Palo Alto Networks and AIMS 3

Cybersecurity and CMMS for Healthcare

Benefits of the Integration

- Unparalleled device visibility by combining device context from AIMS with the security analytics from Palo Alto Networks IoT Security
- Streamlines medical device incident lifecycle management through AIMS
- Supports both on-premises and cloud AIMS deployments

The Challenge

It is more important than ever for healthcare organizations to ensure the safety of their network-connected medical devices. There's too much risk regarding patient health, safety, and privacy to let devices and networks go unmanaged. However, tracking, monitoring, and maintaining these connected devices is complex and time-consuming.

The Solution

A quality IoT cybersecurity solution will provide a seamless integration of asset information and security analytics. It should update asset information automatically in the CMMS system and provide security analytics for all network devices. The ability to analyze the security of devices based on make, model, software version, or other metrics is a crucial component, as well. As security events are found in real time, work orders should be triggered instantly and assigned to the appropriate technicians for remediation. Based on the severity of the security event, automatic notifications can also be sent to the appropriate managers as well. As medical devices are added to the network, they should be discovered instantly by the cybersecurity vendor with real-time network monitoring to ensure the hospital system's safety and security.

Phoenix Data Systems AIMS 3

Phoenix Data Systems has been a CMMS software developer for 40 years. The company's solution, Asset Information Management System or AIMS, has been a leader in CMMS software because of its innovations, responsiveness, and dedication to the healthcare industry. Phoenix is currently producing its fifth-generation software, AIMS 3. This latest release is a culmination of their years of experience and intense collaboration with users. AIMS 3 is a flexible, powerful, API-driven software that can integrate with any third-party application. AIMS 3 is user-friendly enough for a single clinic yet powerful enough for an enterprise-level hospital system.

Palo Alto Networks IoT Security

Palo Alto Networks IoT Security is the healthcare industry's smartest IoT security solution delivering ML-powered visibility, prevention, Zero Trust enforcement, and operational insights in a single platform.

Palo Alto Networks and Phoenix Data Systems

The integration between Palo Alto Networks IoT Security and AIMS by Phoenix Data Systems solves this problem for our users perfectly. Palo Alto Networks IoT Security provides always-on device discovery, medical device risk assessment, security monitoring, segmentation policy, policy implementation, and built-in threat prevention. The native bidirectional integration with AIMS helps clinical engineering and facilities maintenance teams identify vulnerable equipment and secure these devices before they can be exploited.

Use Case 1: Asset Inventory

Challenge

CMMS data is not always up to date. With a dynamic inventory of thousands of medical devices to manage, it is extremely difficult to keep track of all changes. By pulling asset data from AIMS into the Palo Alto Networks IoT Security solution, we ensure complete asset visibility from a single pane of glass.

Solution

IoT Security pulls additional asset details (e.g., serial number, department, asset tag, location, AET, software version) into the Palo Alto Networks IoT solution and merges using device MAC/IP.

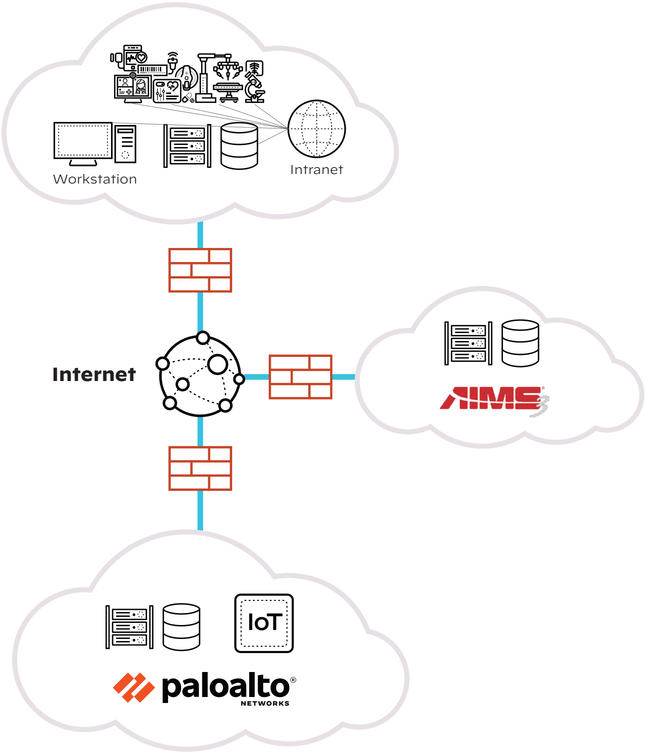

Figure 1: AIMS 3 cybersecurity using Palo Alto Networks

Use Case 2: Risk and Workflow Management

Challenge

Managing alerts and alarms from dozens of different application medical facility operators is a Herculean task without a centralized workflow management system. Palo Alto Networks meets users where they're at so operators can do their best work.

Solution

When a cybersecurity risk or incident is identified by Palo Alto Networks IoT Security, an alert is generated and shared with AIMS so that clinical and incident response teams can close the loop on the threat and implement appropriate remediation strategies. This automated workflow reduces the mean response time for your enterprise.

About Phoenix Data Systems

Phoenix Data Systems, creator of AIMS 3, has been dedicated to producing world class CMMS software for the healthcare industry for 40 years. AIMS 3 is a powerful tool for maintaining and tracking medical devices. Experience how AIMS 3 can increase efficiency in your HTM department by visiting www.goaims.com.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. For more information, visit www.paloaltonetworks.com.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com