Cylera and Extreme Networks Integration

Secure Identity and Network Admission Control for Healthcare

Protect healthcare IoT and connected medical devices from unauthorized access

The Challenge

Ensuring the security of connected devices and managing user access are essential components of any security program, particularly in regulated industries such as healthcare and life sciences. The rapid expansion of healthcare IoT and connected medical devices has made it challenging for organizations to identify and manage these devices effectively. However, unmanaged devices can create security and safety gaps that threaten patient safety and privacy, increase the risk of unauthorized access, and potentially disrupt patient care delivery.

The Solution

Cylera and Extreme Networks have partnered to provide an integrated solution that addresses these challenges. This integrated solution combines the Cylera platform with ExtremeCloud IQ-Site Engine and ExtremeControl to deliver device discovery and classification, risk and vulnerability analysis, and user access and security management for all healthcare IoT and connected medical devices on healthcare networks.

The Cylera and Extreme Networks integration offers organizations a comprehensive and clinically-aware solution to discover and protect healthcare IoT and connected medical devices against unauthorized access by ensuring ExtremeControl is fully aware of all connected healthcare devices.

Benefits

▶ Improved network visibility and control

▶ Enhanced network security and compliance

▶ Faster **threat detection and response**

▶ Maximization of current investments with no additional cost

▶ Seamless integration

Fortify Care. Accelerate Cyber Resilience.

Integration Highlights

▶ **Improved network visibility and control:** Complete device discovery, enabling organizations to have full visibility into all connected devices with device identification, characterization, and categorization.

▶ **Enhanced network security and compliance:** Enhanced network access controls ensure only authorized devices and users can access the network, and includes managed and unmanaged devices, improving compliance with healthcare industry regulations.

▶ **Faster threat detection and response:** More rapid threat identification and response helps minimize the potential impact of an attack and reduces the time needed to isolate or remediate a compromised device.

▶ **Maximize current investments:** Optimization of current tech stack further strengthens healthcare IoT and connected medical device cybersecurity and identity management and access control.

▶ **Seamless integration:** Integration provides the ability to create and sync policies and access Extreme Network screen views all from within the Cylera platform, without requiring additional services or back-end programming.

How It Works
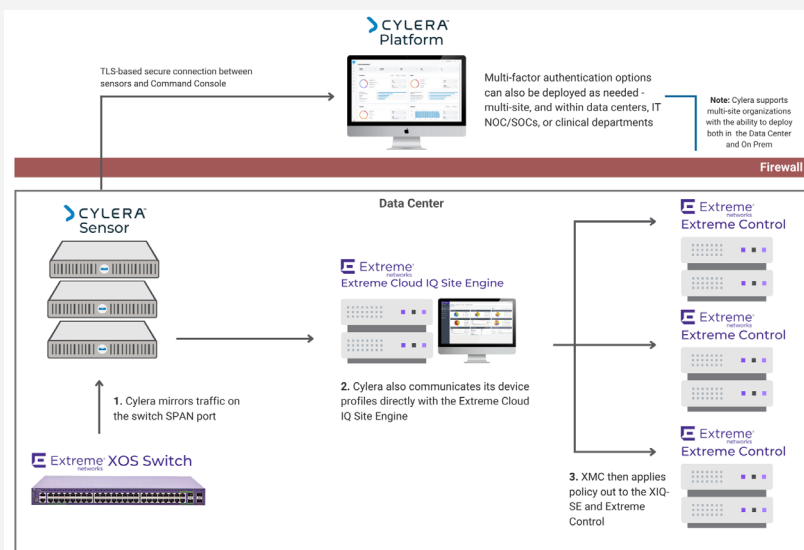
▶ Administrators can push device profiles to the Extreme Management Center either manually or on a schedule, enabling ExtremeControl appliances to identify network assets and manage policies.

▶ Administrators can also pull device attributes from the Extreme Management Center to further enrich inventory accuracy and device location tracking within the Cylera platform.

Summary

The Cylera and Extreme Networks integration is a resource-efficient, clinically-aware way to discover and protect healthcare IoT and connected medical devices against unauthorized access and to keep ExtremeControl fully aware of all healthcare devices on the network. With its ease of deployment, full support, and seamless user experience, the integration gives healthcare delivery organizations the integrated solutions they need to manage their medical devices moire effectively.