ProHealth Care

ProHealth achieves automated discovery and visibility of unmanaged devices and accelerated campus network segmentation with Ordr

ProHealth, founded over a century ago, provides a multitude of services ranging from fitness and wellness, home health care, hospice care, hospital care, occupational health, primary care, rehabilitation, specialty care, senior living, urgent and emergency care, and virtual (telehealth) visits. The diversity of services contributed to IT and Biomed challenges such as accurately identifying and securing all network connected IoT and medical IoT devices across many types of sites.

ProHealth selected the Ordr Systems Control Engine (SCE) to transform its business operations—automatically discovering connected devices, understanding risks and usage, and accelerating segmentation. The Ordr SCE enables both IT and Biomed teams within ProHealth to keep up with HIPAA compliance requirements and automate security operations, ultimately resulting in reduced operational costs and increased quality of patient care.

The Challenge

Multiple teams at ProHealth were leading initiatives to identify all network-connected unmanaged devices, baseline their behavior, and define network security policies to protect them. The primary challenge with these initiatives was the excessive number of manual tasks which resulted in increased operational costs for each step.

ProHealth Care is a leading healthcare provider in Waukesha County, Wisconsin, and surrounding areas. With 4,700 employees and nearly 1,000 doctors and other health professionals, ProHealth Care is the largest healthcare provider between Milwaukee and Madison – treating more than 400,000 patients a year.

BIOMED TEAM CHALLENGES

- Maintain a current list of all medical IoT devices (managed and unmanaged)
- Keep track of which medical devices have vulnerabilities or recalls
- Gain an understanding of how medical IoT devices are utilized

IT NETWORKING TEAM CHALLENGES

- Overarching initiative to identify and secure all types of unmanaged IoT/IoMT devices
- Understand how each type of unmanaged device communicates on the network
- Build security policies to protect many types of vulnerable, unmanaged devices

"We have a robust CMMS (Computerized Maintenance Management System) platform, but medical devices are constantly moving and being added to the network. Tracking thousands of medical devices is a tremendous challenge," said David Yaeger, Biomed Security DBA for ProHealth.

Both teams were aware of gaps in their existing CMMS and CMDB (Configuration Management Database) systems and knew that manually tracking down each unmanaged device would not be feasible given the size of the environment, project deadlines, existing workloads and budgetary constraints. Furthermore, existing network visibility toolsets such as NetFlow, IPFIX, and AVC (Application Visibility and Control) were not able to accurately identify unmanaged devices on the network. Legacy tools capable of providing visibility at the level of IP, MAC address, and L4 source/destination traffic were not practical when working with unidentifiable unmanaged IoT or medical IoT devices (see Figure 1).

"When it comes to segmentation, the information provided by device manufacturers does not adequately or accurately explain basic network communication requirements such as which TCP/UDP ports are required," said Joel Benson, Network Engineer for ProHealth.

The Solution

The teams initially considered using their existing legacy systems and manual processes, but after seeing Ordr SCE, they knew an automated device visibility and security solution was the route to take.

"Ordr automatically identifies all our network connected devices and then monitors the traffic of each device. This enables us to automate the creation of security ACLs (Access Control Lists) which speeds up our entire segmentation process," said Benson.

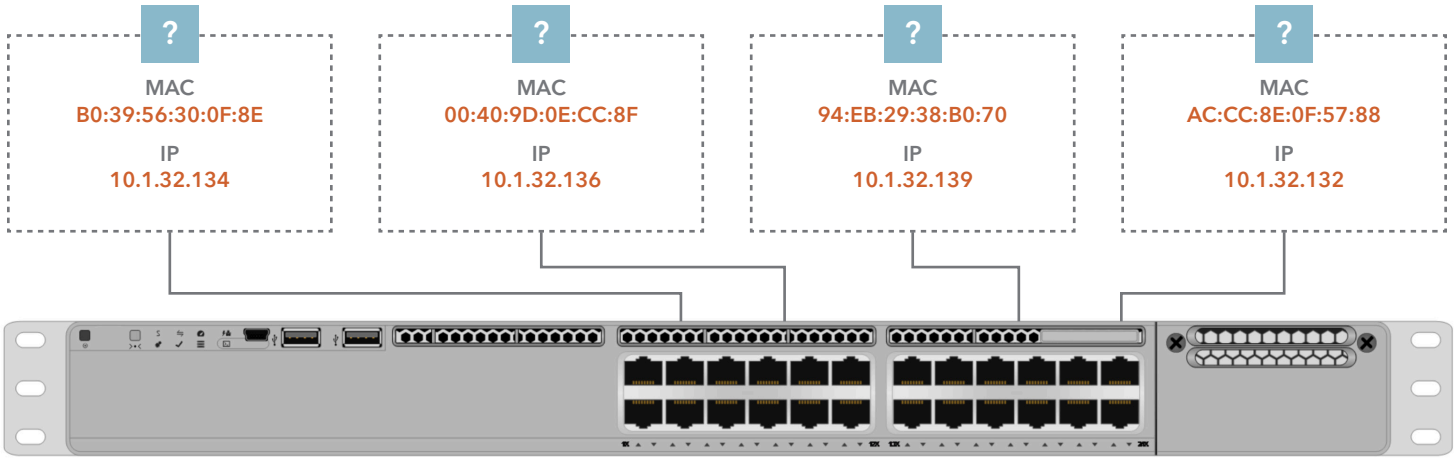

FIGURE 1: MISSING DEVICE VISIBILITY: MAC AND IP AREN'T ENOUGH TO IDENTIFY IOT AND MEDICAL IOT

Ordr accelerates network segmentation by dynamically generating these ACLs based on device identity and behavior over time. These network security ACLs can be applied in many ways including NAC integrations like Cisco ISE downloadable ACLs, switch port ACLs, VLAN SVI (Switch Virtual Interface) ACLs, wireless LAN controller ACLs, or even via powerful edge firewall integrations with vendors such as Palo Alto Networks (see Figure 2).

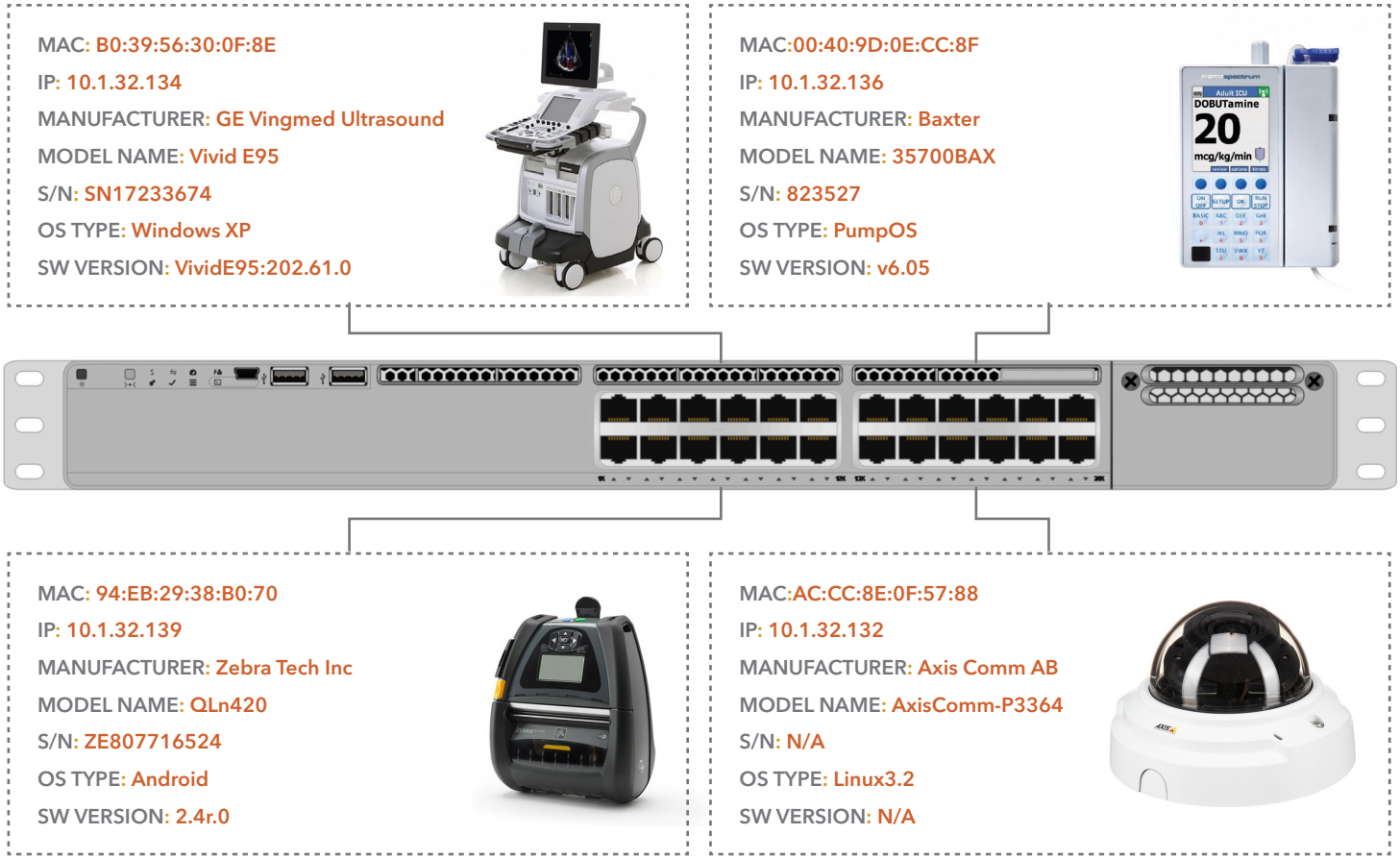

FIGURE 2: ORDR AUTOMATES THE CLASSIFICATION OF UNMANAGED DEVICES

Business Benefits

The benefits of Ordr SCE are not limited to security for unmanaged devices and improvements in operational efficiency. Cutting-edge medical device utilization capabilities allow healthcare facilities to track how much a device is used and can even compare usage across multiple devices to quickly analyze patterns over time.

Ordr SCE offers a wealth of features and functionality, but for the ProHealth Biomed Team, it was the solution's advanced medical device utilization analytics that impressed them the most (see Figure 3).

"Medical devices are expensive. Using this feature allows us to potentially reduce costs by identifying and repurposing underutilized devices. When we do need to buy more equipment, we can now optimize our investments by making intelligent data-driven decisions about the types of devices to buy and exactly which sites need them the most," said Yaeger.

FIGURE 3: ORDR MEDICAL DEVICE UTILIZATION

Looking Ahead

ProHealth Care has a long legacy of delivering outstanding care across a wide spectrum of services. Network-connected IoT and medical IoT devices help enable innovative patient care and more efficient business operations. The Ordr SCE platform automates the visibility and security of these devices so ProHealth teams can focus on patient care without compromising security and compliance.

The teams at ProHealth plan to extend their deployment to track Windows patch levels and domain logins across all managed devices. They are looking to enable advanced Ordr integration features such as Windows Remote Management (WinRM) and Active Directory integration to address these use cases. ProHealth also continues to expand its network segmentation initiatives to protect patient data and all types of vulnerable unmanaged devices.

Ordr secures the millions of enterprise IoT and unmanaged devices such as manufacturing machines, building systems, medical equipment, printers and more that run within global networks. The Ordr Systems Control Engine uses machine learning to automatically discover and classify every IoT and unmanaged device, map all communications, detect and prioritize vulnerabilities, and then proactively secure each device through dynamic policy generation and segmentation. Organizations use Ordr to discover their devices, track usage, achieve proactive protection and compliance. For more information about Ordr, go to www.ordr.net.