CYLERA | FORESCOUT

SOLUTION BRIEF

Cylera and Forescout Integration

Decrease Healthcare IoT Risk and Enforce Medical Device Policies

Dynamically reduce the medical device attack surface and isolate non-compliant, at-risk devices

The Challenge

Modern healthcare delivery organizations (HDOs) are challenged by the rapidly proliferation of healthcare IoT devices. Millions of connected healthcare IoT devices have demonstrated benefits such as cost savings, improved patient outcomes and convenience, reduced errors, increased efficiencies and effectiveness, business data analytics, operations optimization, and more

However, these benefits come with an ever-expanding risk profile that in many cases cannot be properly known or measured and also result in evolving security gaps that can be leveraged by cyber threat actors.

Healthcare IT and security teams know that they can't secure what they can't see or don't know about. It is critical for IT, security, and/or clinical teams to accurately detail the inventory of all connected assets they have on their networks. Further, it is important to have a true assessment of the organization's security risk posture and rapidly respond when a security or compliance lapse occurs. This is only made possible by continuously collecting rich, detailed information on all of the connected medical devices involved in patient care.

The Solution

The Cylera and Forescout integration helps HDOs understand and dynamically reduce their attack surface, stop the progress of an attack or threat, and isolate non-compliant, at-risk devices for further investigation and remediation.

Benefits

- **Automatic asset discovery,** identification, classification, vulnerability assessment, risk scoring, and policy enforcement for all healthcare IoT and connected medical devices
- **Zero-touch**, no disruption to physical devices or patient care services
- **Dynamic risk assessment**, access control, network segmentation, and threat containment for devices across the campus, clinical network, data center, and cloud instances at scale
- **Unified view** across clinical engineering and IT teams enhances security posture, collaboration, and security policy enforcement
- **Regulatory compliance and security frameworks support** for HIPAA, DSPT, NIST CSF, HITRUST, and other standards

How It Works

Together, Forescout and Cylera provide a unique solution for healthcare organizations that passively and continuously discovers, assesses, and classifies all healthcare IoT and connected medical device without requiring an agent.

In specific, Cylera has patented, leading-edge Deep Packet Inspection (DPI) and Artificial Intelligence (AI) technologies that provide customers with more actionable healthcare IoT and connected medical device insights, broader and more informed clinical and patient context, and a patented technique for IoT Device Emulation™ that can apply "zero-touch" vulnerability assessments for healthcare IoT and connected medical devices, which are rarely able to be patched, but must be assessed. With no touch to the actual physical device, or disruption to patient services and workflows, Cylera can provide vulnerability assessment, risk scoring, and built-in response plans to speed the ability of IT teams to identify and respond to a prioritized list of security issues.

In the Cylera and Forescout integration, Cylera uses its proprietary intelligence to analyze medical devices, then provides detailed, highly accurate clinical device data which can then be shared with Forescout, enhancing Forescout's ability to enforce granular clinical security policies.

Cylera enriches Forescout device data with deep clinical device context that can be utilized by Forescout's enterprise-wide policy engine to enforce network access, segmentation, device compliance, and threat or incident response policies.

Further, the integration helps to ensure the right policies are enforced with the right devices at the right time without disrupting critical clinical processes or patient services.

Security teams gain the enterprise-wide asset visibility and control they need. Clinical/biomed engineering gains the security they can trust to ultimately protect patients, their data, and overall safety with advanced medical device cybersecurity and management.

Summary

The integration between Forescout and Cylera brings organizations rich, contextual insight into their clinical and IT networks. Teams benefit from sophisticated clinical network analysis that can detect and contain threats and improve security posture by using policies that automatically enforce network access control, segmentation, device compliance ,policies.

TheCylera and Forescout integration provides a practical solution that fits seamlessly into existing corporate and clinical networks while supporting HDO requirements for safeguarding patient care, safety, privacy,and business continuity.