CYLERA™ | CISCO ISE

SOLUTION BRIEF

Cylera and Cisco ISE Integration

Accelerate Network Access Control Policy Creation

Maximize Cisco ISE investments while improving healthcare IoT device visibility and security

The Challenge

Network Access Control (NAC) solutions, such as Cisco ISE, are vital to ensure that only authorized devices within healthcare systems are granted access to network resources. However, in healthcare and clinical settings, most NAC solutions lack the depth of insight and context required to fully identify all healthcare IoT and connected medical devices and appropriately enforce appropriate device access control security policies.

Many healthcare IoT and connected medical devices present as undiscovered and umanaged on healthcare networks. As a result, NACs struggle to obtain and verify these types of unmanaged devices' software, firmware, and other details required to accurately enforce device access security policies.

Although NAC solutions can enable preventative protection and enforce efficient device authorization and segmentation policies, for healthcare IoT, NAC solutions require more details as to why and under what clinical conditions these systems should take specified action. This requires additional behavioral analytics, baseline device profiling, and an understanding of clinical requirements that complement existing NAC capabilities.

When factored against the range of medical device manufacturers, device and model types, specialized and proprietary protocols, and limited documentation, an integration between Cisco ISE and the Cylera platform becomes essential. The Cylera's platform's clinical risk assessment capabilities, combined with the ability to automatically create and share granular network segmentation security policies with Cisco ISE, ensures the right network access for the right devices at the right times for optimal healthcare network protection.

The Integrated Solution

- Cylera has partnered with Cisco to deliver patented techniques and clinical context through its integration with Cisco Identity Services Engine (ISE).
- Cylera's healthcare-centric cybersecurity intelligence combines intimate knowledge of healthcare IoT device behavior, protocols, medical workflows, patient care, safety, and privacy standards with Cisco's networking and cybersecurity expertise.
- Cylera provides healthcare IT teams that administer Cisco ISE the enriched visibility and advanced capabilities required to automatically generate error-free policies. The generated policies are seamlessly forwarded to Cisco ISE, where they are enforced automatically or after manual review. This minimizes errors and ensures consistent medical device access policy enforcement.

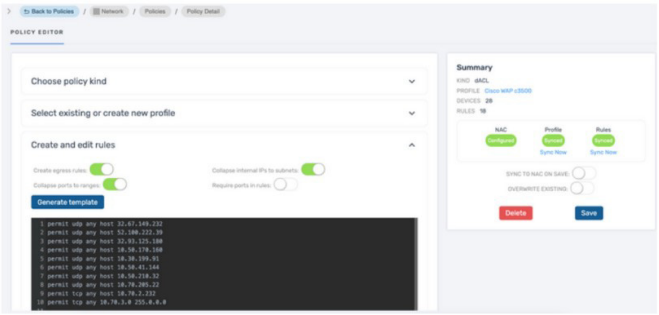
Integrated Solution Benefits

- **Enhanced Security:** Cylera's detailed device profiling and risk analysis, combined with Cisco ISE's access control capabilities, strengthens the overall security posture, reduces vulnerabilities, and protects sensitive patient data.
- **Improved Operational Efficiency:** Automated policy creation and seamless enforcement save IT teams time and effort, allowing them to focus on strategic initiatives rather than on manual, repetitive tasks prone to human error.
- **Uninterrupted Patient Care:** With robust security and efficient operations, clinical workflows remain uninterrupted, enabling healthcare professionals to focus on delivering quality patient care.
- **Cost Savings:** By reducing the risk of cyber attacks and streamlining operations, the integration minimizes potential financial losses and optimizes resource allocation.

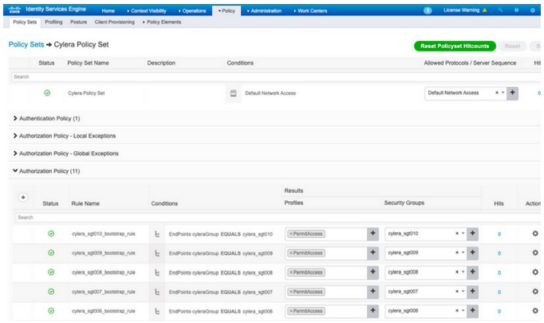
How It Works

Cylera's sensor is easily deployed to monitor network traffic through SPAN or tap ports on a switch. Connectivity to Cisco ISE and data sharing is through Cisco's Platform Exchange Grid (pxGrid).

- The Cylera sensor passively monitors network traffic, discovering and profiling IT, IoT, and connected medical device assets with zero disruption to patient care services and normal device operations.
- New and updated IT, IoT, and connected medical device identification data from Cylera is forwarded to Cisco ISE, updating ISE device inventory with granular device information based on a deep clinical understanding of device operational norms, workflows, and risks.
- Within Cylera, administrators can create Cisco TrustSec or dACL/SGACL policies, then automatically forward the policies to Cisco ISE.



- Once Cylea forwards the policies to Cisco ISE, the Cylera policies display in the Cisco Management Console.



Summary

The Cylera and Cisco ISE integration enhances healthcare IoT and medical device security by providing enriched visibility and automated policy enforcement. Cylera profiles connected devices, sharing detailed insights with Cisco ISE to enable precise medical device identification and security management. The integration automates medical device security policy creation and deployment, reducing manual effort and minimizing errors. It also supports dynamic network segmentation, isolating devices based on risk levels and operational needs. For healthcare organizations, the integration ensures robust security, uninterrupted clinical workflows, and compliance with regulatory standards such as HIPAA and HITECH in the US, and NIS, CAF, DSPT, and GDPR in the UK. By safeguarding sensitive patient data and streamlining operations, the Cylera and Cisco partnership helps ensure secure, reliable, high-quality patient care.

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.

CYLERA™

www.cylera.com