

5 Critical Insights for Securing & Optimizing Medical Devices



Table of Contents

Overview	3
Understanding Your Medical Device Security Maturity Level	4
Actionable Insight 1: Visibility: Unobtrusive and Comprehensive	6
Actionable Insight 2: Contextual Information: The Key to Rapid Threat Detection and Response	8
Actionable Insight 3: Risk Prioritization	10
Actionable Insight 4: Data Enrichment	12
Actionable Insight 5: Asset and Process Optimization	14
Key Takeaways	16

Overview

By **Timur Ozekcin**, Co-Founder & CEO, Cylera

Drawing on extensive experience with hospitals and healthcare systems worldwide, Cylera has identified five essentials for securing and optimizing healthcare IoT and connected medical devices. These insights form the foundation of a cybersecurity and resilience strategy that enhances patient safety, compliance, and operational efficiency. People must know and understand how to build a cybersecurity and resiliency plan for their medical IoT devices.

1. Visibility

Developing a robust cybersecurity and resilience strategy for medical IoT devices starts with comprehensive visibility. You can't defend what you can't see.

2. Contextual Information

Contextual information includes understanding what the device does, who it belongs to, and its primary operating parameters. Establishing these patterns enables device security without compromising patient safety or decreasing revenue streams.

3. Risk Prioritization

Unlike traditional patch management for Windows desktops and servers, not all healthcare IoT or connected medical devices are equal, even if they

have the same type and function. The device's role and location within the hospital must be considered. Is the device in the ER, or in a rarely used exam room in an outlying clinic? Surfacing and triaging risks based on this context enables more efficient risk remediation.

4. Data Enrichment

Understanding how to leverage data effectively is crucial for optimizing medical device security. Combining information from a patient record system with data about a particular device and other sources is key to understanding how to assess, secure, and optimize a specific device. In addition, you need to determine both patient care delivery and business impacts, as well as whether you can use the data to make decisions related to procurement or vendor selection.

5. Team Collaboration & Process Optimization

Promoting collaboration, streamlining processes, and optimizing teamwork enables timely and appropriate decisions that prioritize patient care, maintain revenue streams, and ensure the smooth operation of healthcare facilities.

Without effective communication between security and biomedical engineering teams, security staff may not fully grasp the intricacies of healthcare IoT and connected medical devices, leading them to hastily take devices offline without considering patient care consequences.






Understanding Your Medical Device Security Maturity Level

Where does your organization fall on the maturity spectrum for securing connected medical devices? At Cylera, we define these maturity levels as follows:

Beginning the Journey
“Hospital A” is just starting out. They have limited visibility into their devices. Teams operate in silos, with minimal collaboration. Typically, the most significant hurdle

teams in this type of hospital face is that they have no automated tools to provide device information. Manual processes strain limited financial and personnel resources. However, Cylera can help. The Cylera platform’s automated asset discovery, and inventory capabilities can alleviate this burden, enabling hospitals to optimize their already scarce resources more effectively.

Connected Medical Devices: What Cylera Sees Where Are You?

	 Hospital A	 Hospital B	 Hospital C
IIoT Discovery and Inventory	Limited, siloed, manual	Partial, some automation	Automated, “single pane of glass”
Risk Management	Reactive, no prioritization, undefined process	Ad-hoc, partially defined, some prioritization	Proactive, fully defined, prioritized, and measured
Threat Response	Limited, siloed, reactive, highly manual.	Partially defined, some automation, some remediation playbooks	Fully defined, highly automated, detailed remediation guidance, efficient
Analytics and Compliance Audit-Readiness	Manual, time-consuming, point-in-time, audit delays and penalties	Partially automated, point-in-time, costly	Fully automated, rich analytics and continuous audit-readiness

Making Progress
“Hospital B” is progressing in the right direction. They have implemented automation and are integrating various systems. They gain valuable insights into their supply chain with a clear understanding of their devices and vendors. Grouping devices enables them to make informed assessments about potential threats to their environment. However, partial automation yields incomplete results. Some manual effort remains necessary, although this type of hospital typically has far fewer manual systems and processes than Hospital A.

Achieving Maturity

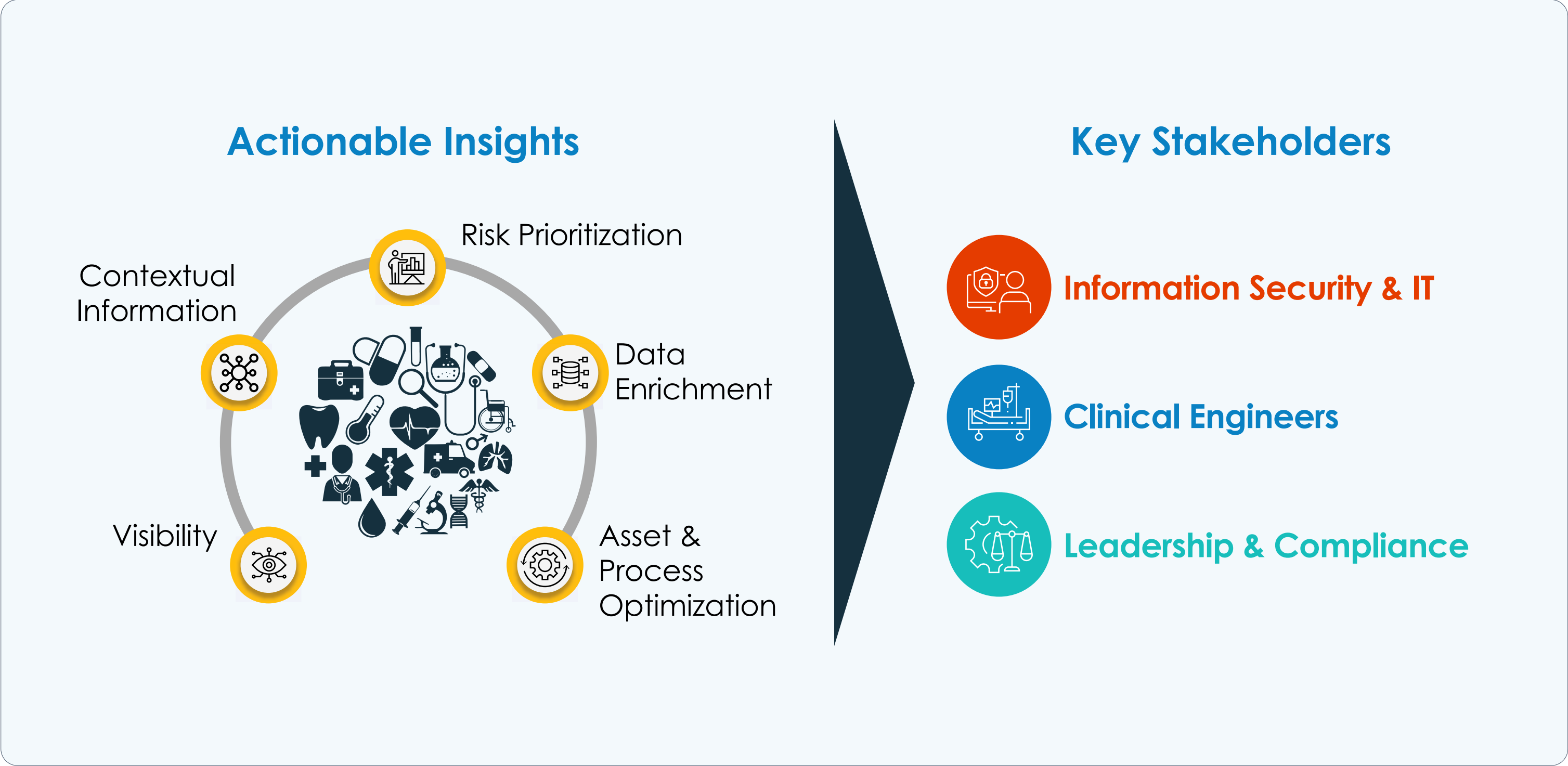
“Hospital C” exemplifies best practices. They have fully automated processes and harness analytics to guide cybersecurity, business, and procurement decisions. They have a single pane of glass that brings together diverse teams across the organization, fostering collaboration and enabling data-driven decision-making. Hospital C represents the ideal state that the vast majority of hospitals aspire to achieve.

What’s Your Goal?

Consider where your organization currently stands on this spectrum. What is your maturity level, and where do you envision being in the next 6 to 18 months?

By setting clear objectives and working towards them, you can progressively enhance your organization's security posture and better protect your healthcare IoT and connected medical devices. Cylera is committed to supporting healthcare delivery organizations at every stage of their journey, offering tailored solutions to enhance visibility, reduce cyber risks and threats, streamline processes, and ensure the safety of patients and healthcare data.

You can see a 40% improvement in medical device security maturity by aligning key stakeholders to insights.



Importance of Stakeholder Alignment

Aligning key stakeholders with actionable insights is crucial for achieving optimal results. Information security, clinical engineers, leadership, and compliance teams require access to the information gathered from contextual data, risk prioritization, and asset and process optimization to make informed decisions.

Many cybersecurity or compliance tools are acquired to serve a single team, which can leave other groups without a holistic view of the situation. At Cylera, our goal is to provide a consolidated view that gives all stakeholders the same critical insights. With everyone on the same page, the entire organization can make timely decisions based on a shared understanding.

Actionable Insight 1

Visibility: Unobtrusive and Comprehensive

Prioritizing Uninterrupted Operations

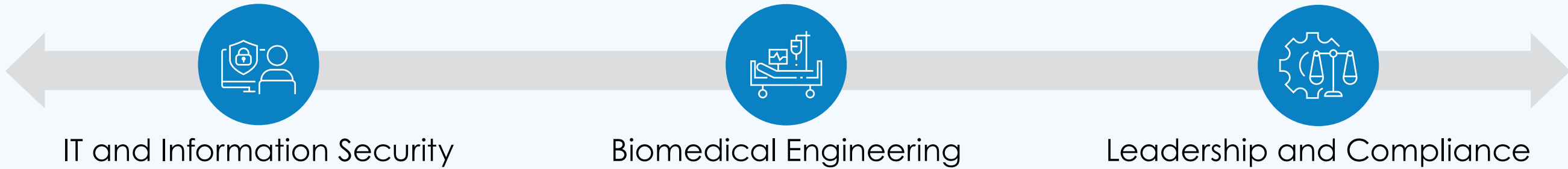
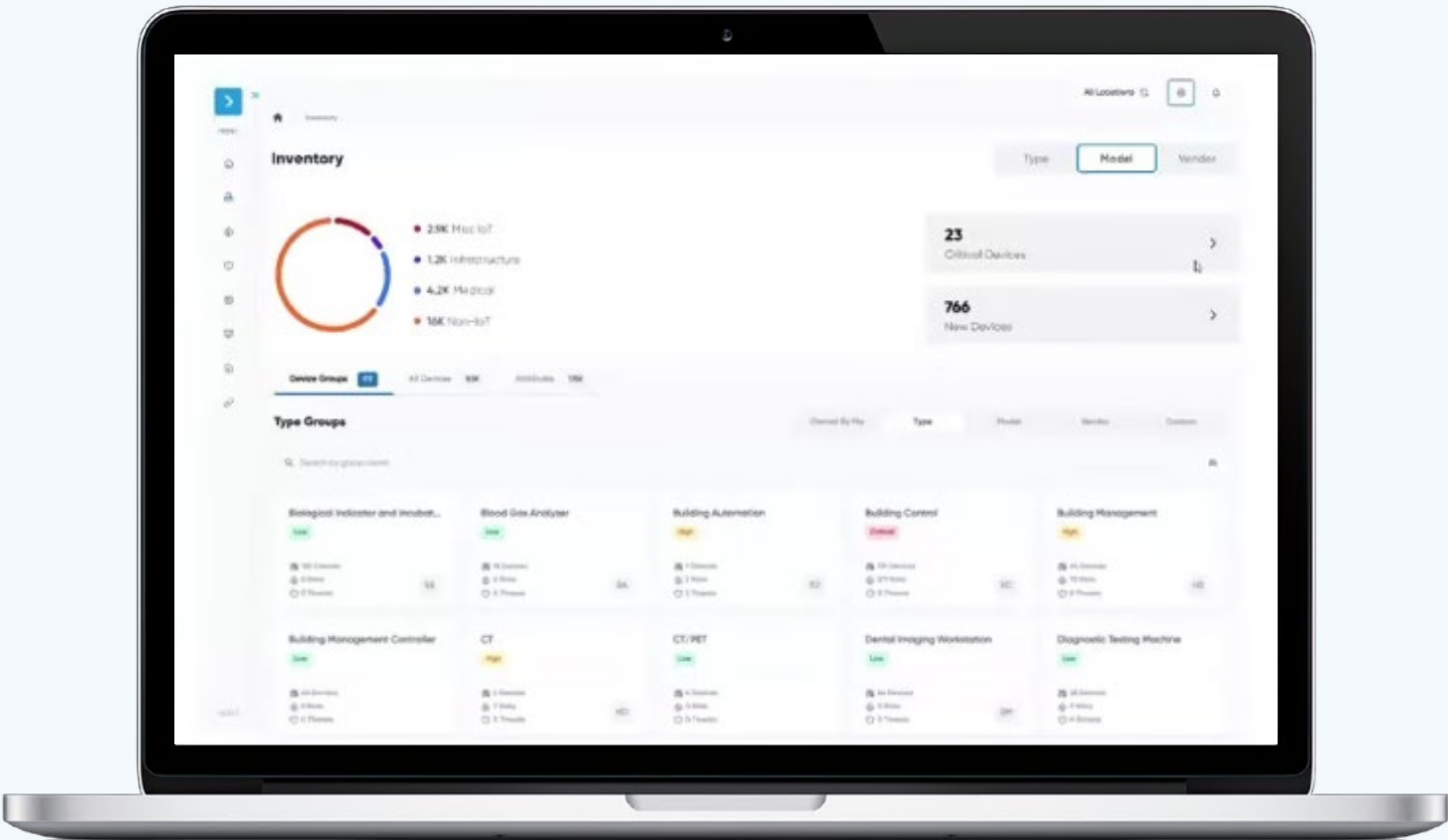
At Cylera, we understand the importance of monitoring medical devices without disrupting their operation. Unlike many traditional IT security providers, the team of healthcare experts at Cylera clearly understands how scanning medical devices can negatively affect the device and potentially disrupt patient care delivery.

The Cylera team also understands the negative effects that can result if a device is taken offline while in the middle of a medical procedure or when being used to monitor patient health or medication delivery. Therefore, the Cylera approach is to passively discover and obtain visibility into all healthcare IoT and connected medical devices on the network. Cylera's approach delivers real-time visibility without disruption, ensuring comprehensive device discovery and inventory without compromising patient care and safety or disrupting operational continuity.

1

Visibility

- ✓ Agentless, passive, non-disruptive discovery
- ✓ Auto-classification and grouping of devices
- ✓ Deep HIoT device intelligence
- ✓ Identification of both known & unknown devices



Overcoming Inventory Inaccuracies

One significant challenge in managing medical device security is maintaining an up-to-date asset inventory for all the healthcare IoT and connected medical devices currently on the network and in use. Hospital IT, information security, and biomedical teams are frequently forced to rely on outdated spreadsheets that fail to account for recently added devices. These aging records do not reflect the current medical device landscape, making assessing and mitigating potential cyber vulnerabilities, risks, and threats difficult.

Understanding Where You Have Risk

Comprehensive visibility is the foundation of risk management. It enables hospitals to identify vulnerable devices, prioritize remediation, and optimize investment decisions. Knowing which devices are up-to-date—and which require immediate attention—reduces security gaps and ensures compliance.

Deep device intelligence offers valuable insights that inform critical business decisions. For example, if a device's behavior shows it only operates four hours per day and is in a remote clinic, you could turn off those devices at night. This would result in reduced power consumption and cost savings.

Identifying All Connected Devices, Both Known and Unknown

Identifying all known and unknown healthcare IoT and connected medical devices on the hospital network is essential. Security teams must be alerted when any rogue or unknown IT device connects to the network. They must also understand what devices are expected to regularly connect and disconnect to maintain a secure environment.

How Teams Benefit From Visibility

Comprehensive healthcare IoT and connected medical device visibility provides advantages to multiple teams, including IT, information security, biomedical engineering, leadership, and compliance. In healthcare settings, IoT devices extend beyond medical equipment and include building controls, video cameras, and more. To comprehensively assess risk across the entire environment, it's vital to provide visibility into these assets.

IT and Information Security: Joint Visibility Strengthens Security

For IT and information security professionals, understanding connected medical devices enables the development of robust detection rules and proactive risk mitigation strategies tailored to specific devices.

Comprehensive medical device visibility also allows your technical staff to prioritize threats efficiently and bolster your organization's security.

Biomedical Engineering: Streamlining Device Management

Visibility enables biomedical engineering teams to maintain accurate asset inventories, reduce device loss, and efficiently monitor calibration and preventive maintenance schedules. Device visibility also provides precise information on which medical devices are approaching maintenance dates or end of life, making upkeep more efficient.

Leadership and Compliance: Enabling Informed Decision-Making

Device visibility gives leadership teams insights to inform crucial business decisions, such as optimizing device procurement based on current usage data. It also simplifies compliance reporting.

Actionable Insight 2

Contextual Information: The Key to Rapid Threat Detection and Response

The more contextual information a healthcare delivery organization has about its healthcare IoT and connected medical devices, the better equipped it is to rapidly identify and contain cyber threats. Security teams can significantly improve their threat detection and response times by understanding key medical device characteristics and monitoring for behavioral changes.

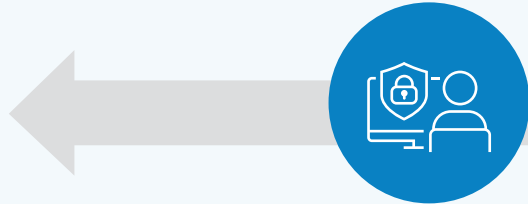
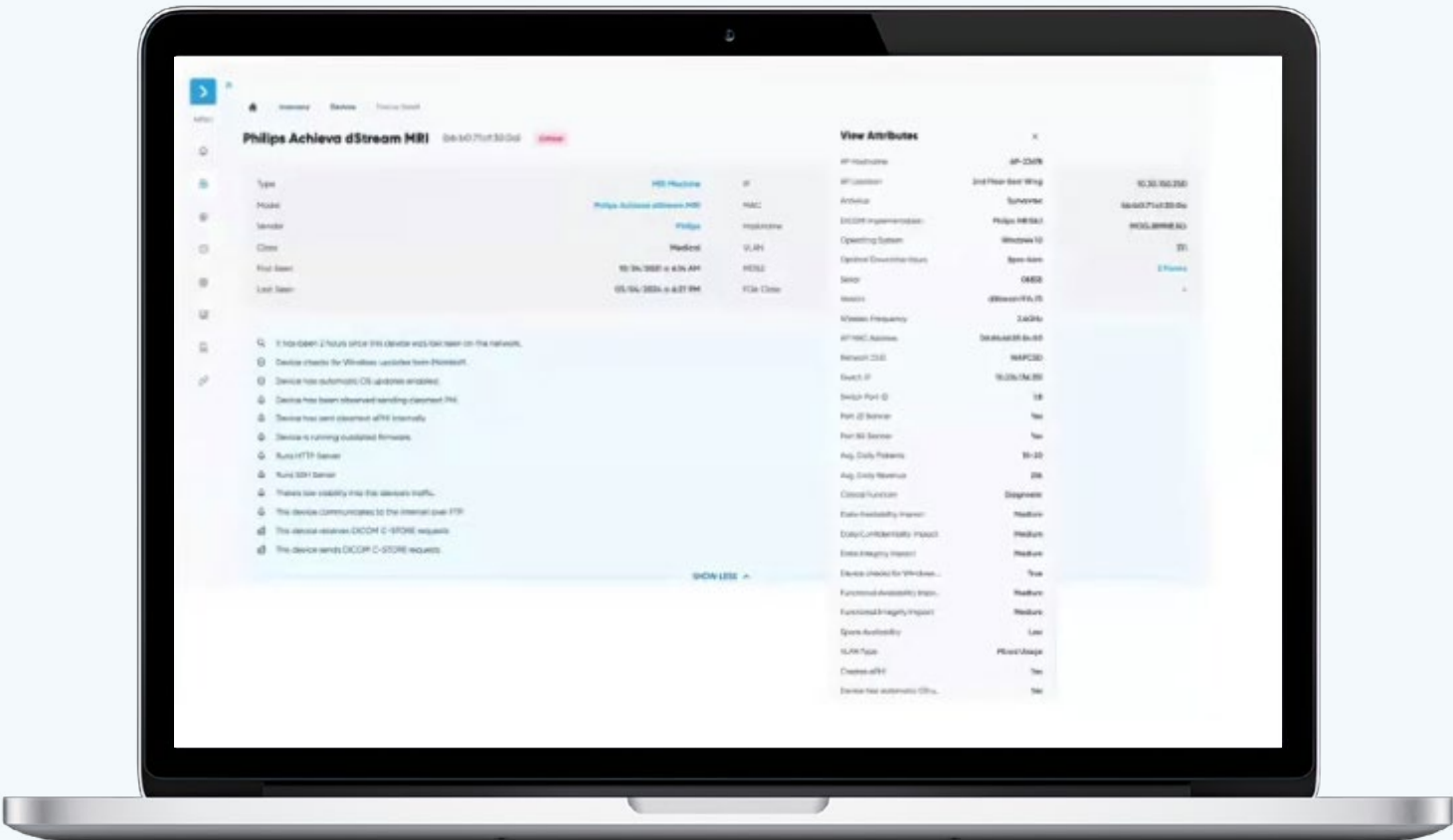
Device Identification

Quickly detecting and responding to threats is essential, particularly when dealing with fast-spreading threats like ransomware. If only a MAC address and an IP address are known, the mean time to detect and respond increases. The longer response is delayed, the more the threat can propagate and spread laterally throughout the environment.



Contextual Information

- ✓ Device identification
- ✓ Device classification (MRI machines, infusion pumps, manufacturer, model, and operating system)
- ✓ Behavioral analysis



IT and Information Security



Biomedical Engineering



Leadership and Compliance

Device Classification

The more contextual information you have about your healthcare IoT and connected medical devices, the faster you can identify and contain potential security incidents, minimizing damage. For example, having a full understanding of how a particular device, such as an MRI machine, operates within the environment, including the best times to take it offline and whether it is currently in use, will allow compensating controls and mitigations to be put in place much more quickly compared to dealing with an unknown device. The key steps are identifying the device, understanding what it is, who makes it, and whether any known vulnerabilities are associated with its operating system.

Behavioral Analysis

Surfacing behavioral anomalies early is also crucial for proactive security. If a device has been operating in the same manner for 90 days but suddenly exhibits a behavior change, it could indicate potentially malicious activity. These types of issues should be identified before they become problems.

It's essential to extend threat monitoring beyond servers and workstations. While these are often the focus of traditional digital forensics and incident response

(DFIR), IoT devices like medical equipment and security cameras can serve as entry points for attackers or conduits for lateral movement. Contextual information about these devices strengthens an organization's security posture and DFIR capabilities, as well as supports adherence to healthcare industry compliance standards.

How Teams Benefit From Contextual Information

Contextual information about medical devices significantly benefits various teams within healthcare organizations. By leveraging these insights, groups can enhance security, optimize device performance, and meet compliance goals more effectively.

IT and Information Security: Implementing Tailored Security Measures

Contextual information enables IT and information security teams to implement tailored security measures. Detailed insights into how a medical device operates enable security practitioners to develop customized compensating controls, data sets, and rule sets. With this level of understanding, creating controls to prevent and mitigate cybersecurity issues becomes easier.

Biomedical Engineering: Ensuring Devices are Up-to-Date

Biomedical engineering teams use contextual information, such as vulnerabilities and details on how a device is used and how frequently, to ensure that the devices operate effectively and are up to date with the latest patches and remediations. This helps maintain a secure and efficient medical device ecosystem.

Leadership and Compliance: Satisfying Audits and Gaining Insights

Leadership and compliance teams leverage contextual information to satisfy audit requirements with ease. Moreover, the business insights from this data serve as a compass, guiding the organization's strategic direction and decision-making process.

Actionable Insight 3

Risk Prioritization

Not every risk or healthcare IoT device is the same, nor does each device have the same function within the environment. As a result, being able to identify vulnerabilities and at-risk connected medical devices that can negatively impact secure, reliable patient care is crucial.

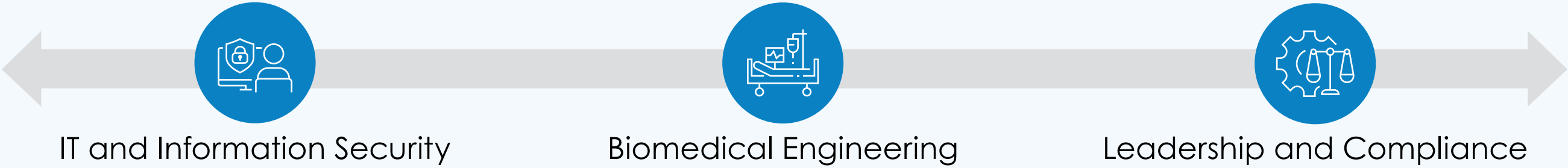
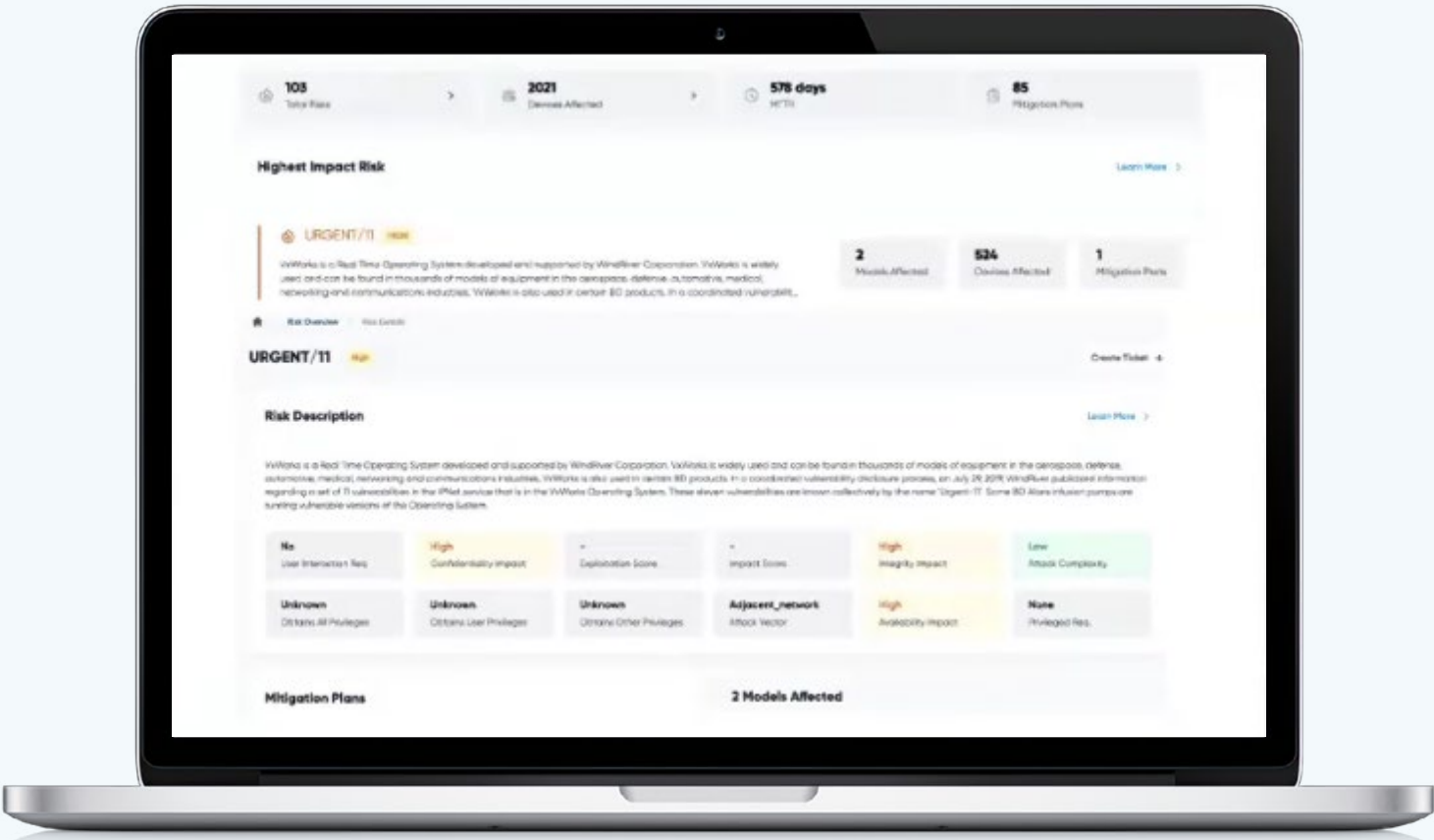
Identify Vulnerabilities and At-Risk Devices

Every device plays a distinct role within the healthcare ecosystem. When vendors report vulnerabilities, the first inclination is to inspect each device individually. However, this may not be necessary. For example, assume an infusion pump vendor reports a vulnerability. Rather than examining each pump individually, Cylera can help streamline and optimize this process. For instance, if you have 1,000 pumps, Cylera may identify only 75 that need remediation. This targeted strategy simplifies fixes and minimizes the resources needed, saving you time and effort.

3

Risk Prioritization

- ✓ Identify vulnerabilities and at-risk devices
- ✓ Inspect and assess device traffic
- ✓ Determine where to take action based on dynamic risk scoring and Cylera's curated, industry-leading remediation playbooks



Inspect and Assess Device Traffic

To effectively prioritize risks, you must examine the traffic patterns of your medical devices. Understanding whether your devices communicate internally or externally and if they are receiving or sending packets provides key information that should be visible directly within the platform.

Determine Where and How to Take Action

When real-time risk alerts are triggered, taking prompt action is crucial. Rather than simply notifying your biomedical engineering team that action is required, the Cylera platform provides them with clear, step-by-step instructions on applying a patch or implementing a remediation strategy. It also offers guidance on the potential impact these actions may have on your business operations. Having well-defined playbooks readily available ensures that your team can efficiently and effectively address any security issues with your medical devices.

By prioritizing risks based on device role, evaluating device communication patterns, and utilizing actionable remediation playbooks, you can significantly enhance the security of your medical devices while minimizing disruption to patient care. This

comprehensive approach helps safeguard patient care delivery and ensures your devices are protected.

How Teams Benefit From Risk Prioritization

Imagine a rural healthcare delivery organization where outlying clinics are open just one day a week, but the emergency room (ER) must function around the clock every day of the year. In this scenario, securing devices in the ER takes precedence due to the critical nature of their role. This example underscores the importance of prioritizing risks based on their potential impact on the business and patient care.

IT and Information Security: Know Where to Focus First

IT and information security teams should concentrate on addressing the healthcare IoT and connected medical devices with the most pressing needs first, such as MRI machines, rather than on devices that can wait for attention, such as smart TVs, which may not be in a critical department.

Biomedical Engineering: Keeping Devices in Service

The biomedical engineering department's top priorities include proactive maintenance to minimize device

failure, protecting devices against potential security breaches, and safeguarding devices from exploitation. Well-defined playbooks enable the biomedical engineering team to rapidly make informed decisions in high-pressure situations, ultimately improving device performance and patient safety.

Leadership and Compliance: Ensuring Secure, Reliable Service

From a leadership and compliance perspective, it's essential to acknowledge that resources and efforts should be allocated to mitigating the risks that pose the greatest threat to the organization's ability to operate effectively and meet regulatory requirements. By concentrating on the most critical areas, teams can effectively allocate resources and ensure compliance with regulations while maintaining business continuity.

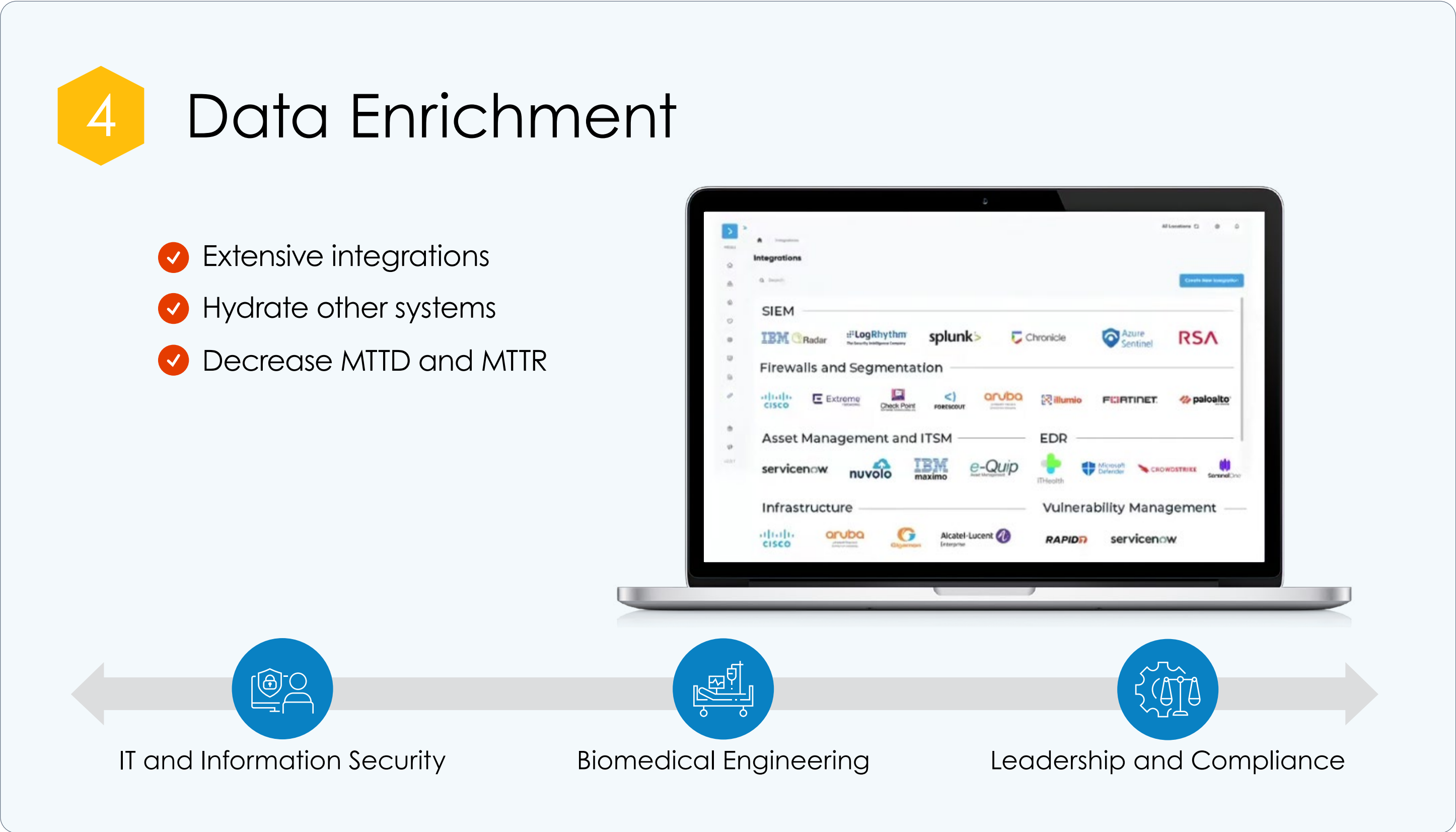
Actionable Insight 4

Data Enrichment

Implementing data enrichment across your technology stack unlocks valuable insights, enhances decision-making, and drives operational improvements. Enriched data helps healthcare providers understand their device ecosystem better. It also makes it easier to monitor, secure, and optimize device performance.

Unifying Siloed Data for Comprehensive Insights

From a data enrichment perspective, Cylera focuses on taking the existing information within the environment, from security tools, biomedical tools, and patient record systems, and combines it into a single source of truth. Traditionally, this information is siloed and must be manually integrated.



Cylera consolidates this data into a unified platform that provides a comprehensive view of what needs to be done, how things are being used, and how to optimize processes going forward. This leverages existing investments while also extending the lifespan of those tools. If a particular tool is underutilized by one group, pooling it with other data sources for context increases its value and prolongs its usefulness.

Enriching Systems and Accelerating Issue Resolution

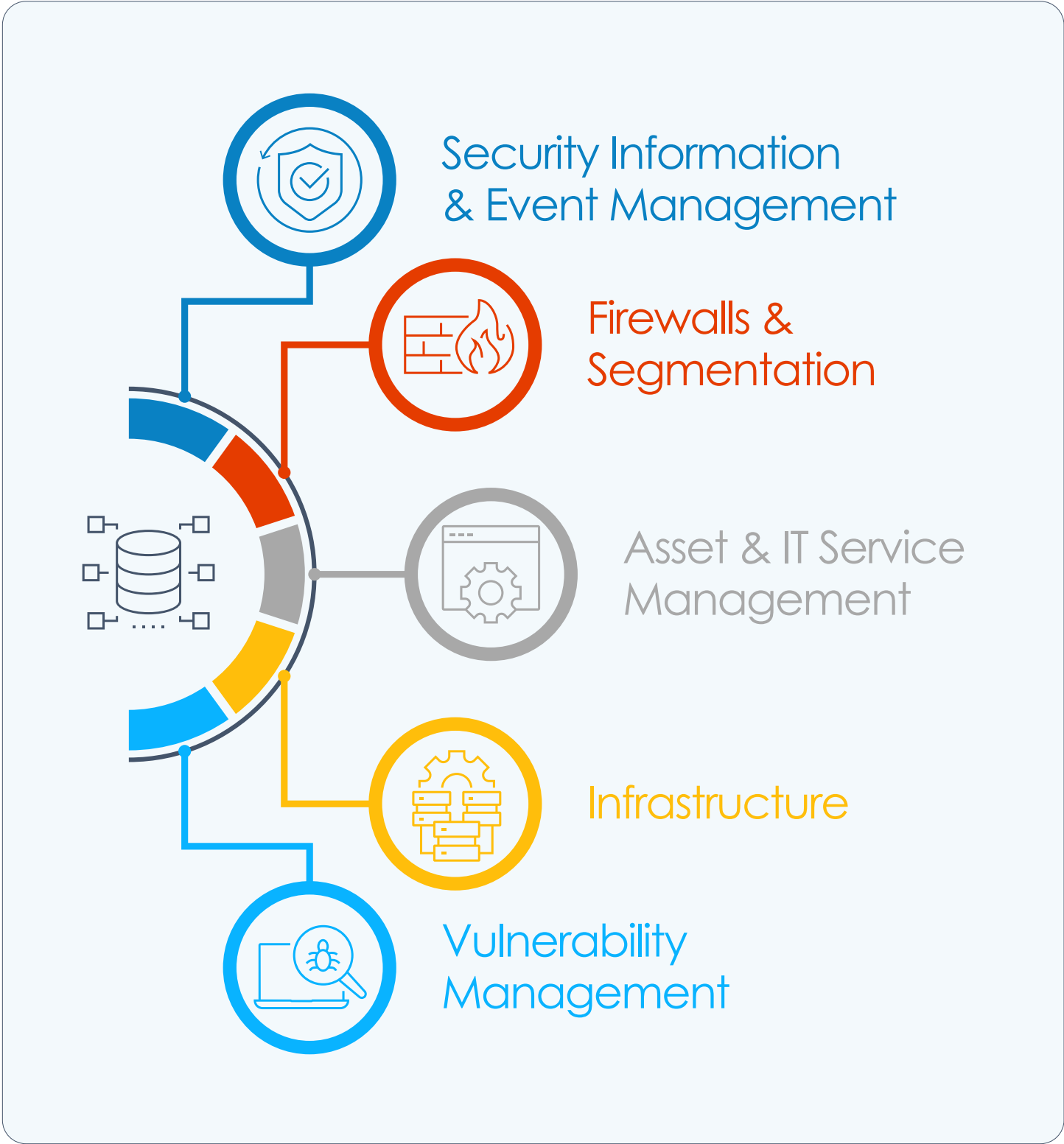
Cylera enriches your systems with insights from a unified data set. Sharing relevant information makes systems smarter, enabling faster issue detection and response times. Without comprehensive context, issue detection often demands further investigation to identify the affected device, its purpose, and its owner. Cylera streamlines this process by presenting all available information in a more intuitive and actionable format, providing the full context to quickly resolve issues.

How Teams Benefit From Data Enrichment

Data enrichment delivers substantial value across various tools and domains, providing a more thorough understanding of your healthcare IoT and connected medical devices. Integrating multiple data sources can enhance threat detection, optimize performance, and streamline auditing processes.

IT and Information Security: Stronger Security Controls

In IT, data enrichment bolsters network and security threat detection through integrations. When you correlate threat data from multiple tools, you must understand the potential impact on your operations.



With Cylera enrichment, you can understand and respond to security incidents with greater precision and effectiveness.

Biomedical Engineering: Optimizing Device Performance

Data enrichment proves valuable in biomedical applications by helping to optimize device usage. By analyzing data on device usage frequency, teams can identify underutilized devices and develop strategies to increase their utilization. This ensures that your biomedical devices deliver the greatest value to your organization.

Leadership and Compliance: Streamlined Audits

Incorporating enriched healthcare IoT and connected medical device security information into your Governance, Risk, and Compliance (GRC) tools simplifies auditing and reporting processes. Comprehensive, correlated data makes verifying adherence to relevant regulations and standards easier, saving time and reducing the risk of non-compliance.

Actionable Insight 5

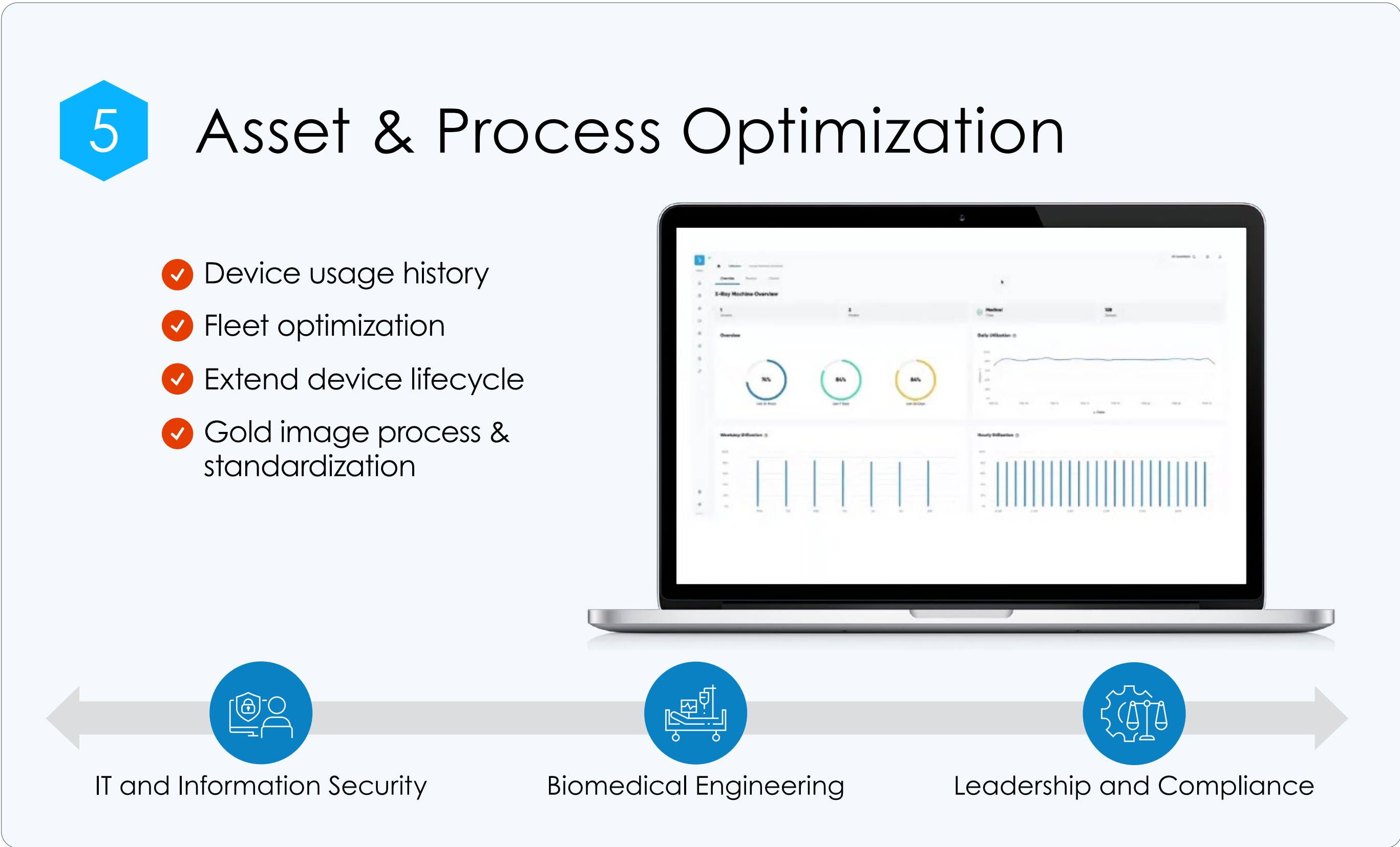
Asset and Process Optimization

To ensure your medical devices operate at peak efficiency, it's essential to analyze how they are used and develop a plan to optimize your fleet. By establishing performance standards, developing gold-standard images, and then consistently applying these standards and images across the healthcare IoT device fleet ensures you can maximize your devices' security, useful life, and value.

Device Usage History

A dedicated monitoring platform that tracks your healthcare IoT and connected medical devices' activity provides invaluable visibility into their performance and usage patterns. This history allows you to understand how devices are being used, the best way to optimize the fleet, and how to prolong the useful life of current devices within the organization.

Establishing what “good” looks like and putting that standard into the fleet is crucial. Gold standard images help achieve this. By leveraging a platform that monitors devices 24/7/365, everything the device is doing can be seen. Analyzing behavior patterns from this data allows for building an optimization plan for that particular device or set of devices.



Fleet Optimization

Fleet optimization involves determining if the right number and mix of devices are in place to meet the organization's needs. Are you overbuying or underbuying? Do you have enough of a particular medical device to meet the needs within the organization? Understanding day-to-day device usage and predicting future usage are directly enabled in the Cylera platform.

Extend Device Lifespan While Effectively Managing Risk

Safely prolonging a device's useful life requires understanding the associated risks, such as outdated operating systems or limited vendor support. However, certain devices may still offer value if approved by the FDA. By implementing compensating controls and isolating these devices within your network, you can continue utilizing their specific functions while adhering to the core principles of zero-trust security.

Gold Standard Image Device Process and Standardization

Gold standard configurations guarantee that new devices are set up to the same optimal standards as other devices in your fleet. For example, if the standard for a good MRI is known, there's no reason the next MRI

put into service shouldn't be configured to the same standard. Establishing clear criteria for what a well-configured device looks like and then applying these standards to every new device put into service lays the foundation for future success.

How Teams Benefit From Asset and Process Optimization

Prioritizing 24/7 monitoring, strategic lifecycle management, and gold standard configurations empowers you to optimize your medical device fleet's performance and maximize its value. This proactive approach enhances device effectiveness and helps you efficiently manage risk.

IT and Information Security: Efficient Oversight and Protection

The Cylera platform delivers enhanced network device management, data management, and security capabilities. This empowers IT and information security teams to efficiently oversee and protect the organization's critical infrastructure and sensitive information. It also results in improved efficiency in managing and monitoring connected medical devices, enhanced data management practices, and allows for more robust security controls.

Biomedical Engineering: Improved Utilization and Cost Savings

The Cylera platform provides a centralized system for biomedical engineering teams to manage and maintain medical device inventory effectively. By analyzing device utilization data, teams can identify devices that do not adhere to maintenance schedules, as well as devices sitting idle or in a closet for months. These insights guide discussions with equipment vendors to revisit and renegotiate service contracts, which can result in significant cost savings.

Leadership and Compliance: Strategic Insights

The Cylera platform equips leadership with improved reporting and actionable intelligence to optimize processes and investments. If data reveals that only a portion of devices are regularly used while many remain idle, it presents opportunities to increase patient intake and reduce backlog. This information can also be used to reroute patients to another hospital within the system if they can be seen more quickly.

Armed with this valuable strategic insight, healthcare leaders can make data-driven decisions to improve operational efficiency, ensure investments are well-informed, and ultimately enhance the quality of patient care delivery.

Key Takeaways



Streamline process and workflows with automation



Gain comprehensive connected medical device visibility



Accelerate healthcare cyber security program maturity and compliance audit-readiness



Reduce operational and security risk



Empower teams to mitigate threats more efficiently



Optimize allocation, procurement, and governance

Streamlining Processes and Workflows with Automation

Automating processes and workflows empowers healthcare organizations to achieve significant efficiencies that save time and resources. Although implementing these changes requires effort, Cylera's extensive experience implementing cybersecurity and automation solutions for healthcare providers worldwide ensures a smooth transition that maximizes the benefits for your team.

Achieving Comprehensive Device Visibility

To effectively secure connected medical devices, you must gain comprehensive visibility into every device in your environment. Without this complete picture, you risk inadequately protecting devices and purchasing unnecessary equipment due to a lack of awareness of what is already in use.

Maturing Your Healthcare Cybersecurity Program

Enhancing device visibility accelerates the maturity of your healthcare cybersecurity program, enabling you to identify gaps, strengthen compliance and audit

readiness, and bolster resiliency. A mature program will have well-defined plans to increase resiliency. It will also help you identify gaps so that if something does go down, you can quickly respond and recover.

Reduce Operational and Security Risk

Advanced monitoring allows for swifter threat detection than ever before, equipping your team to rapidly take action to mitigate risks.

Detecting and Mitigating Threats Efficiently

The FDA and device vendors offer guidelines for efficient threat mitigation, which often involve implementing compensating controls and minimizing unnecessary ports and protocols, which are great ways to mitigate risk.

Optimizing Allocation, Procurement, and Governance

Data gathered over 60 to 100 days provides valuable insights into device usage, misuse, or underutilization. This information supports informed business decisions regarding procurement and optimizing the allocation of resources. In addition, effective governance is vital. Maintaining up-to-date inventories of devices and associated risks is key to effective preparation.



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.

