Cynerio

WHITE PAPER

The State of Healthcare IoT Device Security 2022

Table of Contents

Executive Briefing 3

The Healthcare Cyberattack Landscape 4

Overarching Security Considerations 5

Microsegmentation Specific Considerations 6

- Network Level Device Profiling Segmentation 6
- Network Workflow Segmentation 8
- Optimized Virtual Local Area Network (VLAN) Segmentation 10
- Microsegmentation Policy Deployment 12

Additional Considerations 13

Check List: Microsegmentation Considerations 15

About Cynerio 16

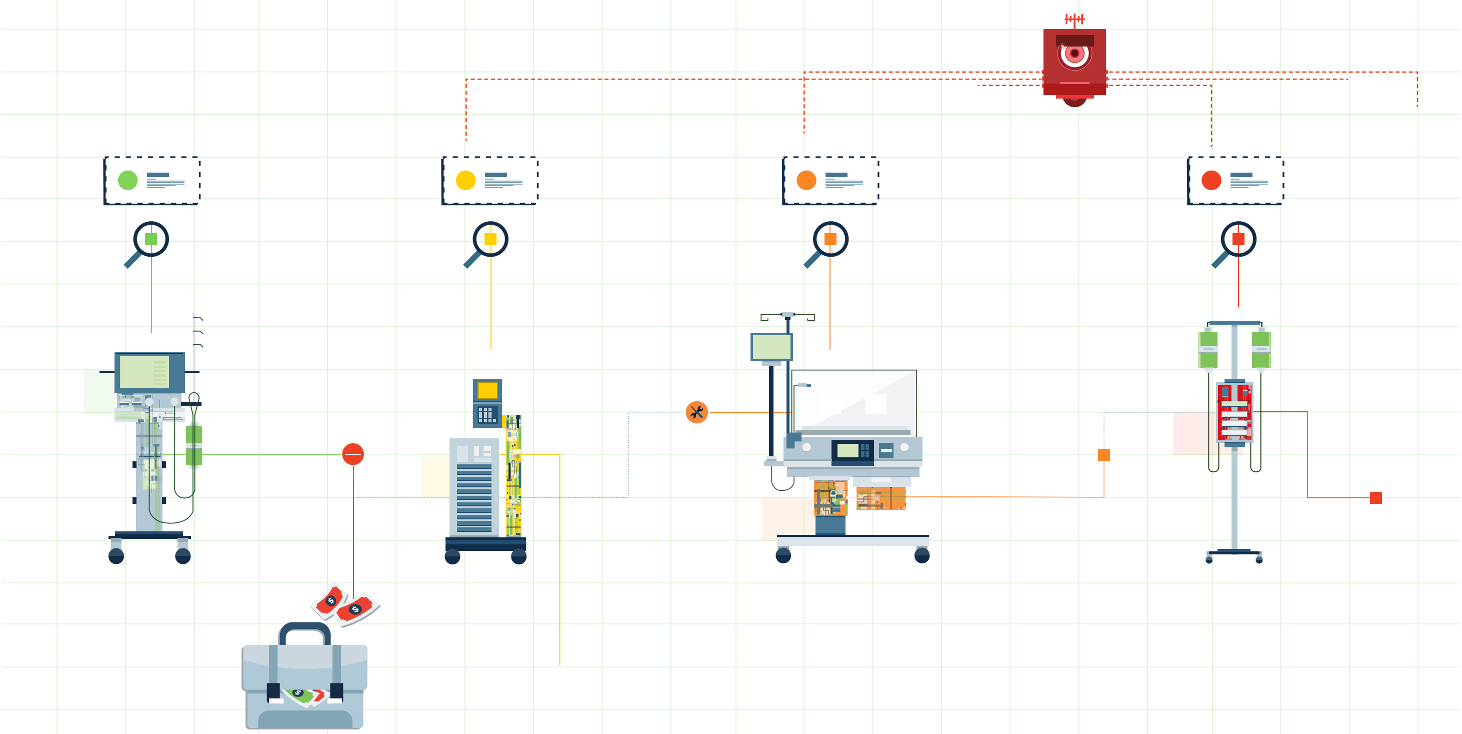
Executive Briefing

Adoption of connected technologies in healthcare has significantly accelerated in the last decade. In addition to the management and security of traditional IT devices (PCs, Laptops), the healthcare industry is quickly realizing the risks associated with the hundreds and thousands of IoT devices they have adopted to improve patient care. While rarely a source of direct attack, the complex technical components of infusion pumps, CT machines, glucometers and many others have created an efficient web of connectivity that enable cyberattacks to spread, infect and attack.

The impact of attacks are clear, but often not widely known. For every report about Scripps spending more than $100 million to recover from a ransomware attack there are hundreds of smaller, less publicized attacks that go unknown. For every piece of ransomware recovery guidance provided by leadership at University of Vermont Medical, there are hundreds of healthcare organizations that have been forced to pay a ransom in order to better serve their community.

Simply put, healthcare is disproportionately targeted by cyberattackers with high degrees of success. The rapid technological adoption paired with lagging security practices relative to other industries make it a prime target and source of revenue. Among the most commonly recommended technical practices to prevent the impact of attacks is implementing a Zero Trust architecture fueled by microsegmentation which has been shown to address 92% of device-level critical risks in healthcare environments.

The below guidance covers healthcare specific considerations and is paired with industry specific use cases to further illustrate the value and achievable nature in healthcare facilities of all size, complexity and resource availability.



The Healthcare Cyberattack Landscape

The past decade has seen rapid adoption of new healthcare technologies throughout the world. From infusion pumps to CT machines, connected devices have improved timeliness, insight and patient care. Unfortunately, this rapid adoption has introduced new threats, vulnerabilities and attack vectors. These new threats paired with valuable patient data and a high willingness among organizations to restore operations by ransom payment have resulted in healthcare becoming the most attacked industry in the world.

With each new attack healthcare leaders are challenged with the question of "how secure are we?" This struggle is further exacerbated by a lack of insight into IoT and IoMT devices, silos of third-party security practices, incohesive data, and outdated understandings of risk.

To help organizations extend their current protections to modern technologies, Cynerio has worked with researchers, partners and customers to create the below guidance for broader microsegmentation initiatives. The frequently changing nature of cyberattacks requires constant vigilance, so we invite readers to contact our team at info@cynerio.com for deeper discussions at their convenience. From clarifying guidance to discussing attack trends, ongoing research or developing defense methods being identified and developed by our research team our goal is to provide expertise and technologies that will reduce the financial burdens and impacted care introduced by ongoing cyberattacks.

The 2022 Healthcare Cyberattack Landscape in Numbers

over 50M
US Patient Records Exposed (HHS "Wall of Shame")

89%
of hospitals experienced at least one cyber attack in last 12 months (ProofPoint)

57%
of global HCOs compromised by ransomware in previous 3 years (Trend Micro)

3/4
of infusion pumps have known security issues (Cynerio, Palo Alto)

24%
of cyberattacks result in increased mortality rates (Cynerio)

92%
of device-level critical risks are addressed by microsegmentation (Cynerio)

Expanding the time, resources and budget for new cybersecurity practices is often a daunting task with no guaranteed results and difficult to measure successes. To help ease these challenges, the below guidance is broken down into several concise sessions focused on specific considerations related to microsegmentation efforts:

- **Overarching Considerations**
- **Microsegmentation-Specific Considerations**
- **Additional Considerations**

Overarching Security Considerations

At the highest level, Cynerio sees microsegmentation successes among organizations that focus on four specific areas:

- **Visibility -** 360 degree visibility across all connected (IoT, IoMT, IT, etc) devices. This visibility extends individual device insight to known vulnerabilities, identifies potential behavioral risks associated with insecure protocols and documents exploitability factors. The combined risk insights collectively inform organizational security posture measurements that are automatically tracked and updated over time.

- **Risk Mitigation -** To properly address risk factors including impact, likelihood and mitigation options must be considered. In-depth risk analysis provides clear guidance for security practitioners including patch details, network-level mitigations, severity and probability of an attack. Industry standard frameworks including CVE, CVSS and EPSS are used to standardize and guide security practitioners in their efforts.

- **Real-Time Defense -** During a cyberattack early detection and response is critical. Healthcare-specific offerings such as Cynerio's Attack Detection & Response technology combine passive analysis with Deep Packet Inspection (DPI) to identify abnormal behavior and trigger additional investigation. During the immediate investigation performed by research teams, false positives are eliminated to reduce the noise often encountered in traditional systems. The result is a first line of defense and expertise typically considered unachievable by most healthcare IT teams.

- **Regulatory Compliance -** Regulatory compliance differs greatly based on individual countries. The continually increasing impact of cyberattacks on healthcare combined with improved insight to patient impacts will likely lead to increased global regulation in the coming years. Proactive healthcare organizations should search out leading regulatory requirements such as the United Kingdom's Data Security and Protection Toolkit (DSPT) for best practice guidance. Such resources enable organizations to better protect patient information and gain 360-degree visibility across all known IoT and IT assets

Microsegmentation Specific Considerations

Core to any security practice is the ability to implement the core components of a Zero Trust architecture without requiring unachievable levels of effort, resources or long-term maintenance. Enhancing network protections by implementing microsegmentation is a core component of Zero Trust architectures that is both effective and achievable in all healthcare environments.

Network Level Device Profiling Segmentation

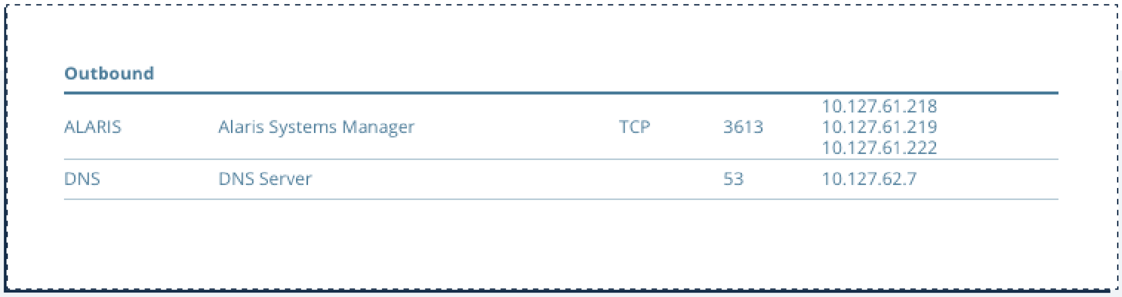
Regardless of functional use, connected devices (IoT, IoMT, IT, etc) must be analyzed and monitored in an automated, repeatable manner. Among the components that must be analyzed are:

- Manufacturer specifications, guidance and patches
- Observed device communication patterns across global organizations
- Consideration of HDO-specific deployments, architectures and protocols

Beyond the analysis of the individual devices and data points, broader analysis of an entire ecosystem must also be considered. Healthcare organizations must consider analysis engines that use Machine Learning (ML) to broadly analyze network-level behaviors, identify deviations from the norm, validate issues and provide clear, prioritized guidance on how to create, test and deploy resulting microsegmentation policies.

Use Case: Benefits of Network Level Profiling - Alaris IV Pump PCU 8015

In this use case, the analysis engine automatically discovered all Alaris IV Pump PCU 8015 on the customer network and used machine learning to build a network profile of the devices. In detecting and passively analyzing the devices, the network profile automatically accounted for HDO network configurations specific to the Alaris System Manager including IP and DNS services.



Outbound

ALARIS	Alaris Systems Manager	TCP	3613	10.127.61.218 10.127.61.219 10.127.61.222
DNS	DNS Server		53	10.127.62.7

Device Network Profile for Alaris IV Pumps

Via integration with this HDO's Network Access Controls (NAC), the analysis engine was able to tag relevant endpoints and build a group of devices that is dynamically updated to account for changes in IP address, locations and other considerations. For both initial and ongoing deployments, the CDO has used the analysis engine to review, analyze and push updated Access Control List (ACL) policies to the NAC periodically. In sensitive cases where the utmost caution is required, the CDO takes advantage of the ability to configure and update the resulting policies manually.

Network Workflow Segmentation

In many cases microsegmentation must analyze beyond individual device profiles and account for the complex environments in which they are deployed. Where IV pumps or patient monitors may only need to communicate with a handful of other technologies, more complex systems including Radiology, Lab or PACs servers are highly connected to multiple internal and external systems.

For devices that require more complex deployment, additional analysis of network workflows must be performed to properly microsegment the devices. This process should include analysis of the in-place network, autogenerated creation of enhanced security policies and automated analysis of those policies to ensure no impact on patient care.

Network Analysis and Policy Creation

- Comprehensive device network map
- Creation of individual device network profiles
- Consideration of common and HDO-specific service configurations (DNS, DCHP, AD, etc)
- Recommendations based on the principle of least privilege

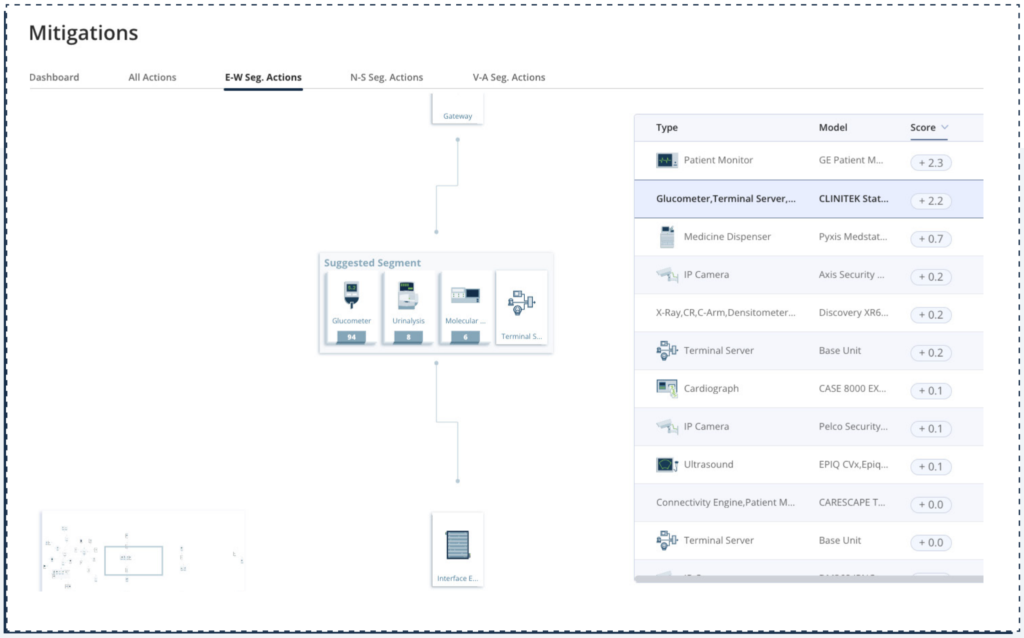
This approach should initially form a baseline to apply initial microsegmentation policies against while being automated and flexible enough for routine, periodic updates.

Policy Analysis

All policies created above should then be tested in an automated manner. Systems using "virtual segmentation/ sandboxing" will use copies of real network traffic for a predetermined amount of time (typically 30 days) to identify potential policy violations, unexpected connections or other deviations that require further investigation. The result is a well tested, known-good set of policies that require sporadic investigation from often over-burned HDO teams.

Use Case: Lab Device Segmentation

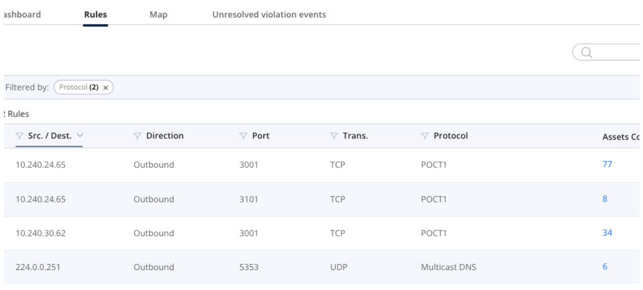
In this use case, the analysis engine analyzed network traffic to discover a group of lab devices using the same workflow, gateway connection and interface engine. The resulting map displays the devices, allows for further user device investigation, suggests a logical segment and provides the relevant ACL rules that can be tested and deployed.



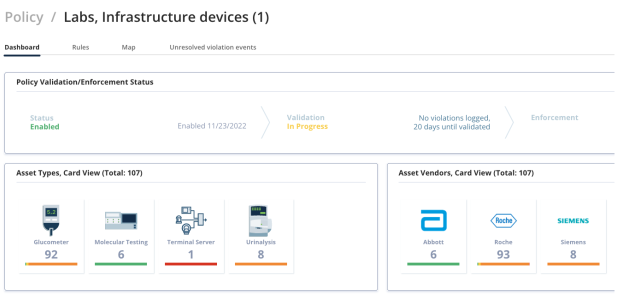
Type	Model	Score
Patient Monitor	GE Patient M...	+ 2.3
Glucometer,Terminal Server,...	CLINITEK Stat...	+ 2.2
Medicine Dispenser	Pyxis Medstat...	+ 0.7
IP Camera	Axis Security ...	+ 0.2
X-Ray,CR,C-Arm,Densitometer...	Discovery XR6...	+ 0.2
Terminal Server	Base Unit	+ 0.2
Cardiograph	CASE 8000 EX...	+ 0.1
IP Camera	Pelco Security...	+ 0.1
Ultrasound	EPIQ CVx,Epiq...	+ 0.1
Connectivity Engine,Patient M...	CARESCAPE T...	+ 0.0
Terminal Server	Base Unit	+ 0.0

Auto-generated device discovery and recommended device segmentations

Given this information, the HDO used virtual segmentation to test the resulting ACL rules against copies of live communication patterns for 30 days. When policy violations occurred, the customer received alerts with guidance and insight enabled further policy tuning and testing. The result is a low-touch, highly accurate approach to microsegmentation policy creation and management that can be pushed to NAC without impacting the operation of devices.



Src. / Dest.	Direction	Port	Trans.	Protocol	Assets Co
10.240.24.65	Outbound	3001	TCP	POCT1	77
10.240.24.65	Outbound	3101	TCP	POCT1	8
10.240.30.62	Outbound	3001	TCP	POCT1	34
224.0.0.251	Outbound	5353	UDP	Multicast DNS	6


Policy / Labs, Infrastructure devices (1)
Dashboard
Rules
Map
Unresolved violation events

Policy Validation/Enforcement Status

Status: Enabled — Enabled 11/23/2022

Validation: In Progress — No violations logged, 20 days until validated

Enforcement

Asset Types, Card View (Total: 107)

Glucometer	Molecular Testing	Terminal Server	Urinalysis
92	6	1	8

Asset Vendors, Card View (Total: 107)

Abbott	Roche	Siemens
6	93	8

Resulting ACL microsegmentation rules

Policy validation dashboard

Optimized Virtual Local Area Network (VLAN) Segmentation

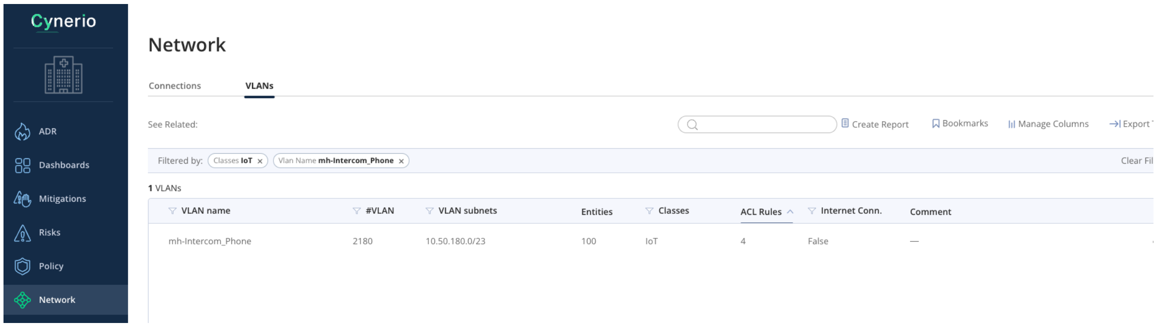
Many HDOs have some number of VLANs that can see significant improvements in security posture with relatively limited efforts. Any microsegmentation project should include the analysis of HDO network topologies to detect current VLAN configurations and identify these areas for "quick wins". This analysis should result in guidance that includes:

- The number of endpoints in each VLAN
- The types of devices in each VLAN (IoT, IoMT, IT, etc)
- VLAN connectivity to the Internet and other external systems
- ACL rules that can be applied to the VLAN while maintaining current connectivity

Such reports help HDOs identify securely configured VLANs, with common patterns being those that have a high number of similar devices requiring a small set of communication rules. More broadly, this approach can be used to identify VLANs consisting of mixed device types that may introduce unnecessary additional risk. This information can be used to better organize and secure the network by the separation of disparate devices.

Use Case - Intercom Phone Device VLAN

In this use case the analysis engine detected a pre-configured VLAN that included many of the intercom systems used at an HDO. Further analysis created a core set of ACL rules that were quickly deployed to secure the VLAN and the ~100 devices within it.



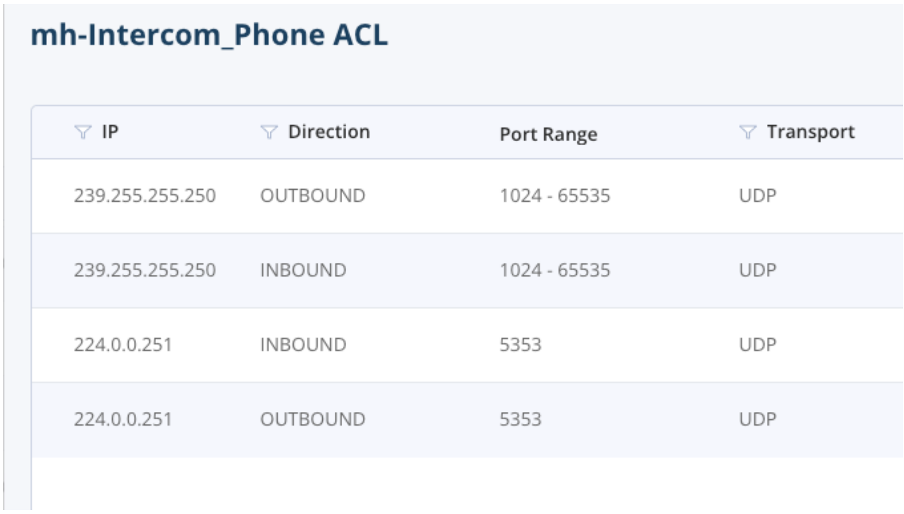
Network

Filtered by: Classes **IoT** × Vlan Name **mh-Intercom_Phone** ×

1 VLANs

VLAN name	#VLAN	VLAN subnets	Entities	Classes	ACL Rules	Internet Conn.	Comment
mh-Intercom_Phone	2180	10.50.180.0/23	100	IoT	4	False	—

Individual VLAN Report



mh-Intercom_Phone ACL

IP	Direction	Port Range	Transport
239.255.255.250	OUTBOUND	1024 - 65535	UDP
239.255.255.250	INBOUND	1024 - 65535	UDP
224.0.0.251	INBOUND	5353	UDP
224.0.0.251	OUTBOUND	5353	UDP

Identified VLAN ACLs

Microsegmentation Policy Deployment

The varied nature of HDO networks requires flexibility in deploying microsegmentation policies and protections. Among the most flexible methods for achieving these protections are segmentation using NAC tags.

Nearly all modern NACs provide the ability to ingest data and enrich their protections. When considering microsegmentation efforts, ensure all technologies have a capability to enrich NAC data with device and endpoint tags. This will allow for creation of device groups and ACLs that are beneficial when microsegmenting an environment and enforcing need-based communication levels at the device level.

The varied nature of network hardware and configurations requires flexibility in policy deployment. Beyond the capabilities provided by NAC tags, enabling policy deployment to common hardware including switches and wireless controllers is a necessary concern. Most modern microsegmentation tools provide support for both automated and manual deployments to meet individual needs of their users.

Policy deployment is not limited to NAC tags

Reference: Example NAC Vendor-Specific Guidance

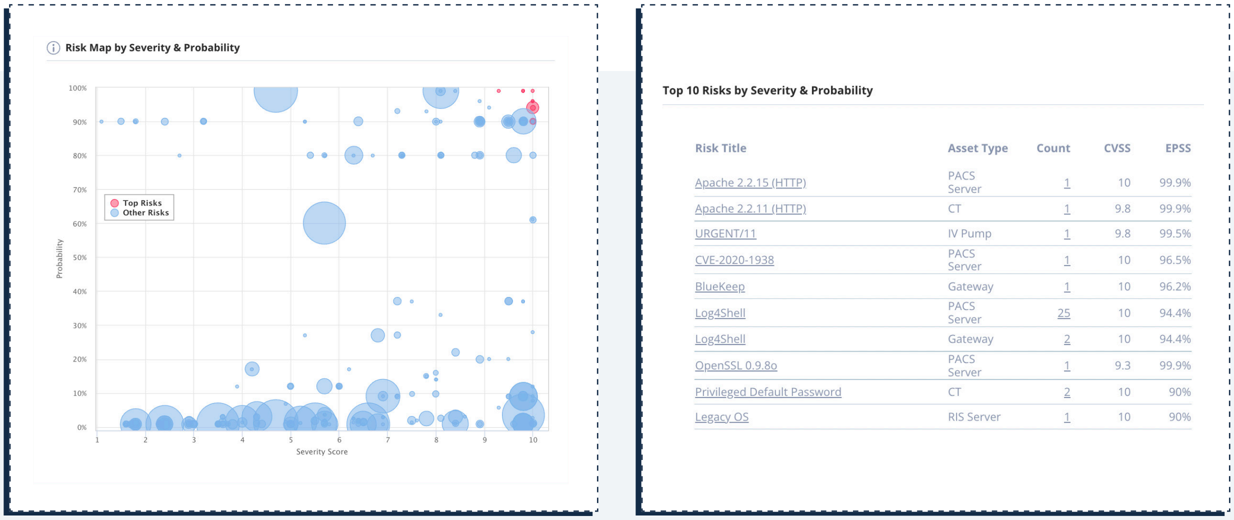
- Cisco TrustSec (SGTs)
- Working with Forescout Segments
- Aruba Filter ID-Based Enforcement Profile

Additional Considerations

The above recommendations are highly focused on specific microsegmentation considerations that must be made for modern healthcare environments. These will naturally exist adjacent to numerous legacy cybersecurity and IT systems, tools and practices. That said, there are several adjacent components that align well with microsegmentation efforts, both in terms of education and deployment. Any microsegmentation efforts should additionally consider:

- **Emerging Guidance -** Guidance is scattered regionally with new components frequently emerging. Many healthcare systems find that the guidance provided by the UK's National Health Service (NHS) is both achievable and provides improved protection. Two new components in particular have been introduced that align well with microsegmentation efforts. Namely, the Data Security and Protection Toolkit (DSPT) and Digital Technology Assessment Criteria (DTAC). Each of these resources provide research, guidance and insight in a clear and constructive format. From increased visibility during device procurement (DTAC) to analysis of current practices compared to best practices (DSPT), the self assessment tools provide guidance and insight that often require significant time commitments for teams to build. As microsegmentation efforts are considered, these two valuable resources should be introduced and adopted by all teams.

- **Risk Scoring and Prioritization -** A consistent theme among IT and security team members is lack of fiscal resources and team members. Among the many concerns, the "noisiness" of new and existing tools is often presented as a blocker to adoption or advancement of efforts including microsegmentation. Specifically, high volume analysis results that don't provide clear guidance often prevent teams from systematically addressing the risks in their environments.



Top 10 Risks by Severity & Probability

Risk Title	Asset Type	Count	CVSS	EPSS
Apache 2.2.15 (HTTP)	PACS Server	1	10	99.9%
Apache 2.2.11 (HTTP)	CT	1	9.8	99.9%
URGENT/11	IV Pump	1	9.8	99.5%
CVE-2020-1938	PACS Server	1	10	96.5%
BlueKeep	Gateway	1	10	96.2%
Log4Shell	PACS Server	25	10	94.4%
Log4Shell	Gateway	2	10	94.4%
OpenSSL 0.9.8o	PACS Server	1	9.3	99.9%
Privileged Default Password	CT	2	10	90%
Legacy OS	RIS Server	1	10	90%

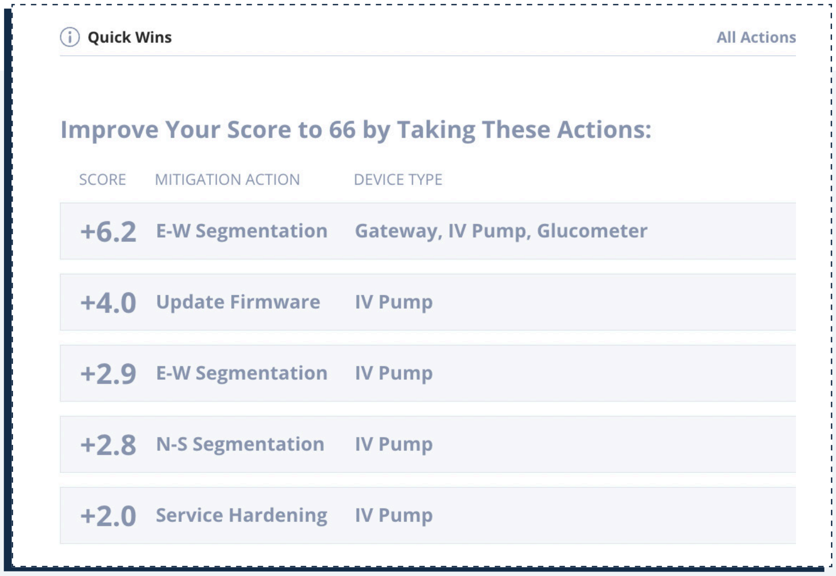
Prioritized Risks Guide Remediation

As microsegmentation efforts are made, a core consideration of automated scoring and prioritization of findings should be a top priority. Among the considerations:

- **Standardized Scoring Frameworks -** The adoption of standardized frameworks for scoring and prioritizing findings enables teams to be more effective. Among those found most beneficial for advanced IT and Security teams are the Common Vulnerability Scoring System (CVSS) and the Exploit Prediction Scoring System (EPSS). Adopting offerings that provide insight based on both of these frameworks will help in properly assessing risks present and prioritizing the order that they should be addressed based on likelihood of an exploit.

- **Validation of Findings -** Beyond scoring and prioritization of findings it can often be useful to have access to teams that validate findings and risk levels. As the teams investigate microsegmentation approaches, considering how IT and Security teams collaborate with outside experts such as Managed Security Service Providers (MSSPs) to validate and address findings will be particularly beneficial.

- **Actionable Recommendations -** Many security engagements have been hampered by a lack of clear guidance to address findings. In worst cases you may encounter a plausible deniability mindset where it's considered better to be unaware of a security issue than to know about it with no clear recourse. Technologies adjacent to microsegmentation efforts are no different, and some level of focus on clear, concise and achievable recommendations should be considered. From providing device patch details and instructions to generating fully tested microsegmentation policies, all technologies and procedures should strive to present both findings and solutions.



Improve Your Score to 66 by Taking These Actions:

SCORE	MITIGATION ACTION	DEVICE TYPE
+6.2	E-W Segmentation	Gateway, IV Pump, Glucometer
+4.0	Update Firmware	IV Pump
+2.9	E-W Segmentation	IV Pump
+2.8	N-S Segmentation	IV Pump
+2.0	Service Hardening	IV Pump

Quick Wins Provide Risk Insight with Direct Remediation Guidance

Check List: Microsegmentation Considerations

□ Focus Areas

- □ Visibility
- □ Risk Mitigation
- □ Real-Time Defense
- □ Regulatory Compliance

□ Microsegmentation Specific Considerations

- □ Network Level Device Profiling Segmentation
- □ Network Workflow Segmentation
  - □ Network Analysis and Policy Creation
  - □ Policy Analysis
- □ Optimized VLAN Segmentation
- □ Policy Deployment

□ Additional Considerations

- □ Emerging Guidance
- □ Risk Scoring and Prioritization
- □ Standardized Scoring Frameworks
- □ Validation of Findings
- □ Actionable Recommendations

About Cynerio

The constantly evolving threat landscape faced by the healthcare systems worldwide has impacted patients, finances and facilities in immeasurable ways. Microsegmentation is a proven method used by industry leaders (Finance, Insurance, Retail, etc) to prevent spread of attacks and minimize the impact of ransomware, malware and other attacks.

To combat these threats a combination of modern proactive and reactive measures must be introduced to HDOs that are often 15-20 years behind other industries. Microsegmentation is a core building block on this journey.

Cynerio was founded to provide healthcare organizations the tools, expertise and guidance that makes securing their environments more achievable. 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.

To speak with a member of the Cynerio team,
please contact us at info@cynerio.com