DATA SHEET

Asimily + CrowdStrike Integration Solution

Securing Healthcare Devices, Systems, and Resources

In the face of constantly evolving cyber threats, protecting healthcare systems is more important than ever. Asimily Insight integrates with the CrowdStrike Falcon® platform to provide your team with additional insights and context surrounding threats in your healthcare environment, enabling you to detect and respond with speed.

By correlating rich threat intelligence from the Falcon platform with Asimily's anomaly alerts and automatically querying the data to uncover suspicious or compromised domains or IPs, you can stay ahead of modern adversaries. To accelerate your investigations, Insight also seamlessly displays Falcon's verdict for Indicators of Compromise (IOCs), so that you know if CrowdStrike classifies the IOC as malicious. With additional visibility into your environment, you can secure medical, laboratory, IoT/ OT, and IT equipment, ensuring your business-critical devices and data are safe.

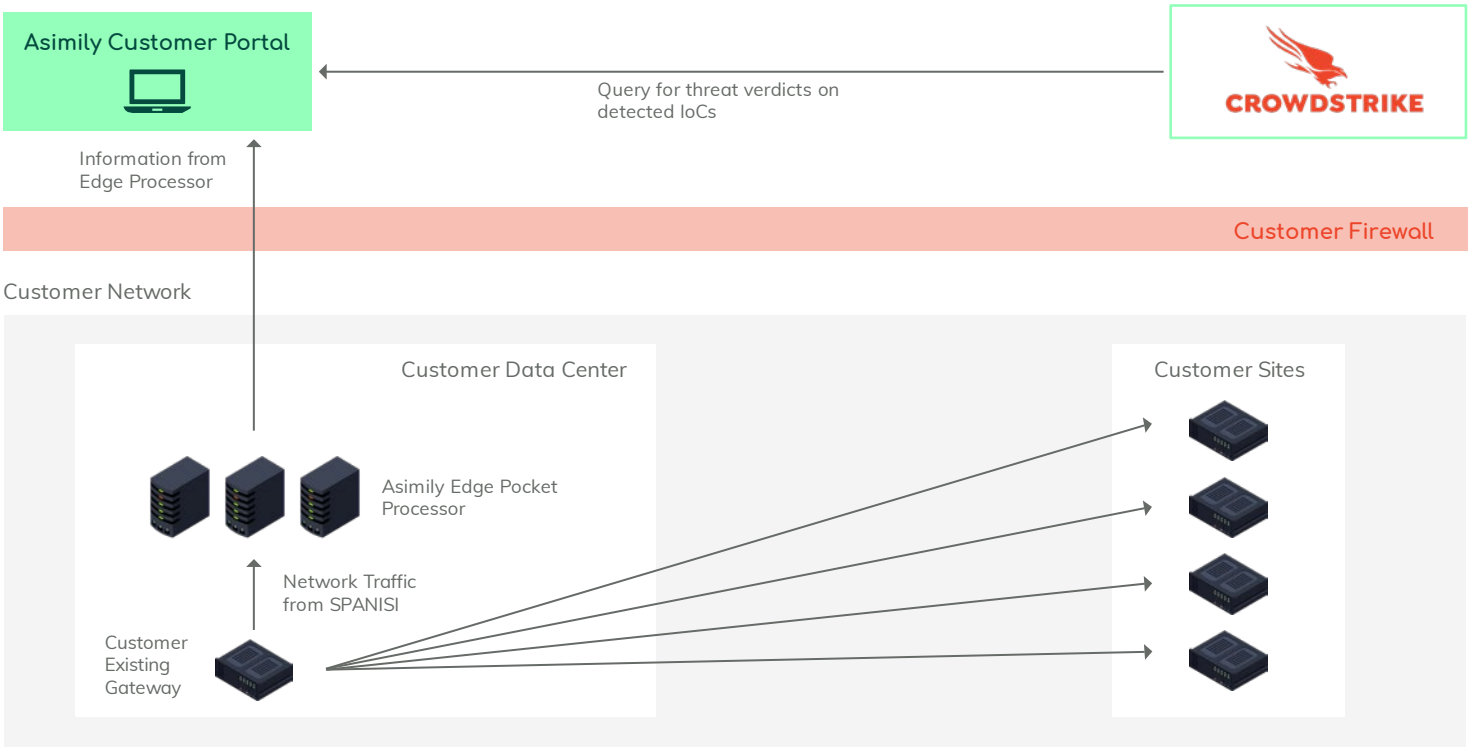
Key Solution Benefits

- Improve device monitoring and classification of risk with Asimily's knowledge base of IoT Security Protocols
- Faster threat context with Asimily Insight's threat and anomaly detection interface
- Identify potential compromises related to domains or IPs by easily viewing CrowdStrike Falcon's verdict from the Asimily Insight console

USE CASE	FUNCTIONALITY	BENEFITS
Complex healthcare environments cause a lack of visibility over devices and risk.	Gain access to Asimily's vast knowledge base of IoT and security protocols and CrowdStrike's enriched threat intelligence.	Get full visibility over your environment with improved monitoring of devices and classification of risk.
Evolving attackers and dispersed systems can slow down threat detection and response.	Easily see CrowdStrike Falcon's verdict on external IPs and external domains within the Asimily Insight interface.	Get rich threat intelligence in one place and investigate threats more quickly without having to switch consoles.
High volumes of alerts make it difficult to gain context surrounding threats to prioritize critical actions.	Quickly identify indicators of compromise and anomalies in your environment.	Combine CrowdStrike Falcon's threat intelligence and unique IOCs with Asimily Insight's threat and anomaly detection for faster, more accurate threat identification and remediation.

Technical Solution

This integration requires the CrowdStrike Falcon® Intelligence module in order to enable threat intelligence in the Asimily platform. After generating an API Client within the Falcon UI under API Clients and Keys, users can enter the details in the applicable Insight configuration tile within the Asimily platform. Thereafter, Falcon Intelligence threat intelligence will automatically be populated for any anomalous IOCs under "Threat Intel Verdict."



Key Capabilities

Asimily queries CrowdStrike's threat intelligence to gather verdicts about external IPs and external domains. These verdicts are then displayed within the Insight portal in two places:

1. Within Destination IP View under the top-level Anomaly tab
2. Within External IPs and External Domains under Asset Details for a specific device

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity, and data.

www.crowdstrike.com

CROWDSTRIKE

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
dineshk@asimiliy.com

asimily