2024 IoT Security Crisis: By The Numbers

(650) 263-8225 | sales@viakoo.com | viakoo.com

Table Of Contents

100% of IT Leaders Have Network Connected IoT Devices, and 50% Don't Believe They Have Effective IoT Security

Based on commissioned research by Viakoo, this ebook provides the numbers on how IT leaders view the significance of the IoT threat to their organizations, what the impact of those key threats are, the missing pieces of the IoT security technology stack to improve defenses, and how governance is more focused on IoT applications and device system security.

The Key Data in The Survey That Makes This an IoT Security Crisis:

- 83% of IT leaders agree **their attack surface grew one application at a time**, and should be remediated one application at a time
- 22% of organizations have had a **serious or business-disrupting IoT security incident** in the past 12 months
- 71% of IT leaders **wish they had started their IoT security efforts differently** in order to get to remediation faster
- Only 35% of IT leaders **believe they are successful in using agentless network-based asset discovery** for managing IoT vulnerabilities
- Half of IT leaders believe that **IoT is the weakest part** of their security efforts

Introduction

- ***The Problem: IoT Systems Are Cyber Catnip to Threat Actors and Most Enterprises Lack Effective IoT Security***
- ***The Solution IT Leaders Want: To Shrink the IoT Attack Surface the Same Way It Grew - One Application at a Time***

IoT application and device systems are a significant investment made by organizations to drive their operations. They must perform reliably all the time to realize a full return on that investment, and must be cyber-secure. However, in spite of having top-of-the-line technology, first-class networking, continuous IT monitoring, and top-notch people manning and maintaining IoT systems — half of all organizations have had an IoT security incident in the past 12 months, and believe that IoT is the weakest part of their security.

- IoT vulnerabilities are particularly threatening, as they are present in cyber-physical systems (such as industrial controls) where they can be exploited to create physical damage and destruction just as much as it could lead to data theft.
- Unlike traditional IT systems, finding and locating vulnerable systems is much harder for IoT technology. Most of these systems are managed outside of IT, and often are “unmanaged” because they were designed to be set-it-and-forget-it. Organizations need different solutions than for IT, such as using an agentless application-based asset discovery solution to locate and assess infected IoT applications and devices.
- Unfortunately the reality for most IoT application and device systems is that they are behind on firmware updates, making the chances very high of a system being vulnerable to malicious attacks.

1. How Serious Is The IoT Threat Landscape?

In surveying IT leaders across a range of organizations it's clear that poor IoT security is currently causing serious security incidents and more effort is needed to bring IoT security to the same level as IT security.

In terms of IoT security there has been a decades-long evolution in the volume, velocity, and persistence of cyber threats, which is tied to both the increased computational capabilities of IoT and critical infrastructure systems, as well as increased sophistication by threat actors. From the Mirai botnet attacks through to 2023's IoT exploits at MGM, vulnerable IoT systems are increasingly the focus for breaching an organization and this will continue for the foreseeable future.

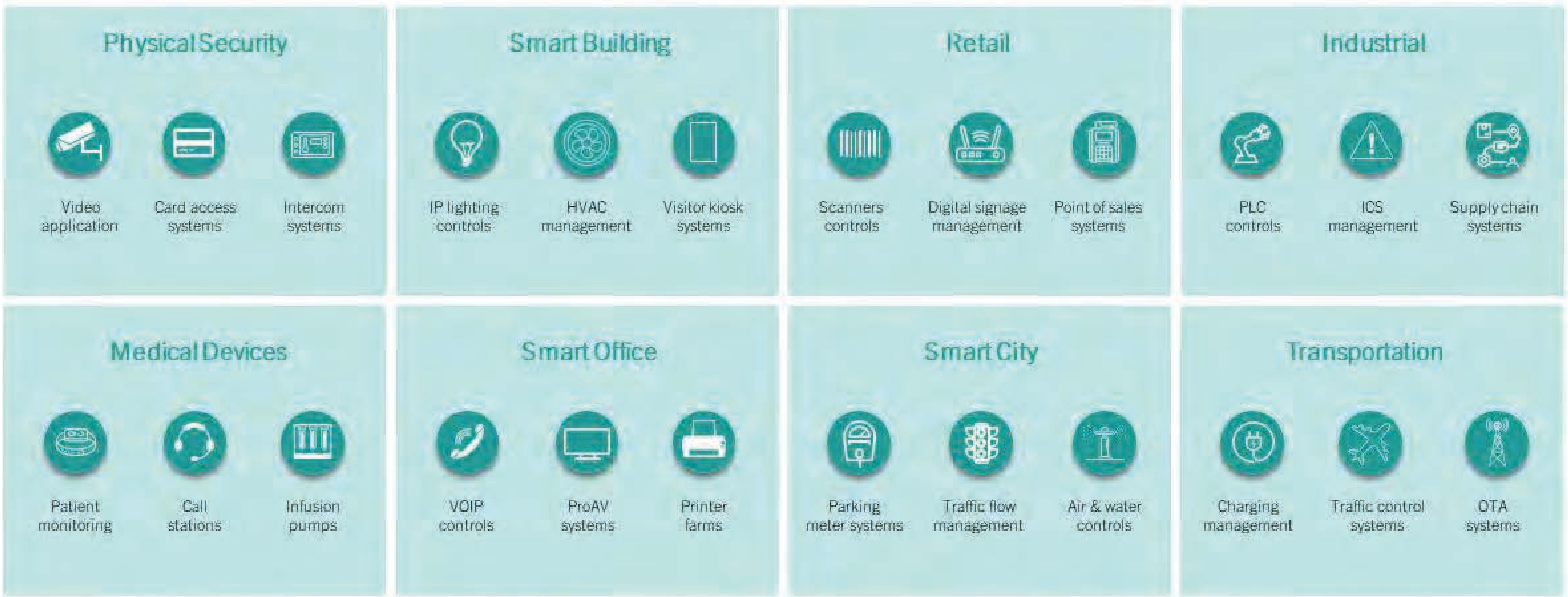
Of IT Leaders Surveyed in November 2023,

- ***95%** have an IoT security plan but only **51%** feel confident in their IoT security efforts*
- ***50%** of IT leaders say IoT is the weakest part of their security*
- ***50%** of companies have experienced an IoT cyber incident in the last 12 months - of which **44%** were serious and **22%** threatened business operations*
- ***55%** of IoT cyber incidents could have been prevented with better security measures*
- *Average cost of a cyber incident in 2023 is **$4.45M** (Source IBM: www.ibm.com/reports/data-breach)*

Increased IoT Threats

IoT Vulnerabilities Exist In Critical Systems Across The Enterprise

Figure 1 - Enterprise IoT Examples



Physical Security
- Video application
- Card access systems
- Intercom systems

Smart Building
- IP lighting controls
- HVAC management
- Visitor kiosk systems

Retail
- Scanners controls
- Digital signage management
- Point of sales systems

Industrial
- PLC controls
- ICS management
- Supply chain systems

Medical Devices
- Patient monitoring
- Call stations
- Infusion pumps

Smart Office
- VOIP controls
- ProAV systems
- Printer farms

Smart City
- Parking meter systems
- Traffic flow management
- Air & water controls

Transportation
- Charging management
- Traffic control systems
- OTA systems

2. Key IoT Security Threats

Vulnerable IoT applications and devices form a massive attack surface capable of disrupting an organization, causing both cyber and physical damage. IT leaders report that these are their chief concerns of the impact of an IoT system breach:

The top emerging IoT threats:

- *Data breaches* - ***69%***
- *Ransomware attacks* - ***60%***
- *Supply chain attacks* - ***45%***
- *Artificial Intelligence & Machine Learning (AI/ML) attacks* - ***43%***
- *Denial of Service (DDoS) attacks* - ***42%***

The top IoT security priorities in 2024:

- *Data security and privacy* - ***75%***
- *Vulnerability assessment and mgmt.* - ***50%***
- *Awareness and Training* - ***48%***
- *Risk mgmt.* - ***44%***
- *Incident response* - ***40%***

Why companies worry about their IoT security:

- *Data breaches* - ***64%***
- *Ransomware attacks* - ***52%***
- *Emerging threats* - ***38%***
- *Supply chain attacks* - ***37%***
- *Denial of Service attacks* - ***34%***

3. The Right Technology Stack for IoT Security

The major finding of this survey is that organizations have key missing pieces in their IoT security solution, specifically around application-based discovery and getting to remediation faster. In reflecting on their ability to secure vulnerable IoT applications and device systems IT leaders are reporting a desire to improve their IoT security technology stack.

The Good News: Organizations are Focused on IoT Security

90%

believe that agentless security solutions are the foundation for successful IoT security

86%

have threat assessment to identify IoT vulnerabilities

83%

of IT leaders agree their attack surface grew one application at a time, and should be remediated one application at a time

The Bad News: But There Are Missing Pieces

91%

Have solutions in place for IoT discovery

71%

But 71% wish they deployed IoT discovery differently so they would get to remediation faster

93%

93% use agentless network-based asset discovery to help mitigate or remediate IoT vulnerabilities

35%

But just 35% feel they are successful with those efforts

83%

83% of companies have plans to extend Zero Trust initiatives to their IoT environment

53%

But only 53% feel confident to set up network segmentation, including for Zero Trust

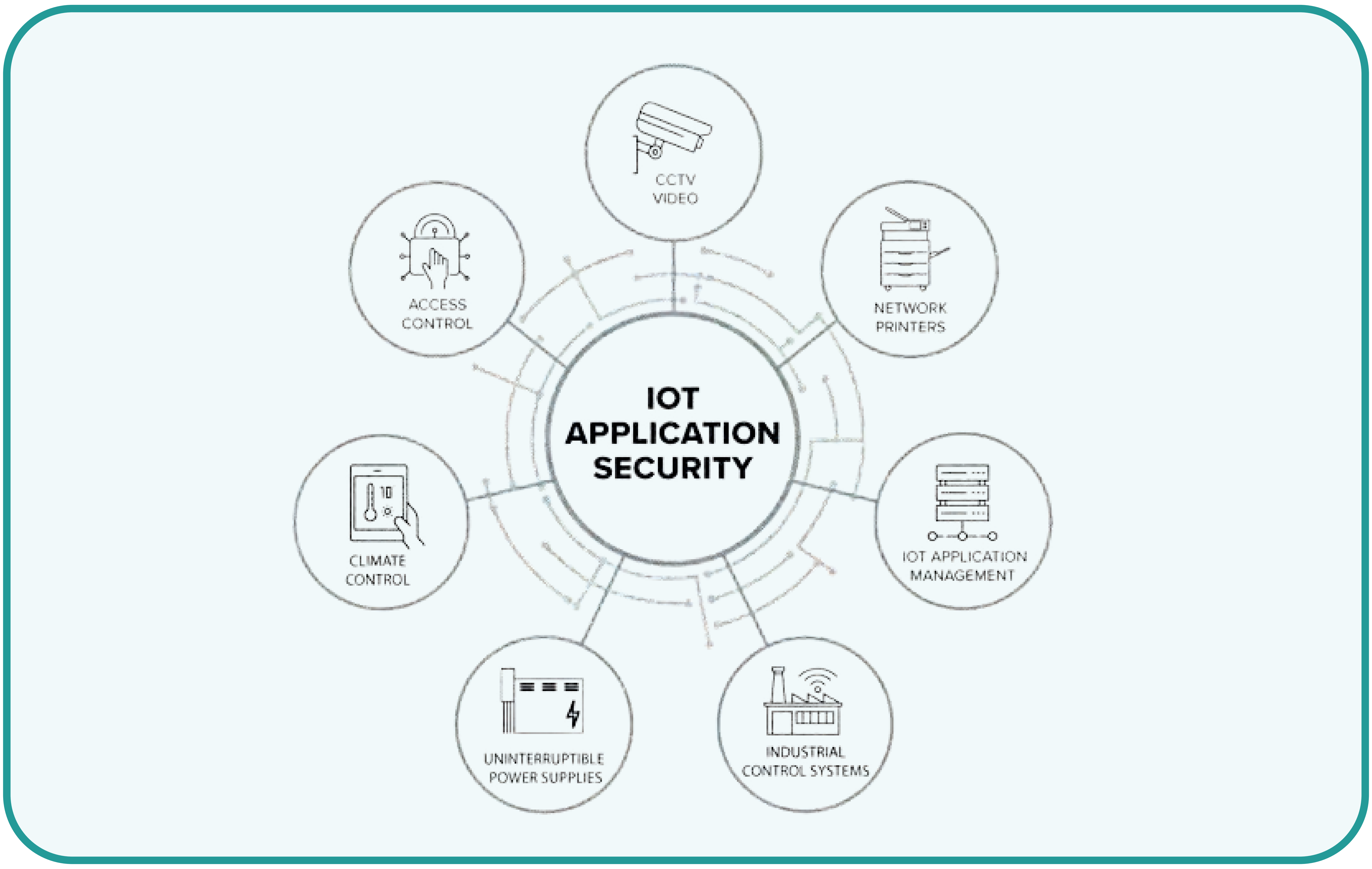
60%

60% of IT leaders don’t have enough information on the application context of IoT cyber threats

65%

65% of companies that deployed agentless network-based asset discovery feel they are not successful with those efforts

Figure 2. Application-Based Discovery



4. Governance for IoT Security

From the Board of Directors to multiple levels of management, here is how organizations are adding more governance over IoT systems.

87% of companies spent more on IoT security this year than last year

89% of companies plan to spend more next year on IoT security than this year

54% of Boards of Directors regularly discuss IoT security oversight
But only **63%** of Boards have enough information on IoT Security to make informed decisions

- **Multi-department teams of IoT system owners meet twice per month on average to discuss IoT security**

- **The IoT Security issues most discussed by them are:**
  - **Data Security & Privacy**
  - **Emerging Threats**
  - **Vulnerability Assessment**
  - **Risk Management**
  - **Secure Communications**

Conclusions & Next Steps

The numbers presented here put a spotlight on how the IoT applications and device systems that organizations rely on are vulnerable, are being attacked, and lack the proper technology to secure them to the same level that traditional IT systems have been. While there is board-level visibility into IoT security and internal discussions between the managers of IoT systems, most organizations lack accurate application-based discovery, remediation, and governance to ensure that IoT systems are always visible, operational, and secure.

Ready to take steps to improve your IoT security? Here are 4 key areas to focus on.

1. **Application-based Discovery:** Unlike any IT systems, most IoT systems are a tightly-coupled environment of devices and applications. Start with agentless application-based discovery to make visible the application, device, and port relationships, as well as vulnerabilities that exist in IoT devices or applications.
2. **Remediation Automation:** IoT devices exist in fleets spread across the organization. Manual approaches to firmware patching and password rotations simply do not scale or act fast enough to contain threats.
3. **Bring IoT into Zero Trust:** Ensure that all IoT devices have an automated method for certificate management, and use application-based discovery to ensure network segments are set up correctly.
4. **Repatriation and Compliance:** Increasing mandates, compliance requirements, and cyber insurance documentation means that your IoT security solution must be capable of tracking and reporting all cybersecurity operations over time.