



Evaluating Risk with CMMS Data

Cynerio and e-Quip Enable Device Security Snapshot

How much risk do your Trust's IoT devices present?

Despite risk prevention being on the tops of all healthcare executive minds, many hospitals lack the bandwidth, budget, or team members to identify and remediate risks. To help ease resources related challenges to identifying device level risks, Cynerio has developed a low-touch CMMS Risk Evaluation.

Cynerio's innovative approach to calculates the risk that IoMT and IoT devices present at your hospital by cross-referencing your CMMS data with the latest intelligence from Cynerio implementations at hundreds of global hospitals. The result is deeper insight into vulnerable devices, the risks they present to patient safety, and how to remediate security issues.

How It Works

- Provide your e-Quip CMMS data through a secure channel
- Cynerio's analysis engine will perform a full risk analysis of the healthcare IoT devices on your network with a detailed list of remediation recommendations for potential security issues
- Schedule a readout call with Cynerio Live team members to review your full device risk report

That's it! No hardware deployment or agent installation needed.

What You'll Receive

- Device risks across your IoT infrastructure classified by severity level
- A list of healthcare IoT asset types susceptible to malware
- Device risk prioritisation using Exploit Prediction (EPSS) and Common Vulnerability Scoring System (CVSS)
- Risk mitigation actions broken down by asset type and potential risk score reduction

CMMS Risk Reporting Insight

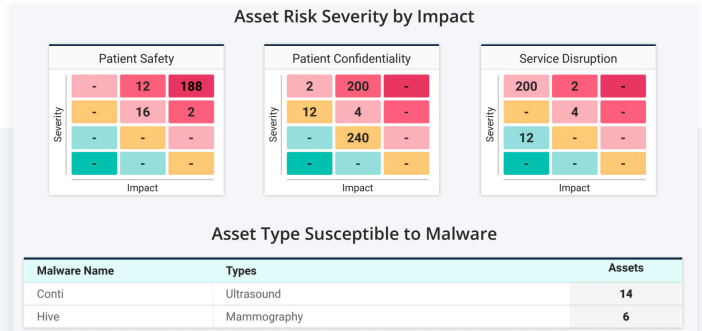
IoT Devices 78	IoMT Devices 1895	Device Types 98	Security Posture Score (out of 100) 47.2 74.8 Score Benchmark
--------------------------	-----------------------------	---------------------------	---

Top Risks	Affected Devices	CVSS Score	EPSS Score	#
URGENT/11	Infusion Pumps	9.8	93%	188
EternalDarkness	GE Ultrasounds	9.5	95%	12
BlueKeep	Mammography	9.8	96%	2
Weak Credentials	GE X-Rays	9.0	80%	4
Default HTTP Credentials	Hematology Analyzers	8.4	90%	12

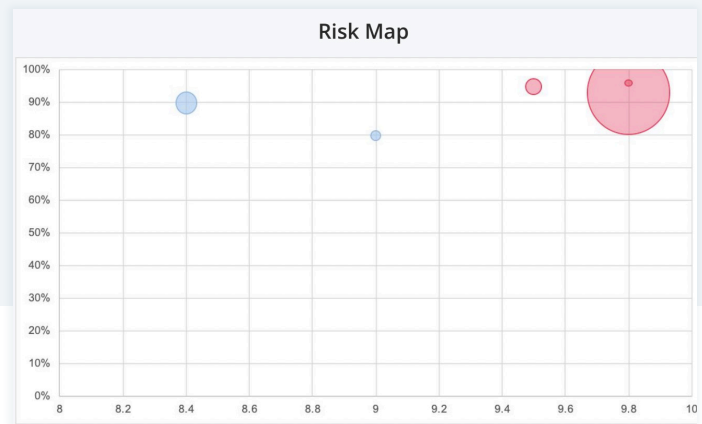
Device summary and risk details

Mitigations Action Score				
Mitigation Actions	Type	Model	Assets	Score Rank
Update Firmware	Infusion Pump	8015	188	1.89
Apply E/W Segmentation	Ultrasound	Logiq S8, Vivid E9, Vivid E95	12	1.12
Apply E/W Segmentation	Mammography	Selenia Dimensions	2	0.83
Change Credentials	X-Ray	Precision 500D	4	0.82
Change Credentials	Hematology Analyzer	I-STAT	16	0.81
Upgrade SSH Server	NM	Discovery	4	0.55
Upgrade Firmware	Patient Monitor	VC150	99	0.04

Mitigation guidance



Asset risk summary



Prioritized risk map

Ready to learn more about the risks presented by medical devices?

Start today by contacting us at support@integra.co.uk

About Cynerio

Cynerio has one simple goal - to secure every IoT, IoMT, OT and IT device in healthcare environments. 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](https://twitter.com/cynerio) and [LinkedIn](https://www.linkedin.com/company/cynerio).

About e-Quip

e-Quip is the market leading medical device asset-management software in the UK. With over 20 years of experience supporting the largest Medical Physics, Clinical Engineering and EBME departments in the UK, there is no other system available that combines the ease-of-use with power and flexibility of e-Quip. Learn more about e-Quip at www.e-quip.uk.net