CyberMDX

The CyberMDX

Healthcare Security Suite

We protect the **things** that protect **human lives.**™

Introduction

The mission of healthcare delivery organizations is to provide the highest quality medical care they can for the well-being of their patients. To do this, healthcare providers rely on connected medical and IoT devices for their clinical workflows, interactions, and lifesaving treatments.

Unlike other IT assets, connected medical and IoT devices are often unprotected or unmanaged. As a result, they are extremely vulnerable to breaches, ransomware, or other attacks which could adversely impact patient safety, data privacy, and regulatory compliance.

The overwhelming majority of medical devices (approximately 55-80%) runs on outdated systems. Most hospital networks lack visibility and control of these, and all the other devices connected to their network. This gap limits the ability to identify critical events, pinpoint the source of the problem, and effectively respond.

Safe and Efficient Care Delivery

Patient Data Defense

Penalty and Reputational Avoidance

"While advanced devices can offer safer, more convenient and timely health care delivery, a medical device connected to a communications network could have cyber security vulnerabilities that could be exploited resulting in patient harm."

Dr. Amy P. Abernethy, M.D., Ph.D,
Principal Deputy Commissioner, FDA

CyberMDX

How We Secure Your Hospital Network

The CyberMDX solution focuses on IoT, medical devices, and assets connected to clinical networks, providing complete visibility and network protection by leveraging our expertise with Artificial Intelligence (AI) technology, medical device vulnerability research, and a wide range of cyber capabilities. The CyberMDX solution detects and evaluates potential threats by implementing four layers of security.

The CyberMDX solution provides a comprehensive suite of capabilities that helps you protect these unmanaged devices with a full security stack.

Why Do Connected Medical Devices Need To Be Protected?

Connected medical devices are typically not visible to native IT control systems. As a result, many hospitals don't know how many medical devices are connected, the type of medical device, or any awareness of their cyber security risk status. Worse yet, there is hardly any visibility to whether medical devices have already been hacked.

Medical devices introduce a wide range of operating systems and communication protocols and current cyber security solutions do not fully understand these devices or their protocols and cannot provide adequate security.

6.2

Average number of vulnerabilities on medical devices

Source: Cyber security Ventures

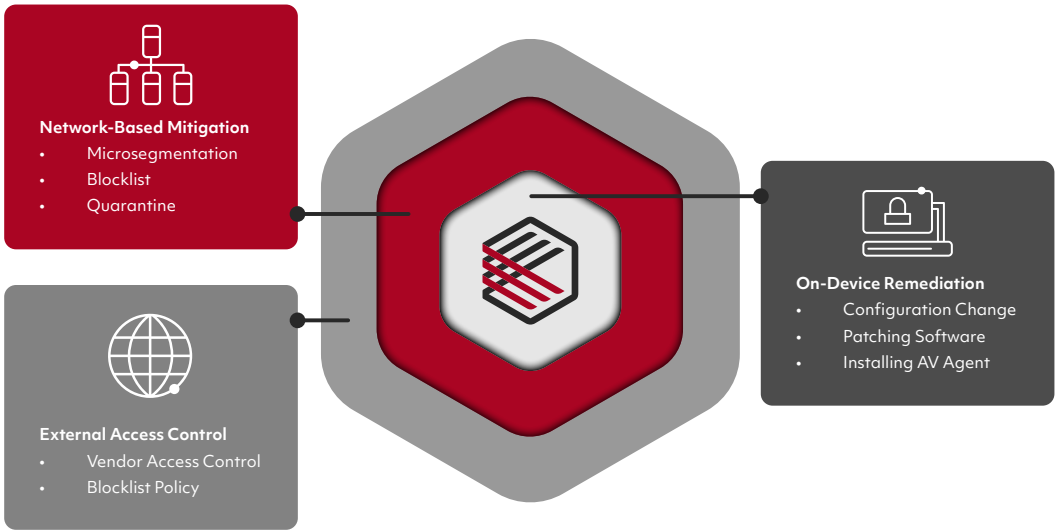
"CyberMDX automatically identified all connected medical devices on our network including model numbers and MAC addresses, showed us what they are connecting to, and helped us prioritize by providing a risk level for each device."

John Weller, CISO
Metro Health-University of Michigan Health

CyberMDX

Device-Centric Risk Management (DCRM)

CyberMDX provides on-going risk assessment of all your connected assets including vulnerability and compliance profiles. But we don't stop there - the solution offers a prioritized list of asset groups and recommended actions to remediate or mitigate the risks associated with these assets on three distinct protection layers: on-device, on-network, on-perimeter. This is inherently more robust than other solutions which focus their security and risk management solely on the network layer.



Streamlining Vulnerability Remediation and Mitigation

Fundamental questions drive the risk management process. What vulnerabilities affect an asset? What is the severity? What are the factors that could impact patient safety or other business objectives?

First you need to consider your on-device remediation options – including patching or applying configuration changes, and understanding what the expected risk reduction is in each case. CyberMDX technology enables the collection and analysis of meaningful data to provide answers to these questions and drive decisions and actions towards fixing these issues. Our DCRM approach also includes kickoff workflows and security orchestration to help you effectively manage the risks.

93%

Of healthcare organizations have experienced a data breach

Source: Black Book Market Research LLC

"The product is able to identify risk levels proactively based on factors such as device behavior, device utilization, clinical use, and device dependencies. Segmentation and containment rules are automatically suggested based on identified risk.".

The Forrester New Wave™: Connected Medical Device Security, Q2 2020 – By Chris Sherman

CyberMDX

Layers of Security:
An Agentless, Scalable and Integrated Architecture

CyberMDX built its technology from the ground up around meaningful data. We acquire data from network traffic and data integrations and enrich it from our healthcare and security-focused knowledge base. Our artificial intelligence engine then analyzes the data to create a comprehensive asset inventory together with 360° actionable security insights around those assets. Closing the loop, we translate insights into actions via security orchestration and workflow automation.

Scales from Small to Large

Built to cover even the largest healthcare delivery organizations – or the providers that secure them.

Integrates with What You Have

Drives actions and workflows via integration and orchestration engines

Customizes for Your Needs

Define and design exactly how you want to enable workflows or orchestrate security.

CyberMDX RESEARCH

Backed by the industry's most skilled team of healthcare cyber security researchers and analysts

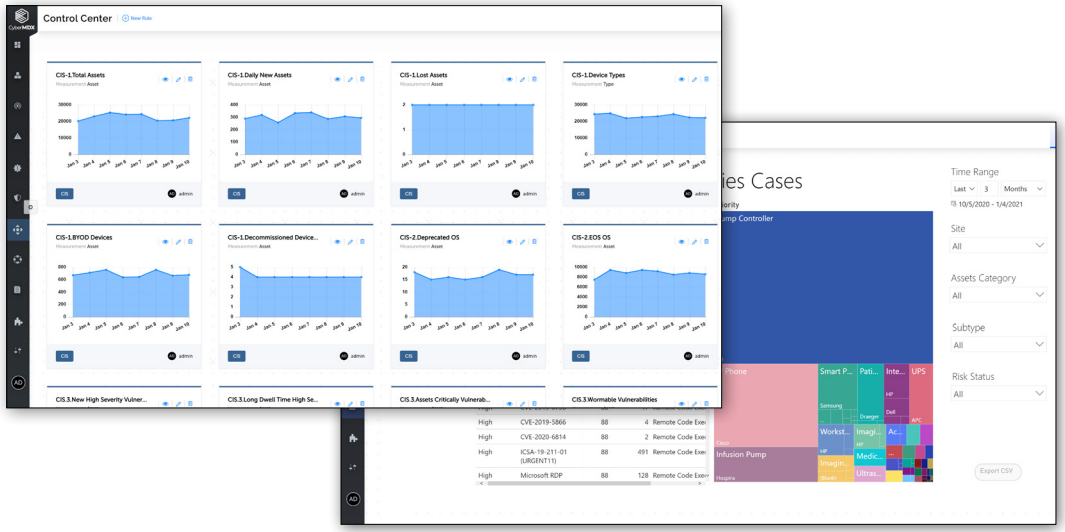
"We joined forces with CyberMDX to help ensure patient safety and improved care with 360-degree visibility and security into all of our connected technologies".

Vince Rosati, Director of Biomedical Engineering
Englewood Health

CyberMDX

Let the CyberMDX Control Center Work for You

The CyberMDX Control Center is how smart healthcare organizations make the most of available technologies. Save labor and increase accuracy and updatability by converting daily user routines into automated rules. Powered by our flexible, rule-based policy engine, the CyberMDX Control Center enables you to fine-tune and customize the system behavior by defining granular rules and policies. Easily review, validate, and enforce the policies underpinning digital governance across your entire organization.



Command Control for Your Security and Policy

Define rules/policies to put asset management, policy validation, compliance alignment, and asset tracking on autopilot.

- Create custom rules or choose from pre-defined best practices. Rules can be based on various asset or network attributes (such as asset type, location, risk level, detected vulnerabilities and much more) or behavior (such as communication with a high-risk country).
- Track all matching assets in real time. Zoom in on a specific set of results for a more in-depth investigation.
- Decide whether you want only a visualization of matching results, or additional actions that will be triggered by them. For example, creating tickets, sending email notifications, modifying asset attributes, implementing a smart security policy, and more.

100+

CyberMDX Control Center includes 100+ best practices out of the box, based on common cyber security frameworks (NIST, CIS, HITRUST), allowing asset management, network segmentation, progress tracking, and policy validation to be automated.

CyberMDX

CyberMDX Advanced Reporting Delivers Powerful Insights

CyberMDX Advanced Reporting empowers you to provide C-level executives with easy-to-read reports on your overall cyber security posture and progress towards meeting goals. With an intuitive interface and automated data capture across all platforms and devices, Advanced Reporting creates documented intelligence in real-time, so critical information is at decision-makers' fingertips immediately.

Advanced Reporting aggregates and cross-filters your data while presenting it clearly, allowing you to act on it efficiently and effectively - your way.

- Overall Security Posture
- Trend tracking of the panoramic cyber risk exposure and actions
- Fleet utilization – i.e., for medical devices, with cross-site comparison.
- In-depth cyber risk reports for each risk type with rankings
- Detailed analytics – utilization, error message frequency, distribution, and analytics on injected medication.

Multi-Tenant Access for Large Hospitals and MSPs

Secure and Manage Your Network of Hospitals on a Single Platform.

- With a single instance of the CyberMDX Healthcare Security Suite, you can manage multiple hospital locations with just a click. The CyberMDX Multi-Tenant Management Console is API driven and enables the user to query CyberMDX APIs of all managed tenants, enabling hospitals to identify, detect, and defend against potential cyber attacks across all locations and campuses. This ensures the operational continuity of critical assets and the security of patient and facility data.
- Provides a single pane of glass that unites the individual dashboards into one, while preserving the separation of the core systems in a SOC-like environment.
- The console aggregates and presents data from multiple locations, providing cross-tenant, and per-tenant visibility through flexible dashboards and reports.

"Frost & Sullivan sees tremendous value in CyberMDX's platform because it offers deep and contextual visibility, enabling healthcare stakeholders to manage and mitigate risks, prevent threats, provide incident response, and perform lifecycle management."

Frost & Sullivan
2020 North American Medical Devices and Assets Security Technology Innovation Leadership Award

CyberMDX

The CyberMDX Core Software Platform

The CyberMDX core software enables hospitals to identify, access, detect, and defend against potential cyber-attacks with continuous discovery of IoT and medical devices, comprehensive risk assessment, and AI-based containment and response. It's enterprise-grade, with support of SSO, MFA, and RBAC.

Additionally, the core software provides comprehensive information about the medical devices connected to your network. It can identify appropriate metadata including manufacturer, model, serial numbers, MAC address(es), IP addresses, and operating systems.

The core software detects and evaluates potential threats with comprehensive vulnerability and threat detection. It provides real-time threat analysis and operational status using an agentless deployment model, without requiring client software on those devices in your network.

Connecting Our Cloud-based Core to Hospital Networks

CyberMDX Sensors are cost and performance-optimized appliances. Choose your preferred option – hardware (pictured), software (e.g., Cisco Catalyst 9300 switch), or virtual appliance form factor.

The sensors provide superior performance and high resiliency for enterprise class deployments. The largest appliance supports 10Gbps of application inspection, which results in throughput of hundreds of thousands of transactions per second. Add as many as you need. To maximize system uptime, they include redundant hard drives, power supplies, and a wide variety of network interface options.

Sensors can cover single or multiple facilities according to the network architecture and deployment plan.

75 Billion

Total IoT devices connected to the Web ay 2025

Security Today – "The IoT Rundown For 2020: Stats, Risks, and Solutions"
Gilad David Maayan (Jan 13, 2020)

CyberMDX

Easy Integration with Third Party Software and Hardware

We know that making the most of your current investments is an important part of your goals. That's why we work hard to create a partner ecosystem that integrates with what you already have. Below are some of the leading technologies that CyberMDX solutions work with out of the box.

Microsoft Azure · Cisco · aws · splunk>

Check Point Software Technologies Ltd · IBM Radar · ArcSight · AIMS

tenable · Fortinet · Rapid7 · aruba a Hewlett Packard Enterprise company

vmware · nuvolo · servicenow · Qualys

Infoblox · paloalto Networks · Member of Microsoft Intelligent Security Association · Forescout

Integral Part of Cyber Security Service Programs

From security consultancies that provide risk and vulnerability assessments, to services that can help create response and recover plans, maintain secure systems, access and audit your security posture or manage overall detection and identification of your medical assets 24/7 using CyberMDX, we partner with industry experts to enrich these value-add solutions for your organization.

PHILIPS · relyens · Witz Cybersecurity

ALPHATRON Medical · accenture · VERINT

Deloitte. · KPMG

"Philips is pleased to work with CyberMDX to provide health technology customers with vendor-neutral solutions to protect connected medical systems and devices."

Conrad Smits
Head of Global Services and Solutions
Philips

CyberMDX

About CyberMDX

Healthcare Delivery has more security challenges than most sectors. Facing a constant combination of cyber criminals, nation-state actors, hacktivists, and malicious insiders, the need for strong defense of all devices on managed or unmanaged networks is paramount.

We are CyberMDX. We provide a single place to view and prioritize all device groups. We'll tell you where to start and what to do next. We help you mitigate or remediate by empowering your team to simulate different actions and see the risk reduction impact of each action. This enables faster response — and with fewer required hands. We research, track, alert, validate, analyze, and help you comply. You won't need to re-architect your network because we believe it's about layering protection around medical and IoT devices.

CyberMDX solutions are designed to support industry standards, regulatory compliance, as well as a large partner ecosystem.

We work with a worldwide network of technology leaders who bring together superior competence in their respective fields along with commitment to delivering results for our joint customers.