illumio | CYLERA™

SOLUTION BRIEF

# Illumio and Cylera for Healthcare IoT, OT and IT Security

The integration of Illumio and Cylera technology provides unprecedented security for IT, OT and IoT healthcare applications, data and devices

## Securing Diverse Healthcare Networks

Healthcare providers have become prime targets for ransomware. Attackers are exploiting the fact that most providers have incomplete visibility of diverse inventories of medical IoT (MIoT) and OT devices, including how they're connected to IT systems.

With the proliferation of devices and applications containing digital health records, healthcare networks tend to lack sufficient segmentation to protect these assets.

The interconnectivity between and within MIoT, OT and IT networks represents an expansive digital landscape that is becoming increasingly difficult to protect. Without proper segmentation, criminals and ransomware can rapidly move through a network and across networks — sometimes within a matter of minutes.

As the past two years have shown, endpoint security tools will eventually detect the presence of ransomware in a given node, but that is often after the ransomware has already spread laterally. Healthcare providers need a better way to preemptively limit the spread of cyberattacks and malware across their IoT, OT and IT networks.

## Full Visibility and Zero Trust Control for Healthcare Systems and Devices

The integration of Illumio and Cylera technology provides unprecedented protection for IT, OT and IoT healthcare provider applications, data and devices. With Illumio and Cylera, you can:

- **Discover, categorize and map** all medical IoT, OT and IT systems and communications in a single view, regardless of location: in the cloud, data centers, hospital networks or remote locations with physicians on laptops.
- **Conduct "zero-touch" vulnerability analysis** using patented techniques. Identify exposed systems and implement Zero Trust policies with no impact to physical devices or patient safety.
- **Identify and ring-fence high-value systems** to protect them from the spread of breaches. By segmenting medical assets from IT systems, only verified communications will be allowed, preventing the movement of any malware.
- **Build an automated incident response system** to apply extra restrictions should an attack be detected.

## Simplified Protection for Medical IoT, OT and IT Networks

**Preemptively Isolate Breaches**
By segmenting the network before an attack occurs, organizations can limit the spread and impact of a breach.

**Identify and Respond Faster**
By combining identification of unauthorized connection attempts with other detection methods, attacks can be spotted earlier.

**Stop Ransomware in Its Tracks**
Move quickly to block pathways of attack in real-time, either manually or automatically using a SOAR platform.

## Illumio and Cylera Joint Solution: How It Works

By integrating Cylera with Illumio Core, it is now possible to see the flow of communications among your entire estate of medical devices, operational systems, IT systems and applications — all in a single, interactive map.

Illumio uses compute workload metadata and flow information to map communications between workloads. Using your existing naming structure, simple labels are applied to each workload to display the entire infrastructure. These IT systems could be traditional Linux and Windows systems, AIX, IBM Z Series, containers and cloud platforms.

Cylera uses patented AI to discover, identify, catalog and create a "digital twin" of each connected medical device, OT system and regulated IT device. It provides vulnerability analysis, risk assessment and threat intelligence.

The combined contextual data of Illumio-labeled systems and Cylera-analyzed systems is imported into the Illumio application dependency map and displayed in a single view. Vulnerabilities that indicate points of higher risk within the infrastructure can be identified and prioritized, with appropriate measures put in place.

For example, with only a few simple clicks on the map, Zero Trust Segmentation policies can be implemented to protect IT systems and OT devices. All the devices and systems within a function can be compartmentalized to isolate them from potential threats in other areas of the infrastructure.

Illumio's mapping and Zero Trust Segmentation capabilities powered by Cylera give healthcare providers the comprehensive visibility and control needed to reduce risk and increase cyber resilience.

If and when a breach occurs, Illumio and Cylera's integrated solution can help you quickly identify and contain its spread, avoiding a major shutdown of critical systems and healthcare services.

Illumio's mapping and Zero Trust Segmentation capabilities powered by Cylera give healthcare providers the comprehensive visibility and control needed to reduce risk and increase cyber resilience across their IT, OT and IoT networks.

### Illumio and Cylera Will Help You Move Forward

It is now possible to see your entire estate of medical and IT devices and application workloads in a single, interactive map.

Learn more about how Illumio and Cylera are helping HDOs with their Zero Trust journey.

Visit:
www.illumio.com/solutions/healthcare or www.cylera.com

## About Cylera

Cylera's leading-edge IoT security and intelligence technology provides unique depth in asset identification and management, network analysis, risk assessment, network segmentation, threat detection and intelligence, operational analytics and fleet optimization.

## About Illumio

Illumio is the leader of Zero Trust Segmentation. See your risks, isolate attacks and secure your data to stop breaches from becoming cyber disasters.