CYLERA™ | illumio

SOLUTION BRIEF

Cylera and Illumio Integration

Healthcare IoT Device Visibility and Zero Trust Segmentation

Lower connected medical device risk and build cyber resilience

The Challenge

Ransomware continues to hit a cross-spectrum of industries particularly hard. Attackers are exploiting that most organizations have incomplete visibility about their diverse inventory of managed and unmanaged IoT, OT, and IT devices, including how these systems are interconnected.

As organizations increasingly adopt IoT technology for business benefits, they also face significant security challenges. Often, organizations invest in IoT without implementing adequate security measures, leaving their networks vulnerable to cyber attacks. The growing interconnectivity between IoT, operational technology (OT), and IT networks exacerbates the problem, making it easier for attackers to cripple a company's ability to conduct business. To address these challenges, a layered approach using the best security tools available is required.

The Solution

The Cylera and Illumio joint solution provides comprehensive device visibility and Zero Trust micro-segmentation capabilities to mitigate these risks. By integrating Cylera with Illumio Core, it is now possible to see the flow of communications among your entire estate of IoMT/IT/OT — all in a single, interactive map.

Illumio uses workload metadata and flow information to map the communication between workloads, enabling simple labels to be applied to each workload to display the whole infrastructure. In parallel, Cylera uses patented adaptive data type analysis and network traffic emulation technologies to discover, categorize, characterize, devices, and patented network traffic emulation technology to assess devices for vulnerabilities, risks, and threats.

Simplified Protection

- **Preemptively isolate breaches:** By segmenting the network before the next attacker arrives, organizations can pre-empt the progression and impact of the intruder.
- **Early detection informs faster response:** By combining the identification of unauthorized connection attempts with other detection methods attacks can be spotted earlier.
- **Stop ransomware in its tracks:** Immediately upon detection, the spread radius can be tightened in real-time, either manually or automatically (using a SOAR platform), forcing further lateral propagation to cease.

The combined contextual data of Illumio-labeled systems and Cylera-analyzed systems is then imported into the Illumio 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.

Benefits

The Cylera and Illumio joint solution provides comprehensive device visibility and Zero Trust microsegmentation capabilities to help mitigate risks and ensure business continuity. The benefits of this integration include:

- **Improved Visibility and Visual Mapping:** Complete device discovery and categorization into both IT network and IoT/OT network traffic, and complete visual mapping - regardless of location: in the cloud, data centers, hospital networks, or remote locations with physicians on laptops.
- **Zero Disruption to Business Continuity:** Conduct "zero-touch" vulnerability analysis using patented techniques. Identify exposed systems and implement Zero Trust policies with no impact on physical devices or patient safety.
- **Faster Threat Detection and Response:** A more rapid response to identified threats, minimizing the potential impact of an attack and reducing the time needed to isolate or remediate a compromised device.
- **Validate Existing Assets and Segmentation:** Complete visibility into all connected devices and segmentation in IoT/OT networks and between IT and IoT/OT. Furthermore, identify high-value systems and implement additional policies to protect them from the spread of breaches.

illumio

Illumio, the pioneer and market leader of Zero Trust segmentation, prevents breaches from becoming cyber disasters. Illumio protects critical applications and valuable digital assets with proven segmentation technology purpose-built for the Zero Trust security model. Illumio ransomware mitigation and segmentation solutions see risk, isolate attacks, and secure data across cloud-native apps, hybrid and multi-clouds, data centers, and endpoints, enabling the world's leading organizations to strengthen their cyber resiliency and reduce risk.

www.Illumio.com

CYLERA™

Cylera provides the easiest, most accurate and extensible platform for healthcare IoT intelligence and security to optimize patient care, service availability, and cyber defenses across diverse connected medical device and healthcare environments. The Cylera platform accurately discovers, categorizes, assesses, and monitors known and unknown assets with high fidelity to deliver unparalleled asset inventory, usage telemetry, risk prioritization, analytics, and guided threat remediation. Cylera integrates with popular IT and healthcare systems to allow organizations to advance cyber program maturity, increase operational efficiency,mitigate cyber threats, and enable compliance readiness.

www.cylera.com