

Cylera and Cisco DNA Integration

Quickly Identify Precise Location of Healthcare IoT Devices

Speed cyber risk remediation and manage connected medical device security more cost-effectively

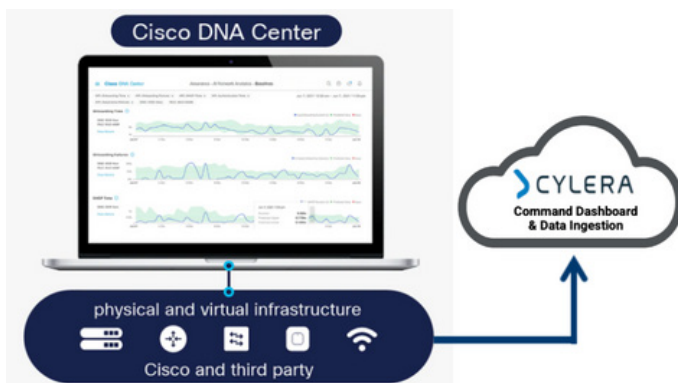


Healthcare delivery organizations strive to achieve full device visibility and security across all of their healthcare IoT and connected medical devices, as well as maximize their existing investments in Cisco solutions.

The Cylera platform’s integration with both Cisco DNA Center as well as Cisco Prime, the predecessor to Cisco DNA Center, gives healthcare organizations a single source of truth across healthcare IoT and connected medical devices on their network.

By using the Cylera platform’s deep device intelligence and cybersecurity capabilities in combination with Cisco DNA Center, organizations can see information about medical devices that they have always needed, but have previously been unable to obtain. These insights benefit both IT security and clinical engineering teams, and help hospitals operate more efficiently,

The Cylera integration with Cisco DNA Center is also seamless and simple. The integration is built in to the Cylera platform, and does not require additional professional services for implementation.



ABOUT CISCO DNA CENTER AND CISCO PRIME

Cisco DNA Center™ was launched in 2017 as the next step in network evolution. This expansive platform encompasses a complete portfolio of software-based network automation and assurance solutions. It is also the dashboard for control and management of Cisco’s intent-based networking (IBN) system. Cisco DNA is designed for use by both Enterprises and Service Providers.

Cisco Prime™ Infrastructure is the predecessor to Cisco DNA Center, and was a network management software suite with an array of different software applications, most geared either to Enterprise or Service Providers. Prime is no longer for sale as of 2020, and end-of-life/end-of-sale on various components began in 2014.

Cylera integrates with both Cisco DNA and Prime.

Integrated Solution Benefits

- ▶ **Automation:** Collects device information from Cisco on an automatic schedule, and integrates data directly into Cylera, machine-to-machine, without human intervention or error
- ▶ **Improved Mean-Time-to-Respond (MTTR):** Cylera provides device location, and with Cylera's vulnerability and risk analysis, you move more quickly, according to device priority, for risk remediation and incident response. This results in a measurable improvement in MTTR.
- ▶ **Device Utilization & Maintenance Optimization:** Devices have scheduled maintenance and Cylera tracks device utilization which can impact maintenance frequency. Cylera also delivers visibility into patches available, and many devices require patching at the device physically. With location information, these devices are faster and easier to find for direct patching when necessary. Direct links to patch information also helps staff determine whether patching could occur during maintenance
- ▶ **Resource Optimization:** There can be large counts of IoT and medical devices. Cylera provides data to simplify device optimization and deliver business value. As an example: there can be hundreds of infusion pumps in a hospital, many of which aren't being actively used. Locating them quickly is one aspect, other factors could be relevant to patient and staff scheduling, rent v. buy decisions, and data from Cylera helps support business decisions such as these.


How It Works

Cylera is an advanced healthcare IoT security and intelligence platform that passively monitors traffic in the network that discovers, identifies, categorizes and analyzes specialty communications of connected devices and processes.

Cylera integrates with Cisco DNA Center™ APIs to query the Cisco DNA controller over a VPN and brings back asset information if available. Cylera can then enrich the device analysis already in place or do new analyses of network, vulnerability, risk factors, and device optimization.

Specific value Cylera can provide to either IT security teams or clinical engineering organizations includes:

- ▶ **Device location provided, with patented techniques for zero-touch visibility** into device vulnerabilities, available patches, and risk scoring without ever touching or disrupting the physical devices.
- ▶ **Relevant analysis applied**, such as device manufacturer alerts, linked CVEs, CVSS data and available patches, industry alert information, etc.
- ▶ **Risk and mitigation/remediation playbooks**, useful to either IT or clinical personnel before, and when incidents may occur.
- ▶ **Device utilization, maintenance and resource optimization support** business decisions such as device rent v buy, personnel and patient scheduling, and counts of hours in use, patients served, and images taken.

Device Info		
MODEL	Roche Accu-Chek Inform II System	VENDOR Roche Diagnostics
TYPE	Point of Care Analyzer	CLASS Medical
MDS2	0 forms	IP 10.70.2.116
HOSTNAME	ACI2-22601	MAC 00:00:2a:01:00:19
VLAN	22	FIRST SEEN 5/3/2021 8:51:14 PM
LAST SEEN	8/27/2021 2:20:49 PM	
Attributes		
DISCOVERED BY	Cisco DNA	NETWORK SSID sandbox
WIRELESS FREQUENCY	2.4	AP GROUP default-group
HOST TYPE	WIRELESS	AP MAC ADDRESS 00:2b:01:00:05:00
SNR	26.0	AP HOST NAME T1-4
WLC MAC	10.10.20.51	AP SERIAL NUMBER 1140K0004
LOCATION	Kurbadet/Bygg X/Floor 420	

Cylera displays the additional device information it receives through its integration with Cisco DNA Center directly within the Cylera dashboard.

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