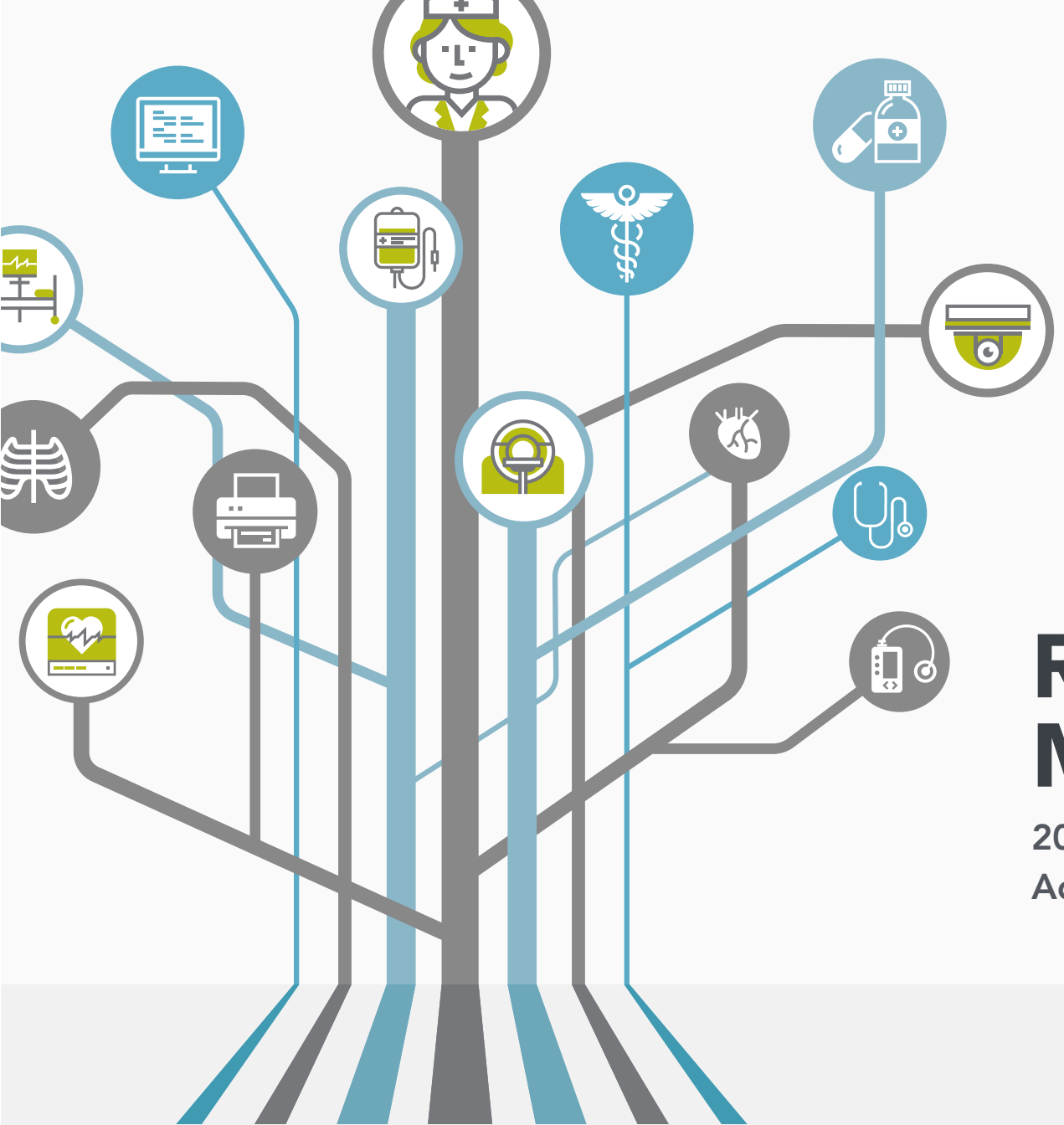

Rise of the Machines:

2020 Enterprise of Things Adoption and Risk Report

ordr

Executive Summary

There is no more dramatic example of the importance of the Internet of Things than in the midst of the COVID-19 pandemic. Within healthcare organizations, a surge of IP-enabled medical devices such as ventilators, infusion pumps, and EKG machines are playing a critical role in patient care—saving lives, collecting medical diagnostics data, facilitating medical functions. At the same time, devices such as HVAC controllers, payment systems and elevator controls are also enabling the patient care ecosystem.

According to a Gartner survey, **86% of healthcare respondents reported having an IoT architecture in place** for most lines of business, while **79% of healthcare providers with revenue over $100 million have put IoT devices into production.**

Medical devices are continuing to be connected at an especially rapid pace.

But while healthcare organizations are blazing the way in IoT transformation, they are not alone. Gartner believes that **the enterprise and automotive Internet of Things (IoT) market* will grow to 5.8 billion endpoints in 2020, a 21% increase from 2019.**

In fact, the pandemic has forced the digital transformation of organizations across many verticals, and IoT will play a key role in this transformation, as shown by this widely distributed "graphic".

The Ordr **Rise of the Machines: Enterprise Of Things Adoption and Risk Report** incorporates analysis of more than 5 million unmanaged, IoT and IoMT devices in Ordr deployments between June 2019 and June 2020. This report is the first of its kind to identify real-world risks across a diverse universe of connected devices, and reaffirms the need for a comprehensive approach to securing these devices—discovery and classification, risk and security identification and micro-segmentation.

Key Findings Include The Following:

Devices With PCI and VLAN Compliance Violations

20% of all deployments have PCI violations. Ordr identified deployments where retail IoT Devices were on the same subnet or VLAN as a tablet, printer, copier, or physical security device. Ordr also identified 75% of deployments with VLAN violations. In one deployment, a number of USB card readers were connected to workstations on the same subnet or VLAN as a tablet, printer, copier, or physical security device. In healthcare organizations, Ordr identified deployments where medical devices were on the same VLAN as other non-medical IoT devices.

Devices With FDA Recalls and Vulnerabilities

Ordr identified that 86% of Healthcare deployments have more than 10 FDA Recalls against their medical IoT devices, while 15 – 19% of medical devices run on operating systems Windows 7 or older (XP, CE, ME, NT, 98, 97, or 95). These devices need to be taken out of service or segmented appropriately.

Devices Behaving Badly

Ordr identified devices being used for bitcoin mining, and showing unusual patterns of communications to hostile countries, including Iran, Russia and North Korea. Ordr also identified a proliferation of undocumented, previously unknown firewalls making outbound VPN connections presumably for remote support of various medical systems.

What Applications Are On Your IoT Devices?

Ordr discovered Facebook and YouTube applications running on MRI and CT machines. MRI and CT machines typically utilize legacy and unsupported operating systems like Windows XP. The challenge when healthcare staff use these devices to surf the Internet, is that the devices become vulnerable to a potential attack, and can sometimes be the first target of a ransomware attack.

It's A Shadow IoT World

95% of healthcare deployments have Amazon Echo and Alexas active in their environment, along with other hospital surveillance equipment. This violates privacy requirements with the risks of attackers eavesdropping and recording conversations.

10-15% of network devices were rogue devices unknown or unauthorized by security and IT teams. Ordr also identified a number of unique devices outside of the typical IoT device portfolio.

Security Risks of Unmanaged, IoT and IoMT Devices

What are the security risks of unmanaged, IoT and IoMT devices? These devices provide mission-critical business operations, but they also pose unique security challenge for organizations:

- **Improperly segmented unmanaged devices** increase the attack surface of the internal network
- **Industrial espionage** may be possible via corporate IoT devices such as unsecured conference room phones and smart televisions
- **Data breaches**, where attackers spy on communications between peers in an IoT network and collect information on the services and technology they implement is possible
- **Unmanaged and IoT devices**, if not properly secured, may be targeted by malware to become part of a botnet attack (example: Mirai and Dark_Nexus)

Security concerns with unmanaged, IoT and IoMT devices have even been acknowledged by the U.S. Federal government. In 2019, as part of the John S. McCain National Defense Authorization Act (NDAA), Congress signed a bill that banned the use of Dahua and Hivision video surveillance cameras for the US government, for US government-funded contracts, for 'critical infrastructure' and 'national security' usage.

The following chart shows some cyberattacks and vulnerabilities that have targeted IoT devices.

IoT Hacking and Vulnerabilities – Many Devices Lack Adequate Security

Hackers Continually Breach Security Cameras	Hackable Cardiac Devices St. Jude	Mirai Botnet (Dyn)	Smart TVs Turned Into Listening Devices	Cyberattacks on IoT Devices Surge 300% in 2019
Millions of network accessible IP cameras are deployed with vulnerabilities. A simple search query usually reveals thousands of accessible IP cameras that can be unknowingly controlled by anyone on the Internet.	Researchers discovered that St. Jude Medical's implantable cardiac devices had vulnerabilities that could allow hackers to access devices such as pacemakers and defibrillators remotely.	Mirai was the largest DDoS attack ever performed and was launched on service provider Dyn using an IoT botnet that used known default usernames and passwords to spread.	The FBI issued a warning that hackers can take control of several popular manufacturers' Smart TVs. Hackers can turn on a camera and microphone and record videos and audio.	Cyberattacks on IoT devices are rapidly accelerating due to the increase in the numbers of IoT devices being deployed and the ease at which IoT devices can be attacked.

Why is securing these devices so difficult?

To start, these devices are not designed to be secure. They come with poor features such as weak passwords, lack of secure update mechanisms or insecure default settings. Many of these IoT devices also run outdated or unsupported operating systems, have an expected service life of many years and cannot be taken out of service.

There may be vulnerabilities associated with these connected devices, but **traditional vulnerability scans cannot be performed because many of these devices are mission-critical, sensitive devices and are susceptible to failure during scans.** Additionally, these devices are sometimes procured and managed by teams outside of security and IT. For example, biomedical and clinical engineering teams may own IoMT devices, while surveillance cameras and badge readers may fall under building management or physical security teams. As a result, asset inventory may be managed by separate teams, and can be outdated and inaccurate, or dependent on manual processes.

Finally, **traditional security tools don't work with IoT endpoints.** The software footprint of these devices is so small that endpoint security agents cannot be installed on the devices to protect them.

Detailed Analysis on Findings

Devices With PCI and VLAN Compliance Violations

As part of PCI Data Security Standard (PCI DSS), all credit card data needs to be segmented from the network. PCI Audits need to verify segmentation is in place for all credit card readers. Often, this is done with VLANs to virtually segment the traffic. Over time, most organization fall out of compliance due to changes in the network and lack of documentation around change control.

In Ordr deployments, we observed that 20% of all deployments had potential PCI violations. These deployments had least one retail IoT Device on the same subnet or VLAN as a tablet, printer, copier, or physical security device, likely violating section 1.2.1 of the PCI DSS.

We also observed that 75% of all deployments with VLAN and subnet violations. Ordr found printers, servers, and vending machines on the same VLANs as medical devices. Cyberattackers targeting these printers, servers and vending machine now have the potential to gain complete access to these medical devices.

Ordr recommends that mission-critical devices be moved to specialized VLANs.

Devices With FDA Recalls and Vulnerabilities

The issue of vulnerabilities is one that has plagued cybersecurity teams for many years now. Threat actors look to exploit vulnerabilities – even ones that have been around for a long time – to gain access to a network or machine. Medical devices, like other computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device.

Ordr also found that 15–19% of Medical Devices run Windows operating systems that are Windows 7 or older (XP, CE, ME, NT, 98, 97, or 95). The global Wannacry ransomware attack in 2017 demonstrated how vulnerable it is to have systems that haven't received security updates. This is a bigger challenge with medical devices as they may be difficult to patch or patches may not be available by manufacturers.

Ordr found that 86% of healthcare deployments have more than 10 FDA recalls against their Medical IoT devices. The FDA uses the term "recall" when a manufacturer takes a corrective action to address a problem with a medical device that violates FDA law, is misbranded or adulterated. This means a medical device is defective, could be a risk to health or both. In 2017, Abbott recalled 465,000 pacemakers after discovering that they could be hacked.

Ordr recommends that these high-risk devices with FDA recalls or vulnerabilities, particularly if they cannot be patched, be properly segmented to ensure they are not at risk from attackers exploiting Windows vulnerabilities.

Detailed Analysis on Findings

Devices Behaving Badly

There are real risks and threats posed by connected devices. If unmanaged, IoT and IoMT devices are not properly secured, they can become a new attack entry point, be used as part of a "botnet attack", or share confidential information with attack entities.

Ordr discovered the following in our deployments:

- **Proliferation of previously unknown firewalls** making outbound VPN connections presumably for remote support of various medical systems.
- **Devices performing bitcoin mining** – Unlike traditional currencies that are handled by financial institutions, bitcoin uses a public ledger system where transactions are confirmed by Bitcoin miners. Anyone can take part in the mining process and profit from it. As a result, threat actors take advantage of computing resources that they can "hijack" to profit from bitcoin mining. In Ordr deployments, we discovered compromised devices being used for Bitcoin mining.
- **Devices with unusual patterns of communications, calling out to hostile countries like Iran, South Korea and China.** Ordr uses machine learning to map device communications patterns and identify anomalous behaviors. During one deployment, a compromised machine was identified as communicating to a command and control in Iran.

What's Running On IoT Devices?

Ordr discovered users were enabling Facebook and YouTube on MRI and CT workstations. MRI and CTI machines are expensive devices that typically have long operating lifetimes. Many of these MRI and CTI machines run older operating systems. The security challenge when applications like Facebook and YouTube run on these applications is that these devices can become the initial attack entry point into the organization.

Ordr recommends organizations understand usage of IoT devices and also the users associated with them. Oftentimes, IoT devices have diverse operational owners and multiple users. Understanding usage and associated users is critical to identify infected devices and to address compliance requirements.

Detailed Analysis on Findings

It's A Shadow IoT World

For years, security and IT teams have been railing about the dangers of shadow IT and how rogue applications introduce risks. Shadow IoT -- IoT, IoMT and other unmanaged devices in use within an organization without IT's knowledge --- may be worse. Without visibility into the connected devices in an environment, IT cannot secure them.

Ordr identified the following shadow IoT devices:

- **95% of healthcare deployments with personal Alexa and Echo devices connecting to the network** – Because of vulnerabilities that allow these devices to eavesdrop and record conversations, these smart speakers are not allowed in a healthcare environment.
- **10-15% of devices are unknown or unauthorized** – A significant percentage of devices in Ordr deployments are unknown or unauthorized. We discovered some unusual devices in the network including the following:
  - **A Tesla connected to the hospital network** – after some investigation, the security teams identified the Tesla as belonging to a doctor who had connected to the network from his car in the parking garage
  - **Elevator controls on the network** – In one deployment, the facilities team had connected hospital elevators to the network. Elevators are essential to patient care even though they are non-medical IoT devices.
  - **Peloton** – In one healthcare organization, Ordr identified a Peloton device on the network, that was being used for physical therapy, but likely had violated Healthcare Insurance Portability and Accountability Act (HIPAA) regulations because of patient data recorded on these devices.

Ordr recommends organizations select an IoT security solution that has a comprehensive integration framework with existing security and asset inventory management systems. This will enable these devices to be detected and IoT context shared with systems such as Security Information and Event management systems (SIEM) and computerized maintenance management systems (CMMS).

Security Best Practices and Takeaways

IT and security tasked with managing and securing unmanaged devices – IoT, IoMT, OT – need to understand the risks associated with these connected devices. After all, we know hackers aren't polite enough to stop attacking organizations, even during a pandemic. To the contrary, in times of crisis, hacker activity increases and today is no different. There has been no respite from ransomware attacks targeting healthcare organizations, and hackers will be hard at work trying to attack and compromise IoT devices to create destructive botnets.

There are four essential steps for securing unmanaged devices; in order to be successful, each step needs to be automated:

Discover devices:

It is vital to gain visibility into every unmanaged and IoT device that connect to your network. This includes ephemeral assets that may go offline at any time and then reappear in a new physical and network location. High-fidelity information is critical to truly understand and classify these devices.

1

Understand behavior:

Once you know what devices you have, you need to know its purpose in the enterprise and understand its normal behavior patterns. Mapping communications patterns and baselining device behavior is crucial to identifying anomalous behaviors.

2

Identify risks:

Are there mission-critical devices? Are there vulnerable devices? Understand the risk profile for these devices, from medical device advisories and vulnerabilities to obsolete device operating systems. Identify anomalous behaviors such as a rogue or infected device communicating to a bad domain.

3

Generate polices:

With all devices accounted for and categorized, IT and security teams can generate and assign appropriate segmentation policies for high-risk, vulnerable and mission-critical devices. These policies can control how each device communicates, what resources they can and cannot access, and to ensure every new device and service is risk-assessed and secured in real time.

4

Ordr Platform for IoT Security

Ordr enables organizations to discover and safeguard the universe of unmanaged, IoMT and OT devices in their environment today. The Ordr Systems Control Engine (SCE) delivers the quickest time to value by enabling the complete life cycle of device security, as described below:

DISCOVER

What devices are connected?

AUTOMATICALLY IDENTIFY, CLASSIFY & LOCATE all network-connected devices and systems

BASELINE

What exactly is everything doing?

MAP ALL CONNECTED DEVICE COMMUNICATIONS, spot anomalous behavior

RISK ASSESS

Which ones are vulnerable?

ASSESS EXPOSED WEAKNESSES IN REAL-TIME AND AT SCALE and determine potential risk

SEGMENT

How do I secure high-risk devices?

DYNAMICALLY GENERATE, AND ENFORCE granular security policies on existing infrastructure

- **Discover** – Within a few hours of deployment – via a network tap or SPAN – Ordr automatically discovers high-fidelity information about every connected device, including make, classification, location, and application/port usage. This visibility is provided in real-time for any new connected device.
- **Security and Risk Assessment** – Ordr identifies a variety of risks for devices including vulnerabilities, FDA recalls and anomalous behaviors:
  - **Identify vulnerabilities** – The Ordr SCE validates the vulnerability, threat, and risk level of each device through an extensive series of security checks. Connected devices are compared against a suite of industry threat intelligence feeds, network vulnerability databases, ICSA–ICS-CERT advisories, FDA lookups for medical device recalls and alerts, and manufacturer-published vulnerability data.
  - **Identify weak ciphers and certificates** – Ordr also detects the use of weak ciphers and non-trustworthy certificates within devices so that at-risk devices can be proactively identified.
  - **Identify anomalous behaviors** – Using machine learning, every device communication pattern is profiled via the Ordr Flow Genome. Communications to other IP/VLAN segments within the organization are easily visualized, as well as communications to external networks. The Ordr SCE identifies anomalous communications, for example traffic going to known malicious sites or command and control.
- **Segment** – Ordr enables practical segmentation that actually works, is scalable and leverages existing infrastructure. Based on the Ordr Flow Genome, the "sanctioned" communications patterns for devices can be identified. The Ordr Policy Generator then takes the tedious work out of creating and implementing policies for micro-segmentation by generating them dynamically for any vulnerable device. These policies can then be pushed to firewalls, network access control products, switches and wireless LAN controllers.
- **Utilize** – Ordr provides deep insight into device utilization, so teams can identify areas of over or under use, to ensure data-driven moves, adds and changes as teams scale their capacity.