A PRACTICAL GUIDE:

IMPLEMENTING CONNECTED DEVICE SECURITY FOR HEALTHCARE ORGANIZATIONS

By Brad LaPorte, Gartner Veteran and Ordr Strategic Advisor
Published in coordination with subject matter experts from Ordr

TABLE OF CONTENTS

Introduction **3**

Understanding the Attackers **4**

Maturity Models in General **5**

The Five Steps of Maturity for Connected Device Security **6**

A word about specific recommendations for each stage 8

Stage One: Asset Visibility **9**

The Business Value 11

Key Operational Tasks 11

Inbound Integrations 12

Outbound Integrations 12

Recommended Device Details to Consider 12

Recommended Actions 12

Stage Two: Vulnerability and Risk Management **13**

The Business Value 16

Key Operational Tasks 16

Inbound Integrations 17

Recommended Device Communication Details to Consider 17

Recommended Actions 17

Stage Three: Reactive Security **18**

The Business Value 19

Key Operational Tasks 19

Inbound Integrations 20

Outbound Integrations 20

Stage Four: Proactive Security **21**

The Business Value 22

Key Operational Tasks 22

Outbound Integrations 22

Stage Five: Optimized Security **23**

The Business Value 24

Key Operational Tasks 24

Summary **25**

Acronyms 26

About the Author 27

Acknowledgements 27

INTRODUCTION

Organizations everywhere are feeling pressured to ramp up their defenses against cybercrime, which has grown to a trillion-dollar enterprise globally. The healthcare sector is no exception.

Healthcare organizations, as in the manufacturing, finance, retail, and infrastructure sectors, are attempting to improve results and lower costs by embracing digital transformation. To achieve these goals, more of their devices are connected to IT systems to help gather data and automate activity. This is a laudatory objective from a business perspective, but it creates more opportunities for cybercriminals, by expanding the attack surface available to them.

The healthcare sector faced the most ransomware attacks of any sector in 2021, according to the FBI's 2021 Internet Crime Report, resulting in losses of $6.9 billion. Healthcare data breaches affected over 550 organizations in 2021, with more than 40 million individuals facing protected health information exposure, as a result, reported Health IT Security. While some organizations have mapped out plans in response, many healthcare providers often are lagging. While more than a third of small providers surveyed by Software Advice have experienced a data breach, nearly half of them acknowledged that they have no plan of action should they experience a data breach.

As significant as these threats are, it is unrealistic to expect healthcare organizations to achieve a fully mature cybersecurity defensive posture overnight. All health organizations – from hospitals to clinics – either have complex information systems internally or are part of a larger information network with untold numbers of connected devices.

Addressing the risks those systems pose requires a deliberate sequence of planning and action. This guide outlines the steps involved in moving from a weak posture to one of greater strength and resiliency. Acquiring the right cybersecurity tools is important, but it is essential first to understand the cybersecurity threat in terms of the attack surface and who or what could attack, and then establish a model to protect your organization.

UNDERSTANDING THE ATTACKERS

While all healthcare organizations potentially are subject to attack through any of their devices, the reality of the threat is more nuanced. Gartner describes three types of attackers:

- **The automated attacker** – this attacker relies on automated attack methods, such as a vulnerability exploit and the use of malicious automation, such as bots and botnets. They are not using manual processes to zero in on specific targets but rather launch wide-scale attacks on multiple organizations at once. Common examples include attackers that commonly exploit vulnerabilities like Log4j (CVE-2021-44228) and PrintNightmare (CVE-2021-1675 & CVE-2021-34527).

- **The opportunistic attacker** – this attacker also uses automated attack methods to gain a foothold within the target organization, but then moves laterally to exploit the victim. Likely targets include popular healthcare and business process software. They are more tactical in their approach. Conti ransomware group is an example of an attacker that leverages opportunistic targeting of their victims.

- **The advanced persistent attacker** – the most dangerous of the group because of a willingness to use novel attack methods but more likely to attack large organizations. They are much more strategic in the tactics they employ and in their intent. APT29 is a prime example of this type of attacker.

In short, it is unlikely that a small clinic of no significant resources or value is likely to attract the attention of anyone but the automated attacker. Additionally, not all vulnerabilities are exploited – 77 percent of software vendors' vulnerabilities do not have published or observed exploit codes, Gartner says. Therefore, Gartner recommends defending against the top five exploited vulnerabilities that represent most automated malware.

Cybercrime patterns do change rapidly, and organizations will continue to expand their attack surfaces by adding more devices to their IT infrastructure. Accordingly, it is valuable to adopt a strategy such as a maturity model that evolves to protect all connected devices as an ongoing operational discipline.

MATURITY MODELS IN GENERAL

The notion of a maturity model is not unique to protecting connected devices. NIST, among others, has developed models that help organizations go from rudimentary security levels to the most advanced level in a logical sequence. Buying the most sophisticated tools doesn't work if the other parts required for an organization to successfully leverage its capabilities have not been established. That is why it is implicit in all these models to start with people and processes.

In terms of a healthcare analogy, think of how a society might provide effective medical care for its citizens. Before even getting to the first stage of providing basic care, society must have a basic understanding of what causes diseases and what is effective in treating them. A society without a scientific grounding will not make any serious progress in healthcare, no matter how much time and effort it puts in.

From there, healthcare providers might mature to delivering treatment in an emergency fashion, dressing wounds, setting broken bones, and assisting with births. With greater knowledge, illnesses can be cured with drugs, and surgeries can remediate potentially fatal injuries and help cure previously incurable conditions. In time, healthcare shifts from a purely curative state to an increasingly preventative one – anticipating threats to the population and applying mitigations including everything from societal-wide hygiene standards to vaccinations against communicable diseases.

One of the great pitfalls in leveraging a maturity model in the world of cybersecurity and an agile environment such as a healthcare network, is to assume that once a step has been taken, it's complete. That's not the case with cybersecurity. While we expect to move from a beginning stage to the most advanced stage, the process is not linear, nor is any stage ever finished. They all need to be reviewed and revisited to align with the evolution of the environment and attack methodologies. In effect, each step needs to be operationalized and monitored actively to detect and protect against new risks and new threats.

There are few physical world comparisons because most projects do move in a sequential fashion and reach a conclusion over time. This analogy may give more of a sense of the challenges involved in creating a highly advanced cybersecurity program for complex systems such as those of healthcare institutions. If one extends the thinking of a healthcare network to the analogy of a human body, survival is based on continual operation and adaptation. Once the heart starts, it doesn't stop and the immune system normally continually detects, adjusts, and responds to new threats to the body. The heart relies on the immune system to protect the body and many of us take steps to strengthen our immune system so it is optimized to respond quickly when we get sick or in the best case, prevent illness altogether.

Take a Deeper Dive into **The parallels of pandemic response and IoT security**, *by Pandian Gnanaprakasam - Chief Product Officer, Ordr*

THE FIVE STEPS OF MATURITY FOR CONNECTED DEVICE SECURITY

The table below summarizes the recommended Five Steps of Maturity for Connected Device Security. These recommendations were developed using expertise representing years of experience in securing and protecting connected devices for healthcare organizations worldwide.

The steps can be applied to a specific part of an organization or the whole. The key to deciding the scope of change is based on the availability of resources, the criticality of the connected devices, the ability to change, and the current threat landscape impacting the organization. For some organizations, the driving forces around security might require the whole organization to address a threat. In other situations, the risks associated and the need to demonstrate success quickly might drive the organization to focus on critical devices first or, conversely, the least risky. Ultimately, a business decision needs to influence the first step in adopting this maturity model.

The core objective of this paper is to improve your ability to **SEE**, **KNOW**, and **SECURE** all your connected devices. As many security and risk practitioners will tell you, having complete visibility (**SEE**), is a foundational requirement. This means not only understanding what devices are connected to your network, but also, what those devices are communicating with across the network. Without this visibility it is virtually impossible to understand (**KNOW**) what risks those devices and their communications present. Without seeing and knowing, your ability to respond to threats targeting connected devices is compromised and your ability to proactively improve protections (**SECURE**) is greatly limited. Improving your ability to **SEE**, **KNOW**, and **SECURE** is a logical, proven framework that allows you to align resources, optimize efforts, and respond in a risk sensitive manner.

> ***NOTE:*** *These objectives can only be achieved by using one fully integrated, central security platform. Attempting to tie together different security systems to achieve the same outcome is a recipe for disaster.*

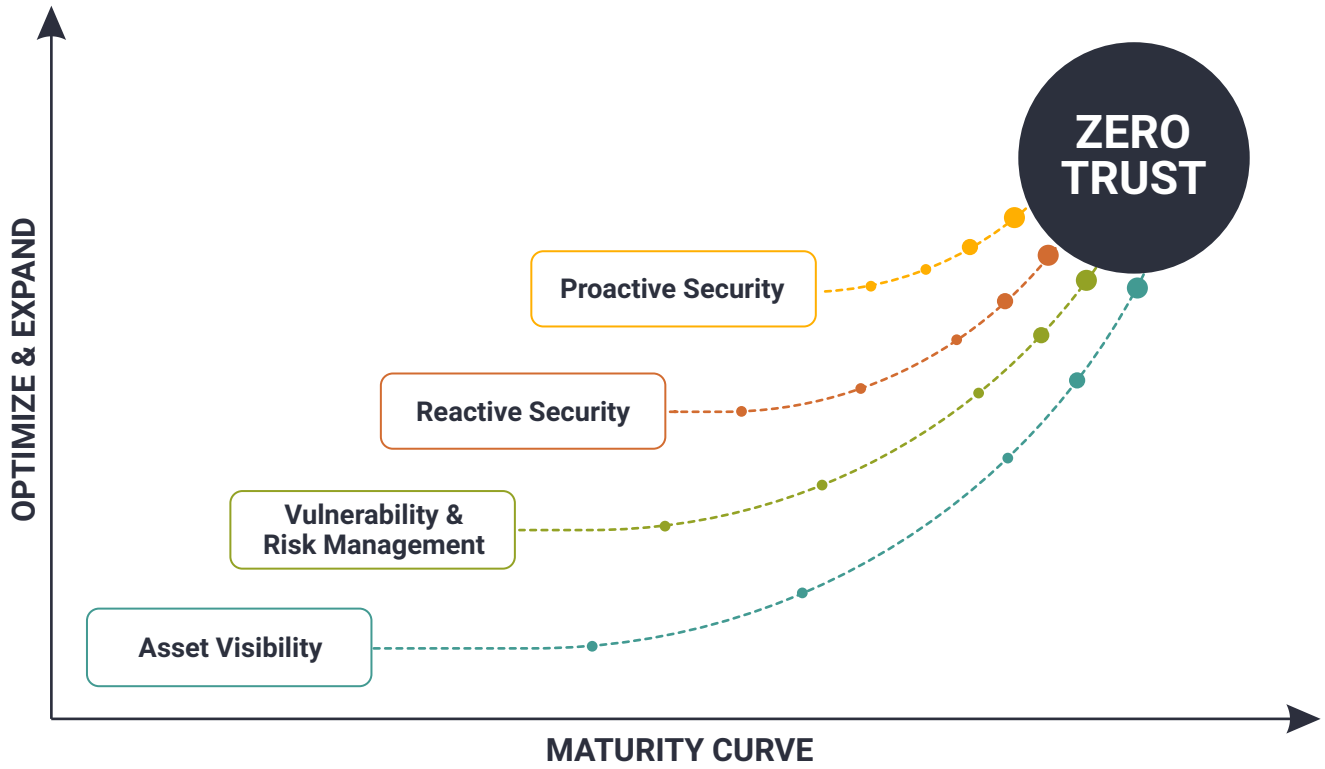
The table is broken down in stages with each stage identifying:

- Recommended integrations that will provide inbound data for insights and outbound connections to enhance operations, improve efficiencies, and enable response.
- For each area of focus (**SEE, KNOW,** and **SECURE**), the recommended activities and goals are documented.
- The final column, Uses Cases, highlights expected results that can be achieved once you have started to establish the technology integrations and operationalized the associated processes.

Stage	Integrations	See	Know	Secure	Use Cases
Asset Visibility	***Inbound:*** • Network SPAN and TAP • Network SNMP, NetFlow, and API data (optional) • CMMS and/or CMDB ***Outbound:*** • CMMS and/or CMDB	• Discover all known, unknown, and new connected devices and maintain an accurate inventory • Automate device classification (make and model) • Identify risk (e.g., outdated operating systems, weak pass- words, weak certificates, etc.) • See granular device details (make, model, MAC, IP, OS, serial number, firmware, etc.)	• Know devices with outdated OS, weak passwords, weak certs • Know what each device is communi-cating with internal/external and risk of that communication		• Gain basic understanding of attack surface (CAASM) • Automate efforts to discover, inventory, and catalog all connected devices including newly attached devices • Improve accuracy of device inventory in asset management tools
Vulnerability and Risk Management	***Inbound:*** • Vulnerability Assessment to understand vulnerabilities on a given device • Threat Intelligence for risk context • Identity providers to correlate IP address changes and user access • NetFlow data to extend device discovery to distributed environments (optional)	• See where devices are connected (network, physical) • Discover newly attached devices automatically • Utilization (target HTM, Supplychain, Security)	• Integrate 3rd party tools for enrichment of device and threat insights • Uncover known threats/vulnerabilities (CVEs, exploits, recalls, etc.) • Baseline device network communica-tions and identify anomalies in communi-cation	• Enhance attack surface/risk view with additional device context • Define and prioritize efforts to eliminate /reduce known threats /vulnerabilities (e.g., upgrades, patches, etc.)	• Gain detailed understanding of attack surface (CAASM) • Address compliance with an accurate asset inventory • Optimize asset management, and procurement efforts with device utilization insights
Reactive Security	***Inbound:*** • ITSM for business context • EDR for threat insights • Vulnerability Assessment to understand vulnerabilities on a given device • Threat Intelligence to understand risk context • NetFlow data to extend device discov-ery to distributed environments ***Outbound:*** • ITSM to provide details about device attribution • Network infrastructure for policy enforcement • EPP for policy enforcement • EDR for policy enforcement • NAC for policy enforcement • NGFW for policy enforcement • SIEM for alerting • Vulnerability Management to track and manage mitigation efforts • Vulnerability Assessment to initiate scans on newly discovered devices or to exclude critical devices from scans • VPT to manage remediation efforts	• Extend tools to discover/manage /secure more devices in more environments	• Prioritize Risk: Device and business context to inform priorities and security efforts	• Mitigate Risk: Response actions to reduce attack surface and harden systems (aka reactive segmentation) • Define the process and workflows. Start to think about and implement automated responses • Policy to block specific inbound/ outbound communications. • Look at internal communications and identify devices in wrong VLAN, commu-nicating with wrong devices, etc)	• Reduce attack surface by hardening systems, and implementing compensating controls including segmentation • Identify and stop active threats with dynamically created, reactive policies
Proactive Security	***Outbound:*** • SIEM • SOAR • XDR • Outbound to network and security infrastructure to enforce proactive policy, reduce the attack surface, and improve security	• Extend tools to discover/manage/secure more devices in more environments	• Device and business context to define proactive security efforts	• Prioritize, define, and implement a proactive segmentation strategy and elevate cybersecurity posture	• Improve security posture with insights to plan and implement proactive segmentation
Optimized Security	***Bi-directional:*** • Optimize bi-directional interactions with deeper tool integrations and automation	• Extend tools to more environments/ locations to discover/manage/secure more devices • Include 3rd party risk/partners	• Device and business context to inform security/business decisions and achieve strategic alignment	• Operationalize and expand proactive security • Fully integrate all connected devices into an organizational wide Zero Trust strategy	• Enforce Zero Trust for connected devices by operationalizing proactive segmentation

A WORD ABOUT SPECIFIC RECOMMENDATIONS FOR EACH STAGE

Most organizations are either just beginning to strengthen their cybersecurity operations or are in an early stage of development. Additionally, the steps to be taken in Stages Three, Four, and Five vary more between organizations because they depend on what was done in the previous steps, the nature of the organization, and the supporting tools. Accordingly, we are providing more details about actions to take in Stages One and Two than in the others. **Stage One (Asset Visibility)** is a foundational exercise that must be launched and operationalized. Once the initial launch of Stage One is running **Stage Two (Vulnerability and Risk Management)** can be used to extend the capabilities of the organization to effectively **SEE** and **KNOW**. Once Stages One and Two have launched and are operationalized, organizations can prioritize efforts to **SECURE** with activities in **Stage Three (Reactive Security)** and/or **Stage Four (Proactive Security)** and/or progress to the **Optimal** security stage. As indicated in the introductory text, this maturity mode can be applied holistically across the whole organization or can be focused on multiple critical areas, in sequence or in parallel.



STAGE ONE: ASSET VISIBILITY

Key Business Goal:

- Create a complete, accurate, and up to date list of devices attached to your infrastructure

Key Capabilities:

- **SEE** all connected devices and maintain an accurate inventory
- Automate discovery and classification for all known, unknown, and new devices
- Identify risk (e.g., outdated operating systems, weak passwords, weak certificates, etc.)

Integrations:

- Inbound to receive network data and other device data to enable device discovery and classification
- Outbound to update and enrich inventory tools

The first order of business is to see exactly what constitutes your attack surface. To protect yourself, you need to see what connected devices could be targeted, compromised, and leveraged by your adversaries. This means discovering all devices that are part of that surface, and quite often, security teams are unaware of at least some of those devices.

Networks don't lie and connected devices cannot hide on the network if you employ the proper methods to look for them. A best practice is to use device flow data from the network as the source of truth for all your connected devices. To discover all your devices – that is, make them visible -- the security platform should be fully integrated with your network, starting with your SPAN and TAP ports to uncover all devices that communicate on your network, including the ones you're not aware of.

The platform should automate the discovery of newly attached devices as an ongoing capability, capture all device details (e.g., operating system, IP address, and firmware status), classify each device (e.g., make and model), and use this data to maintain a base level knowledge pool.

Keep in mind that a device's MAC address is often associated with the network interface, not the device manufacturer and some devices, such as mobile IoMT devices, continually change their IP addresses. Neither is an accurate way to identify a device. As an example, the IP address of an infusion pump will dynamically change as it is moved with a patient around the physical area of a hospital. This makes tracking by IP address alone a futile effort, leading to failed remediation strategies and inventory inaccuracies. By tracking multiple attributes, as well as IP history, these combined device details become much more critical for forensic investigations. The security platform should record those attributes and stay abreast of changes as they occur, but other methods are needed for more accurate device identification.

The next step is to correlate what you learn from the network discovery exercise with other existing inventory data sources that you have available. For example, if a computerized maintenance management system (CMMS), or configuration management database (CMDB) is available, the data in those tools can be used to augment what the security platform discovers when analyzing network data. Correlating the data will give you greater insights into what is known and what is new or unknown. Ideally, the security platform should integrate with those tools to maintain updated device details, ensure accuracy of your inventory, and provide higher fidelity in assessing risk in the future.

One new approach, called Cyber Asset Attack Surface Management (CAASM), was created by Gartner to address asset inventory from a cyber perspective. CAASM has recently become prominent and holds great promise for helping security teams address their needs to solve persistent asset visibility and vulnerability challenges. CAASM relies on other, already deployed technologies for context and enriches the data being pulled in from those technologies to provide a holistic view of an organization's asset inventory. Moreover, CAASM can reconcile duplicates or inconsistent data and automate remediation steps to update data, such as data from a configuration management database (CMDB). CAASM is never a source of record but rather an aggregator of data from other sources. External Attack Surface Management (EASM) is a source of record and feeds into CAASM for added visibility (Gartner).

It is recommended that periodic reviews are conducted to ensure data sources are validated and new device categories are assessed and secured. Operationalizing this step establishes a discipline that continually updates the view of your attack surface and automatically correlates any newly discovered devices against your other source of inventory information. Additionally, the security platform should identify IoMT devices that are using weak passwords, weak certificates, or outdated operating systems. Identifying these risks is critical and these devices should be updated or replaced in a timely manner to ensure the security of the infrastructure. In the event a device's operating system cannot be updated or replacement is not practical, compensating controls can be used to limit exposure with protection from attacks while keeping vulnerable devices operational.

THE BUSINESS VALUE

In this first stage, you're striving to achieve the initial objective of **SEE** by integrating with the network and asset inventory platforms to create a high fidelity source of truth with visibility of all connected devices connected on your networks.

Businesses often adhere to the maxim, "What you can't measure, you can't improve". The cybersecurity variation of that is, "What you can't see, you can't defend."

Another way of understanding the issue is that this first stage shows you details that will take some time to add up to a complete picture. What devices do you have? In subsequent stages you will gain more device insights. What do devices connect to? How do they normally perform? You're first looking at leaves, then branches, then trees, and eventually seeing the whole forest of what you are trying to defend.

And at the risk of repeating ourselves, this is a continuous ongoing process. Because of the dynamic nature of businesses, new devices are continually being added while others are being removed. Using a security platform to automate this process is essential to maintaining a current and accurate view of your attack surface.

KEY OPERATIONAL TASKS

- ☑ **Automate device discovery**
- ☑ **Establish initial device context**
- ☑ **Gain device details**
- ☑ **Identify initial device risk**

INBOUND INTEGRATIONS

- Network SPAN and TAP data to analyze for device discovery
- Network SNMP data to analyze for device discovery (optional)
- Network API data to analyze for device discovery (optional)
- NetFlow data if SPAN/TAP is not available or in distributed environments (optional)
- CMMS and/or CMDB for device reconciliation

OUTBOUND INTEGRATIONS

- CMMS and/or CMDB to enrich and centralize device inventory

RECOMMENDED DEVICE DETAILS TO CONSIDER

- MAC address
- IP address
- Operating system
- Device profile (manufacturer, make, model)
- Device type (exact model number and firmware version)
- Device category (e.g., CT scanner, infusion pump, patient monitor)
- Device group (e.g., medical, mobile, office equipment, facilities)
- Device info - Serial Number
- Organizational data (e.g., CMDB data)
- Device network location (connected network switch or wireless access point)
- Device physical location (location inside the hospital)

RECOMMENDED ACTIONS

- Identify devices running out of date or vulnerable operating systems and establish plans for remediation, mitigation, or replacement
- Identify weak passwords, authorizations, certifications, and cyphers and establish remediation plans for validated risks

STAGE TWO: VULNERABILITY AND RISK MANAGEMENT

Key Business Goal:

- Create a more detailed view of risk for the devices connected to your infrastructure with additional device context and vulnerability insights to gain a risk based view of the attack surface

Key Capabilities:

- **KNOW** device communications and establish communication baselines
- **KNOW** potential threats from anomalous communications
- **KNOW** more device vulnerabilities

Integrations:

- Inbound from external data sources to expand vulnerability identification capabilities

Understanding the risk to your organization requires understanding what is vulnerable (i.e., the attack surface). To fully understand your attack surface and effectively protect it requires visibility (covered in Stage One) and the assessment of risk (covered in this stage). The ideal security platform should provide these insights.

In today's world, the ideal security platform should go beyond just analyzing network data and existing device data for device visibility. It should leverage additional capabilities and inputs to automatically enrich those insights and aid in the analysis of risk. This enrichment is necessary for a realistic understanding of an organization's security posture.

To ensure a complete view of risk, the security platform should be able to:

- Show relationships and traffic patterns between devices
- Identify known vulnerabilities, risks, and threats
- Leverage external sources such as threat feeds to provide up-to date threat awareness
- Analyze high volumes of data with AI/ML to identify anomalous, potentially risky behaviors
- Provide tools to easily identify risky traffic patterns
- Integrate with additional security tools to triage and validate true positive threats and enrich those tools with additional data from the security platform.

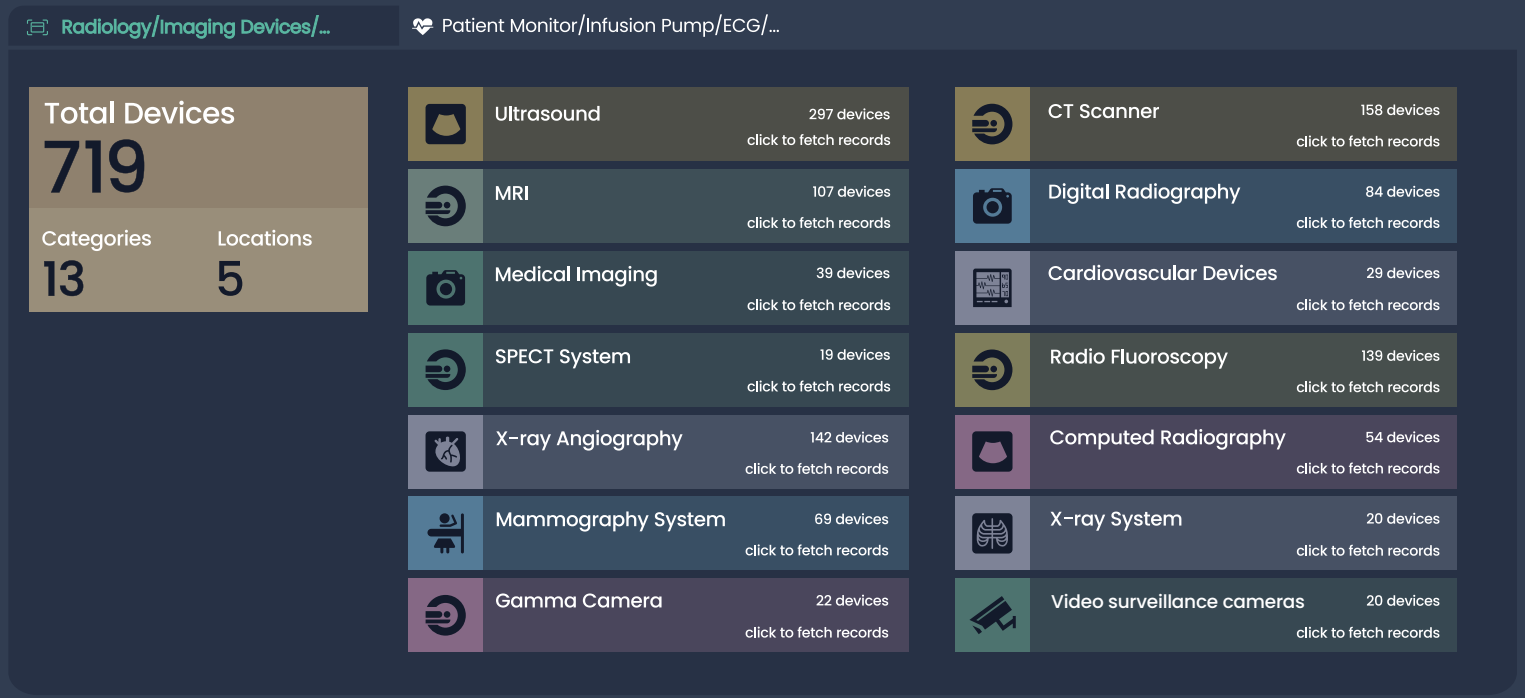
By extending the analysis of network data, the security platform will help provide an understanding of device relationships, communications, and the ability to establish a normal baseline of those communications. These insights uncover potential risks such as unknown connections, unencrypted communications, and vulnerable protocols in addition to providing important context for creating proactive security policies in later stages.

Integrating inputs from endpoint detection response (EDR), vulnerability analytics, and threat intelligence tools, provide security teams with a broader view of potential threats and vulnerabilities. Teams will also gain context essential to defining and prioritizing efforts to address threats through patching, updates, and other prevention or remediation efforts such as applying compensating controls.

Analyzing device communications at a deeper level can also provide device utilization insights to ensure data-driven optimization as teams scale their capacity. For example, device utilization insights help inform maintenance efforts to minimize impact to services. Insights also help support capital spend decisions to ensure current fleet utilization is maximized before new acquisitions are made.

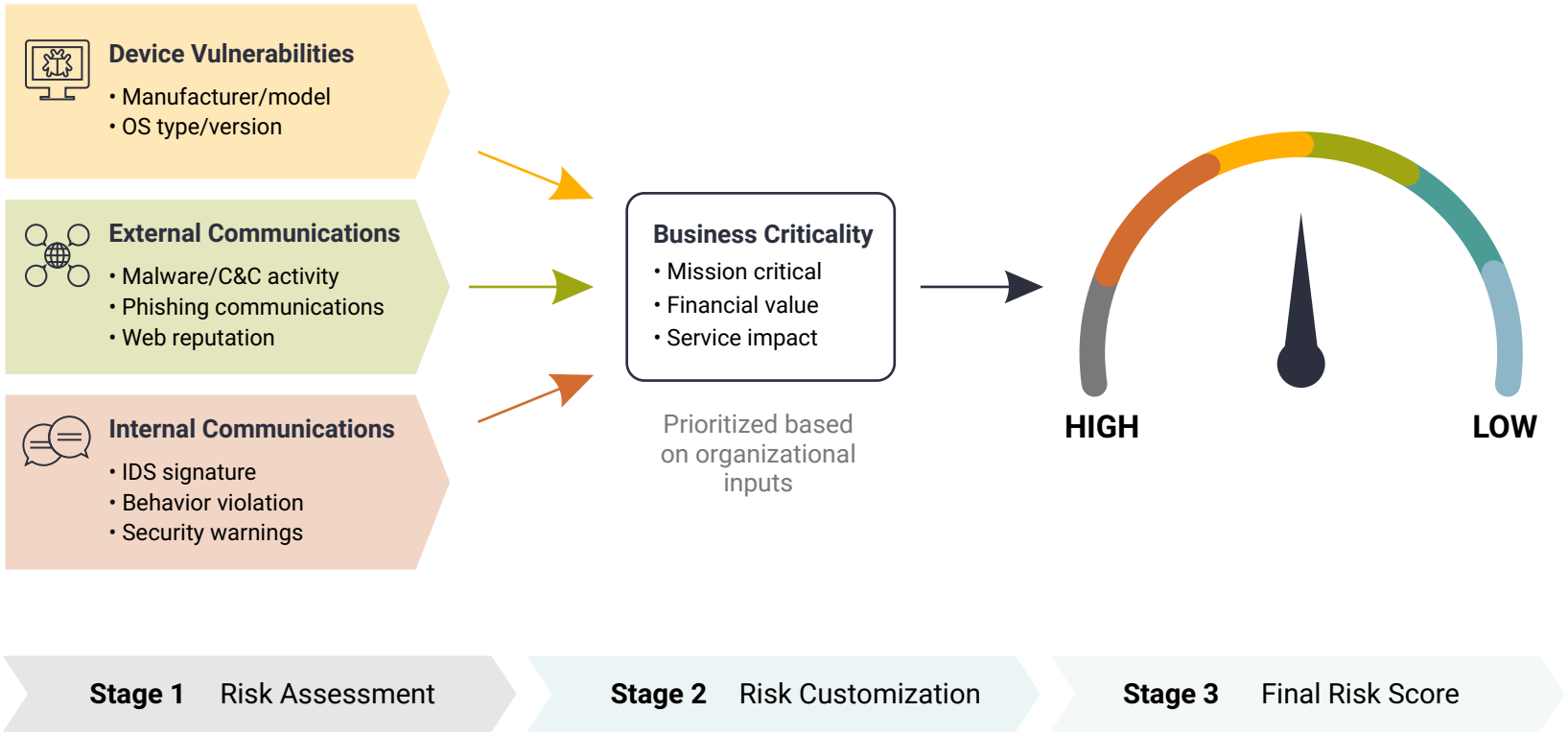
Utilization also provides important context for prioritizing risk remediation efforts. Device risk priority should be assessed with a combination of device vulnerabilities, communication risk, and business context such as utilization.

Device utilization is available natively from some devices, however, a complete view that aggregates insights from all devices, across all locations is critical to ensure maximum efficiency and protection for an organization.



No team can operate effectively if it cannot distinguish high risks from low risks. In a healthcare analogy, this is similar to the cacophony of beeps, buzzes, and alarms on a hospital floor that can overload the nursing staff. Vendors have been developing new ways of distinguishing their device-monitoring sounds from each other to relieve auditory fatigue. Security teams need a similar break from the stress of constant security alerts (aka alert fatigue) so they can address those that actually matter.

Assessing risk at a device level helps teams prioritize and focus mitigation efforts. A security platform can provide a device risk rating by combining inputs that include an assessment of a device's vulnerabilities, communications, and criticality. Since device criticality is unique to each environment and subjective, this input should be adjustable to align with the unique requirements of your organization. Risk for a device can then be calculated as a function of likelihood and impact to the organization to help teams prioritize security efforts.



THE BUSINESS VALUE

In Stage Two the insights gathered in Stage One (**SEE**) are enhanced to provide a higher level of detail and greater confidence in the real threats inside your environment (**KNOW**), and start the first steps to remediate threats and mitigate risks (**SECURE**).

Your organization will run more effectively and efficiently by identifying high-risk devices and prioritizing risk-reduction efforts. By leveraging device and business context to inform this process, you've moved beyond the baseline response to cybersecurity issues to one that's aligned to your organization.

At this level, you're able to focus on controlling external (north-south) communications and use techniques such as geo-blocking to head off threats. The ability to control internal (east-west) communications via segmentation comes in a subsequent stage.

It's critical to establish an operational discipline to review identified risks and start actioning remediation plans to remove validated known threats and risks to your environment. Since the security platform is continually updated with new threats, vulnerabilities, and device information, reviews should be performed regularly. Another key recommendation is to ensure the organization as a whole, including security and HTM teams, develops a common risk scoring approach, so remediations and escalations are handled in a consistent manner.

KEY OPERATIONAL TASKS

- ☑ **Expand capabilities to identify vulnerabilities**
- ☑ **Identify device communication risks**
- ☑ **Establish communications norms to be able to spot anomalies**

INBOUND INTEGRATIONS

- Vulnerability Assessment to understand vulnerabilities on a given device
- Threat Intelligence for risk context
- Identity providers to correlate IP address changes and user access
- NetFlow data to extend device discovery to distributed environments (optional)

RECOMMENDED DEVICE COMMUNICATION DETAILS TO CONSIDER

- Destination IP – internal/external
- DNS to IP - correlate domain name and IP address for all device communications
- Destination domain name – site the communication is going to
- Destination geographic location – mapped to the extent possible
- Incident type – e.g., malicious URL, spam URL, etc.
- Incident Score – aggregate risk score
- URL – website URL
- URL category – e.g., gaming, government, advertisement, military, shopping, etc.
- A-reputation score 1 – obtained by correlating with a leading threat feed URL reputation
- B-reputation score 2 – obtained by correlating with another leading threat feed URL reputation
- Aggregate score – calculated with various factors
- Tx/RX bytes – amount of data transferred and received
- Last activity – timestamp of last activity

RECOMMENDED ACTIONS

- Obtain information from manufacturing databases regarding recalls, prohibited activities, sanctions, and high-risk origins
- Obtain information about blacklisted organizations from sources such as the Bureau of Industry and Security (BIS) database
- Identify device access for each user for further control and forensics
- Identify high-risk devices as determined by high-risk score attribution
- Prioritize patching and other mitigation efforts
- Provide explanations to appropriate staff on how to take action on high-risk devices
- Identify activity (device, application, profile, policy; system perspective) to establish a behavioral baseline and suggests unknown threats when behavior deviates from that baseline
- Identify and stop east-west network threats by:
    - Inspecting all east-west network traffic
    - Blocking the lateral movement of threat actors
    - Increasing network visibility down to the workload level
    - Protecting apps and data vital to the business
- Identify new indicators of compromise (IOCs) with feeds from threat intelligence sources
- Establish custom detections by:
    - Using intrusion detection systems (IDS) signatures to detect new attacks
    - Using threat feeds to detect IOCs associated with these attacks
    - Creating a bubble for new attacks in your traffic analysis screen
    - Using vulnerability engines to scan for well-known malware, such as Ripple 20, Urgent 11, PrintNightmare, and Log4j

STAGE THREE: REACTIVE SECURITY

Key Business Goal:

- With the foundations of **SEE** and **KNOW** established, organizations can start to focus on key risks, using the enhanced data gained by integrating additional data sources in the platform
- The security team will gain operational efficiency and improve efficacy in identifying, prioritizing, and remediating threats using their existing portfolio of security tools

Key Capabilities:

- Leverage what you now **KNOW** about device and business context to prioritize risk management
- Define actions and workflows to **SECURE** devices with response to real-time threats
- Create a foundation for automation in subsequent stages

Integrations:

- Inbound integrations to enhance device context, business context, and vulnerability insights
- Outbound integrations with network and security tools to enforce policy and IT tools to manage mitigation efforts

To address the constantly changing information and device communication needs of an organization, the security platform should align with existing operational applications and security tools. Without this alignment, the attack surface can expand resulting in exposure to risk. Alternatively, changes in the attack surface may mean that some security processes are no longer needed.

As such, the security platform should fully integrate with and help automate functions associated with information technology service management (ITSM) applications, firewalls, intrusion detection systems, intrusion prevention systems (IDS/IPS), network access controls (NAC), endpoint detection and response (EDR), network detection and response (NDR), and security orchestration, automation, and response (SOAR) platforms.

Security teams in this stage are mitigating risks by hardening systems and reducing the attack surface with compensating controls such as segmentation. Teams are also starting to think about and implement automated responses by defining processes and workflows and creating policies to block specific inbound or outbound communications. More specifically, security teams are identifying problems in internal communications caused by such devices in the wrong VLAN or communicating with other devices they shouldn't be communicating with.

THE BUSINESS VALUE

When an organization starts to leverage tools to augment the capabilities of security teams, a process evolution also has to occur. The first stage in the process evolution is to identify and validate a consistent response to a category of threat. In the world of networking, a common way to block traffic is at the firewall or in the network with ACLs and policies. For device teams, the process is commonly to block activity at the device. Automation is the goal, and the appropriate response needs to be defined, validated, and agreed upon before moving forward. An untested procedure or one that lacks alignment and gets automated without validation always leads to problems. And problems in security lead to gaps in your ability to protect your environment.

Automation is essential in effectively running a modern security operations center (SOC). Without automation, your team is hopelessly putting out fires with manual efforts and never getting ahead of the constant barrage of threats. In this stage, automation is primarily one of optimizing awareness of the threats, defining a response, and applying mitigation as they arise. This lays the groundwork to move toward automating response in subsequent stages.

KEY OPERATIONAL TASKS

- ☑ **Establish a security operations system, endpoint detection, and remediation solution, if not already in place**
- ☑ **Add multi-factor authentication (MFA) capabilities and improve vulnerability and patch management**
- ☑ **Make sure all devices (e.g., medical devices, OT devices, video cameras, etc.) are in the proper segmented VLANs**
- ☑ **Augment the NAC with device context and vulnerability data**

INBOUND INTEGRATIONS

- ITSM for business context
- EDR for threat insights
- Vulnerability Assessment to understand vulnerabilities on a given device
- Threat Intelligence to understand risk context
- NetFlow data to extend device discovery to distributed environments

OUTBOUND INTEGRATIONS

- ITSM to provide details about device attribution
- Network infrastructure for policy enforcement
- EPP for policy enforcement
- EDR for policy enforcement
- NAC for policy enforcement
- NGFW for policy enforcement
- SIEM for alerting
- Vulnerability Management to track and manage mitigation efforts
- Vulnerability Assessment to initiate scans on newly discovered devices or to exclude critical devices from scans
- VPT to manage remediation efforts

STAGE FOUR: PROACTIVE SECURITY

Key Business Goal:

- Organizations can start to react to new threats with reduced human intervention based on confidence in the data and insights now available combined with a robust operational discipline
- Security teams can now focus on more complex threats and proactively improving the security posture while relying on the security platform to handle mundane tasks

Key Capabilities:

- Automate reactive efforts to **SECURE** devices against active threats
- Develop and begin to implement a proactive strategy to **SECURE** your environment by reducing the attack surface ahead of threats

Integrations:

- Outbound to enable automation of reactive security efforts
- Outbound to enforce proactive policy, reduce the attack surface, and improve security

Moving further up the ladder of identifying potential vulnerabilities and intervening, this stage extends tools to more environments and locations, discovering, managing, and securing more devices. The security platform in the Proactive Security stage is collaborating not just with SOAR platforms, but also can be extended to security information and event management (SIEM) technology and extended detection and response (XDR) platforms.

At this stage, you're able to use the device and business context gained in earlier stages to define policies that proactively reduce the attack surface and improve security. Referring back to our healthcare analogy, this represents the phase in which the organization has shifted from treating maladies after they have happened to taking preventive measures to head off those maladies to begin with. Projects like microsegmentation, NAC, and Zero Trust become more realistic and attainable at this stage. Without device and business context it's impossible to create policies that are effective and don't disrupt operations.

THE BUSINESS VALUE

While in stage three the automation was being used from a reactionary position, in stage four it is taking proactive measures before the threats are detected. Consequently, the SOC is less stressed, better equipped, and more able to begin the shift to becoming a partner in alignment with the business strategy elements of the organization.

KEY OPERATIONAL TASKS

- **Expand the security platform to all network-connected devices by adopting techniques to reduce the attack surface of IoT and out-of-support operating systems**
- **Boost proactive position with red team-blue team exercises, threat hunting, application control, script control, isolation, micro-segmentation, deception, and mobile threat defense**

OUTBOUND INTEGRATIONS

- SIEM to enable automation of reactive security efforts
- SOAR to enable automation of reactive security efforts
- XDR to enable automation of reactive security efforts
- Outbound to network and security infrastructure to enforce proactive policy, reduce the attack surface, and improve security

STAGE FIVE: OPTIMIZED SECURITY

Key Business Goal:

- Apply the capabilities of the security platform to handle the dynamic nature of the infrastructure as it changes and evolves. This includes adding new devices, aligning with new business strategies, integrating or changing security tools, or supporting M&A activities

Key Capabilities:

- Continuously expand and improve what you **KNOW** about device and business context to inform priorities, strategies, and policy creation to **SECURE** your devices
- Extend earlier stage concepts of **SEE, KNOW**, and **SECURE** to understand and minimize risk from additional environments, external locations, and partners

Integrations:

- Bidirectional to deeply involve security tools and extend automated processes

At this stage, the security platform has reached peak interaction with other tools and deeply integrated its functionality throughout the entire IT and security infrastructure. While security requires regular review and tuning, the security platform is at a state to support full scale automation. Where previously, adding new devices would have a negative impact on the attack surface, at this stage, new devices can be automatically discovered, classified, and have the appropriate policies applied with little to no manual effort and no additional risk.

The platform can be extended to minimize risk in additional environments including external locations and to assess dangers posed by third parties, such as business partners and vendors. The goal of well-functioning security systems is not just to help organizations stay free of threats, but to support security and business decisions and achieve strategic alignment. The ultimate outcome is a security system that fully integrates all connected devices with an organizational-wide Zero Trust strategy.

THE BUSINESS VALUE

At this level, the operational discipline and the operation of the platform will have reached an optimal level. The result is the ability to achieve a highly efficient vision of devices connecting to the infrastructure, with threats being identified, and responses being made in an efficient and timely manner. However, the infrastructure of a healthcare organization is dynamic and evolving with new devices being added, changes being made to network and IT infrastructure, new organizational initiatives, and M&A activity. To handle this, the team must continuously review and identify opportunities to enhance and extend the ability to **SEE, KNOW,** and **SECURE**.

When a department has reached the level of fine-tuning its operations because the majority of the fundamental challenges have been addressed, it can make its best contributions to the organization. For a security team, Stage Five represents the pinnacle of achievement. Even so, the team must continually reassess how well its cybersecurity planning, actions, and effects are meeting the evolving threat that cybercriminals will pose. That means reviewing all five stages to be certain the requirements they each represent are being met.

KEY OPERATIONAL TASKS

- ☑ **Continue to execute and optimize vulnerability identification and mitigation efforts**
- ☑ **Continue to review threats and optimize response including orchestration, and automation**
- ☑ **Continue to review and optimize proactive security policies and strategies to ensure they align with changes in the environment**
- ☑ **Look for issues extending beyond the internal concerns and investigate potential external exposures through supply chains**

SUMMARY

While all industries need to take measures to guard themselves against the perniciousness of cyberattacks, no other sector has so much at risk as healthcare. It may sound overly dramatic to say so, but the difference between a strong security program and a weak one potentially is a matter of life or death. Global tensions are escalating and cyber can, unfortunately, be an effective weapon in the hands of state-sponsored actors trying to do damage to their foes.

At the same time, organizations cannot expect to reach the Optimized Security stage instantly. Each stage builds upon the other. Each base of knowledge needs to be fully established and integrated into the organization before moving to the next level.

Ordr has developed the advanced technology critical for organizations to gain essential insights and enforce protections. We recognize the complexities that security leaders in healthcare organizations struggle with to ensure the ultimate safety of the patients they're tasked with protecting.

We summarize the approach we take in three words: **SEE**, **KNOW**, **SECURE**. At each of the five stages, all three actions are involved. In Stage One, the **SEE** element is most prominent as organizations get a sense of where they are exposed by such fundamental tasks as identifying all the devices that are part of their attack surface. An organization never stops seeing, but next adds the **KNOW** action as the dangers start to become clear. Logically enough, once an organization sees the danger and knows how it works, it can head off the threat with **SECURE** action.

Along the way, each of this trio of Ordr's core security functionality is amplified and refined with automation, integration, AI/ML, and Zero Trust.

Please contact us to learn more about the process for achieving optimized cybersecurity and how Ordr can help you get there.

ACRONYMS

API - Application Programing Interface

BIS - Bureau of Industry and Security

CAASM - Cyber Asset Attack Surface Management

CMDB - Configuration Management Database

CMMS - Computerized Maintenance Management System

EASM - External Attack Surface Management

EDR - Endpoint Detection and Response

EPP - Endpoint Protection Platform

IDS - Intrusion Detection System

IOC - Indicator of Compromise

IPS - Intrusion Prevention Systems

ITSM - IT Service Management

MFA - Multi-Factor Authentication

NAC - Network Access Control

NDR - Network Detection and Response

NGFW - Next-generation Firewall

SIEM - Security Information and Event Management

SNMP - Simple Network Management Protocol

SOAR - Security Orchestration, Automation and Response

SPAN - Switched Port Analyzer

TAP - Test Access Port

TI - Threat Intelligence

VA - Vulnerability Assessment

VM - Vulnerability Management

VPT - Vulnerability Priority Technology

XDR - Extended Detection and Response

ABOUT THE AUTHOR

Brad LaPorte is a Strategic Advisor for Ordr and a former top-rated Gartner Research cybersecurity analyst. He has held senior positions in US Cyber Intelligence, Dell, and IBM, as well as in several startups.

Brad has spent most of his career on the frontlines fighting cybercriminals and advising C-level executives and thought leaders on how to be as efficient and effective as possible. He is currently an advisor with Lionfish Tech Advisors and High Tide Advisors, helping cybersecurity and tech companies grow their go-to-market strategies.

ACKNOWLEDGEMENTS

Danelle Au - Chief Marketing Officer

Paul Davis - Vice President of Customer Success

Michael Kehoe - Director of Strategic Programs

Darrell Kesti - Vice President of Sales

Srinivas Loke - Vice President of Product Management

Greg Murphy - President and CEO

Gnanaprakasam Pandian - Chief Product Officer and Co-Founder

Chris Westphal - Head of Product Marketing