

# Bridging the Healthcare Technology Divide

A Comprehensive Guide to Achieving IT and IoT Asset Visibility for Enhanced Cybersecurity



# Table of Contents

<b>Overview</b>	<b>3</b>
Chapter 1: <b>Healthcare IoT Security Challenges and Industry Approaches</b>	<b>4</b>
Chapter 2: <b>How Cylera Helps</b>	<b>10</b>
Chapter 3: <b>Platform Interface and Device Management</b>	<b>13</b>
<b>Unique Healthcare IoT Asset Intelligence and Security Benefits</b>	<b>20</b>
<b>Why Customers Choose Cylera</b>	<b>21</b>

# Overview

By **Sean McCue**, Principal XIoT Cybersecurity Architect, Cylera

*The shift to digital systems in healthcare has transformed patient care, making it more efficient and patient-centered while introducing significant visibility challenges across expanding technology infrastructure.*

This eBook addresses the critical asset management gap facing IT, security, and biomedical teams. Traditional tools consistently fall short—either missing vital patient care devices or providing outdated snapshots that quickly become obsolete in dynamic healthcare settings.

Without complete asset awareness, security vulnerabilities remain unaddressed, operational inefficiencies persist, and patient care quality is potentially compromised. Healthcare organizations require comprehensive solutions to keep pace with their rapidly changing technology environment.

This guide shares concrete methods to bridge the divide between disparate systems and teams through innovative healthcare asset management. It presents practical strategies for implementing robust inventory solutions that unite IT and biomedical teams, strengthen security postures, and support patient care objectives.

Learn how specialized solutions like the Cylera platform can provide real-time awareness of connected device ecosystems, empowering healthcare organizations to take control of their technology and maximize the benefits of digital healthcare delivery.



## Chapter 1

# Healthcare IoT Security Challenges and Industry Approaches

### Current Healthcare IoT Threat Landscape

Today's healthcare organizations are undergoing significant changes due to digital adoption. The proliferation of connected medical devices—from patient wearables to smart infusion pumps and networked imaging systems—promises unprecedented improvements in care delivery, real-time monitoring, and operational efficiency. However, this same connectivity that enhances patient care also dramatically expands the attack surface, creating complex security challenges for healthcare institutions.

For cybersecurity leaders in healthcare, this presents a critical paradox: how to facilitate the clinical innovations that connected technologies provide while safeguarding vulnerable systems, sensitive patient data, and ultimately, patient safety.

### Healthcare Cyberattack Impact

Healthcare is now one of the most frequently targeted industries for cyberattacks, with devastating consequences that extend far beyond data breaches:

**Clinical Impact:** Cyberattacks disrupt essential care delivery by forcing appointment cancellations, delaying critical treatments, and compromising diagnostic accuracy. During active incidents, healthcare organizations often need to divert emergency patients and revert to manual processes, which increases the risk of medical errors.

**Financial Devastation:** The economic toll of healthcare cyberattacks is staggering. In addition to the immediate costs of incident response and system recovery, organizations endure substantial revenue losses due to suspended services. The Change Healthcare

cyberattack highlighted this vulnerability, as some affected hospitals reported daily revenue losses nearing \$1 million.

**Reputational Damage:** Security incidents undermine patient trust and community confidence—crucial assets for healthcare providers. This weakened reputation can lead to lasting impacts on patient volume and organizational partnerships.

**Regulatory Consequences:** Following breaches, healthcare organizations encounter heightened regulatory scrutiny, possible penalties, and the introduction of additional compliance requirements that further tax their limited resources.

## Current Regulations and Asset Visibility

As the adoption of connected devices accelerates, regulatory frameworks have evolved to address the emerging security landscape, resulting in new compliance requirements for healthcare organizations:

### United States Framework:

- HIPAA (Health Insurance Portability and Accountability Act) and HITECH (Health Information Technology for Economic and Clinical Health Act) regulations establish fundamental security and privacy requirements
- Recent proposed updates to the HIPAA Security Rule (December 2023) strengthen requirements for cybersecurity programs
- HHS Cybersecurity Performance Goals (CPGs) provide specific security objectives
- NIST (National Institute of Standards and Technology) Framework 2.0 (February 2023) offers comprehensive security guidance

### United Kingdom Requirements:

- NCSC Cyber Assessment Framework (CAF) establishes security objectives
- CAF-aligned Data Security and Protection Toolkit (DSPT) provides implementation guidance

- UK GDPR and the Data Protection Act (2018) mandate strict data protection measures

These regulations increasingly emphasize comprehensive asset inventory and management as foundational security requirements.

Knowing what devices exist on your network is fundamental to any security program. Understanding this relationship is essential for developing a mature approach to protecting patient data and clinical systems.

## Relationship Between Asset Visibility & Cybersecurity

Effective cybersecurity in healthcare environments follows a maturity progression that begins with asset visibility. This foundation supports all subsequent security functions:

### 1. Comprehensive Asset Inventory

Complete visibility into all connected devices—including detailed information about specifications, software versions, and network roles—forms the essential first step in healthcare cybersecurity. Without this foundation, organizations cannot effectively implement more advanced security measures.

## 2. Vulnerability and Risk Management

Asset visibility enables precise understanding of the organization's risk profile. With comprehensive device inventories, security teams can:

- Accurately identify vulnerable systems
- Prioritize remediation efforts based on risk severity
- Allocate limited resources to address the most critical vulnerabilities
- Demonstrate compliance with regulatory requirements

## 3. Threat Detection and Response

Real-time monitoring of healthcare IoT assets provides the contextual understanding needed to detect and respond to threats effectively:

- Establishing behavioral baselines for connected devices
- Rapidly identifying behavioral anomalies indicating potential compromise
- Accelerating incident response through precise device identification
- Minimizing disruption to clinical operations during security incidents

#### 4. Network Segmentation

Strategic network segmentation—increasingly recognized as a critical security control—depends entirely on a thorough understanding of:

- Medical device inventories and characteristics
- Communication patterns between clinical systems
- Relationships between IT and IoT assets
- Critical systems requiring additional protection

Proper segmentation contains potential breaches, limiting malware propagation while preserving essential clinical workflows.

#### 5. Regulatory Compliance

Asset visibility directly addresses requirements specified in HIPAA, HITECH, NIST, CAF, DSPT, UK GDPR, and DPA regulations. Detailed asset inventories and monitoring capabilities demonstrate proper security controls and reduce regulatory risk.



**Current State of Healthcare IT & IoT Asset Visibility**

Despite its critical importance, achieving comprehensive asset visibility remains challenging for healthcare organizations for several reasons:

**Device Heterogeneity:** Healthcare environments incorporate thousands of devices from hundreds of manufacturers, each with unique operating systems, communication protocols, and security features. This diversity complicates unified management and visibility.

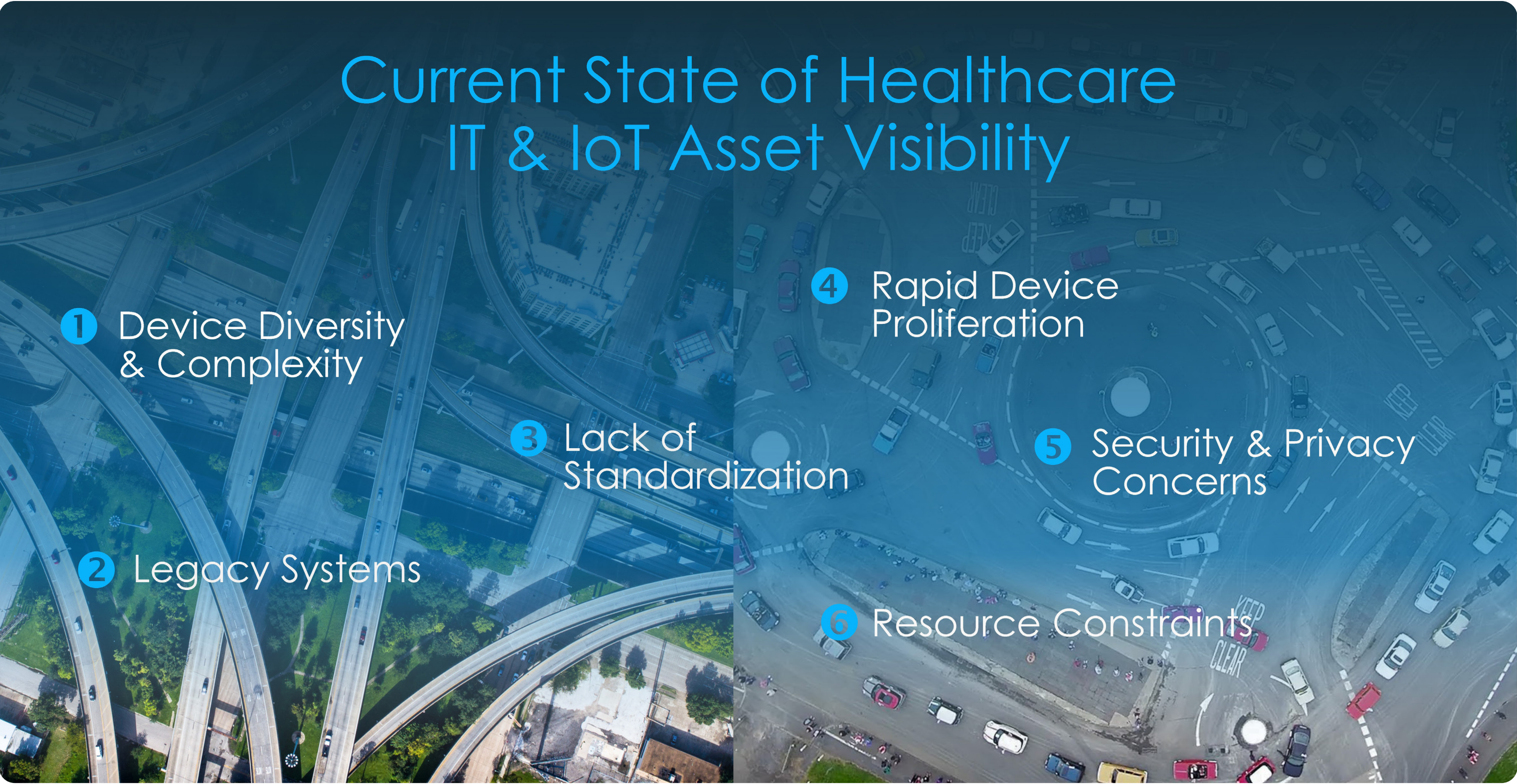
**Legacy System Integration:** Critical clinical systems often rely on outdated platforms not designed for integration with modern security tools, creating significant visibility gaps.

**Rapid Device Proliferation:** The accelerating adoption of connected technologies frequently outpaces healthcare IT departments' ability to track and manage devices, particularly without automated discovery capabilities.

**Security-Driven Isolation:** Some sensitive medical systems are intentionally isolated from broader networks for security reasons, creating potential blind spots in asset management.

**Resource Limitations:** Healthcare organizations frequently lack the specialized personnel and budget resources needed for comprehensive asset management programs.

Industry research confirms these challenges, showing that 30-50% of connected medical devices remain unmanaged in typical healthcare environments, creating substantial security and compliance risks.



## How Others Are Solving the Problem

Forward-thinking healthcare organizations are addressing these challenges through several key strategies:

**Automated Discovery Implementation:** Deploying advanced tools that continuously scan networks to identify and catalog all connected devices provides the foundation for comprehensive visibility. Modern solutions use techniques like deep packet inspection and machine learning to detect both known and previously unidentified devices.

**Network Segmentation:** Implementing strategic network segmentation isolates critical medical systems from general network traffic, enhancing both security and visibility while enabling more focused monitoring of specific network segments.

**Unified Management Platforms:** Adopting centralized asset management systems that integrate both IT and IoT device oversight provides comprehensive visibility across the organization while streamlining device tracking, update management, and compliance verification.

**Proactive Assessment Programs:** Conducting regular security audits and assessments—beyond those required for regulatory compliance—helps organizations identify and address gaps in asset visibility before they can be exploited.

**Collaborative Security Approaches:** Working closely with medical device manufacturers and cybersecurity vendors ensures that IoT devices are provisioned securely from implementation, improving integration with existing infrastructure and enhancing visibility.

## How Others Are Solving the Problem

- ✓ Automated Discovery Tools
- ✓ Network Segmentation
- ✓ Unified Asset Management Platforms
- ✓ Regular Audits & Assessments
- ✓ Collaboration with Vendors

Healthcare IT & IoT Asset Visibility:  
Where Are You?

Healthcare organizations typically fall along a continuum of asset visibility maturity:

**Initial Stage:** The processes for asset discovery and inventory are still largely manual, restricted, and siloed among departments. There are significant visibility gaps, and real-time awareness of connected devices is limited.




**Intermediate Stage:** A combination of manual processes and some automated discovery tools has achieved partial visibility. Specific device categories may have good visibility while others remain inadequately tracked.

**Advanced Stage:** Comprehensive, automated healthcare IoT asset discovery and inventory management systems are implemented, offering a unified view of all connected devices. Real-time monitoring facilitates immediate awareness of new devices and potential security issues.

Building a Resilient Healthcare  
Cybersecurity Foundation

For healthcare organizations dedicated to enhancing their security posture, asset visibility serves as the fundamental foundation. By creating thorough awareness of all connected devices—from conventional IT assets to specialized medical equipment—security teams can develop effective defenses that safeguard patient data, ensure clinical operations, and uphold regulatory compliance.

In a world where cyber threats are escalating and connected technologies are proliferating, healthcare organizations must prioritize this essential capability. With adequate asset visibility established, healthcare providers can confidently embrace the advantages of digital transformation while effectively managing the associated risks.

	 Basic	 Intermediate	 Advanced
Discovery and Inventory	Limited, siloed, manual	Partial, some automation	Automated, “single pane of glass”
Risk Management	Reactive undefined process	Partially defined, some prioritization	Proactive, prioritized, & measured
Threat Response	Siloed, reactive, highly manual	Some automation & playbooks	Defined, automated, & detailed playbooks
Analytics and Compliance	Time-consuming, delays, & penalties	Partially automation, point-in-time, costly	Fully automated & audit analytics

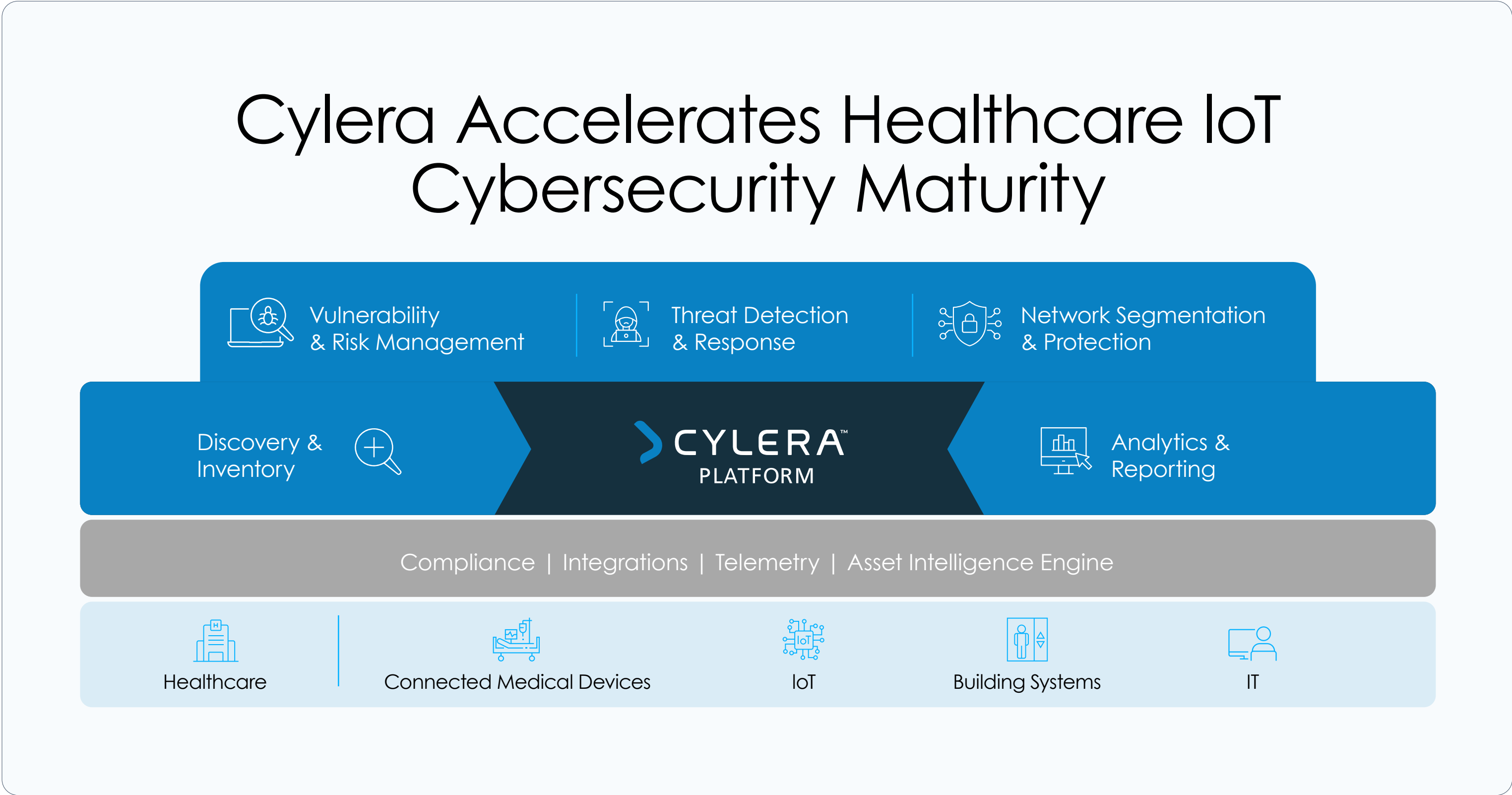
Chapter 2

# How Cylera Helps

Healthcare organizations require comprehensive solutions to tackle the complex challenges of inventory and asset management. By offering deep visibility into the device ecosystem, Cylera enables organizations to improve security, ensure compliance, and streamline their inventory management processes.

## Cylera Accelerates Healthcare IoT Cybersecurity Maturity

At the core of Cylera’s solution lies a hybrid approach that integrates strategically placed physical sensors with a powerful cloud-based platform. The sensors unobtrusively monitor the environment, capturing detailed data on a wide range of devices, including medical devices, connected IoT devices, and general IT components. This non-disruptive, agentless method is tailored to the sensitive nature of healthcare environments, avoiding any interruption to critical networks.



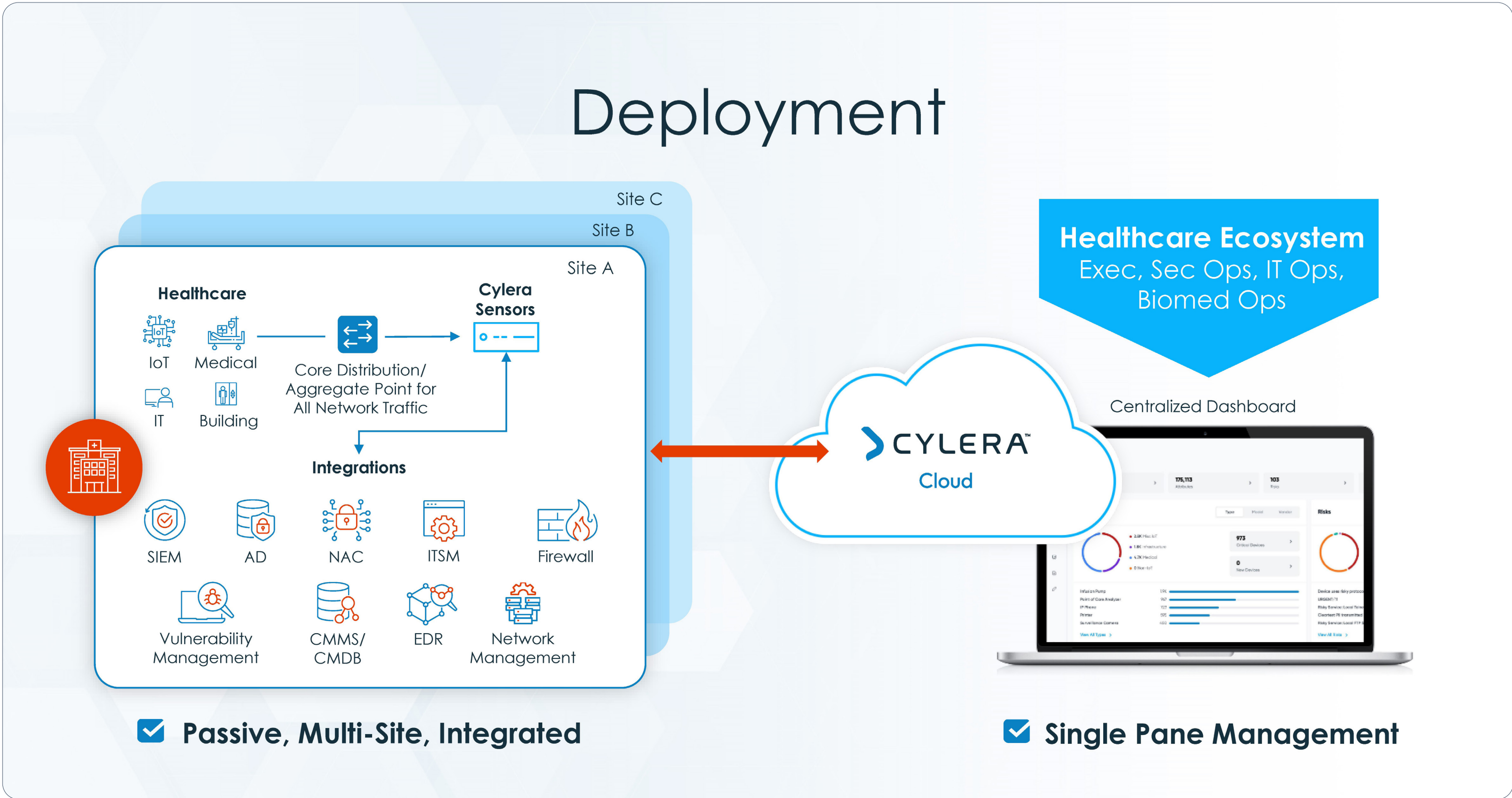
## Deployment

Cylera's intelligent cloud platform processes and analyzes data collected from sensors. By leveraging advanced machine learning algorithms and extensive healthcare domain knowledge, the platform automatically classifies devices into categories such as medical, infrastructure, miscellaneous, and enterprise IoT. This detailed classification allows organizations to gain a comprehensive understanding of their device inventory and how each device operates within the environment.

## Healthcare IoT Discovery & Inventory

The Cylera platform offers continuous, real-time monitoring of the device ecosystem. As new devices come online or unknown devices are introduced, Cylera promptly detects and classifies them, ensuring an always up-to-date inventory. This real-time visibility is essential for identifying potential security risks, misconfigurations, or unauthorized devices.

By analyzing network communications behavior, Cylera develops comprehensive profiles of each device's anticipated actions. This enables the system to detect atypical or potentially harmful activities, allowing organizations to proactively tackle security threats and ensure a secure device environment.



## Integration and Automation for Streamlined Management

The Cylera platform offers a variety of integrations to facilitate seamless information exchange with various systems and tools. These integrations empower organizations to enhance the device data collected by the platform and automate policy enforcement based on established rules. Connecting with existing security and management systems simplifies the inventory management process and improves the overall security posture.

The user-friendly cloud interface offers a centralized view of the entire device ecosystem. IT and security teams can easily navigate the inventory, access detailed device information, and take necessary actions to ensure security and compliance. The intuitive interface empowers users to make informed decisions based on real-time insights and comprehensive device visibility.

Moreover, Cylera seamlessly integrates with a wide range of existing security tools, including SIEMs, firewalls, NAC solutions, and vulnerability management platforms. This interoperability enables organizations to maximize their current investments while enhancing their overall cybersecurity posture and operational efficiency.

## Enabling Secure and Compliant Healthcare Environments

The Cylera platform is designed to address the unique challenges faced by healthcare organizations in managing their complex device inventories. Through its non-disruptive, comprehensive, and automated approach to device discovery and classification, the platform enables organizations to:

1. Gain complete visibility into their device ecosystem
2. Ensure accurate and up-to-date inventory records
3. Identify and mitigate security risks proactively
4. Streamline compliance with regulatory requirements
5. Optimize device utilization and management processes

This approach allows healthcare organizations to secure their devices, safeguard sensitive data, and concentrate on providing high-quality patient care. The blend of advanced technology, healthcare expertise, and a user-focused strategy positions Cylera as the perfect partner for tackling inventory management challenges and creating a more secure and compliant healthcare environment.

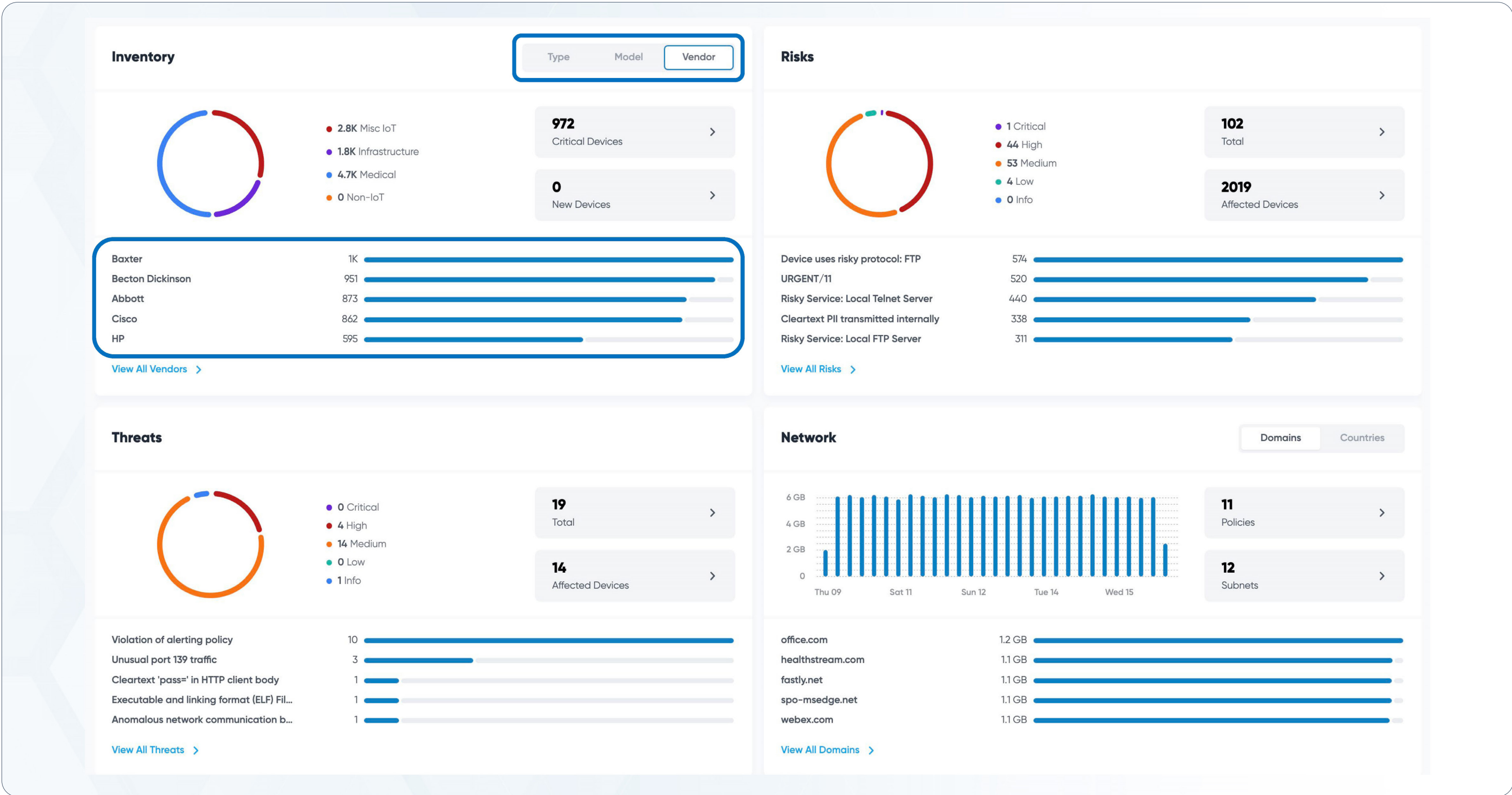
Chapter 3

# Platform Interface and Device Management

## Dashboard and Inventory Visualization

The central dashboard offers an intuitive, customizable interface. When you log in, you'll see a centralized hub that provides an immediate overview of your device inventory. By default, the dashboard organizes your devices by type, such as infusion pumps and point-of-care monitors, displaying them in based on frequency of occurrence. However, the capabilities of the dashboard extend far beyond this initial view.

With just a few simple clicks, you can easily switch between different perspectives, allowing you to analyze your devices by model or vendor. This flexibility makes it simple to quickly identify the most common device types, models, or vendors in the environment, facilitating data-driven decision-making for IoT infrastructure.



Device Information and Attribute Analysis

Diving deeper into the device categories, Cylera's dashboard provides comprehensive information instantly. Hovering over the inventory section reveals insights into all of the devices on your healthcare network, including:

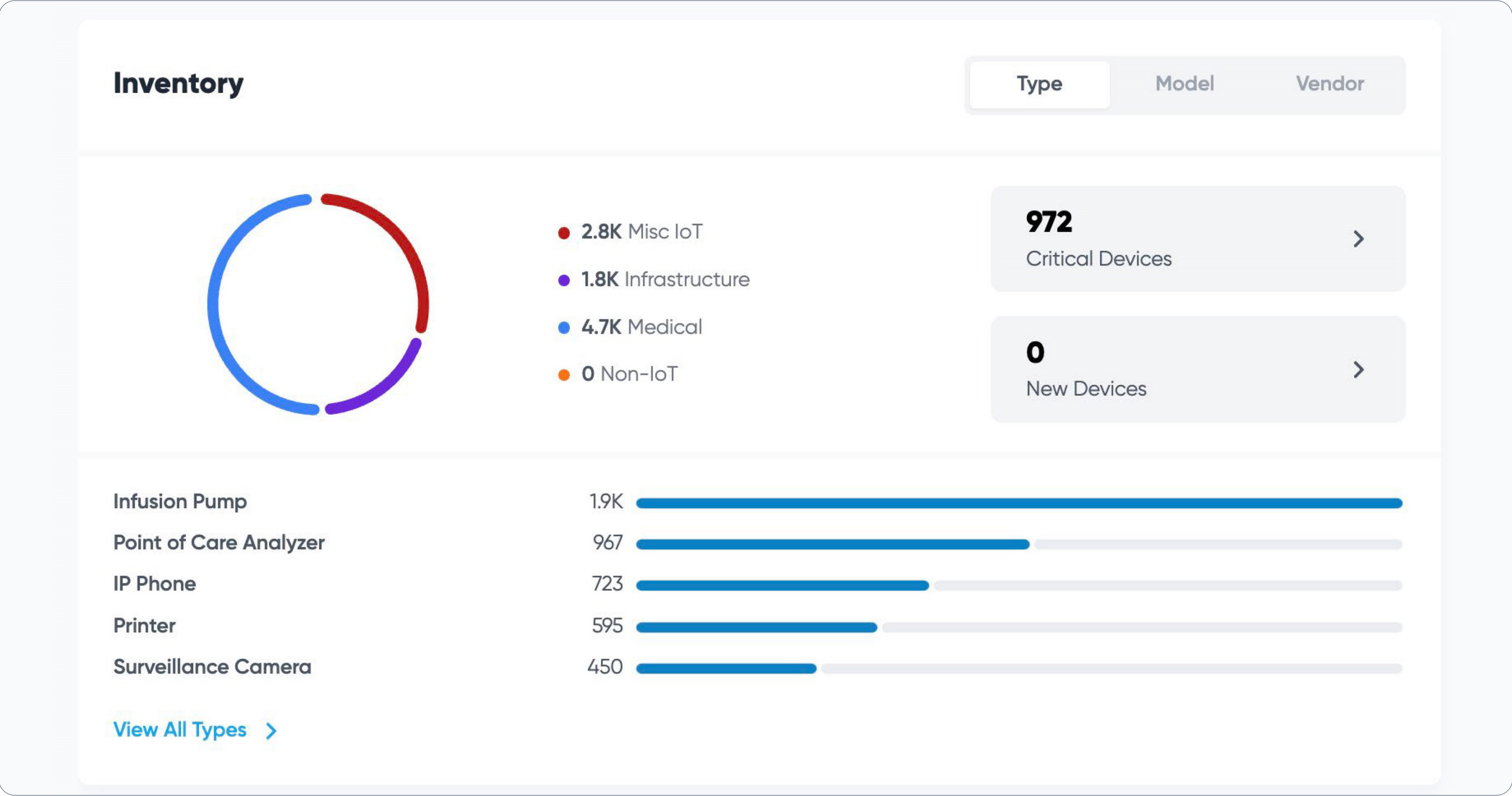
- **Connected medical devices**, such as infusion pumps, patient monitors, or imaging systems, such as MRI machines or CAT scanners
- **Infrastructure devices**, such as networking equipment and uninterruptible power supplies (UPSs), building management systems, which include environmental controls such as HVAC systems and smart thermostats, and security systems, which include devices such as surveillance cameras and access control systems
- **Miscellaneous IoT devices**, such as smart TVs or connected vending machines
- **Non-IoT devices**, such as traditional desktop computers or servers

But Cylera goes beyond simple device quantification. The dashboard highlights the criticality levels of devices that may need updates or patches to address vulnerabilities, ensuring that you can prioritize your remediation efforts. Additionally, a convenient counter

keeps you informed of new devices entering your environment, offering real-time visibility into your ever-evolving IoT landscape.

When it's time to explore your inventory in greater detail, Cylera's inventory management module is your

primary destination. Accessible with a simple click on any component or part of the dashboard graph, this module organizes your devices into groups by device type or lets you browse the entire device list.

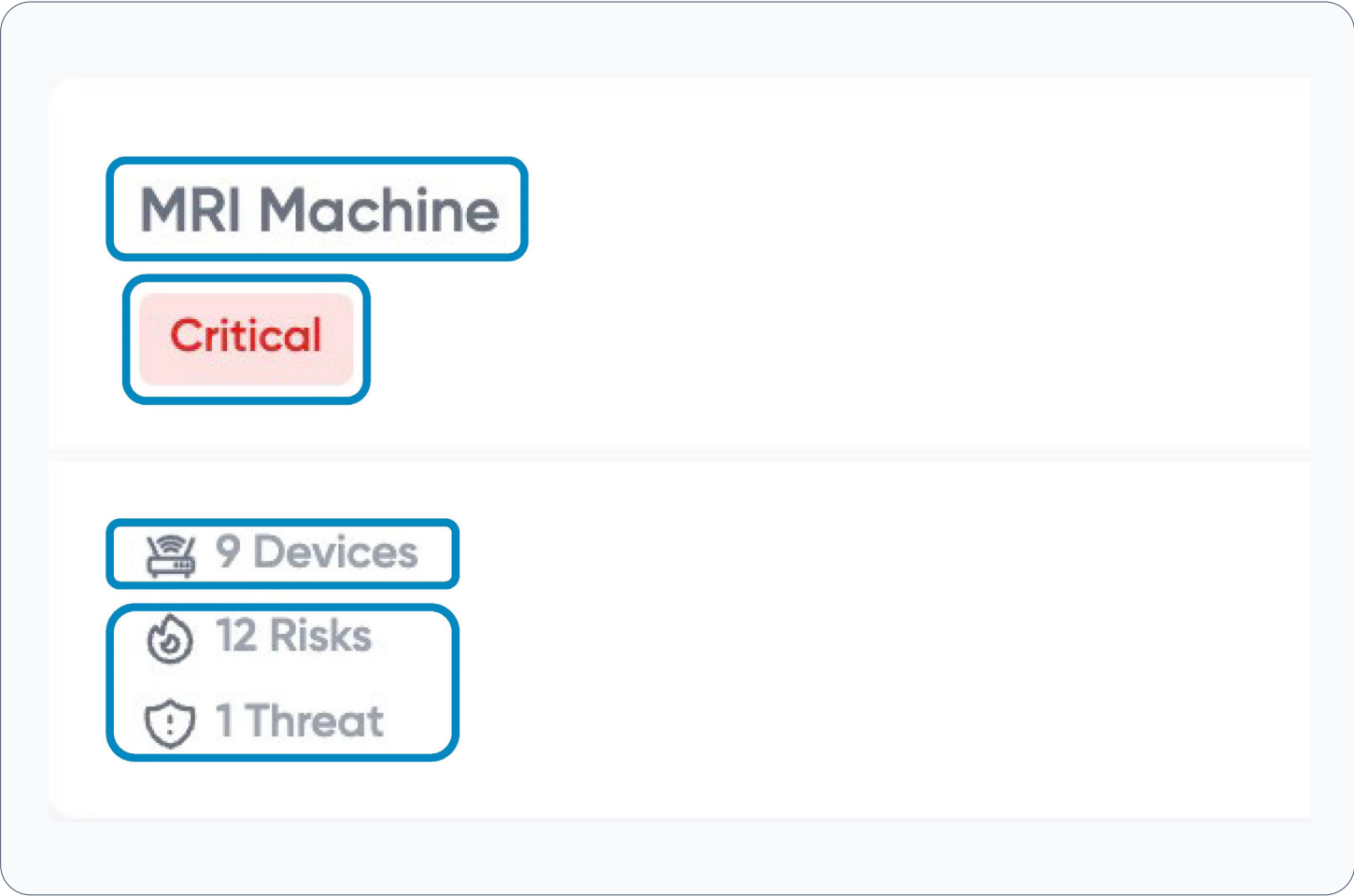
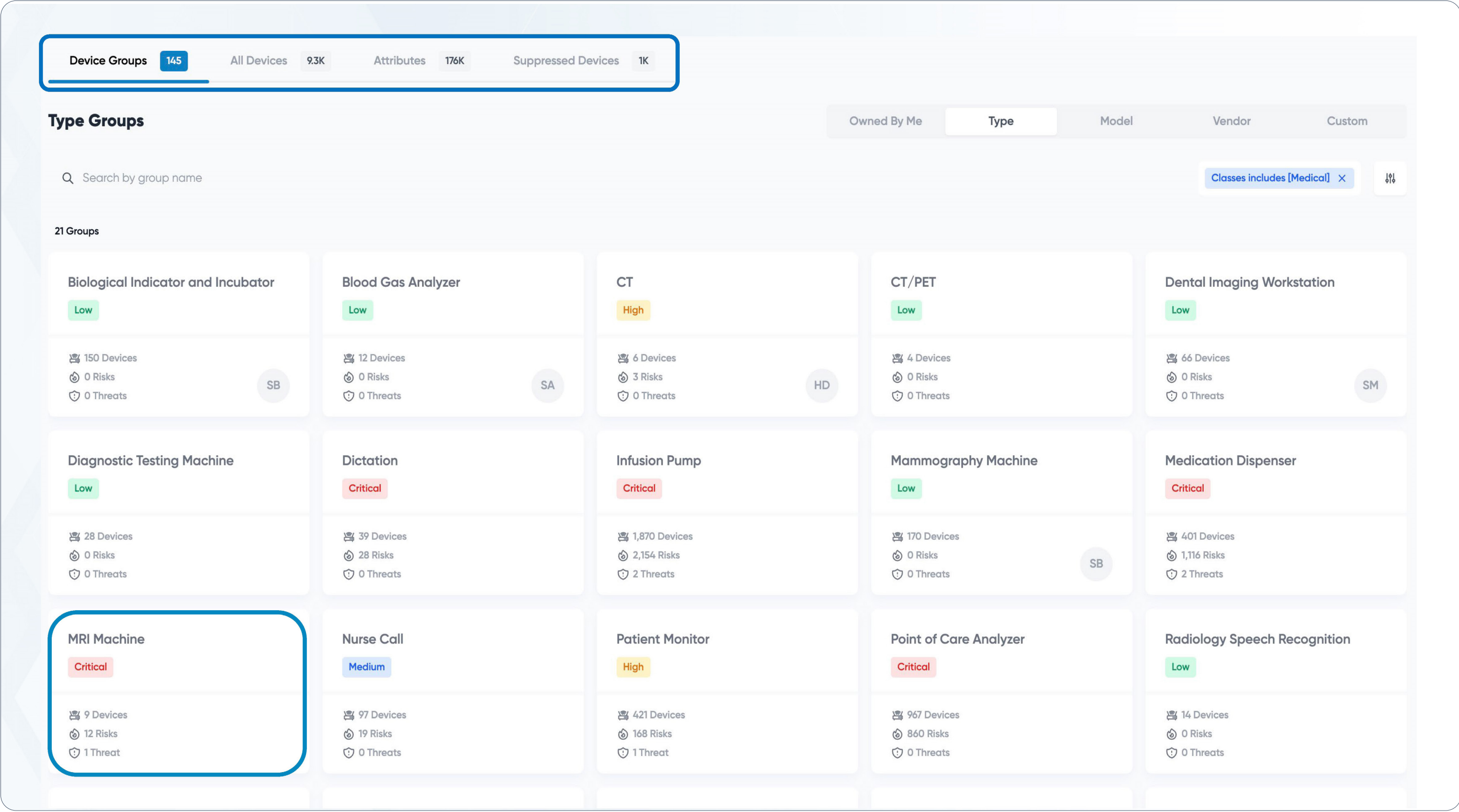


Cylera sets a new standard for device understanding with the introduction of “attributes” – extended information and details that enrich your knowledge of your devices. This data is meticulously gathered through continuous network traffic analysis and

seamless integrations with other systems, such as inventory management devices, network switches, and access points. With Cylera, you gain a comprehensive view of your devices, empowering you to make informed decisions.

Risk Assessment and Policy Management

To illustrate the granularity of Cylera's inventory management, let's examine a real-world example: a group of MRI machines. By selecting the MRI machine “card,” you can quickly identify the number of devices in the group and pinpoint any critical issues requiring immediate attention.



Zooming in on a specific device, such as the Philips Archiva dStream MRI machine, provides comprehensive device details, including essential information like device classification, IP address, and MAC address, as well as hosting details and network connection information. Additionally, the platform offers valuable insights into the device's utilization, highlighting its first detection and most recent presence on the network.

A proactive approach to risk management brings critical insights and areas of interest to the forefront. The platform can identify if a device is running potentially vulnerable services, such as an HTTP or SSH server, or handling sensitive electronic patient health information. It also flags outdated firmware components that may need updating to maintain a strong security posture.

The attributes panel functions as a comprehensive repository of supplementary information, going beyond what can be derived from network traffic analysis alone. By seamlessly integrating with other systems, Cylera enhances the data it offers, providing you with a 360-degree view of your devices.

Device Group: MRI Machine

Search by IP address, MAC or Hostname

Export

9 devices found

IP Address	Class	MAC Address	VLAN	Hostname	Risk ↓	Type	Model	Insights	Last Seen	Vulnerabilities
10.20.211.183		d5:27:29:df:e0:43	751	RNWKHZEEIG	Critical	MRI Machine	Philips Achieva dStream MRI		01/21/2025 @ 3:35 PM	4
10.30.150.250		bb:b0:71:cf:30:0a	311	MOGJBMHEAG	High	MRI Machine	Philips Achieva dStream MRI		01/21/2025 @ 3:35 PM	1
10.50.205.201		cc:32:6d:e2:49:cd	110	RAVBWYXGRB	Medium	MRI Machine	Philips Achieva dStream MRI		01/21/2025 @ 3:35 PM	1
10.20.199.193		a4:2e:08:ef:a6:52	893	PFZZALKUDW	Medium	MRI Machine	Philips Achieva dStream MRI		01/21/2025 @ 3:35 PM	1
10.50.150.200		99:1e:25:83:59:01	110	XRLHLWXZQY	Medium	MRI Machine	Philips Achieva dStream MRI		01/21/2025 @ 3:35 PM	1
10.40.200.150		cb:57:d0:a6:f4:e3	477	GBIFVAXEOO	Medium	MRI Machine	Philips Achieva dStream MRI		01/21/2025 @ 3:35 PM	1
10.30.199.233		e6:b5:05:0f:8c:ad	77	WSRDDDCLOQ	Medium	MRI Machine	Philips Achieva dStream MRI		01/21/2025 @ 3:35 PM	1
10.20.255.3		02:3b:d2:40:a5:81	751	VAEISDSAEC	Medium	MRI Machine	Philips Achieva dStream MRI		01/21/2025 @ 3:35 PM	1
10.30.146.42		3d:e3:b3:23:62:e7	652	WRXNOHCKDR	Medium	MRI Machine	Philips Achieva dStream MRI		01/21/2025 @ 3:35 PM	1

Scrolling further through the device details reveals associated risks, allowing you to prioritize updates and patches to strengthen your inventory. Cylera also presents information about policies linked to the device, highlighting the platform’s capability to encompass multiple aspects of device management and security.

Network Communication Analysis

Cylera empowers you to optimize your IoT infrastructure by providing valuable insights into device usage patterns. The platform highlights utilization information, comparing a device’s active hours with its available hours. This data can help you identify potential utilization gaps or capacity issues, enabling you to make informed decisions about resource allocation.

The Cylera platform provides detailed communication mapping, visually representing the connections between the device in question and other devices it interacts with, as well as the protocols utilized. By exploring the “learn more” section, you can access granular details of network traffic, including currently used services and potential external connections categorized by country or domain. This level of visibility is vital for identifying security risks and ensuring compliance with data protection regulations.

While understanding network communications offers valuable insights into how devices interact logically, healthcare organizations must also remain aware of where these devices are physically located within

their facilities. This spatial context adds another critical dimension to comprehensive asset management by linking digital identities with physical locations.

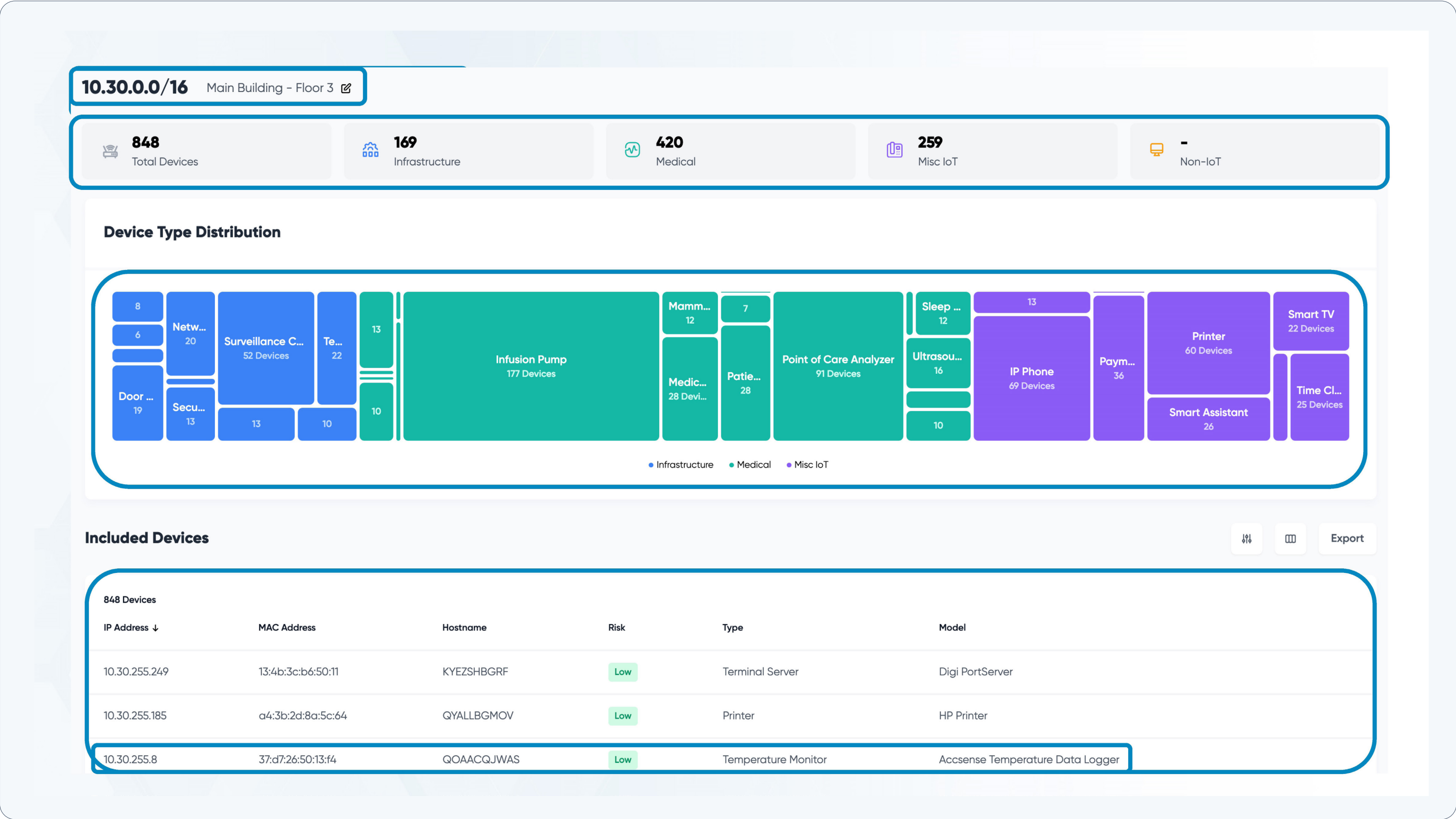


Environmental Context and Location Mapping

Understanding the physical context where your devices operate is crucial for effective management. This approach entails collaborating with healthcare teams to gain a comprehensive view of your devices within the environment, enabling you to visualize them from a subnet or VLAN perspective and observe their distribution across various floors and buildings.

Drilling down into a specific location, such as “main building floor three,” unveils a color-coded map that illustrates device distribution across classifications (medical, infrastructure, miscellaneous IoT) and presents a list of devices that can be dynamically reorganized based on the device type distribution. This intuitive representation empowers you to grasp the layout and composition of your IoT ecosystem at a glance.

Cylera enhances its monitoring capabilities beyond your network boundaries, highlighting potential external communication channels. The platform creates a geographic map of countries to which a device may connect, offering a visual representation of its communication footprint. You can also view this information by domain, showing the specific devices that interact with external services like WebEx.com.



This level of visibility is vital for identifying potential data leakage points and ensuring that your devices communicate only with authorized external entities.

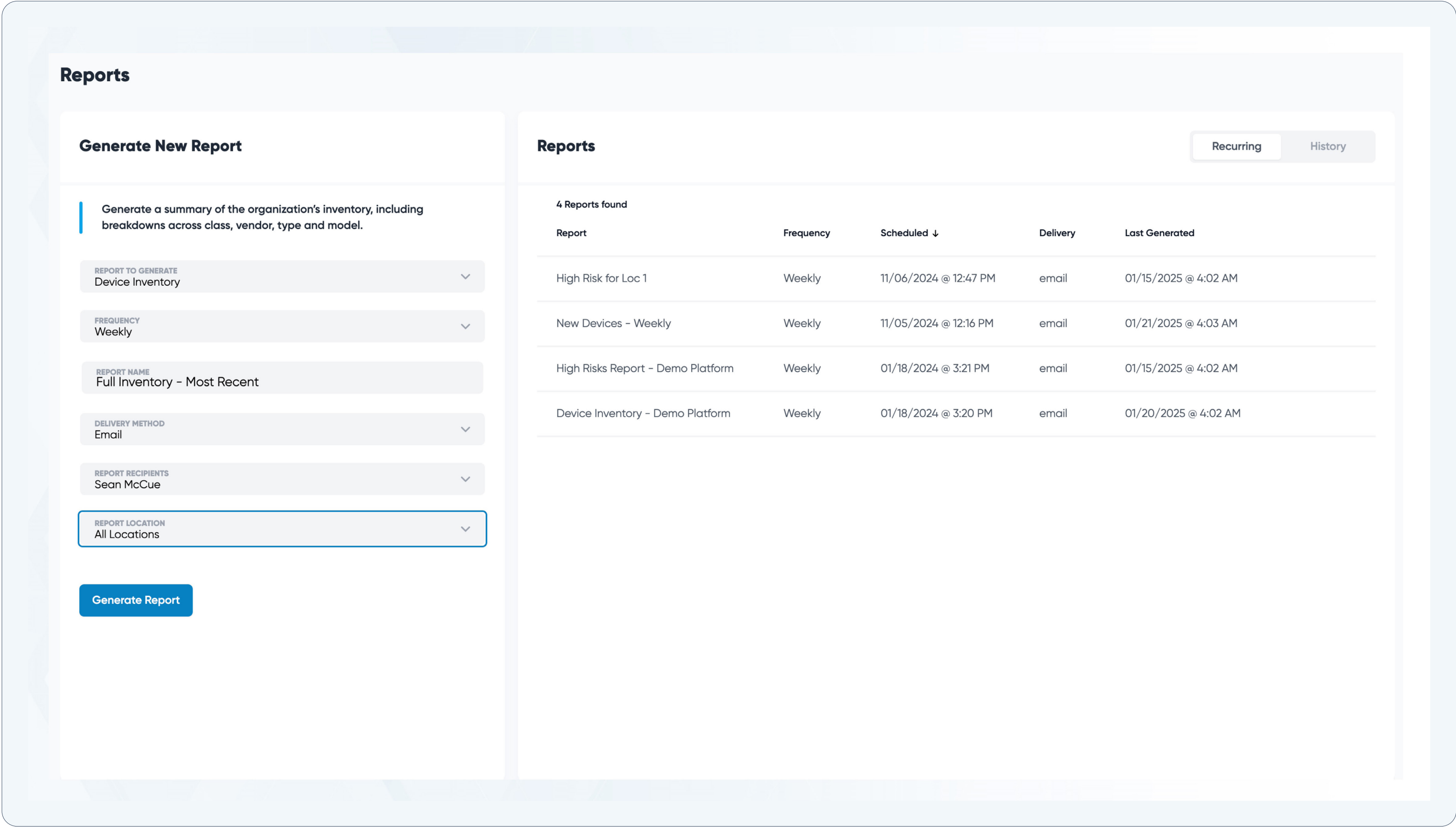
Monitoring external communications strengthens your security posture and maintains compliance with industry regulations.

### Reporting and Compliance Capabilities

Sharing insights and regularly monitoring your IoT environment is easy with Cylera's powerful reporting capabilities. The reporting engine enables access to historical reports and allows for establishing recurring, scheduled reports tailored to your specific needs.

Creating a recurring report is a straightforward process. Just select the desired report type (for example, an inventory report), choose the frequency, assign a meaningful name, configure email delivery preferences, select recipients, and specify the locations to include. The system delivers reports directly to your inbox, providing a comprehensive overview of your device inventory, risk assessment, and device distribution across all your locations.

The Cylera platform is transforming how healthcare organizations secure and manage their connected devices. With its comprehensive approach, deep device intelligence, and seamless integration capabilities, Cylera enables organizations to protect patient data, enhance device performance, and ensure the smooth delivery of care.



The interface capabilities discussed above exemplify the practical application of healthcare IoT security principles. These technical features offer significant organizational benefits that tackle the challenges

outlined at the start of this guide. Let's explore how these capabilities together enhance healthcare cybersecurity operations.

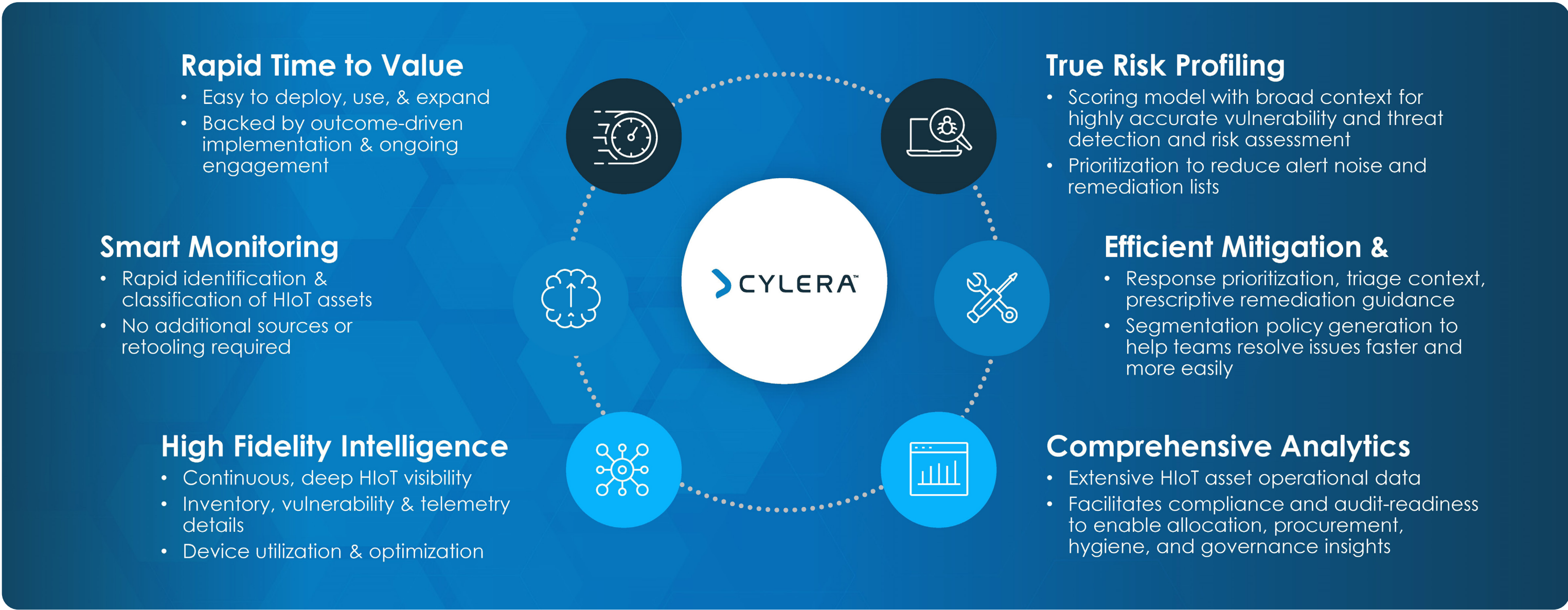
# Unique Healthcare IoT Asset Intelligence and Security Benefits

- At the heart of the Cylera platform lie five core capabilities that address the unique challenges of healthcare IoT and medical device cybersecurity:
- 1. Asset Discovery and Inventory:** Cylera provides comprehensive visibility into all connected devices, creating a comprehensive and always-up-to-date inventory.
  - 2. Vulnerability and Risk Management:** The platform's advanced risk profiling delivers precise, contextual assessments, enabling organizations to prioritize and address vulnerabilities effectively.
  - 3. Threat Detection and Response:** Cylera's advanced threat detection, combined with actionable remediation guidance, allows teams to swiftly identify and neutralize potential security incidents.
  - 4. Network Segmentation and Protection:** By generating automated network segmentation policies and integrating with existing security tools, Cylera helps isolate risky devices and safeguard sensitive data.

**5. Analytics and Reporting:** The platform's robust analytics provide invaluable operational insights, streamlining compliance efforts and informing device management decisions.

Effective healthcare IoT security solutions must provide rapid time to value. The Cylera platform accomplishes

this through intuitive design and implementation strategies focused on healthcare outcomes. The platform's monitoring technology ensures continuous visibility into the healthcare IoT landscape, while contextual risk profiling minimizes alert fatigue and prioritizes remediation efforts.



# Why Customers Choose Cylera

Comprehensive healthcare IoT security solutions deliver several key benefits to healthcare organizations:

- 1. Enhanced Patient Safety:** Thorough device visibility enables prompt identification and remediation of vulnerabilities that could impact clinical systems and patient care.
- 2. Streamlined Operations:** Automating device discovery and management reduces manual effort and improves team collaboration between security, IT and clinical engineering departments.
- 3. Regulatory Compliance:** Detailed device inventories and security monitoring help satisfy requirements from HIPAA, HITECH, and other healthcare regulatory frameworks.
- 4. Operational Efficiency:** By reducing time spent on manual device tracking and vulnerability management, healthcare staff can focus more resources on patient care initiatives.

The Cylera platform is currently implemented in healthcare organizations across the United States and United Kingdom, including in NHS facilities within both NHS England and NHS Scotland. When properly

deployed, healthcare IoT security solutions enable organizations to navigate the evolving cybersecurity landscape while maintaining focus on their primary mission: delivering quality patient care.





Cylera provides the easiest, most accurate, and extensible platform for healthcare IoT asset and intelligence and security to optimize care delivery, service availability, and cyber defenses. The platform accurately discovers, categorizes, assesses, and monitors known and unknown IT, IoT, and connected medical devices with high fidelity to deliver unparalleled asset inventory, vulnerability and risk management, threat detection and response, network segmentation and protection, analytics and reporting, and compliance support. The solution offers rapid implementation and works with other popular IT and healthcare solutions to allow organizations to advance cyber program maturity, increase operational efficiency, mitigate cyber threats, and enable compliance audit-readiness.

