OPTIMIZING MEDICAL DEVICE MANAGEMENT AND SECURITY FOR CLINICAL TECHNICIANS

DURING AND POST COVID-19

ordr

Healthcare providers of all sizes naturally need to get the most out of their limited clinical resources and devices. From Supply Chain teams making strategic procurement decisions to the daily asset management needs of Healthcare Technology Managers and Biomedical Engineers, efficiency is always paramount.

However, the pressure to fully leverage all available resources has become even more magnified due to the unprecedented pressures created by COVID-19. When clinical resources are stretched to capacity, the ability to continually track and fully utilize medical devices is directly linked to an organization's ability to deliver care. Additionally, COVID-19 has brought other changes to the environment with moves to more telemedicine visits, a decline in the number of patients doing elective procedures, patients postponing care, and furloughs of clinical engineering staff. All of these changes have made understanding how medical equipment is being and not being used crucial to driving efficiencies and safety in patient care.

Ordr System Control Engine (SCE) helps healthcare teams address these challenges by providing a fully automated and up to the minute view of all of an organization's devices. Clinical engineering teams can see exactly what devices are in their environment, where they are located, how they are being utilized, and who is using them. In this paper we show how these capabilities can be applied to clinical environments in general, and then take a more detailed look at how these concepts can apply specifically to the challenges of COVID-19.

DEVICE MANAGEMENT AND SECURITY BEST PRACTICES IN CLINICAL ENVIRONMENTS

In order to get the most out of their devices, healthcare teams need to know what devices are available, where they are, what risks they bring and how they are being used. This can be a particular challenge when it comes to clinical devices which are often moved around the facility as needs change, and likewise may not support traditional endpoint management agents and security tools that other IT systems do. Here are the best practices for device management and security in clinical environments:

1

Know What Is Available

Clinical engineering teams need to know and classify all medical devices, ensuring that they have an up to the minute inventory of the devices at their disposal. This includes virtually any type of connected medical device from patient monitors, to high-value imaging devices and lab equipment. This also means staff can know when devices go missing or are taken offline so that they can take corrective action. This visibility should be provided in real-time for any new connected device, and integrated with configuration management database (CMDB) and Computerized Maintenance Management Systems (CMMS) solutions to trigger the proper workflow. Inventory Management is continuous in healthcare and incorporating real time information about devices into CMDB and CMMS systems is paramount.

2

Know Where Devices Are

Clinicians and medical devices are naturally on the move as they respond to patient needs throughout the day. As a result, staff often need to scramble and search for important devices, leading to lost productivity and delays in care. A GE healthcare report1 found that medical devices were frequently unaccounted for, with only some assets recorded centrally – and rarely tracked in real-time. Nurses typically spend more than 20 minutes per shift simply looking for needed equipment. This oftentimes leads to staff hiding or hoarding crucial patient care devices like Infusion Pumps, which further complicates identifying where devices are and understanding how they are used.

3

Know How Devices Are Being Used

The more valuable a device is, the more important it is to make sure the device is fully utilized while minimizing bottlenecks. Clinical engineering and procurements teams then have the data they need to make highly-informed decisions, for example, ensuring all devices are being fully utilized before acquiring additional devices. By tracking utilization trends, staff can know when it makes the most sense to buy vs rent devices, when devices are likely to need service, and when to end-of-life devices. Understanding device utiization can also be important for schedule appropriate timing for device maintenance.

4

Know What Risks Devices Are Bringing

Medical devices pose a unique challenge to healthcare organizations because they may not always be designed with security in mind, but because of cost reasons, will exist in the environment for a long time. The traditional IT lifecycle for computer systems, which is generally three to five years, is much different than the lifecycle for medical systems that may run for decades. As a result, clinical engineering teams need to understand the risks that they bring – vulnerabilities, manufacturer recalls and FDA recalls – and manage them appropriately. Managing this risk is a continuous process as operating systems and software versions become obsolete and new vulnerabilities and exploits are created against these systems. Additionally, managing FDA recalls is continuous as this information is updated and published.

ORDR PLATFORM FOR MEDICAL DEVICE MANAGEMENT AND SECURITY

Ordr puts clinical teams in control by automatically discovering and classifying all connected devices in the environment down to the specific model of device and detailed attributes such as the current version of

software, vulnerabilities detected and the location of the device. This discovery is performed in real-time, is continuous, utilizes a passive approach and does not impact sensitive medical equipment or the performance and availability of the networks these devices are connected to.

Next, the platform uses artificial intelligence to profile every device and how it is behaving. This includes not only mapping and baselining device communications and risks, but also visually mapping it to the organization's network topology. This allows Ordr to deliver deep understanding of device insights – from identifying normal versus malicious behaviors (that may indicate a security attack in progress) to understanding device utilization. Ordr also provides a view into vulnerability information and can provide context around Common Vulnerabilities and Exposures as well as FDA recall notification information for these systems. This information can assist not only clinical teams but the organization's extended security and networking teams, but also gives them a platform to work together to ensure availability and safety of patient care from these devices.

Finally, based on the rich context of the device, how it is behaving, and its risk profile, Ordr can automate appropriate actions. These include the automated creation and enforcement of policies, or alerting and triggering a specific security or operations workflow. Figure 1 provides the Ordr framework for visibility and security of all unmanaged devices – IoT, IoMT and OT.

AI PLATFORM FOR VISIBILITY AND SECURITY OF ALL UNMANAGED DEVICES

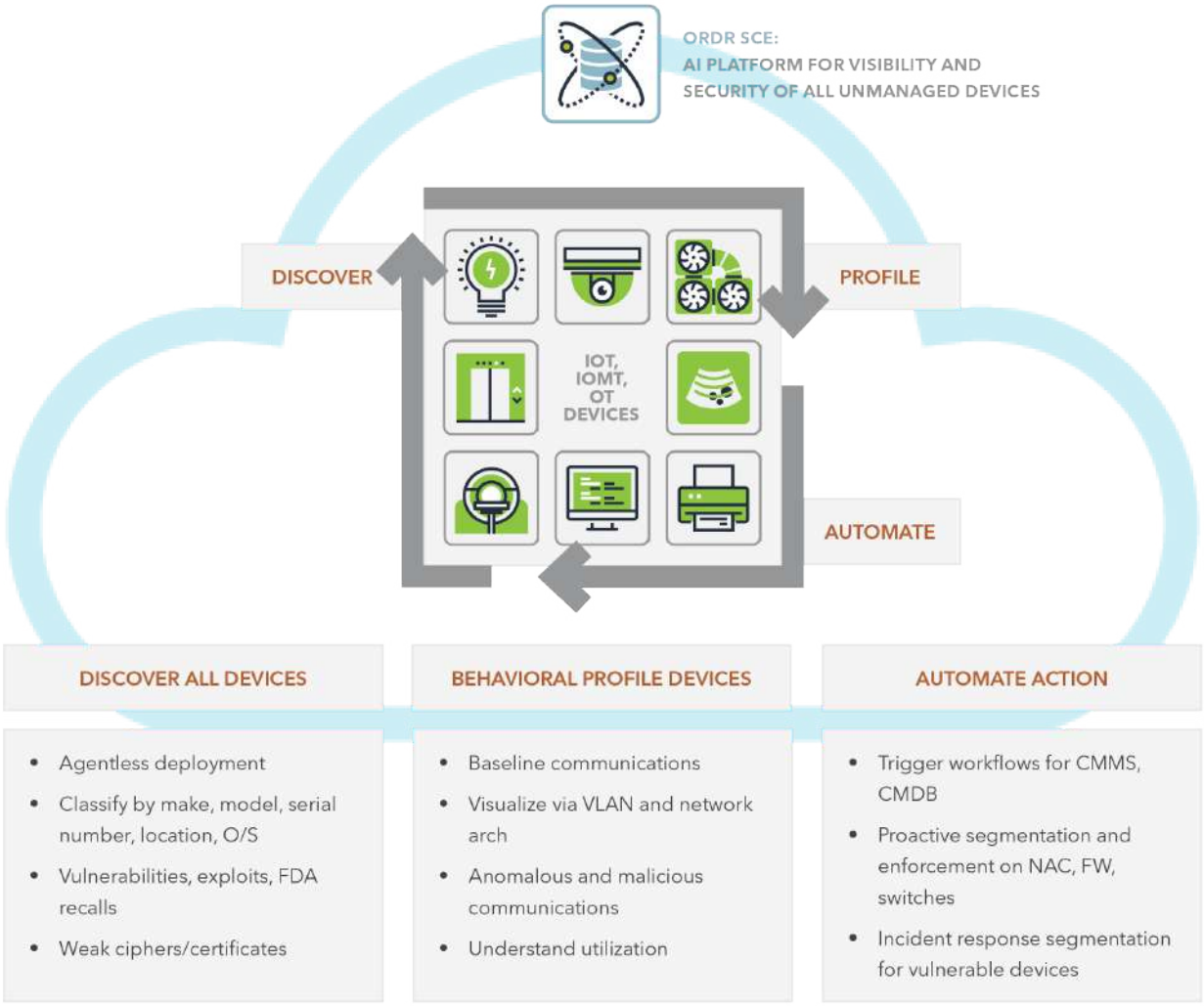

FIGURE 1: ORDR DEVICE SECURITY FRAMEWORK

The Ordr platform can be deployed on-premise or in the cloud, and offers a zero-touch, agentless deployment. Ordr has been effectively implemented at-scale to secure connected devices in large, complex networks, across all industries.

THE ORDR PLATFORM ALLOWS CLINICAL TEAMS TO DELIVER THE FOLLOWING USE CASES:

Real-time Visibility and Classification

Challenges such as COVID-19 can quickly and unexpectedly stretch clinical environments to their maximum capacity. In these cases, nimble and accurate visibility and classification of devices becomes not just an issue of efficiency, but a determining factor in the ability to deliver patient care. Ordr provides high fidelity visibility and classification of all unmanaged devices in the network, wired or wireless, without impacting device operations. Although this document is targeted to clinical engineering teams, the ability for Ordr to provide comprehensive security for all devices in the healthcare organization – IoT, IoMT and OT – ensures that the Ordr platform value can be extended to security and network teams as well.

Asset Inventory and Management

The Ordr and CMMS integration can address the following use cases:

Discover Med Devices NOT in the CMMS solution: This can be a concern for clinical engineering teams, and allows these teams to identify systems that are not being procured through standard channels

3rd Party Managed Equipment: With operational costs being impacted moving forward, there are lots of 3rd party equipment that is being managed or leased. Ordr helps clinical engineering teams track these devices and how they are being utilized

Legacy Operating Systems: Healthcare organizations purchase medical equipment and have it running in their environments far beyond the traditional 3 – 5 year IT lifecycle. Ordr can help identify the vulnerable systems running legacy operating systems.

Medical Devices Offline: Ordr can track assets that HAVE NOT connected in 30 days, 60 days to open up a new investigation into where these devices are.

Ramp-up and Ramp-down of Medical Devices: During the COVID-19 pandemic Ordr has seen new trends and behavior as Health Delivery Organizations have ramped up new treatment facilities, created dedicated care areas, built testing centers, and added additional Intensive Care Unit beds. In some cases, Ordr had detected up to one thousand new medical devices a week. As the impact and treatment of COVID-19 changes, knowing the details around the location, utilization, and trending information will be key in ramping down to new clinical demands.

Track Device Location

It is not enough to just know what devices are in your network. During a pandemic, the ability to locate devices or bring them back into compliance after deployments in field hospitals is important. The Ordr location data has helped reduce detective work for clinical engineering teams, potentially saving 20mins per shift per employee.

Manage Vulnerabilities and Recalls

Ordr delivers comprehensive view into risks for every device. In addition to the initial device visibility and classification during deep packet inspection, the device context is also enriched with threat intelligence, vulnerability data, FDA/device manufacturer alerts, and a risk score is provided. This allows clinical engineering teams to prioritize the management of vulnerabilities and recalls on the right medical devices. More importantly, clinical engineering can quickly reduce their window of risks by triggering the right automate actions to address the vulnerabilities and recalls such as putting a medical device into a quarantine VLAN until it is ready to be patched.

Optimize Procurement Planning

Ordr sees the device the moment it becomes active in the network, records operational activity, and records the time it goes offline. Ordr provides insight into clinically relevant metrics such as the number of scans or studies performed down to the parts of a patient's body analyzed and clinicians who used the device.

In addition, the Ordr platform also enables auto grouping of fleet devices to present fleet utilization. This is done by category of device, independent of the specific manufacturer. The utilization is customizable for the working hours of the hospitals/departments in order to provide meaningful data. For example, clinical teams can identify consistent high usage or bursty usage to decide whether to buy or rent fleet equipment. Teams can identify fleet devices that are offline and put them back in service, and compare usage across facilities and decide how well they can be distributed.

Integrate with Key Platforms

Ordr offers the most comprehensive integrations, extending IoT, OT, and IoMT device context to NGFWs, NACs, WLAN controllers, ITSM, SIEM, Vulnerability Management, CMDB and CMMS solutions in the market. For clinical engineering teams, the Ordr platform can integrate with CMDB and CMMS solutions to automate tasks, and enhance the asset inventory process. For example, Ordr can trigger the appropriate alert or workflow in CMMS systems when a new medical device is discovered in the network, or a new high severity vulnerability is discovered on a new medical device. This frees staff from manual processes of tracking devices, and allows them to focus more on patient care.

Optimize Limited Staff

To further complicate things in the response to COVID-19, many Healthcare organizations are being asked to reduce staff in total, furlough individuals, and move more of their support teams to less than full time hours. The Ordr technology is key in helping this reduced staff operate more efficiently to ensure there is not an impact to care delivery or patient safety.

CONCLUSION

Efficient device management and security is critical to clinical efficiency and efficacy even in the best of times. During periods of unusual stress such as COVID-19, the stakes are raised considerably. By ensuring the automated discovery and visibility of all medical assets, Ordr can ensure clinical engineering teams always have full insight into the assets at their disposal. Teams can next take the next important steps to understand the risks that these devices bring, and track how devices are being used both in terms of overall utilization as well as detailed usage information unique to each device. Whether for the daily operational management of devices or making long term procurement decisions, Ordr ensures clinical teams can quickly and accurately make decisions based on real-time, real-world data.