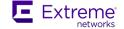# Asimily Insight & ExtremeCloud IQ Controller

Healthcare and life sciences facilities have seen a surge in the number of connected IoT devices, and as connectivity has increased so, too, have cyberattacks. Managing and securing connected medical and IoT devices is a challenge but essential to stop unauthorized access, data breaches and disruption to patient care.

Asimily's IoMT risk remediation platform holistically secures the mission-critical healthcare devices that deliver care. Asimily passively monitors medical devices on the network to inventory every device, identify, prioritize, and mitigate vulnerabilities and anomalies, create and enforce policies, and isolate, segment, and micro-segment devices on the network.

Extreme Networks ExtremeCloud IQ Controller is a key offering within the Extreme solution targeted for the on-premise campus solution. It incorporates extensive policy and control to securely manage users and devices.

The Extreme Networks and Asimily joint solution addresses these challenges by integrating the Asimily Insight platform with ExtremeCloud IQ Controller. After Asimily identifies, classifies medical devices on a network and determines the risk and impact, Insight invokes the IQ Controller API to centrally enforce network access policies to isolate, segment, and micro-segment the devices on the network. Once the system has been configured, Asimily enables administrators to apply enforcement actions such as quarantining or blocking external traffic via the Insight console directly to IQ Controller.

While ExtremeCloud IQ Controller is the first Extreme solution Asimily has integrated with, Asimily and Extreme are strong partners and can add other integrations to offer similar capabilities as required.

Integration Benefits

- Precise medical device classification and profiling that are essential for driving network policies

- Rapid network isolation for compromised medical devices

- Automatic service restoration upon remediation