Cynerio

Healthcare IoT Cybersecurity Platform Secure. Faster.

Cynerio 360 Addressing Modern Healthcare Cyber Risk

Despite increasing cyber threats to the healthcare industry being well known, the steps to prevent and address attacks are often lagging. Staff shortages, unpredictable budgets, rapid adoption of caregiving technologies and mounting technical debt often leave healthcare leaders unsure where to begin improving their security practices. To address these challenges Cynerio is the leading provider of a new breed of technologies using Deep Packet Inspection (DPI) and Passive Analysis to quickly secure healthcare environments. The Cynerio 360 platform provides device insight, risk analysis, prioritized guidance and industry-focused expertise to implement proactive protections and respond quickly to security incidents.



Preventative Measures, Reactive Response

The Cynerio 360 platform is entirely focused on securing healthcare environments from the most common cyber threats that lead to ransomware attacks and data breaches.

Day One Protections

Cynerio Attack Detection & Response provides day one protections against common attacks including ransomware, malware and data exfiltration.

Active Attack Detections

Ongoing analysis of potentially malicious activity is performed by the Cynerio Live research team to reduce false positives and respond to attacks often missed by traditional technologies within minutes.

Manageable Microsegmentation

Automated policy creation, testing and deployment enables hospitals to implement a Zero Trust architecture more quickly with fewer resources.

BioMed Benefits

Healthcare Technology Management teams are the lifeblood of device-level security. Improve their efficiency with improved devices tracking, clear, upgrade guidance and improved access to security requirements. Inventory and Visibility Cynerio Preventative Risk Management identifies all connected devices in a healthcare environment and provides detailed asset visibility in real-time.

Industry Expertise

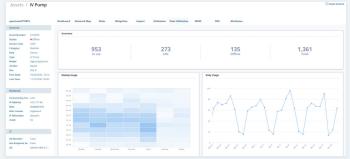
Cynerio Live researchers provide ondemand expertise during a hospital's most critical moments while Technical Account Managers supply the dedicated, ongoing guidance need for long term success.

Cynerio 360 Platform

Comprehensive Asset Inventory

<u>``</u>	0		T	-	Duilding Automation	5.4		_
Access Point 940	Anaesthesia Machine 41	BIS Meritor 6	Blood Coagulation Meter 4	Blood Gas Analyzer 76	Controller 20	CAB 10	Cardiograph 16	C.Arm 3
Communication Device	Communications Server 69	B Connectivity Engine 92	ca 6	с. п	CVIS Server 1	DICOM Primer	Dicom Scanner 8	DICON Werkstation 59
Docking Station	Fluerascopy 2	Garning Console	Gateway 55	Glacometer 523	Heenatology Analyzer	immunessay 3	intercores 6	interface Engine
P Gamera 379	N Party 1,361	Label Printer 72	LIS Server 13	Mailing System	Media Controller 41	Medical Device 46	Medicine Dispenser 266	Melecular Testing
NAS 2	Necessatal Meesitor 10	Nurse Call Station 206	мия 15	ост 2	OT Device 7	PACS Migration	PACS Server 43	Patient Merikor 710
Point of Care Analyzer 2	Printer 3,210	Radiation Dose Management 1	RS Server 3	(1) RTLS 8	Sample Handler 1	Single-Board Computer 2	Smart Bed 28	Smart Speaker 1

Device Utilization and Risk Insight



Prioritized Guidance and Customizable Reporting



Attack Detection & Response

Attack Detection and Response

ncidents By Status							
3 Total		2 New	In	0 Progress		Onore	1 Archive
Suspicious Connection to Malicious	Domain						NE
Description IRI machines are accessing a domain ass Click for more details	ociated with	malware		Immediate Respo			Critica
A Threat Actor	Threat Actor 🔷 Targets					Top Related Risks	
External Address 2.59.176.		MRI	10.101.160.23	Events	31	Legacy OS	End of Life OS
	>	G MRI	10.101.160.128	Connections	2	Suspicious Outbound Connections	Suspicious Connections
JRGENT/11 Exploit on Medicine Di							NE
indentifier explore on medicine bis	penser						

Detailed Device Insight

dicom_cf2d9fe1	•	Dashboard	Network Map	Risks	Mitigation	Impact	Utilization	MDS2	FDA	Attributes
General										
		Overview	'							
Status	Online									
Device Class	IoMT			Asset Im		Risks				
Category	Radiology		-							
Role	Device		\frown	Patient S		Legacy OS	•			
Туре	CR		9.8	Service D	isruption •					
Model	Kodak QC		Critical 39	Patient C	onfidentiality •					
Vendor	Kodak									
Site	Site D									
First Seen	10/24/2022 11:42									
Last Seen	11/26/2022 22:03	Connectiv	on Profiles				Kodak QC	Behavior Compa	rison	
Network				• Internal			5			
Connectivity Te	cLAN									
IP Address	10.30.70.222						4			
IP Allocation	static									
VLAN	30									
							3			
п										
		Nedical								
AD Member	False						-			
Has Endpoint Se	False									

Microsegmentation Policy Creation

Risk Remediation and Mitigation Actions

Action Type	Actions	Assets
Network Segmentation Actions		
Apply East-West Segmentation	<u>62</u>	2802
Apply North-South Segmentation	<u>59</u>	2939
Network Configuration Actions		
Apply Service Hardening	<u>118</u>	1780
Device Remediation Actions		
	<u>164</u>	1,541
Device Remediation Actions Change Configuration Change Credentials	<u>164</u> <u>28</u>	1,541 156

Increasing cyberattacks on healthcare environments require a comprehensive, modern security approach. Learn more about how the Cynerio 360 platform provides proactive protections and expert response by visiting **www.cynerio.com** or contacting us at **info@cynerio.com**.

About Cynerio

Cynerio has one simple goal - to secure every IoT, IoMT, OT and IT device in healthcare environments. Our dedicated focus on the healthcare industry has led to the creation of technologies that help in preventing and responding to attacks. With capabilities ranging from microsegmentation and improved device insight to identifying exposed ePHI and stopping ransomware, Cynerio provides the technology and expertise needed to protect hospitals from a variety of cyberattacks. Learn more about Cynerio at cynerio.com or follow us on Twitter @cynerio and LinkedIn.

