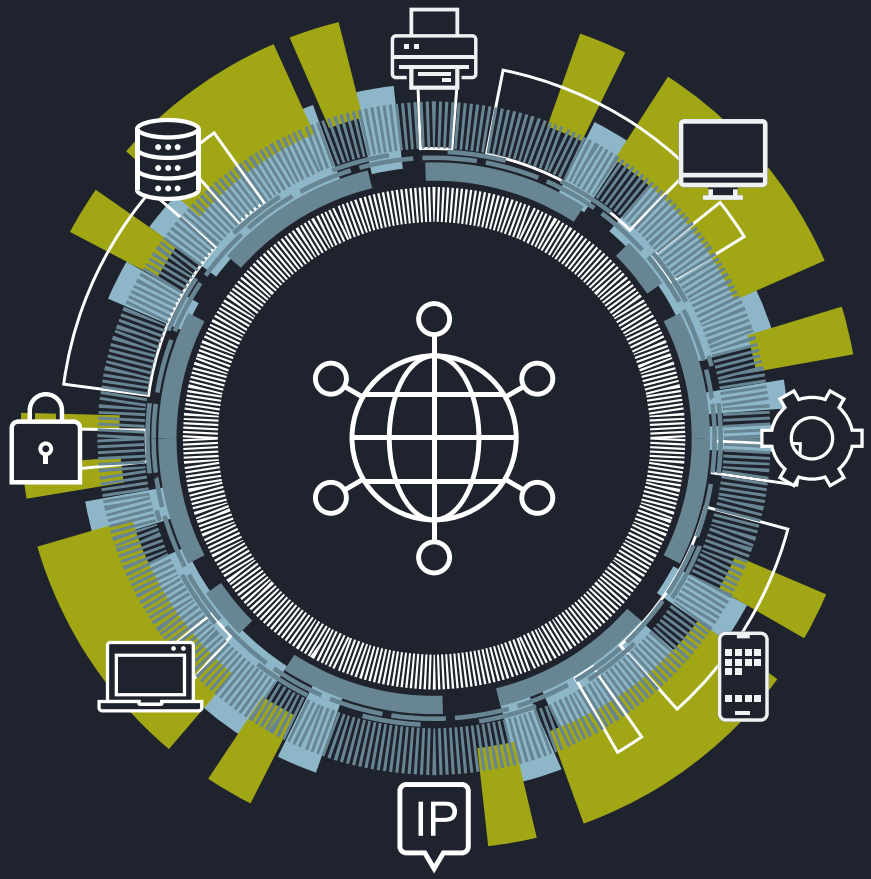


Rise of the Machines 2021

STATE OF CONNECTED DEVICES — IT, IoT, IoMT AND OT

ōrdr

Rise of the Machines

Many of us watched the 2011 Steven Soderbergh movie Contagion. The movie was uncanny in "predicting" scenarios like enforced social distancing (10 feet in the movie instead of 6 feet), grocery store panic runs, school closings, homeopathic miracle cures, and even vaccine development efforts.

The only scenario the movie didn't predict was the increase in cyberattacks in the midst of a pandemic, perhaps a premise unfathomable even for Hollywood. But it was the unfortunate reality faced by many organizations last year.

Healthcare organizations had to deal with the security of devices that were rapidly procured and deployed not only in their organization but in field hospitals, to address the surge in COVID-19 patients. Other organizations scrambled to deal with new work-from-home requirements. During the chaos and confusion, threat actors launched cyberattacks. We saw an increase in ransomware, where attackers not only encrypted traffic to halt operations but also transitioned to a new business model of releasing sensitive data if the ransomware wasn't paid.

If that wasn't enough to deal with, towards the end of 2020, we learned that threat actors had added malicious code to SolarWinds Orion software, used by more than 33,000 customers to manage IT resources. Beginning in as early as March of 2020, SolarWinds sent software updates to its customer that included the malicious code, creating a backdoor to 18,000 customer networks.

This year's Rise of the Machines Report shines a spotlight on these cyberattacks, and the growth of agentless devices in the network . Using anonymized data from Ordr's deployments across more than 400 deployments and 12 million devices, we analyzed the security risks and trends with connected devices for the past 12 months, from June 2020 through June 2021.

THE RESULTS ILLUMINATED SOME INTERESTING FINDINGS:

- 42% of connected devices are agentless devices, suggesting that almost half of your devices cannot be protected via traditional endpoint security agents.
- The top agentless devices included industry-based devices, IP phones, printers, and facilities devices like video surveillance cameras and badge readers.
- Internet of stranger things discovered in Ordr deployments included Teslas, Alexas, Pelotons, Sonos speaker devices and gaming devices.
- Outdated operating systems present the greatest risks. Almost 19% of deployments are still running outdated operating systems such as Windows 7 and older.
- 46% of all IoT devices are vulnerable to medium and high severity attacks.
- Healthcare organizations are seeing significant risks. 68% of healthcare deployments have more than 10 FDA recalls, 32% of medical imaging devices run on unsupported operating systems and 15% of medical devices run on unsupported operating systems.
- In Ordr deployments, we found that 55% of deployments had devices with "orphaned users", and 20% of deployments had devices with local users.

Challenges With Connected Device Security

Before we dive into our connected device findings, it's probably prudent to define the challenges with connected devices. Technically, all devices connected to the network are in the scope, but they fall into two categories – the "agentable" devices like laptops and PCs, and the "un-agentable devices".

The former uses software security agents to protect the devices they are installed on. Devices are secure as long as the agents are updated with the latest release and patches, which frankly isn't always the case.

The second category encompasses a rather large, broad group — the traditional IT devices or endpoints, such as routers and switches that cannot support agents, and the newer, more vulnerable IoT (Internet of Things), IoMT (Internet of Medical Things) and OT (Operational Technology):

- **Traditional IT devices:** While laptops and PCs can support endpoint security agents, there are a myriad of other devices like servers and routers that cannot support agents.
- **IoMT/Medical devices:** Medical devices are critical to patient care, but not always designed with security in mind. They often remain in operations for years and run outdated operating systems, yet cannot be patched.
- **IoT Devices:** IoT devices such as smart displays, fax machines, and printers can be compromised and become an attack vector.
- **OT Devices:** OT devices are part of business and manufacturing operations. They are instrumental in optimizing efficiencies, improving safety or enhancing business processes. Because of digital transformation, OT systems are no longer air-gapped from IT/IoT network. As OT devices connect to IT (and IoT devices), they need to be secured.
- **Building Facilities Systems:** HVAC systems, elevator controls, and cameras are part of building facilities and operations for many organizations.

Challenges With Connected Device Security

These devices aren't designed with security in mind. Many are in operations for years, and often run vulnerable operating systems but cannot be patched. In fact, IoT and OT vulnerabilities have continued to grow over the past several years; In the National Vulnerability Database of the National Institute of Standards and Technology (NIST), IoT-related vulnerabilities have surpassed 2% of total disclosed vulnerabilities each year since 2019. This is after not rising above 0.4% in any previous year. Traditional vulnerability scans cannot be performed because many of these devices are mission-critical, sensitive devices and are susceptible to failure during scans.

What does this mean for security teams? First, the visibility and security of ALL connected devices is critical. The Colonial Pipeline attack showed us that the security of traditional IT (and IoT) devices are just as important as operational technologies (OT) security. Any downtime with IT devices and systems such as printers, billing systems, elevator control systems can impact business operations. Additionally, any cyberattack on an IT and IoT device can move laterally to the OT environment. Second, network visibility, threat detection and response are critical to understanding what devices are in the network, what they are doing and what risks they bring. This becomes even more important with the growth of "agentless" and "un-agentable devices".

This report focuses on all connected devices but with a "network" centric view of what these devices are actually doing in the network, and what vulnerabilities, threats and risks they bring. Our goal is to identify the top risks and trends we've found in our deployments to empower all organizations with better security best practices.

IOT SECURITY IS BECOMING A LEGISLATIVE PRIORITY

December 2020:

The U.S. Government passed the IoT Cybersecurity Improvement Act, which defines baseline security and vulnerability disclosure standards established by NIST for connected devices procured by the Federal Government. While this Act is limited to devices procured by the Federal Government, other organizations will also demand similar security features.

April 2021:

On 21 April 2021, the UK Government published its response to request for views on the cybersecurity of smart devices. The government also announced plans to introduce new legislation to regulate the security of consumer IoT devices.

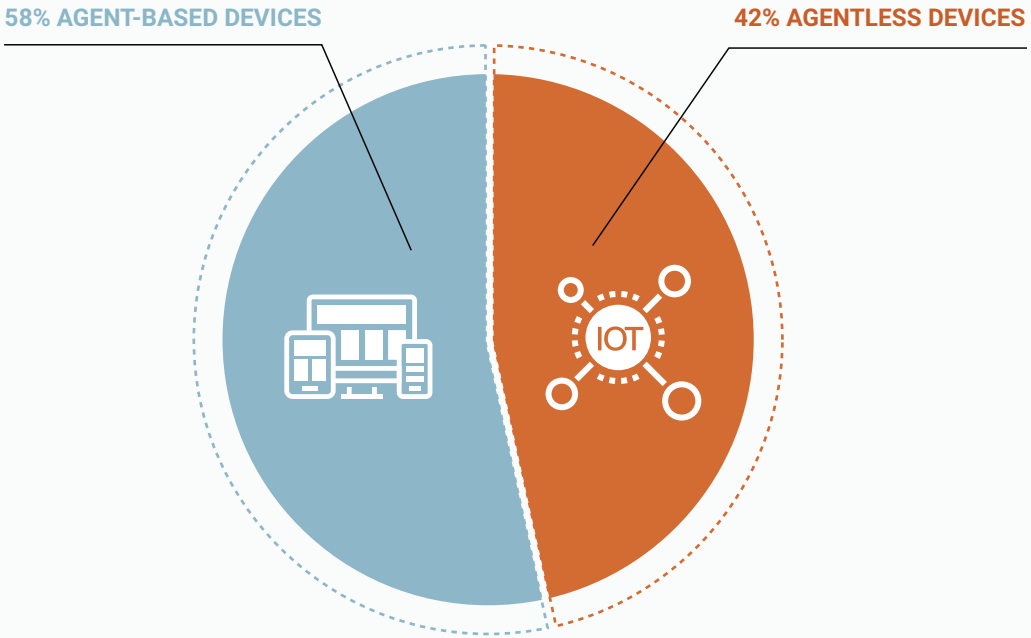
May 2021:

In May 2021, President Biden signed an Executive Order on Improving the Nation's Cybersecurity. The new Executive Order called out the need to focus attention not just on information technology (IT), but on operational technology (OT), and stipulates that government contractors must adopt architectural frameworks such as Zero Trust.

Key Findings

HOW MANY DEVICES ARE AGENTLESS DEVICES?

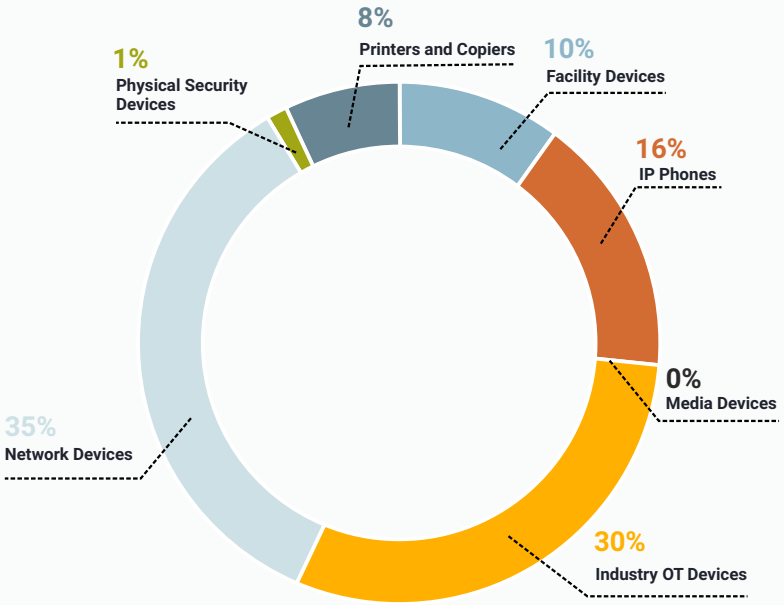
42% OF NETWORK DEVICES WERE AGENTLESS DEVICES



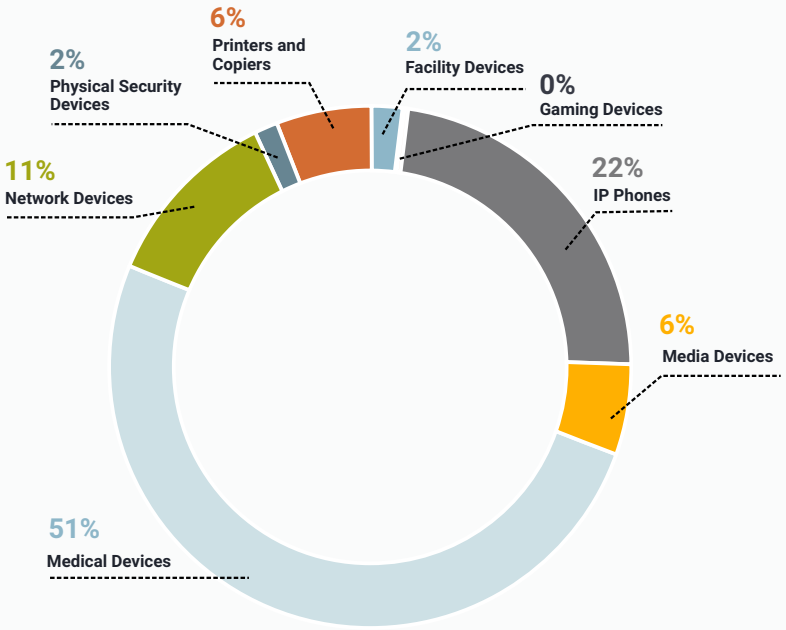
What were the top agentless devices? The answer wasn't too surprising. There were industry-specific devices (for example medical devices within healthcare, and OT devices within manufacturing), network devices, IP phones, printers, physical security cameras and facility devices. We see slightly different percentage breakdowns when we looked at manufacturing versus medical facilities. The proliferation of these "agentless devices" can serve as an an easy entry point for threat actors before lateral movement to other more critical parts of the network.

Key Findings

MANUFACTURING ORGANIZATIONS



MEDICAL FACILITIES



Key Findings

CONNECTED DEVICES AND RISKS

IP PHONES – The humble IP phone is not immune to threat actors taking advantage of vulnerabilities that are unpatched, as shown in a 2020 campaign that targeted Sangoma and Asterisk VoIP phones or 2019 campaign targeting Avaya IP phones.

PRINTERS – Printers are an easy entry point for threat actors. They are ubiquitous, connected to the network, typically run an operating system like Windows with many vulnerabilities (such as the PrintNightmare vulnerability). They typically have to connect to the outside world for maintenance. Many printers also have default or weak passwords that may not be a priority for organizations to address. A printer was a key component of the Lazarus cyberattack on Bangladesh's national bank. Microsoft PrintNightmare vulnerabilities have also surfaced recently that would allow attackers to take control of vulnerable systems.

SECURITY CAMERAS – Security cameras can be a big source of risks as they are fairly low-cost devices designed without security in mind. Most ship with weak default passwords that are never changed, and have vulnerabilities that can be exploited. Security camera footage may hold critical data and subject to compliance. While the Verkada breach was a result of a compromised cloud admin password, it was a wake up call on the potential of what a breach may expose. Security cameras should be monitored for behavioral anomalies and segmenta- tion can stop lateral movement.

BADGE READERS – Badge readers are a critical part of physical security and business operations, enabling employees and contractors to access the appropriate part of a building based on their role. These badge readers are connected to a network, and can be an entry point to other devices on the network. In 2018, a Google engineer demonstrated that he was able to use a vulnerability to bypass any RFID-based keycard controlled badge reader.

INTERNET OF STRANGER THINGS ABOUND

What were some of the more unusual, connected devices we saw in Ordr deploy- ments?

Last year, we called out a proliferation of Alexa devices. We also saw Teslas connected to the network. The trends were similar this year with Alexas and Teslas discovered in our customers' networks. For many of our healthcare customers, Alexas actually served specific business functions. Within a children's hospital, Alexas were used in lieu of nurse call buttons and also facilitated turning on lights and devices like TVs in a patient room.

We saw an increase in deployments of Sonos devices and Peloton. We saw Peloton's popularity reflected in these devices being discovered and profiled in a broad range of verticals like hospitality, healthcare, universities and enterprise gyms. Despite vulnerabilities such as a leaky API, few organizations were focused on the security and segmentation of these devices. Finally, we saw a lot of gaming machines in manufacturing verticals, presumably because employees are working long hours and gaming machines delivered entertainment.

INTERNET OF STRANGER THINGS:

- **Alexas**
- **Teslas**
- **Sonos speakers**
- **Pelotons**
- **Gaming machines**

Key Findings

OUTDATED OPERATING SYSTEMS PRESENT THE GREATEST RISKS

Why is this the case? Certain devices like OT or IoMT are a critical part of business operations and can be in service for years at a time. As a result, they often run outdat- ed operating systems that cannot be patched. However, it can be cost-prohibitive to replace them. Newer devices may not offer the same features, or may be too complex to deploy.

The challenge from a cybersecurity perspective is that when operating systems reach end-of-life, vulnerabilities will remain on the system. The manufacturer no longer issues patch updates to resolve issues. Threat actors may use these vulnerabilities to gain access.

In Ordr deployments, we identified about 19% of deployments with devices running outdated operating systems Windows 7 and older:

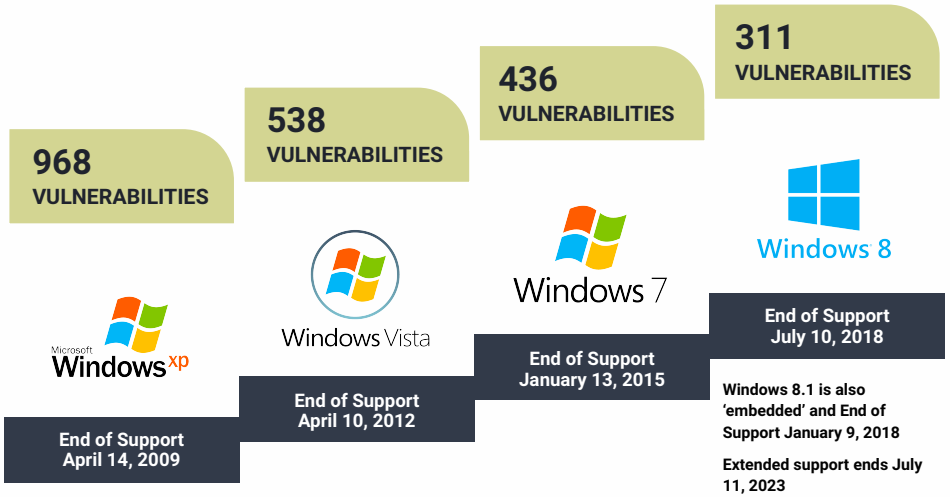
13% of deployments had devices running Windows 7

5% of deployments had devices running Windows XP

1% of deployments had devices running Windows CE

We also saw almost 24% of deployments are still running Windows 8 and 38% running Windows 10, which are expected to end-of-life in 2023 and 2025 respectively.

LEGACY AND UNSUPPORTED OPERATING SYSTEMS



THERE ARE ROUGHLY 5-8 BILLION MEDICAL DEVICES IN THE FIELD, OF WHICH ROUGHLY 20%-25% RUN WINDOWS, AND 70% OF THOSE RUN-ON UNSUPPORTED SOFTWARE.

Key Findings

HEALTHCARE ORGANIZATIONS ARE SEEING SIGNIFICANT RISKS

Healthcare verticals continue to be one of the most targeted verticals by threat actors. They also face significant risks from connected devices in their network.

ORDR IDENTIFIED THE FOLLOWING:

68%
OF HEALTHCARE DEPLOYMENTS HAVE MORE THAN 10 FDA RECALLS

32%
OF MEDICAL IMAGING DEVICES RUN ON UNSUPPORTED OPERATING SYSTEMS

15%
OF MEDICAL DEVICES RUN ON UNSUPPORTED OPERATING SYSTEMS

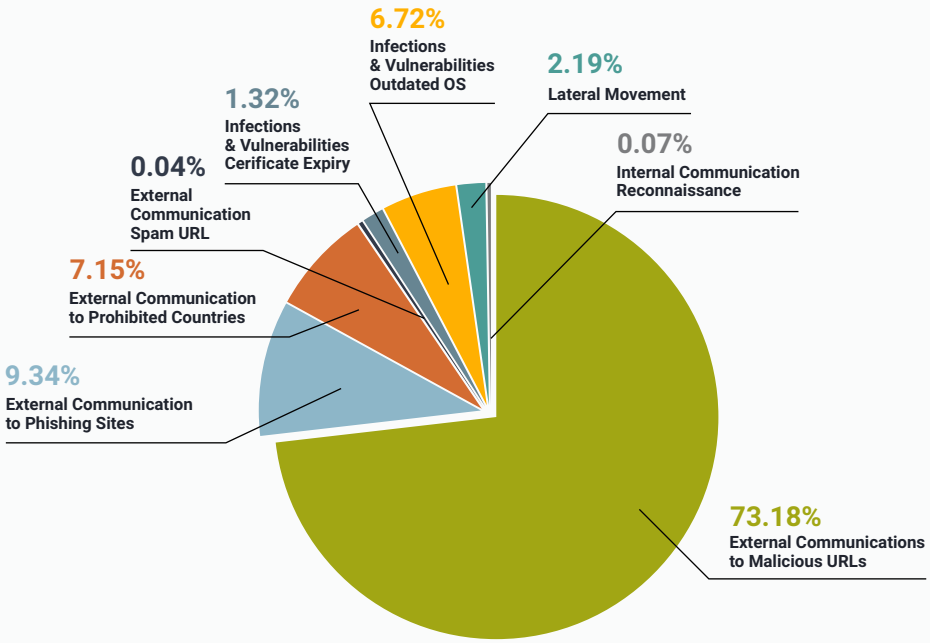
WHAT WERE THE TOP MEDICAL DEVICES?
THE TOP FIVE DEVICE CATEGORIES WERE THE FOLLOWING:

48%	INFUSION PUMPS
15.2%	PATIENT MONITORING
4.5%	GLUCOSE MONITOR
4%	MEDSTATION SYSTEM
3.78%	POINT OF CARE ANALYZER

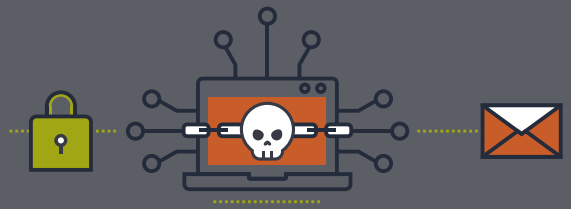
Key Findings

46% OF CONNECTED DEVICES ARE VULNERABLE TO MEDIUM AND HIGH SEVERITY ATTACKS

Ordr discovered that about 46% of connected devices are vulnerable to attacks. When we looked at the details of the attacks and divided them into types of attacks, the top attacks were external communications to malicious URLs, phishing URLs and prohibited countries, followed by attacks due to vulnerable operating systems and finally lateral movement such as exploits, anomalous behavior, and active threats/tools like CobaltStrike or Eternal Blue.



MALWARE AND RANSOMWARE, OH MY!



In many Ordr deployments, visibility via the network shed the light on various cyberattacks in progress:

- Darkside ransomware was detected via anomalous communications to international sites weeks before the FBI announced the C2 and indicators of compromise.
- When the SolarWinds cyberattack was first reported, a healthcare customer insisted they had no SolarWinds instances. Ordr discovered an instance deployed in a lab, unbeknown to the security team.
- In an industrial manufacturer's unsegmented network, Ordr discovered three different types of malware including WannaCry and Eternal Blue spreading laterally across the flat network.
- A medical organization discovered that ransomware was trying to attack their network via a partner connected to them via VPN. They used Ordr to track where it had spread, what devices were infected, and where the compromised devices were. They were able to recover in hours whereas the partner took 6+ weeks.

Key Findings

DEVICES WITH ACCESS BY ORPHANED AND LOCAL USERS ARE AN ISSUE

In Ordr deployments, we found that 55% of deployments had devices with “orphaned users”, and 20% of deployments had devices with local users.

Orphan accounts retain the same access rights as when they were associated with an active user. Therefore, in the event of a security incident, orphans represent an opportunity for privilege escalation and lateral movement as they still retain access to systems, resources and data within the organizations.

HOW ARE ORPHANS CREATED?

- When an employee switches their role, gets promoted, or exits an organization, they leave behind an inactive user account. Unless an organization puts a deprovisioning process in place, this account will still retain access to all the resources the employee could previously access.
- Leaving Orphans active can lead to compliance risks, network pollution, and security risks.

HOW ARE LOCAL USERS CREATED?

In certain verticals, multiple users access a common device and often create “local users” with a common user name and password to expedite access. For example, we see local users being created on radiology devices in healthcare organizations because busy doctors and nurse get tired of logging in and out. Unfortunately, this introduces cybersecurity and physical security issues.

5 Steps To Zero Trust for Connected Devices

In last year's Rise of the Machines, we provided recommendations for securing connected devices. It's worth to revisit this in the context of Zero Trust since it is an architectural framework referenced in the Executive Order.

Zero Trust for Devices

To fully adopt a ZTX framework, security pros must be able to monitor, isolate, secure, control, and remove every device that is connected to the network at any given moment.

"A Practical Guide To A Zero Trust Implementation Roadmap: The Zero Trust Security Playbook"
by Steve Turner, David Holmes, Chase Cunningham, Jinan Budge, Paul McKay, Andras Cser, Heidi Shey, and Merritt Maxim

STEP 1: IDENTIFY THE PROTECT SURFACE

It is vital to gain visibility into every connected device and risks on your network. This includes IT, IoT, IoMT or OT devices. It 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 for example, make, model, operating system, location, applications and more.

Are there mission-critical devices? Are there vulnerable devices? Understand the risk profile for these devices, from manufacturing recalls, medical device advisories and vulnerabilities to devices that are running outdated device operating systems.

STEP 2: MAP TRANSACTION FLOWS

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 such as a rogue or infected device communicating to a bad domain. This can be accomplished using AI and machine learning, as devices have very deterministic communications patterns based on their functions.

5 Steps To Zero Trust for Connected Devices

STEP 3: ARCHITECT THE ZERO TRUST NETWORK

With all devices accounted for, identified and categorized, and their risks understood, IT and security teams can architect the appropriate Zero Trust network based on the appropriate level of trust and least privilege access. The concept of "trust" for connected devices should be determined based on the following attributes:

WHO ARE YOU?

- User/Machine/App identity
- Authentication type (certificate, username/password, MFA, OTP)
- Group membership

WHAT ARE YOU?

- Device type
- HW/SW, OS/firmware
- Managed/Unmanaged asset
- Asset value/criticality

WHERE ARE YOU CONNECTING FROM?

- Local, Remote internal network
- External network w/wo VPN
- Gelocationasset

ARE YOU BEHAVING AS EXPECTED?

- Is behavior normal/anomalous?
- Spoofed/compromised
- Comparison to peers or past trends

COMPLIANCE/RISK STATUS?

- Patched, AV/FW current and active
- Risk score and posture status
- Vulnerability or IoC detected

STEP 4: CREATE THE ZERO TRUST POLICIES

Once you architect the Zero Trust network, you will need to create policies. You should be modeling flexible policies based on business context and the concept of trust as determined above. Both macro and flow-based micro-segmentation policies are critical to enable Zero Trust, and these policies can be both proactive and reactive:

- **Macro/Top-down policies:**
  - Restrict all managed workstations from guest network.
  - Block RDP, VNC, and SMB for all IIoT/IoMT running Windows XP/7.
  - Prevent consumer IoT from accessing corporate network.

5 Steps To Zero Trust for Connected Devices

- **Micro/Bottom down policies:**
  - All security cameras used to monitor parking spaces can only talk to specific video recorders and management stations
  - All Infusion Pumps at Hospital A used in Clinical Practice can only talk to their medical servers...and nothing else.
  - All PLCs as a specific manufacturing plant can only talk locally or to designated MRP/jump servers for vendor maintenance...and nothing else.
- **Hybrid:**
  - Monitor all communications from any device in VIP patient room within a hospital for baseline violations.
  - Monitor and segment mini-cluster "cells" of IT, IoT and Operational Technology devices for a specific function within manufacturing.

Depending on where the devices are located, and the types of communications flows, these policies that can be enforced at the access, network edge and data center and enforced across multiple points (switches, wireless, firewalls, NAC, data center solutions).

STEP 5: MONITOR AND MAINTAIN THE NETWORK

As new devices are discovered and come onto the network, policies should be automatically extended to them. Device details, along with risks and threat insights should be shared with other security solutions for enrichment. Updated threat intelligence and network data should be incorporated to monitor the network for anomalous behavior and threats such as lateral movement.

About Ordr

As organizations embrace digital transformation, billions of devices are being connected to enterprise networks to facilitate operations, improve safety and enhance operations. The promise of digital transformation can only be realized with the visibility and security of these devices – enterprise IT, IoT, medical/IoMT and OT.

The Ordr platform was designed for this.

Ordr Systems Control Engine (SCE) delivers visibility and security for every connected device. Our solution is agentless and SaaS-based. There is no impact to any device that we discover and secure. Within a few hours of deployment, our platform discovers every connected device, profiles behavior and risks, and automates action:

- **CONTINUOUS VISIBILITY** – Rapid AI-powered discovery and classification of devices includes not just what the devices are at a granular level, but also what risks they bring (vulnerabilities, recalls, weak passwords/certificates and more). We also deliver the complete mapping of communications for every device.

- **INTELLIGENT INSIGHTS** – Within the Ordr Nucleus, our Data Lake, we enrich device insights with external threat intelligence and network data to build the richest profiles for every connected device. In addition, our integrated Threat Detection Engine and Machine Learning models deliver insights into known and unknown threats, including anomalous communications that may indicate lateral movement or communications to a C2 domain.

- **AUTOMATED ACTION** – With hundreds of thousands of devices in your network, automation is critical. Ordr enables true mitigation and prevention policies across campus, DC and edge infrastructure. Once Ordr detects an exploit or a device behaving in a suspicious manner, we create policies to automatically contain threats through NGFW policies, ACL blocks, quarantine VLAN assignment, port shutdown, or session termination--either directly to existing firewalls, switches, wireless controllers, or via NAC platforms. These policies are all automatically generated by Ordr, and can also be enforced on existing security and networking infrastructure.

We've helped hundreds of organizations on their cybersecurity journey, and we are eager to partner with you on yours. Ordr is backed by top investors including Battery Ventures, Wing, and TenEleven Ventures. Reach out to us at **www.ordr.net** today