to segment IoT devices from critical systems to reduce risks.

## 3 What regulations must I comply with?

Compliance requirements depend on your industry and location. For example, the GDPR applies to businesses in Europe handling personal data, while the IoT Cybersecurity Improvement Act applies to U.S. government devices. Other regulations like ISO/IEC 27001 or NIST guidelines may also be relevant.

## 4 Should I use a specialized or generalized security platform?

Your environment more than likely includes a mix of IT, OT, and IoT devices, choose a platform that covers all these assets. A solution that offers device-specific protection, threat detection, and monitoring, while also securing your broader IT/OT environment, will help future-proof your security.

## 5 How can OT and IT teams collaborate to enhance IoT security?

Collaboration between OT and IT teams is crucial. Aligning both teams on security goals, mapping risks together, and implementing joint incident response plans will improve security. Regular training and shared management tools help foster better cooperation.

## 6 Is the solution scalable for different business units and locations?

Ensure the solution can scale as your business grows or expands. A scalable security platform will maintain consistent protection across multiple locations and devices without causing inefficiencies or gaps in coverage.

## 7 Does the solution meet specific compliance requirements (e.g., HIPAA, GDPR)?

Evaluate how well the solution adheres to the relevant compliance standards for your industry. For example, healthcare businesses need HIPAA compliance, while manufacturers may need to follow IEC 62443. Ensure the solution provides the necessary auditing and reporting capabilities.

## 8 Does the solution offer automated risk assessments and remediation?

Look for features like automated risk scoring, patch recommendations, and workflow integrations that help identify vulnerabilities and quickly address them. Automation reduces the window of opportunity for attackers to exploit weaknesses.

## 9 Can it integrate with network segmentation tools to isolate compromised IoT devices?

Network segmentation can help limit the spread of threats. Make sure the solution integrates seamlessly with network tools to isolate compromised devices and contain potential breaches before they escalate.

## 10 How does it handle firmware vulnerabilities and patching?

Firmware vulnerabilities are a common entry point for IoT attacks. Ensure the solution can identify and prioritize these vulnerabilities, offering timely patching recommendations and management tools to minimize security risks.

## 11 What is the total cost of ownership?

Understand the full financial commitment, including licensing, deployment, and ongoing maintenance costs. Factor in both the initial investment and the long-term operational costs to accurately assess the solution's value.

## 12 How does the solution demonstrate ROI?

A good IoT security solution should reduce risks, minimize security incidents, and improve operational efficiency. Ensure that the solution delivers measurable outcomes that justify the investment.

### 13 Does the vendor have experience securing IoT in my industry?

Check if the vendor has specialized experience securing IoT in your industry. Expertise in specific sectors like healthcare, manufacturing, or critical infrastructure can make a big difference in addressing unique challenges.

### 14 What support and threat intelligence does the vendor provide?

Getting Proactive is critical, using an early warning product that can alert you to attacker trends in your industry is a great way of directing your efforts to assets that are more vulnerable to exploitation. Reliable customer support and timely updates on emerging threats are essential. Make sure the vendor offers solid support, threat intelligence feeds, and useful documentation for troubleshooting and planning.

### 15 Is there ongoing innovation and roadmap transparency?

Since IoT threats evolve rapidly, ensure that the vendor is committed to continuous product updates, new features, and a clear roadmap to keep the solution effective against future threats.

# Best Practice Solutions for IoT Security

As IoT devices become more integral to business operations, securing these devices is critical. Organizations must adopt tailored strategies to mitigate risks and address IoT's unique vulnerabilities effectively. Here are key best practices to ensure robust IoT security:

## 1 Implement a Zero Trust Security Model

A Zero Trust approach is essential for IoT security, as it assumes no device or user is inherently trustworthy. This proactive model reduces risk by continuously validating all access requests.

**Device Identification and Authentication:** Continuously monitor all devices connected to your network. Use unique identifiers for each device to track and categorize them effectively. Implement strong authentication mechanisms for devices to prevent unauthorized access.

**Least-Privilege Access Controls:** Restrict device interactions to only those connections and functions necessary for their operation. This minimizes exposure and ensures that even compromised devices have limited impact.

**Multi Engine Detection Model:** Assist with Anomaly Detection, Device profiling with the Asset Intelligence Engine Leverage AI-driven tools to analyze device behavior and detect unusual activities in real time. Early detection of anomalies allows for quick responses to potential threats.

## 2 Clear Ownership and Oversight

IoT security requires collaboration and accountability. Assign responsibilities across an integrated team of IT and Operational Technology (OT) professionals.

**Defined Roles and Responsibilities:** Clearly outline who is responsible for securing IoT devices, maintaining updates, and responding to incidents.

**Scheduled Updates and Patch Management Prioritized based on greatest risk to the business:** Ensure a regular maintenance schedule for firmware updates and patches, avoiding outdated devices that may expose vulnerabilities.

**Proactive and Ongoing Risk Assessments:** Conduct frequent vulnerability assessments to identify risks before they become exploitable. Use these insights to strengthen your security posture.

## 3 Patch and Vulnerability Management

IoT devices often lack standard updating mechanisms, making patch management critical.

**Automated Tools for Detection and Deployment:** Deduplicate, contextualize, prioritize, assign and mitigate vulnerabilities. Use automated systems to identify vulnerabilities quickly and deploy security patches. This ensures that devices remain protected without manual intervention.

**Firmware and Software Updates:** Prioritize updating firmware and software regularly to address newly discovered flaws. Schedule maintenance windows and focus on creating a structured update process for your IoT environment.

**Vendor Collaboration:** Work closely with IoT device manufacturers to stay informed of updates, patches, and emerging vulnerabilities. Enable the ability to work in conjunction with the existing tech stack for “team sport” security.

## 4 Network Segmentation

Separating IoT devices from critical systems is a vital layer of protection.

**Establish Network Zones:** Create isolated zones for IoT devices to limit their interaction with sensitive systems. This reduces the impact of a potential breach.

**Firewalls and Access Controls:** Deploy firewalls to monitor traffic between IoT segments and critical networks. Use access controls to enforce strict communication boundaries.

## 5 Continuous Monitoring and AI-Driven Insights

IoT security is an ongoing effort that requires continuous vigilance.

**Real-Time Monitoring:** Use advanced monitoring tools to track IoT device behavior 24/7. These systems can quickly identify abnormal activities, such as unauthorized access attempts or unexpected data transfers.

**AI and ML:** Use Early Warning systems to get ahead of the curve. Implement AI-driven analytics to gain actionable insights into device performance and threat trends. This helps in predicting and preventing attacks like ransomware or botnet exploitation.

**Incident Response Automation:** Equip your monitoring systems with automated response capabilities to contain threats immediately upon detection.

## 6 Compliance and Auditing

Regular auditing is essential to maintaining security and meeting regulatory requirements.

**Compliance Standards:** Employ C Suite reports with insights that can be drilled down into. Streamline your compliance efforts with policy packs for specific industries. Align your IoT security measures with industry standards such as ISO/IEC 27001, GDPR, or NIST guidelines. This ensures a structured approach to managing security.

**Device Inventory Audits:** Maintain an up-to-date inventory of all IoT devices and their configurations. Regularly audit these devices to identify and mitigate risks.

## 7 Encryption and Data Security

Securing data at every stage of its lifecycle is crucial for IoT environments.

**End-to-End Encryption:** Encrypt data both in transit and at rest to protect sensitive information. This ensures that even intercepted data cannot be exploited.

**Secure Data Storage:** Store IoT-generated data in secure, access-controlled environments.

**Key Management:** Implement strong encryption key management practices to prevent unauthorized decryption.

## 8 IoT Device Lifecycle Management

Manage IoT devices effectively from deployment to decommissioning.

**Secure Onboarding:** Use secure protocols during device setup to prevent unauthorized access.

**End-of-Life Security:** Ensure devices are securely decommissioned to avoid data leaks or exploitation of outdated hardware.

# Typical Attack Pathways

## Default Credentials or Weak Passwords

Many IoT devices ship with default login credentials that users fail to change, making them an easy entry point for attackers.

## Unpatched Vulnerabilities

Devices often have outdated firmware or software, leaving them exposed to known exploits.

## Lack of Network Segmentation

IoT devices connected to the same network as critical systems provide attackers with lateral movement opportunities.

## Man-in-the-Middle (MitM) Attacks

Cybercriminals intercept unencrypted data in transit between IoT devices and their controllers.

## Malware and Ransomware

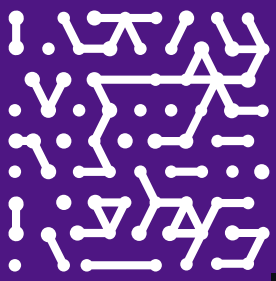
IoT devices can be infected with malware to disrupt operations or demand ransom payments.

## Spoofing and Impersonation

Attackers can exploit weak authentication protocols to mimic legitimate devices or users.

## Physical Access

Industrial IoT devices in remote or poorly secured locations are more vulnerable to tampering or theft.



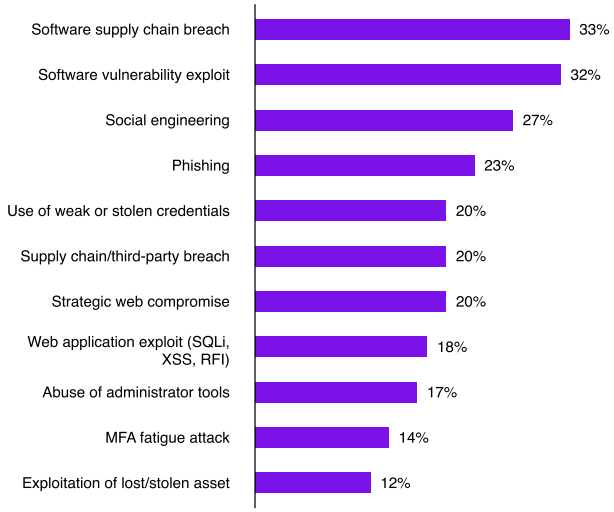
## How was the external attack carried out?

Source: Forrester's Security Survey, 2024

Base: 720 Security decision-makers who experienced an external attack when their company was breached

Applied filter: Target of External Attack-IoT, ICS/OT, Employee IoT selected

Answer "Other" removed




# IoT Security Checklist Enhanced with Armis Capabilities

As IoT devices become more integral to business operations, securing these devices is critical. Organizations must adopt tailored strategies to mitigate risks and address IoT's unique vulnerabilities effectively. Here are key best practices to ensure robust IoT security:

## 1 Comprehensive Asset Intelligence

- ☐ Leverage Armis' Asset Intelligence Engine to gain complete visibility into all IoT devices, including unmanaged devices.
- ☐ Continuously monitor device inventory to identify anomalies, unapproved devices, and asset misconfigurations.
- ☐ Ensure real-time risk assessment of all connected devices using Armis' extensive knowledge base of device behaviors.

## 2 Early Warning to Preempt Attacks

- ☐ Utilize Armis' Early Warning System to proactively identify potential risks and prioritize vulnerabilities in your IoT environment.
- ☐ Monitor for unusual behavior patterns and potential threats using AI-driven insights provided by Armis.
- ☐ Receive real-time alerts on device anomalies or suspicious activities to enable swift remediation.

## 3 Attack Pathway Visibility

- ☐ Rely on Armis to map potential attack pathways within IoT networks and identify at-risk assets.
- ☐ Conduct thorough assessments of how compromised devices could be exploited to infiltrate critical systems or data.
- ☐ Deploy mitigation strategies based on actionable insights from Armis' network activity analysis.

## 4 Secure Device Communication

- ☐ Utilize Armis to detect insecure communication channels and enforce encryption standards like TLS or VPNs.
- ☐ Identify unapproved connections between devices and block unauthorized external access with automated policies.
- ☐ Ensure secure authentication protocols are in place, leveraging Armis' capabilities to validate device behaviors.

## 5 Patching and Vulnerability Management

- ☐ Rely on Armis to provide detailed insights into firmware versions and identify vulnerabilities in IoT devices.
- ☐ Proactively address risks using Armis VIPR recommendations for patching and updating devices.
- ☐ Automate the scheduling and monitoring of maintenance activities with insights derived from Armis' platform.

## 6 Secure Remote Access

- ☐ Implement secure remote access policies using Armis to ensure authorized personnel can manage IoT devices safely.
- ☐ Monitor remote access activities and prevent unauthorized connections via Armis' robust detection and alert systems.
- ☐ Authenticate remote sessions with granular permissions, powered by Armis' policy enforcement capabilities.

## 7 Employee Awareness and Training

- ☐ Train staff with insights derived from Armis' reports on IoT security risks specific to your organization.
- ☐ Develop internal guidelines that emphasize the use of Armis' platform for deploying and managing IoT devices securely.
- ☐ Incorporate Armis into your larger cybersecurity program to enhance protection across connected assets.

# Leveraging Enterprise Solutions Like Armis Centrix™

Platforms like Armis Centrix™ provide state-of-the-art security capabilities, including:

**100% Visibility** of network-connected IoT devices.

**Proactive Threat Detection** to mitigate risks in real time.

**Seamless Integrations** with existing IT and OT networks.

**Zero Trust Enforcement** for maximum protection.

# Final Thoughts

The rapid adoption of IoT devices shows no signs of slowing down. However, with this growth comes an urgent need for robust security practices. By implementing best practices, investing in Zero Trust security models, and choosing comprehensive solutions like Armis Centrix™, organizations can manage IoT risks effectively.

**Appendix:**

# Typical IoT/ IIoT Devices in Operational Settings

IoT adoption spans various industries, making these devices integral to business operations but also vulnerable to cyber threats. Here are some examples commonly found in OT environments:

### Industrial Sensors

- Temperature sensors
- Pressure sensors Humidity sensors
- Vibration sensors
- Proximity sensors
- Gas leak detectors

### Light sensors

- Industrial Control Systems (ICS) Components
- Programmable Logic Controllers (PLCs)
- Remote Terminal Units (RTUs)
- Supervisory Control and Data Acquisition (SCADA) systems
- Human-Machine Interfaces (HMIs)
- Distributed Control Systems (DCS)

### Industrial Robotics & Automation

- Autonomous mobile robots (AMRs)
- Collaborative robots (Cobots)
- Industrial robotic arms
- Automated guided vehicles (AGVs)
- Smart conveyors

### Smart Manufacturing & Production Equipment

- CNC machines
- 3D printers
- Smart assembly lines
- Digital twin systems
- Condition monitoring systems

### Connected Infrastructure & Utilities

- Smart meters (electricity, water, gas)
- Power grid monitoring devices
- Pipeline monitoring systems
- Smart HVAC systems
- Industrial lighting control systems

## Connected Safety & Security Devices

- Smart fire suppression systems
- Biometric access control systems
- Industrial surveillance cameras
- Wearable safety devices (e.g., smart helmets, exoskeletons)
- Gas and chemical exposure monitors

## Asset Tracking & Supply Chain Devices

- RFID tags and readers
- GPS tracking devices
- Smart warehouse management systems
- Fleet telematics devices
- Cold chain monitoring sensors

## Healthcare & Pharmaceutical Manufacturing IoT

- Smart sterilization equipment
- Pharmaceutical environmental monitoring systems
- Connected medical device manufacturing systems
- Lab automation devices

## Industrial Wireless Communication Devices

- 5G-enabled IIoT devices
- LPWAN (LoRa, NB-IoT) devices
- Industrial Wi-Fi routers and access points
- Private 5G networks for industrial environments