DATA SHEET

Asimily + Qualys Integration Solution

Introduction

Asimily's industry leading IoMT risk remediation platform enables Customers to holistically secures mission-critical healthcare devices so they can deliver safe and reliable care.

Challenge

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. Securing connected medical and IoT devices is a challenge but essential to stop ransomware attacks and disruption to patient care.

Together Asimily and Qualys provide a comprehensive solution to meet this challenge. Asimily Insight supports integration with Qualys VMDR, an vulnerability management (VM) solution that conducts authorized "active" vulnerability scanning against systems deployed in your environment. This integration enhances Insight's exploit analysis by importing vulnerabilities discovered by Qualys and using them as part of Insight's Likelihood scoring.

Key Solution Benefits

- Higher productivity in identifying and remediating at risk device due to enriched exploit analysis
- Improve patient safety by eliminating the need to actively scan any medical device
- Reduce risk through prioritization

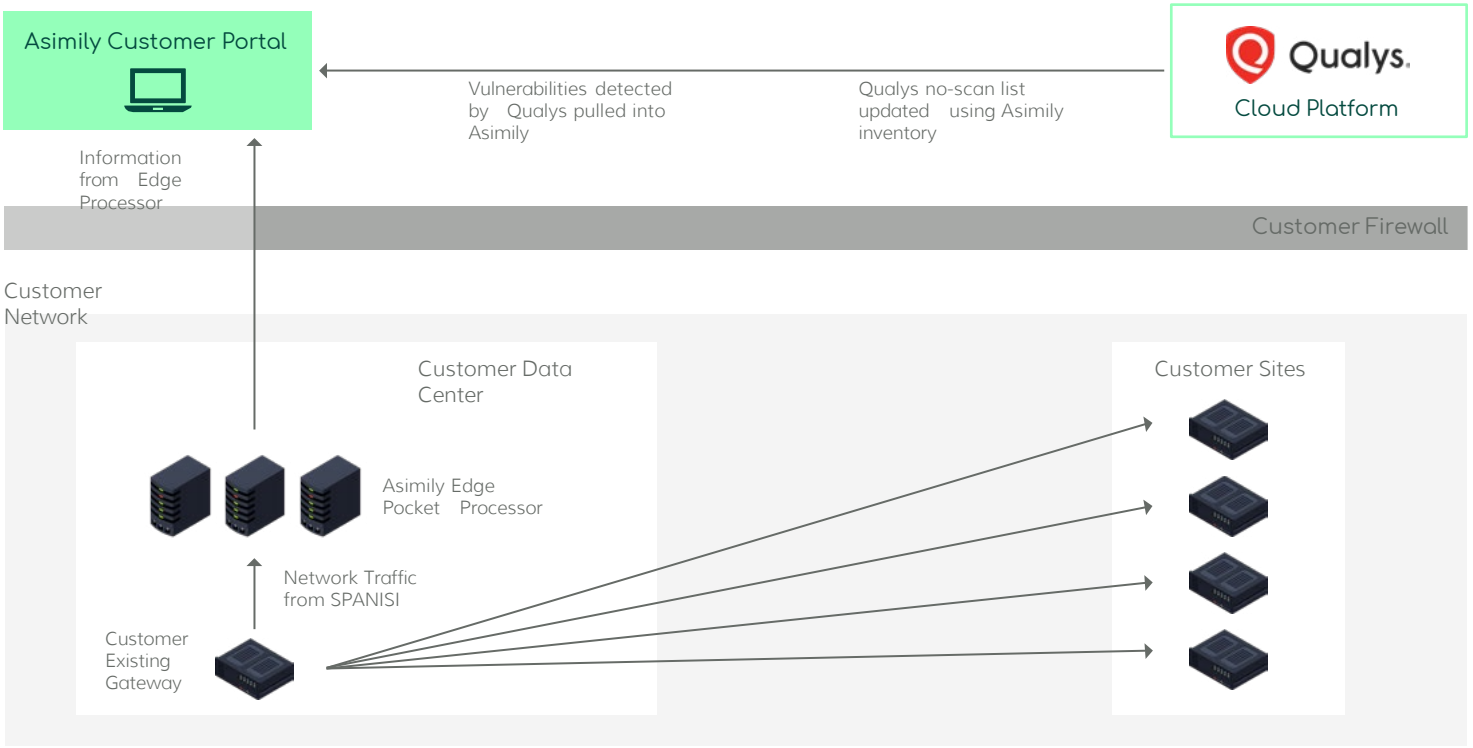
USE CASE	FUNCTIONALITY	BENEFITS
Vulnerability Identification	Asimily can augment its passive vulnerability identification with Qualys's active scanning of devices	Greater accuracy in vulnerability identification and the ability to use Insight's exploitability analysis to determine the severity of Qualys-detected vulnerabilities and filter out "in name only" vulnerabilities that are not exploitable in the medical device context
Quarantine Device	Asimily can populate Qualys's no-scan list using its real time categorization and inventory of all connected devices	Ability to automatically exclude devices from scans that are not safe to scan, such as medical devices that are deployed in the field

Technical Solution

Asimily Insight supports both on-premises and cloud deployments of Qualys. Additionally, Insight itself can be deployed in the cloud or on-premises.
If your Insight deployment is cloud and your Qualys deployment is cloud - Collector configuration is not required.

If your Insight deployment is cloud and your Qualys deployment is on-premises - You must designate a specific Collector, which can be a configured Edge or a dedicated virtual machine that you deploy in your environment. The Collector acts as a proxy to allow the Asimily cloud to communicate with BlueCat, so it must be able to reach the BlueCat Address Manager server over the network. After the Collector is configured, ensure that it is able to make outbound connections to the Asimily cloud server on ports 22, 5568, 5570, 5572, and 5574. Your Asimily cloud server is the address you use to log in (e.g., mysystem-portal.asimily.com).

Network Diagram



About Qualys

Qualys, Inc. (NASDAQ: **QLYS**) is a pioneer and leading provider of disruptive cloud-based security, compliance and IT solution.. Qualys helps organizations streamline and automate their security and compliance solutions onto a single platform for greater agility, better business outcomes, and substantial cost savings.

www.qualys.com

Qualys.

About Asimily

Asimily is an industry-leading risk management platform that secures IoT devices for medical, diagnostic, life sciences, and pharmaceutical companies in the healthcare industry.

www.asimily.com

asimily