Asset Discovery Made Simple Using Ordr

Asset Inventory And Unparalled Visibility Into Devices And Their Behaviors

You can't protect what you can't see.

Gaining visibility over an organization's many devices is one of the most fundamentally important yet challenging tasks facing IT and security teams today. Without an accurate and up-to-date asset inventory, managing cybersecurity risks can be complicated. Yet, many IT and security teams struggle to answer the fundamental question of what devices are in their network.

This is because the number of connected endpoints has exploded both in terms of overall volume as well as diversity. In addition to traditional managed devices, IT teams must also corral a massive proliferation of unmanaged devices including IoT and OT, IoMT (Internet of Medical Technology), and employee BYOD (Bring Your Own Device). Further, these devices are constantly changing, with new devices being added or taken offline, and new ones being onboarded by different stakeholders within the organization.

There are specific questions to consider in an asset discovery solution:

- How complex is the process to discover all connected devices?
- Will your asset discovery solution accidentally disrupt the operations of sensitive devices?
- Can the solution answer the question of "what devices are connected" at a granular level?
- Can the solution answer the question of what exactly the devices are doing?
- Does it provide real-time and not a point-in-time approach to visibility?
- Does it continuously observe and monitor for anomalous and malicious behavior?
- Does it integrate with existing CMDB, CMMS or ITSM solutions?

Introducing Ordr Systems Control Engine (SCE)

This is where Ordr excels.

Ordr offers a unique differentiated platform for asset discovery. Using passive, agentless discovery, Ordr can automatically find and classify all connected devices whether managed or unmanaged. Each device is classified in granular detail including the make, operating system, serial number, application/port usage, location, and much more. This information can be shared with IT Services Management (ITSM), Configuration Management Database (CMDB) or Computerized Maintenance Management System (CMMS) as the single source of truth for all connected devices.

In addition to discovering and classifying devices, Ordr uses machine learning to profile and baseline device behavior. Ordr Flow Genome shows what systems devices are communicating with. These details can also be mapped via the Ordr Constellation Map for visual understanding of devices within network topologies such as VLANS and subnets.

With these insights, organizations not only have complete visibility into devices and what they are doing, but can also address critical security use cases:

- ✓ Identify devices running obsolete operating systems such as Windows 7
- ✓ Identify devices that are banned by the government
- ✓ Monitor devices with external Internet communications
- ✓ Monitor devices that are subject to compliance such as credit card readers, smart TVs and smart assistants
- ✓ Identify if high-value assets are in the wrong VLAN or in the same subnet as other vulnerable devices

Why Ordr is Asset Discovery Made Simple

There are a number of reasons why Ordr is a superior asset discovery solution:

1. Agentless and Passive Scanning

Some IoT and unmanaged devices like medical devices or industrial control systems (ICS) can be sensitive to active scans. Ordr employs various agentless and passive methods of data collection to identify and profile connected devices. There is no impact to any device or its operations in the network.

In addition, Ordr can also enrich insights from passive discovery with information from network infrastructure such as SNMP, IPAM, CMMS, Cisco Meraki etc. With proper deployment, Ordr can passively obtain a treasure trove of information to provide an accurate inventory of every device connected to the network.

2. Unified Visibility and Classification of Connected Devices

Much like a chess player needs to be able to see all the pieces on the board, IT and Security teams need to see all the devices on their network. Unfortunately, today that view is highly fractured with critical parts of the metaphorical chess board often being completely invisible.

Ordr brings all of an organization’s many connected devices into a single unified context, including managed and unmanaged devices. In one view, staff can see traditional managed devices like laptops and servers as well as unmanaged devices of all types, IoT, OT assets, medical devices, mobile and personal devices, and more. Visibility into this latter category of unmanaged devices is particularly important as it is the area of the greatest growth in most organizations.

Ordr also automatically classifies each device in granular detail. By combining Advanced Machine Learning with DPI (Deep Packet Inspection), Ordr passively reveals a wealth of critical context for every device. This includes:

Device Type and Function

Instead of merely seeing an IP address, teams can quickly distinguish between laptops, security cameras, HVAC systems, Building Automation Systems, or an infusion pump

Device Details

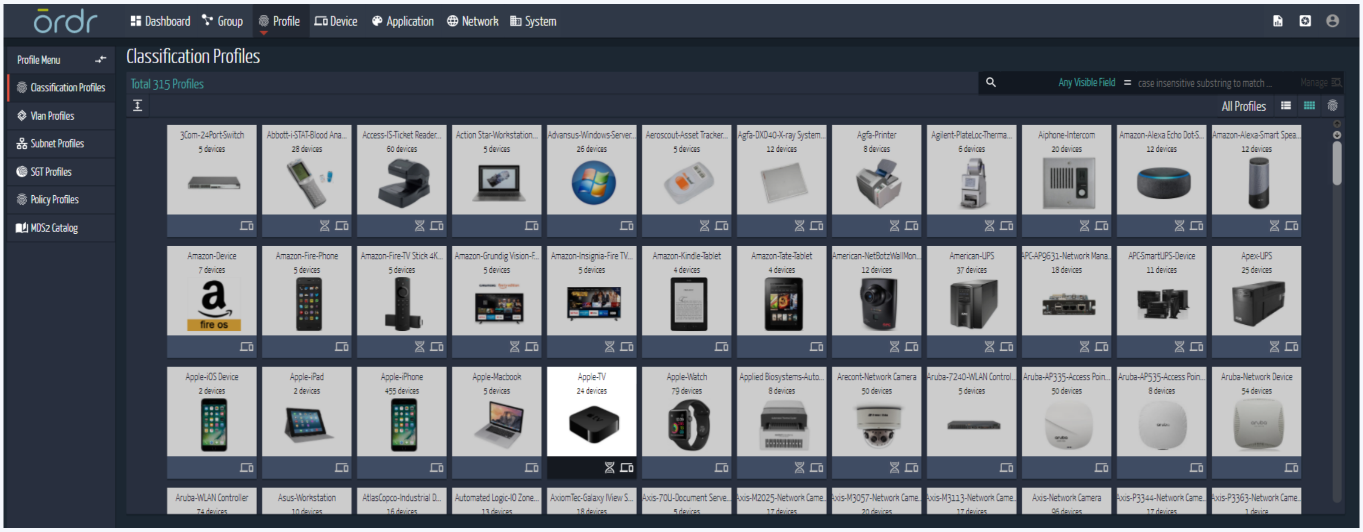
Find critical information on each device including the specific device make, model, serial number, OS version, and more

Network Context

See device network properties such as MAC/IP address, subnet, interface, VLAN, SSID, CDP/LLDP data, and other statistics

Location

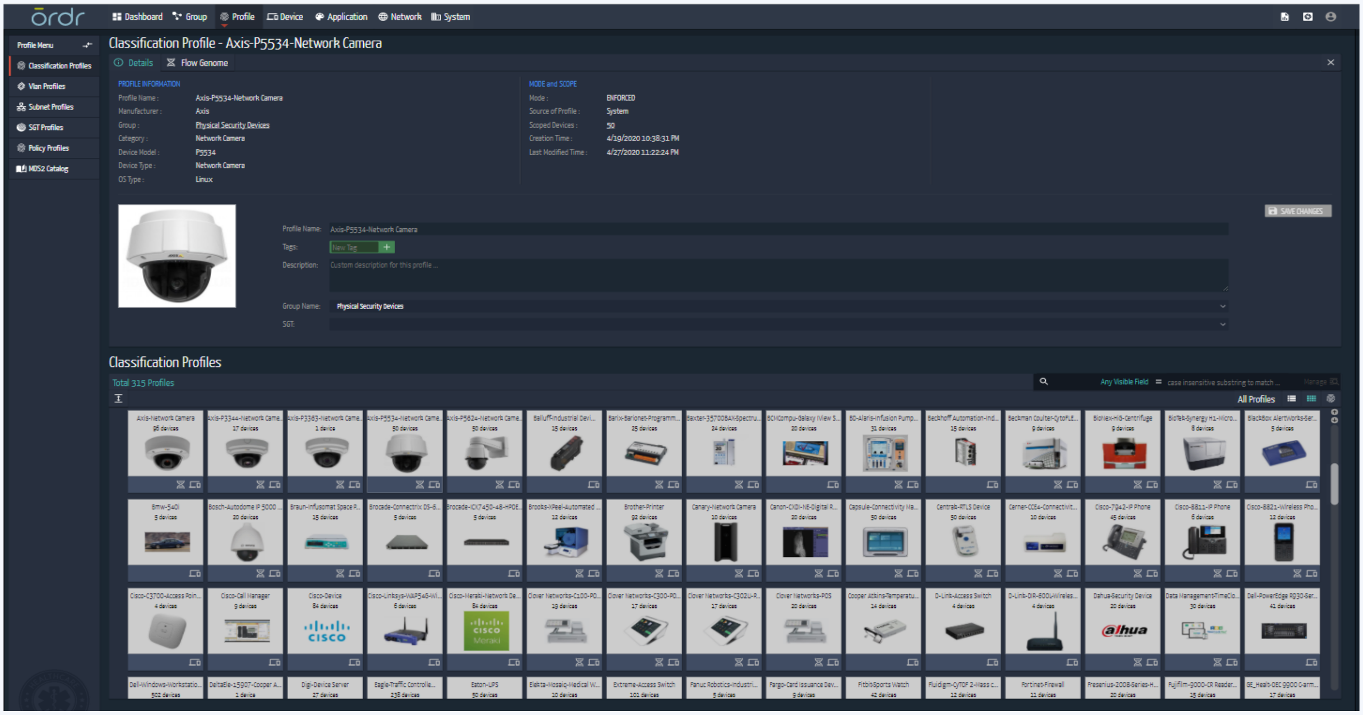
Devices can be identified in terms of their location in the organization



Classification Profiles

Total 315 Profiles

3Com-24Port-Switch 5 devices	Abbott-i-STAT-Blood Ana... 28 devices	Access-IS-Ticket Reader... 60 devices	Action Star-Workstation... 5 devices	Advansus-Windows-Server... 26 devices	Aeroscout-Asset Tracker... 5 devices	Agfa-DXD40-X-ray System... 12 devices	Agfa-Printer 8 devices	Agilent-PlateLoc-Therma... 6 devices	Aiphone-Intercom 20 devices	Amazon-Alexa Echo Dot-S... 12 devices	Amazon-Alexa-Smart Spea... 12 devices
Amazon-Device 7 devices	Amazon-Fire-Phone 5 devices	Amazon-Fire-TV Stick 4K... 5 devices	Amazon-Grundig Vision-F... 5 devices	Amazon-Insignia-Fire TV... 5 devices	Amazon-Kindle-Tablet 4 devices	Amazon-Tate-Tablet 4 devices	American-NetBotzWallMon... 12 devices	American-UPS 37 devices	APC-AP9631-Network Mana... 18 devices	APCSmartUPS-Device 11 devices	Apex-UPS 25 devices
Apple-iOS Device 2 devices	Apple-iPad 2 devices	Apple-iPhone 455 devices	Apple-Macbook 5 devices	Apple-TV 24 devices	Apple-Watch 79 devices	Applied Biosystems-Auto... 8 devices	Arecont-Network Camera 50 devices	Aruba-7240-WLAN Control... 5 devices	Aruba-AP335-Access Poin... 50 devices	Aruba-AP535-Access Poin... 8 devices	Aruba-Network Device 54 devices
Aruba-WLAN Controller 74 devices	Asus-Workstation 10 devices	AtlasCopco-Industrial D... 16 devices	Automated Logic-IO Zone... 13 devices	AxiomTec-Galaxy iView S... 18 devices	Axis-70U-Document Serve... 5 devices	Axis-M2025-Network Came... 17 devices	Axis-M3057-Network Came... 20 devices	Axis-M3113-Network Came... 17 devices	Axis-Network Camera 96 devices	Axis-P3344-Network Came... 17 devices	Axis-P3363-Network Came... 1 device



Classification Profile - Axis-P5534-Network Camera

PROFILE INFORMATION

Profile Name : Axis-P5534-Network Camera
Manufacturer : Axis
Group : Physical Security Devices
Category : Network Camera
Device Model : P5534
Device Type : Network Camera
OS Type : Linux

MODE and SCOPE

Mode : ENFORCED
Source of Profile : System
Scoped Devices : 50
Creation Time : 4/19/2020 10:38:31 PM
Last Modified Time : 4/27/2020 11:22:24 PM

Profile Name: Axis-P5534-Network Camera
Tags: New Tag
Description: Custom description for this profile ...
Group Name: Physical Security Devices
SGT:

Classification Profiles

Total 315 Profiles

Any Visible Field = case insensitive substring to match ... Manage

Axis-Network Camera 96 devices	Axis-P3344-Network Came... 17 devices	Axis-P3363-Network Came... 1 device	Axis-P5534-Network Came... 50 devices	Axis-P5624-Network Came... 50 devices	Balluff-Industrial Devi... 15 devices	Barix-Barionet-Programm... 25 devices	Baxter-35700BAX-Spectru... 24 devices	BCMCompu-Galaxy IView S... 20 devices	BD-Alaris-Infusion Pump... 31 devices	Beckhoff Automation-Ind... 15 devices	Beckman Coulter-CytoFLE... 9 devices	BioNex-HiG-Centrifuge 9 devices	BioTek-Synergy H1-Micro... 8 devices	BlackBox AlertWorks-Ser... 5 devices
Bmw-540i 5 devices	Bosch-Autodome IP 5000 ... 20 devices	Braun-Infusomat Space P... 15 devices	Brocade-Connectrix DS-6... 5 devices	Brocade-ICX7450-48-HPOE... 5 devices	Brooks-XPeel-Automated ... 12 devices	Brother-Printer 92 devices	Canary-Network Camera 10 devices	Canon-CXDI-NE-Digital R... 20 devices	Capsule-Connectivity Ma... 50 devices	Centrak-RTLS Device 50 devices	Cerner-CCE4-Connectivit... 10 devices	Cisco-7942-IP Phone 45 devices	Cisco-8811-IP Phone 6 devices	Cisco-8821-Wireless Pho... 12 devices
Cisco-C3700-Access Poin... 4 devices	Cisco-Call Manager 9 devices	Cisco-Device 84 devices	Cisco-Linksys-WAP54G-Wi... 6 devices	Cisco-Meraki-Network De... 84 devices	Clover Networks-C100-PO... 19 devices	Clover Networks-C300-PO... 17 devices	Clover Networks-C302U-P... 17 devices	Clover Networks-POS 20 devices	Cooper Atkins-Temperatu... 14 devices	D-Link-Access Switch 4 devices	D-Link-DIR-600L-Wireles... 4 devices	Dahua-Security Device 20 devices	Data Management-TimeClo... 30 devices	Dell-PowerEdge R930-Ser... 41 devices
Dell-Windows-Workstatio... 502 devices	DeltaEle-15907-Cooper A... 1 device	Digi-Device Server 27 devices	Eagle-Traffic Controlle... 238 devices	Eaton-UPS 50 devices	Elekta-Mosaiq-Medical W... 10 devices	Extreme-Access Switch 101 devices	Fanuc Robotics-Industri... 5 devices	Fargo-Card Issuance Dev... 9 devices	Fitbit-Sports Watch 42 devices	Fluidigm-CyTOF 2-Mass c... 12 devices	Fortinet-Firewall 11 devices	Fresenius-2008-Series-H... 20 devices	Fujifilm-9000-CR Reader... 15 devices	GE_Healt-OEC 9900 C-arm... 17 devices

3. Always-On, Continuous, Real-Time Asset Inventory

For many organizations, inventory management is performed as a periodic point in time audit. This can lead to considerable gaps in visibility when devices are missed or offline during an audit or if there are significant changes between scans. These gaps can mean organizations are often exposed for weeks or even months before the problem is identified.

Ordr ensures that asset inventory and management is a continuous process so that information is always up-to-date. Since all traffic is continuously analyzed, Ordr detects new devices and can inform security and IT teams, or device owners as soon as the device first connects. This real-time visibility allows staff to see a variety of devices that would typically be missed and left unmanaged including:

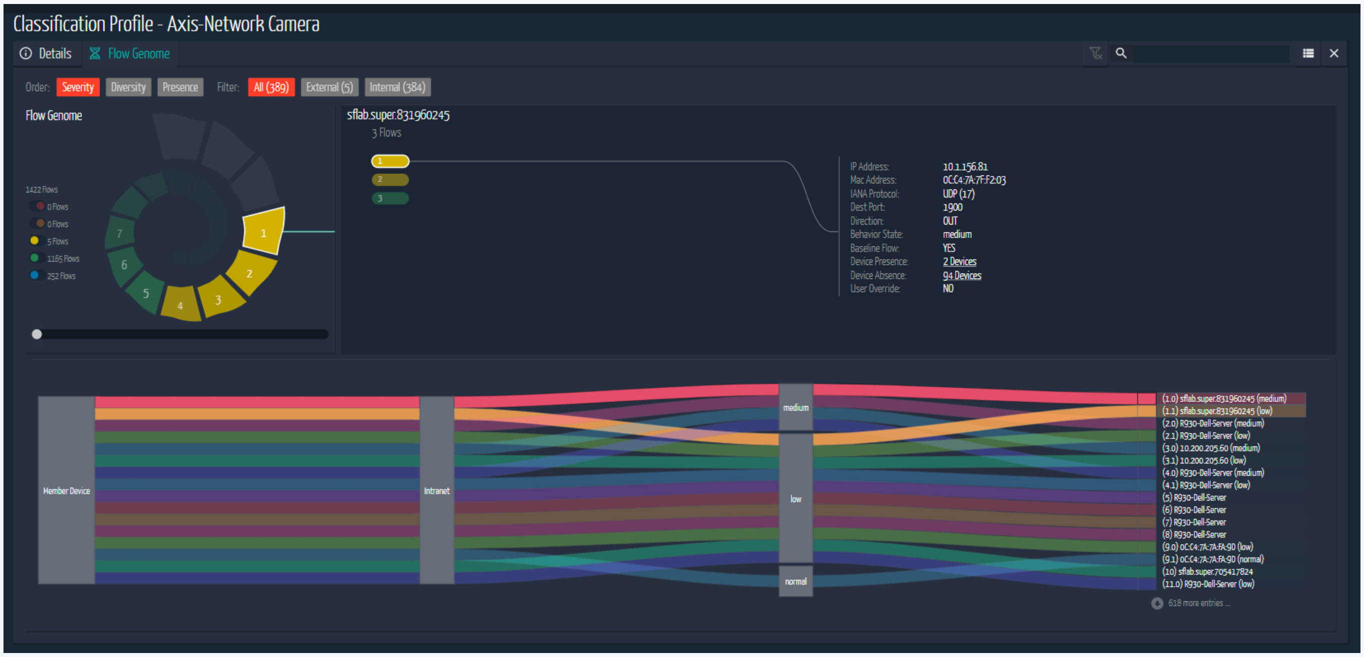
- ✓ Employee laptops and mobile devices that are often out of the office
- ✓ Devices owned by visiting partners or contractors
- ✓ Devices that were temporarily offline
- ✓ New employees or newly deployed devices
- ✓ Changes in device configuration or security posture between regularly scheduled scans

4. Monitoring Device Behavior

The Ordr Systems Control Engine monitors device behavior using machine learning and creates a conversation map, called a Flow Genome, of the communications pattern of every connected device. Ordr Flow Genome also learns the network topology — the VLANs, subnets, routing, and the access-layer connectivity graph of what is connected to each switch port and wireless AP. Security and networking teams can analyze this information and analyze communication mappings based on individual devices, groups of like devices, groups of devices based on business function, and even overlays based on the network topology. This can also be viewed via a constellation map featuring network topology details.

Ordr's device behavior monitoring can help organizations with the following:

- ✓ Audit the communications of every device and see every other system it communicates to including IP address, web site/URL, and application protocols used
- ✓ View the communication patterns for all devices of the same type, such as Axis surveillance cameras, Rockwell PLCs, and Phillips patient monitoring systems to identify outliers
- ✓ Spot devices that communicate outside the organization, including traffic to “known bad sites” such as phishing, malware, and crypto-mining systems
- ✓ Reveal communication patterns of devices based on their business purpose, such medical devices, manufacturing line equipment, and retail systems



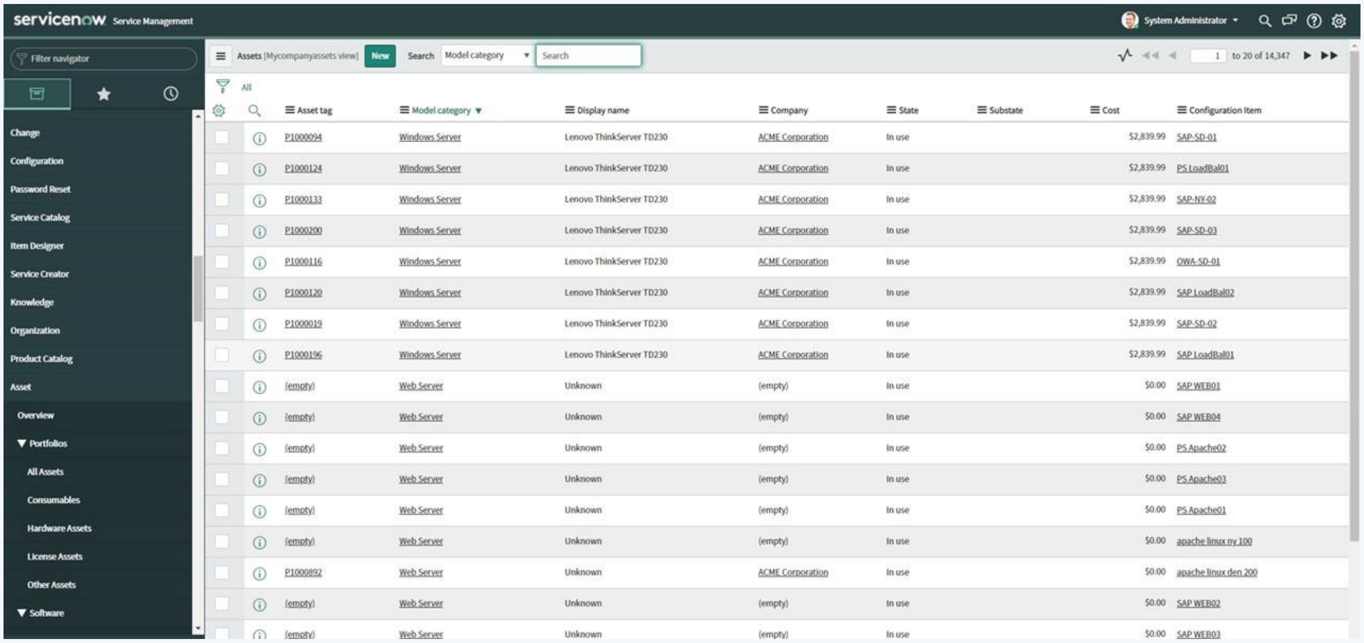
Classification Profile - Axis-Network Camera

IP Address: 10.1.156.81
Mac Address: 0C:C4:7A:7F:F2:03
IANA Protocol: UDP (17)
Dest Port: 1900
Direction: OUT
Behavior State: medium
Baseline Flow: YES
Device Presence: 2 Devices
Device Absence: 94 Devices
User Override: NO

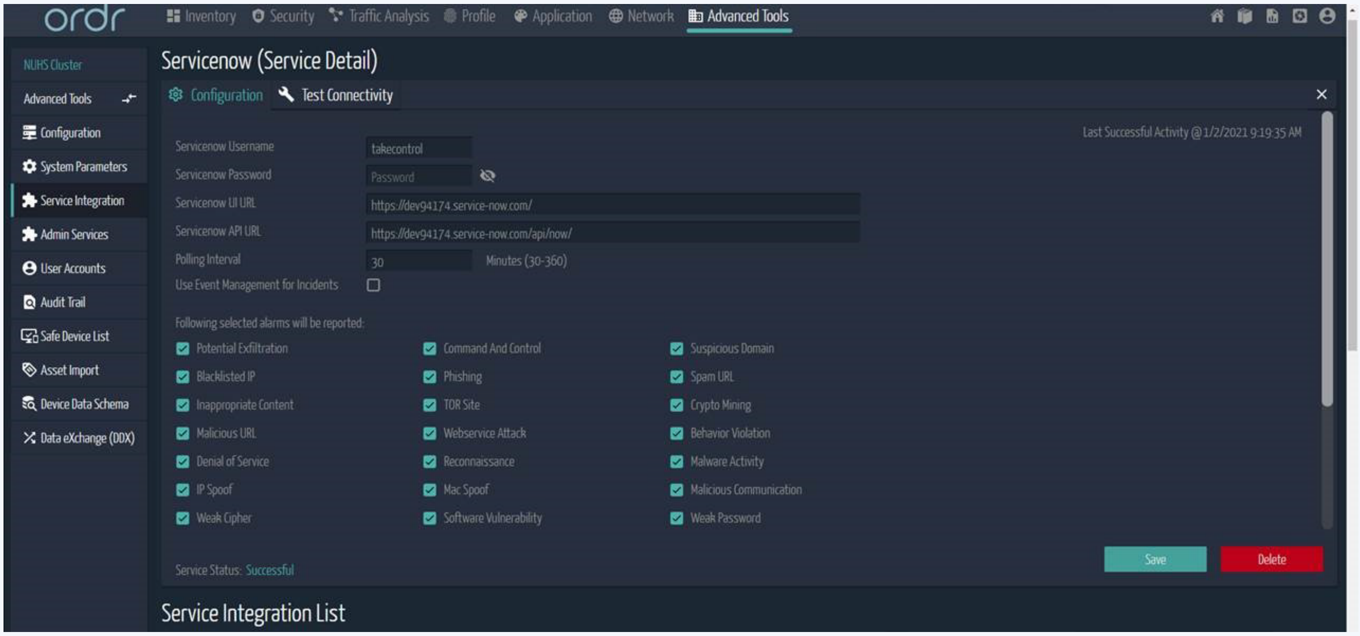
(1.0) sflab.super.831960245 (medium)
(1.1) sflab.super.831960245 (low)
(2.0) R930-Dell-Server (medium)
(2.1) R930-Dell-Server (low)
(3.0) 10.200.205.60 (medium)
(3.1) 10.200.205.60 (low)
(4.0) R930-Dell-Server (medium)
(4.1) R930-Dell-Server (low)
(5) R930-Dell-Server
(6) R930-Dell-Server
(7) R930-Dell-Server
(8) R930-Dell-Server
(9.0) 0C:C4:7A:7A:FA:9D (low)
(9.1) 0C:C4:7A:7A:FA:9D (normal)
(10) sflab.super.705417824
(11.0) R930-Dell-Server (low)
618 more entries ...

5. Integration with ITSM, CMDB and CMMS

Having an asset inventory that is reliable and real-time is critical for security teams. But it can be challenging for traditional asset management solutions typically owned by IT to keep up with assets and devices outside their domain. Ordr integrates with ITSM, CMMS and CMDB solutions to enrich them with connected device insights. As shown in the diagram below, when integrated with ServiceNow CMDB, Ordr ensures that the latest granular insights on devices and their behavior is shared with ServiceNow.



Asset tag	Model category ▼	Display name	Company	State	Substate	Cost	Configuration Item
P1000094	Windows Server	Lenovo ThinkServer TD230	ACME Corporation	In use		$2,839.99	SAP-SD-01
P1000124	Windows Server	Lenovo ThinkServer TD230	ACME Corporation	In use		$2,839.99	PS LoadBal01
P1000133	Windows Server	Lenovo ThinkServer TD230	ACME Corporation	In use		$2,839.99	SAP-NY-02
P1000200	Windows Server	Lenovo ThinkServer TD230	ACME Corporation	In use		$2,839.99	SAP-SD-03
P1000116	Windows Server	Lenovo ThinkServer TD230	ACME Corporation	In use		$2,839.99	OWA-SD-01
P1000120	Windows Server	Lenovo ThinkServer TD230	ACME Corporation	In use		$2,839.99	SAP LoadBal02
P1000019	Windows Server	Lenovo ThinkServer TD230	ACME Corporation	In use		$2,839.99	SAP-SD-02
P1000196	Windows Server	Lenovo ThinkServer TD230	ACME Corporation	In use		$2,839.99	SAP LoadBal01
(empty)	Web Server	Unknown	(empty)	In use		$0.00	SAP WEB01
(empty)	Web Server	Unknown	(empty)	In use		$0.00	SAP WEB04
(empty)	Web Server	Unknown	(empty)	In use		$0.00	PS Apache02
(empty)	Web Server	Unknown	(empty)	In use		$0.00	PS Apache03
(empty)	Web Server	Unknown	(empty)	In use		$0.00	PS Apache01
(empty)	Web Server	Unknown	(empty)	In use		$0.00	apache linux ny 100
P1000892	Web Server	Unknown	ACME Corporation	In use		$0.00	apache linux den 200
(empty)	Web Server	Unknown	(empty)	In use		$0.00	SAP WEB02
(empty)	Web Server	Unknown	(empty)	In use		$0.00	SAP WEB03



Servicenow (Service Detail)

Last Successful Activity @ 1/2/2021 9:19:35 AM

Servicenow Username: takecontrol
Servicenow Password: Password
Servicenow UI URL: https://dev94174.service-now.com/
Servicenow API URL: https://dev94174.service-now.com/api/now/
Polling Interval: 30 Minutes (30-360)
Use Event Management for Incidents ☐

Following selected alarms will be reported:

☑ Potential Exfiltration
☑ Blacklisted IP
☑ Inappropriate Content
☑ Malicious URL
☑ Denial of Service
☑ IP Spoof
☑ Weak Cipher
☑ Command And Control
☑ Phishing
☑ TOR Site
☑ Webservice Attack
☑ Reconnaissance
☑ Mac Spoof
☑ Software Vulnerability
☑ Suspicious Domain
☑ Spam URL
☑ Crypto Mining
☑ Behavior Violation
☑ Malware Activity
☑ Malicious Communication
☑ Weak Password

Service Status: Successful

Service Integration List

Conclusion

There are many ways that organizations will benefit from having a complete asset inventory of their connected devices. Using Ordr, security teams will benefit from a unified view of all managed, unmanaged and IoT, IoMT or OT devices. Just as importantly, by monitoring the behavior of each device, organizations can ensure each device is behaving appropriately based on its unique role in the enterprise. And by integrating with an organization’s ITSM, CMMS or CMDB solutions, Ordr can help organizations get more value out of the solutions they have already invested in.