ASIMILY

FORESCOUT

Dynamically Secure Healthcare Organization Networks

ASIMILY FORESCOUT

Why Solution Integration

Healthcare and life sciences facilities have seen a surge in the number of connected IoT devices, including medical devices, and as connectivity has increased, so have the cyberattack incidents. Approximately 25% of cyberattacks involved IoT devices in 2020, and by 2025 attacks are expected to grow by 500%. Many IoT devices subject to attack are vital to patient care, including blood glucose monitors, infusion pumps, imaging devices, patient monitors, and laboratory processing equipment. Managing and securing connected medical and IoT devices is a challenge but essential to stop unauthorized access, data breaches and disruption to patient care

Medical Device Cybersecurity Risk Mitigation

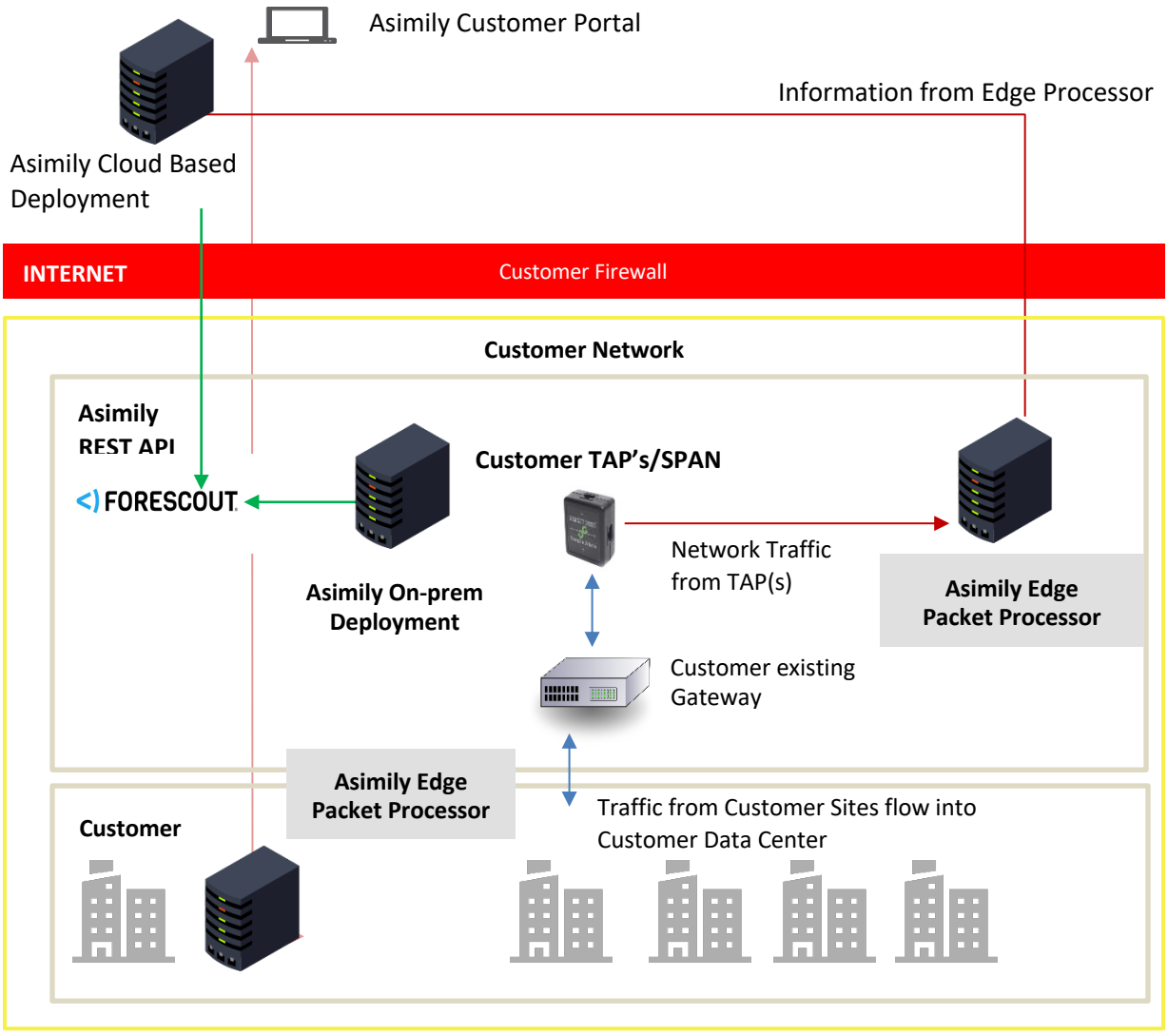
Asimily's Internet of Medical Things (IoMT) risk remediation platform holistically secures the mission-critical healthcare devices that deliver safe and reliable care. Asimily passively monitors medical devices on the network to inventory every device, track device location, identify, prioritize and mitigate vulnerabilities and anomalies, discover detailed flows, create and. Through integrations like Forescout, enforce policies, isolate threats, segment and micro-segment devices on the network.

With so many agentless devices being deployed every day, it's never been harder to protect your network from threats. Forescout provides real-time enterprise-wide actionable insight for all connected devices across IT, IoT, IoMT and OT and utilizes this intelligence to automate context-aware policy-driven actions to enforce device compliance, network access control (NAC) and segmentation. Forescout uses Asimily's REST API to import Asimily medical device context and risk information to further enhance its actionable visibility and enforce granular security policies without disrupting critical operations such as medical services. Asimily and Forescout customers are able to streamline risk reduction across both clinical and IT environments.

Benefits

- Precise medical device classification and profiling that are essential for driving network policies
- Rapid network isolation for compromised medical devices
- Automated service restoration upon remediation

Integration Architecture



Integration Data Flow

1

Asimily monitors and classifies medical devices on the network, monitors utilization, detects exploitable vulnerabilities, anomalies and associated risk and impact on those devices.

2

Forescout uses Asimily REST API to import Asimily medical device context, vulnerability, risk, impact, recall, utilization information as host attributes. Forescout uses this information to create granular security policies based on medical device identifiers, risk, impact and utilization.

3

Forescout automates device compliance, network access and segmentation enforcement workflows based on context aware policies. Forescout applies network controls to contain and mitigate cybersecurity risks detected by Asimily and/or Forescout.

About Asimily

Asimily's IoMT risk remediation platform holistically secures the mission-critical healthcare devices that deliver safe and reliable care. Asimily helps customers inventory their devices, prioritize and remediate vulnerabilities and monitor, detect and mitigate anomalies and security threats. Through Asimily's platform, Health Systems of different sizes across different countries have been able to reduce their risk, improve organizational security, reduce operational expense and meet compliance standards. Asimily Heals the Devices that Heal. Learn more at www.asimily.com.

About Forescout

Forescout Technologies, Inc. actively defends the Enterprise of Things by identifying, segmenting and enforcing compliance of every connected thing. Fortune 1000 companies trust Forescout as it provides one of the most widely deployed, enterprise-class platforms at scale across IT, IoT and OT managed and unmanaged devices. Forescout arms customers with extensive device intelligence, data and policies to allow organizations across every industry to accurately classify risk, detect anomalies and quickly remediate cyberthreats without disruption of critical business assets. Don't just see it. Secure it. The Enterprise of Things – Secured. Learn more at www.forescout.com.