JOINT SOLUTION BRIEF

Cubro & **Cynerio** partner to address modern healthcare cyber risk

The Challenge

Staff shortages, unpredictable budgets, rapid adoption of caregiving technologies & mounting technical debt often leave healthcare leaders unsure where to begin improving their security practices.

Integrated Solution

Cynerio provides the technology and expertise needed to protect hospitals from cyberattacks and ransomware.

Cynerio integrates with Cubro Network TAPs and Packet Brokers to access network traffic in any complex hospital network environments. Cynerio also uses Cubro's purpose-built features for creating microsegmentation policies that are easy to deploy and manage.

Customer Benefits

- **Reduce attack surface** - Integration with Cubro allows Cynerio to see all network traffic, resulting in higher visibility of network connected assets. Increased visibility allows hospitals to secure & harden previously unseen devices.
- **Ease of network segmentation** - Cynerio and Cubro have strong features for network segmentation. By leveraging Cubro's support for leaf-and-spine network architecture, Cynerio can create easy to deploy and manager network segmentation policies.
- **Stop attacks on day one of implementation** – no need to wait for inventory or segmentation processes to finish to receive protection.

Cynerio has one simple goal:

Secure every IoT, IoMT, OT and IT device in healthcare environments.

Introduction

Every 7.1 minutes, a cyberattack occurs in Healthcare. Hospitals and other healthcare organizations are under severe threat of cyber attack. A major problem is the proliferation of connected medical devices, many of which are not secure by design and are difficult to lock down with traditional security approaches.

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.

Key functions & features of Cynerio 360 platform:

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

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

Inventory & Visibility
Cynerio Preventative Risk Management identifies all connected devices in a healthcare environment and provides detailed asset visibility in real-time.

Active Attack Detection
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.

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.

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

Cynerio Inventory and Visibility

Knowing what type of devices exist on a hospital network is the first step on the security journey. Cynerio recognizes all connected devices that interact with any part of the network in real time. The platform compiles an automated high-level asset inventory including device types, quantity of each, and details for each device, including category, vendor, IP address, operating system, and more.

Cynerio's dashboard denotes each device's overall risk in three areas — patient safety, data confidentiality, and service disruption. It lists each device's software vulnerabilities along with mitigation actions, and any information from the FDA databases on proper security configuration of the devices.

Cynerio Attack Detection and Response

The Cynerio IoT Attack Detection and Response module provides the tools to keep patients and any devices connected to them, safe from harm.

It allows hospitals to immediately identify attacks and quarantine connected devices exhibiting malicious or suspicious activity. The high-fidelity attack alerts are based on deep healthcare IoT expertise and are complemented by attack detection data from other Cynerio deployments, machine learning, and dozens of vulnerability and threat intelligence feeds collected from global sources.

Any attack observed on a device protected by Cynerio can be immediately isolated in a medically safe manner that enables hospitals to cut off the device's online connections and further remediate the incident later without impacting service availability or patient care.

The Cynerio platform provides detailed reporting on potential PHI (Protected Health Information) exfiltration, how risk exposure is decreasing over time, and step-by-step instructions broken down by affected device and attack type to ensure full remediation and recovery going forward.

The Power of Micro-Segmentation

Network segmentation is a proven strategy to improve security and control over large-scale network environments. Network segmentation divides a network into multiple parts, known as segments. Each segment acts as an isolated fragment of the network. Network administrators can assign different monitoring policies to different segments and put access controls on the traffic between segments

Cynerio not only provides information on device inventory—the what and why of medical devices—but provides the essential medical context hospitals need regarding how and why devices operate and communicate the way they do. This mapping makes it easy to identify which devices might represent a risk to the organization, and how the network should be segmented to avoid disrupting critical functions

Cynerio helps organizations define network segmentation rules to protect devices representing a high risk. Integration with top-tier security tools enables the enforcement of these policies.

The Need for Cubro Visibility

In order to perform its function, the Cynerio platform needs **visibility** into packet traffic on the network. This is the role of Cubro Visibility products: its Network TAPs and Packet Brokers.

Cubro Network TAPs

Cubro Network Taps work like Fiber Patch panels, however, a small percentage of the light traveling through the fiber is used to create an exact copy of all traffic passing on the network. TAPs are inexpensive devices that need no software, do not require power, and are transparent to normal network operations.

Some enterprises may be tempted to use spare router or switch ports to duplicate the traffic, rather than implementing TAPs.

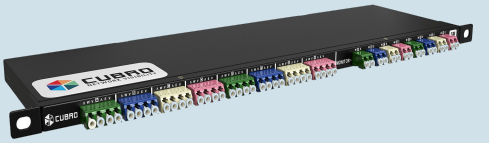
The limitation of these "SPAN" ports are shown in the text box. The risks of packet loss is too high to use Span Ports as a basis for critical security solutions.

Cubro Packet Brokers

The copied network traffic from the network TAPs is terminated onto Packet Brokers in order to aggregate, filter, and load-balance traffic onto Cynerio probes.

TAPS vs SPAN Ports

- SPAN ports are often built-in to LAN routers
  - Needs configuration and management
- But this application is the lowest priority after packet switching, ACL processing, logging, and other function
  - Packets will be dropped!
- Aggregates Uplink and Downlink (e.g 10G + 10G into a single 10G SPAN port
  - Packets will be dropped!
- Doesn't forward any error or malformed packet, and alters the timing
  - Does not reflect the network reality



Cubro Network Packet Broker

Network Traffic:

- Aggregated
- Filtered
- Load Balanced
- Burst protection
- De-duplication
- Header Removal
- Removal of Personal
- Metadata generation:
  - **Netflow**
  - **Enriched IPFIX**

Modern Hospital networking environments are typically very complex, with-variety of networking needs for:

- Patients and Guest
- Nurses and Doctors
- Administration and Accounting
- HVAC
- "Micro-Segments" supporting different classes of Medical devices.

The hospital also needs multiple Internet connections for Cloud-based applications and supports a variety of wireless and wired networking technologies.

Cubro packet brokers interface a variety of tools into this complex environment.

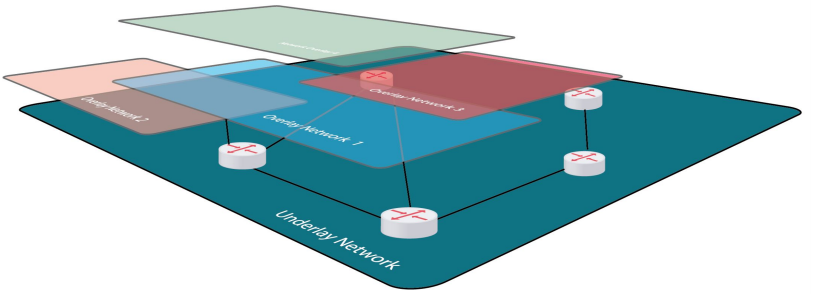
More on Micro-segmentation

Micro-segmentation is one of the key tools the Cynerio platform uses to secure devices. Micro-segmentation can address the following concerns:

- Misuse of a medical IoT device happens when either an application or a person uses the device to connect to unauthorized external networks.
- Most medical devices connect to external networks for operating systems and software updates. Attackers can hijack the session and reroute the communication to a server that will provide a malicious update, instead of a legitimate one, thus infecting the device.
- Some medical devices require a continuous external connection for standard operation. Unauthorized users can take advantage of unprotected external connections to penetrate patient-critical devices and exfiltrate data, like PHI.
- Medical devices often require vendor access for OS updates, to receive support services, and to send logs. Communication with vendors is usually conducted over a VPN. Organizations must control and monitor VPN connections.
  Patient-critical devices often include software with a 3rd-party library component (commonly open source). These libraries may contain vulnerabilities or backdoors of which IT is unaware.

Cubro Network Packet Brokers -- Built for Micro-segmentation

Most of the Network Packet Brokers on the market are built over commodity switching platforms, based on older Broadcom chips. These switches were designed for 1 to 10 gigabit per second links in flat, spanning-tree type networks. Today's networks are very different; they are much higher speed with 40, 100, and even 400 Gigabit per second links. Rather than flat bridged networks they use new leaf-and-spine architecture that provide increased performance, manageability, and have the capability to support 1000's of overlay networks that provide a built-in segmentation capability.



Visibility options:

- Visibility of the underlay network.
- Visibility of a specific overlay network.
- Visibility of all overlay networks.
- Visibility of the underlay and overlay at the same time, a "full end to end view"

New leaf-and-spine architectures offer extensive performance and segmentation features above and beyond traditional Virtual LANs (VLANs) and Access Control Lists. These new architectures can provide challenges for network tools not built for dealing with the new protocols needed. Cubro products have been designed to support these environment and can provides significant advantages in the number ports required, system footprint, power consumption, and overall cost to support network tools in micro-segmented hospital networks.

For more information please visit www.cubro.com and www.cynerio.com