



Ordr and Cisco: Rich IoT Visibility, Simplified Segmentation

The Cisco Identity Services Engine (ISE) and Cisco Software-Defined Access (SDA) solution includes a rich set of services to authenticate users and devices, classify user devices and common IoT endpoints such as printers, cameras, phones, and network equipment, as well as validate endpoint compliance of desktop PCs and mobile devices. However, additional tooling is needed to provide granular classification and compliance validation of IoT devices which comprise a significant portion of networked endpoints.

The Ordr Systems Control Engine (SCE) compliments Cisco ISE and SDA by providing agentless, passive data collection to automate discovery and classification for all IoT and non-IoT devices. It then feeds the rich contextual data including make, model, serial number and software versions to Cisco ISE. While monitoring all devices for known threats and vulnerabilities, the SCE is also keeping close watch on communication flows and anomalous traffic. Here the Ordr SCE can notify Cisco ISE of at-risk, vulnerable, and compromised devices to trigger the necessary quarantine and remediation response.

Providing advanced IoT device information to ISE is only one piece of the puzzle. While Cisco ISE and SDA provide powerful tools to enforce Zero Trust and microsegmentation policy, additional intelligence is needed to understand what comprises that policy. For example, "Which endpoints should be in the same group or segment?", or "What are the minimal communication permissible between endpoints in the same or different groups or segments?" To move to microsegmentation and the enforcement of policies, ISE administrators must understand which traffic to allow and deny. Ordr's Analytics Server provides this insight to Cisco ISE and SDA to automate the provisioning of group and segmentation policy.

Cisco ISE and SDA Services

In an effort to secure confidential data and protect vulnerable systems from compromise or service disruption, customers are rapidly embracing new security models including Zero Trust and microsegmentation. To execute these goals, many customers have deployed Cisco ISE and SDA for industry-leading identity-based policy access control and segmentation services for network endpoints.

Often the first task in securing network resources is detecting and identifying all devices and users that connect to the network and applying appropriate access and segmentation policy based on the device type or user identity. Many factors, also known as context, can impact policy decisions regarding appropriate access. This context may include group affiliations (for example, is a user an employee, partner or guest?), whether a device is a managed asset or under supervisory control, the role of the device/user in the network, and the compliance, vulnerability, or threat status of the device.

The Cisco ISE and SDA solution provides a number of benefits in delivering identity and context-based access control:

- Comprehensive detection and tracking of all network-connected devices
- Strong machine and user authentication for employees, partners and guests via RADIUS using 802.1X and Web-based Authentication across wired, wireless, and VPN
- Integration with popular identity stores including AD, LDAP, SQL, OAUTH, and PKI (certificates)
- Broad device classification (profiling) to compliment authentication services, especially when used with MAC-based authentication—a method heavily leveraged for IoT devices
- User device onboarding services, also known as BYOD
- Compliance validation and remediation via agent-based posture and Mobile Device Management (MDM) services
- Threat-Centric NAC - The ability to influence access policy based on vulnerability and threat data learned from external systems
- Strong enforcement controls including ACL and VLAN methods
- Software-Defined Access (SDA) powered by virtual network segmentation and group-based microsegmentation
- Integration with Cisco and external parties through APIs and Platform Exchange Grid (pxGrid)

The IoT NAC Challenge

A major challenge in securing network access today is the meteoric rise in the number of Internet of Things (IoT) devices on the network. IoT spans a wide range of devices including media/entertainment, building automation, manufacturing control, healthcare services, financial transactions, office equipment, power generation, and location/tracking. Virtually any device including a coffee maker or refrigerator can be connected to the network to offer unprecedented automation, management, monitoring, and data sharing.

IoT devices present unique challenges to network access control. Most are useless (no user associated with the device) and offer no means to authenticate themselves to the network. Very few support network authentication using common protocols such as 802.1X. For the small subset of IoT devices that do support 802.1X, many customers find the implementation cost prohibitive. Consequently, IoT devices are most commonly granted access using MAC Authentication Bypass (MAB). As the name suggests, the device bypasses explicit network authentication and the MAC address serves as the basis of identity. While not ideal, the alternative of “no authentication” leaves network ports open to attack.

In order to reduce costs and simplify network connectivity, IoT devices often run rudimentary or minimized versions of legacy operating systems. Most are closed systems with minimal or no patching capabilities to defend themselves. The installation of posture or other device management agents is rarely an option. Direct scanning or interrogation by profiling and security assessment tools are often restricted due to the fragile nature of the device’s operating system or networking stack. This leaves critical devices vulnerable to service disruption, data theft, or compromise to serve as a launchpad for other attacks.

Accurate device classification also presents a challenge since common profiling methods offer little or no indication of an IoT device’s actual type, functional role, or other details that permit policy assignment.

Advanced Device Classification and Context Sharing

Cisco ISE Profiler automates the classification of user devices such as workstations (Windows, Mac OS, Linux, etc.), mobile devices (Android, iOS, Chrome, Blackberry, etc.) as well as non-user devices including IP phones, cameras, printers, and networking equipment. Typical methods used to classify endpoints are limited to network telemetry such as MAC address, DHCP option data, SNMP MIB data from the access device (for example, CDP/LLDP table data), and the interception of browser user agents. However, many IoT devices are statically addressed (no DHCP data), present no CDP/LLDP information, do not have a web browser, and may even experience service disruption if scanned or interrogated! MAC address and its corresponding OUI data are frequently the sole attributes available to make a classification decision.

MEDICAL IoT CLASSIFICATION EXAMPLE

Device Type: X-Ray Angiography
Manufacturer: Siemens
Model: AXIOM-Artis
OS Type: Windows XP 64bit
Software Version: VC21C 161026
MAC Address: 00:E0:81:B6:63:D3
MAC OUI: TYAN COMPUTER CORP.




In this example, Cisco ISE would detect the OUI of the network interface card (NIC) manufacturer, Tyan Computer Corp, which is very common and widely used across many different device types. Even if DHCP was employed, the operating system would be detected as Microsoft Windows. Random NMAP scanning would not be desired if system in active use.

Here, neither the knowledge of the NIC manufacturer nor OS kernel provides insight into the device type or its role on the network. Such a device would likely be authorized only after static whitelisting upon direct inspection or manual review of asset database records.

Using the Ordr SCE, you can quickly discover the true nature of the device along with a rich set of endpoint attributes and security metrics—all without the use of agents:

DEVICE INFORMATION FOR X-RAY ANGIOGRAPHY

DEVICE INFORMATION	CLASSIFICATION	CONNECTIVITY
Mac Address : 00:E0:81:B6:63:D3	Classification State : Classified	CPN Sensor : abc-cpnanalytics-en
Device Description : Xray Angiography	Classification Source : PROFILE_LIB	IP Address : Offline (last IP = 10.
Manufacturer : Siemens	Device Type : Xray Angiography	Subnet : 10.22.144.0/21
Model Name/No. : AXIOM-Artis	Group : Medical Devices	VLAN : Vlan(0028)
Serial No. : 153342	Profile : Siemens-AxiomArtis-Xray Angiography	Access Type : WIRED
OS Type : Windows XP 64bit	End Point Type : IoT Endpoint	Network Device : N/A
OS Version : 5.2	Criticality : LEVEL_3	Access Interface : GigabitEthernet1/0/
SW Version : VC21C 161026	Alarm Count : 427	First Seen : 4/11/2018 12:09:4
FQDN : xray-n13d.abchealthcare.com	Risk Score : 60	Last Seen : 6/18/2018 2:05:03
DHCP Hostname : N/A	Incident Score : 0	



Device Name: xray-n13d.abchealthcare.com

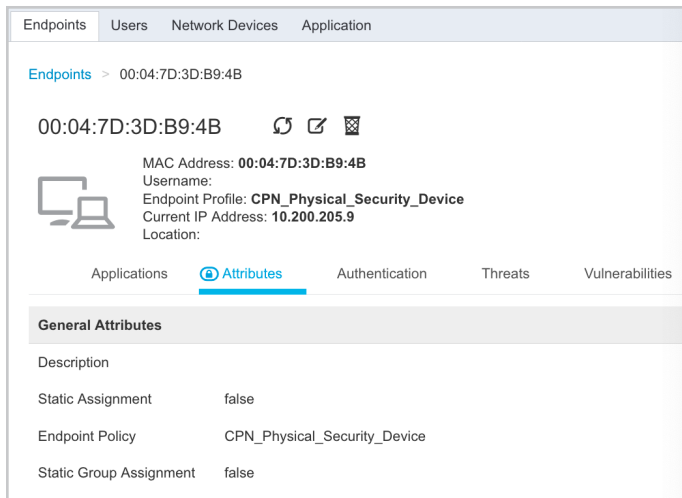
Tags: Untitled +

Description:

ProfileName: Siemens-AxiomArtis-Xray Angiography

Beyond detailed classification, the SCE dynamically groups devices by Device Type, Class of Device (Group), and Category. Additional details such as manufacturer, model/serial number, hardware/software versions, as well as flagging healthcare devices that contain protected health information (PHI) are collected. Devices behind IoT gateway devices or medical workstations are also detected and individually tracked. Through data exchange with existing IT Service Management (ITSM) and Configuration Management Databases (CMDBs), the Ordr SCE augments and reconciles asset records.

Detailed device attributes are automatically pushed to Cisco ISE over pxGrid. This extensive context sharing occurs for all connected devices including IoT (building automation, healthcare, manufacturing, office equipment, etc.) and non-IoT endpoints such as user workstations and mobile devices. The following sample depicts the type of useful attributes populated into ISE for a security camera device. SCE-derived attributes have the prefix "asset" and are highlighted below.



Endpoints > 00:04:7D:3D:B9:4B

00:04:7D:3D:B9:4B

MAC Address: 00:04:7D:3D:B9:4B
 Username:
 Endpoint Profile: CPN_Physical_Security_Device
 Current IP Address: 10.200.205.9
 Location:

Applications | **Attributes** | Authentication | Threats | Vulnerabilities

General Attributes

Description	
Static Assignment	false
Endpoint Policy	CPN_Physical_Security_Device
Static Group Assignment	false

Attribute Name	Attribute Value
assetProfile	Pelco-Sarix IME219-Network Camera
assetEndPointType	IOT_ENDPOINT
assetVlanId	205
assetSubnet	10.200.205.0/24
assetNetworkDevice	Switch
assetAccessInterface	GigabitEthernet1/0/22
assetCategory	Physical Security Devices
assetCriticality	LEVEL_3
assetClassificationState	Classified
assetDhcpHostname	IME219-AEFKQ75
assetDescription	Network Camera
assetRiskScore	80
assetIncidentScore	0
assetVlanName	VLAN0205
assetClassificationSource	PROFILE_LIB
assetAccessType	WIRED

Other Attributes

DeviceRegistrationStatus	NotRegistered
ElapsedDays	50
EndPointPolicy	CPN_Physical_Security_Device
EndPointProfilerServer	customerDemoISE.cpn.lan
EndPointSource	PXGRIDPROBE
IdentityGroup	Profiled
InactiveDays	0
LogicalProfile	Cameras
MACAddress	00:04:7D:3D:B9:4B
MatchedPolicy	CPN_Physical_Security_Device
OUI	Pelco
PolicyVersion	9
PostureApplicable	Yes
StaticAssignment	false
StaticGroupAssignment	false
Total Certainty Factor	100
assetConnectedLinks	[{"key":"assetId","value":"ef299c87-95f2-41c"}, {"key":"assetDeviceType","value":"WIRED"}]
assetDeviceType	Network Camera
assetId	00:04:7D:3D:B9:4B
assetIpAddress	10.200.205.9
assetMacAddress	00:04:7D:3D:B9:4B

All custom attributes learned from the Ordr SCE are accessible to ISE for creating new Profiler conditions. Customers can choose to use the new Profiler conditions to augment existing ISE Profiler Policies, or to create new Profiler Policies.

Threat-Centric NAC – ISE Policy Based on Security Compliance and Risk

Cisco ISE offers advanced posture assessment and remediation services for desktop devices using the AnyConnect Secure Mobility Client. Through integration with Mobile Device Management systems, posture assessment and remediation can be extended to mobile devices.

To compliment these endpoint security features targeted specifically at user devices, the Ordr SCE provides comprehensive security threat and vulnerability analysis for each IoT and non-IoT endpoint. This information is then dynamically updated to Cisco ISE to allow network access and segmentation policy decisions based on the compliance and risk of all connected devices, not just user devices.

Ordr SCE security monitoring is performed for all devices and includes:

- ICSA - ICS-CERT Advisories
- NVD - Data Feeds (CVE data)
- Password scanning and weak/open password detection
- FDA - Medical Device Recalls
- MDS2 - manufacturer-published vulnerability data
- Embedded IDS engine that utilizes feeds from different sources including Talos and Emerging Threats Intelligence
- URL/IP Reputation - IP reputation for command and control and other bad sites
- IP/Geo for fraud sites
- Built-in vulnerability assessment scanner; also detects open ports

The Ordr SCE examines every flow to/from the device for the presence of well-known malware signatures such as the use of the SMBv1 protocol to exploit inherent vulnerabilities in unpatched Windows XP machines. The SCE performs an IDS and URL reputation verification based on all the threat feeds listed above. The SCE can also integrate with Tenable and Rapid7 for more comprehensive vulnerability and threat analysis.

Results are sent to ISE over pxGrid. Attributes such as asset Criticality, Incident Score, Risk Score, Vulnerability, and Alarm Count allow ISE administrators to apply access policies that take into consideration the risk to other devices on the network or to the device itself. For example, highly critical devices known to have severe vulnerabilities may be assigned a more restrictive access policy or be subject to deeper inspections by the firewall or IPS system.

The diagram below is an example ISE Authorization Policy Rule which uses conditions based on the Ordr SCE security attributes and assigns matching devices to a Limited_Access policy with a High_Risk Scalable Group Tag (SGT).

ISE AUTHORIZATION POLICY EXAMPLE

▼ Authorization Policy (28)			
Status	Rule Name	Conditions	Results
			Profiles
✔	TC-NAC Policy	AND <ul style="list-style-type: none"> OR <ul style="list-style-type: none"> EndPoints-assetRiskScore GREATER 100 EndPoints-assetIncidentScore GREATER 3 EndPoints-assetAlarmCount GREATER 1000 EndPoints-assetVuln CONTAINS WannaCry EndPoints-assetCriticality EQUALS HIGH 	× Limited_Access + High_Risk × ▾ +

Anomaly Behavior Detection

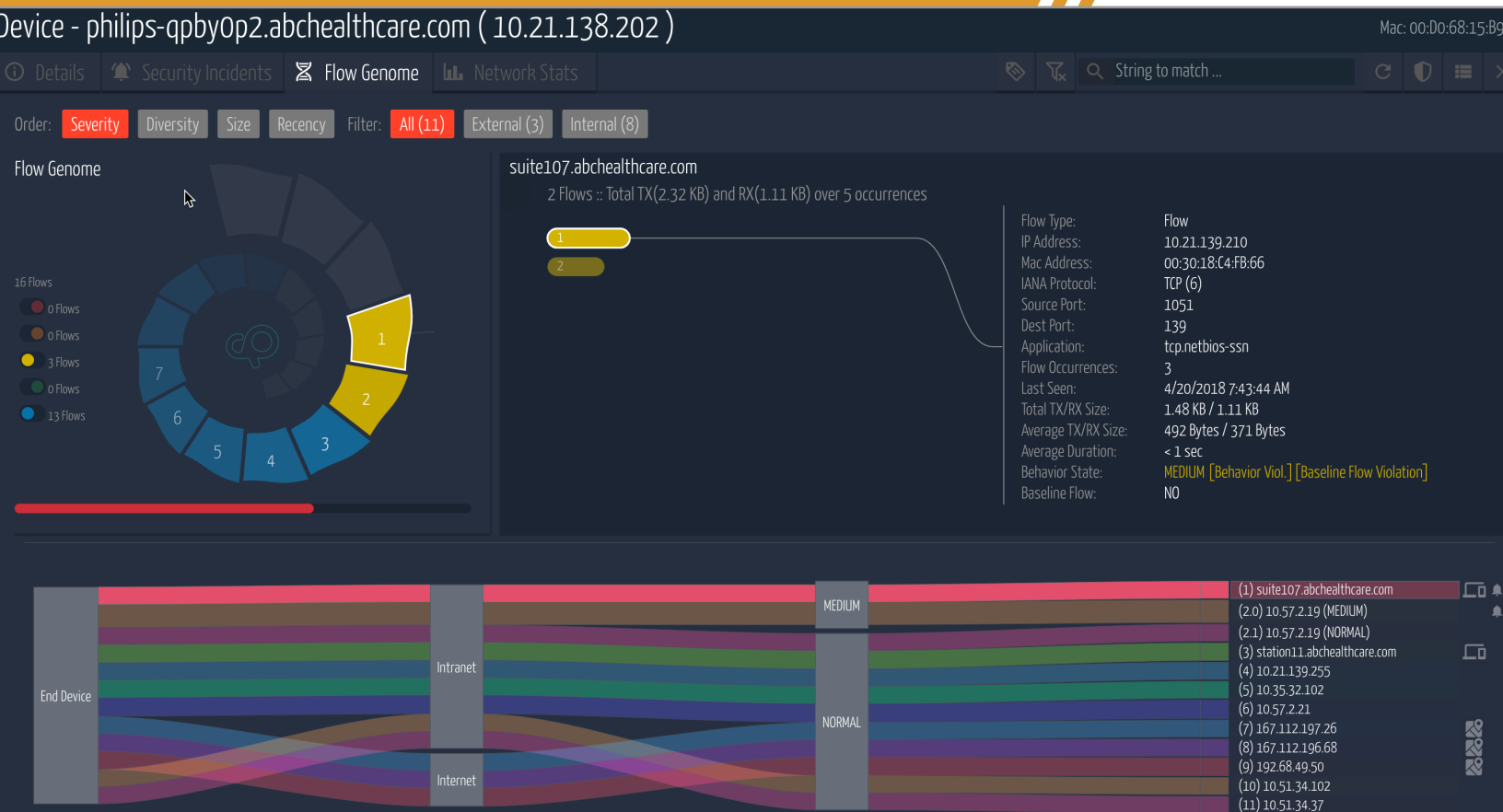
The reliance on MAC address alone to grant access to IoT and other non-authenticating devices increases the risk for unauthorized access through the exploitation of MAC address spoofing. While not formally positioned as an anti-MAC spoofing feature, Cisco ISE does offer basic anomaly behavior detection features based on changes in device profile or specific profiling attributes. However, these anomalies are often triggered by other endpoint attributes that can be easily forged such as DHCP.

The Ordr SCE significantly extends the ability to detect anomalous endpoints by monitoring actual device communication and traffic behavior, not just the endpoint attributes themselves. While endpoint telemetry including MAC address, DHCP options, CDP/LLDP agents, and SNMP values can all be spoofed and true values hidden from view, and endpoint's communications "fingerprint" cannot be hidden. The traffic to and from each endpoint can be made visible to the Ordr SCE so that attempts to spoof an endpoint's MAC address and engage in anomalous activity can be detected and contained.

The Flow Genome – Dynamic Baselining of Device Communications

The Ordr SCE observes all network traffic through a SPAN mirror, network tap, or flow export (NetFlow, IPFIX, or sFlow). Communication baselines are established for each device and each group of like devices by profile. This learned behavior – referred to as the Flow Genome – forms the basis of the Ordr SCE’s Anomaly Behavior Detection.

FLOW GENOME EXAMPLE



As depicted above, the Flow Genome is represented using both a helical graph (top left) as well as a Sanky diagram (bottom half). In the helical graph, each wedge or step represents a different communication peer. Clicking on a wedge reveals all flows with that peer including time, port, protocol, application, and session, packet and byte TX/RX counts. Flows are color coded to easily visualize security risk rating. The Sanky diagram is an alternate way to view the same information where each peer on the right side is flagged as Internal or External. Internal peers are cross-linked to the device details in the SCE while external peers are

cross-linked to their geolocation.

Baselines also serve as the foundation for generating network access and segmentation policies. Each flow genome can be translated into a Zero Trust policy definition. In the example below, three flows have been deemed to present Medium risk and are not included as part of the default baseline.

DEVICE FLOW LIST EXAMPLE

Device Flow List

Total 16 Flows from Device "philips-qpby0p2.abchealthcare.com"

String to match ...


No.	Peer Type	Src IP	Src Name	Direction	Dst IP	Dest Name	Protocol	Dst Port	App	Last Seen	Risk	Baseline
1	Internal	10.21.138.202	philips-qpby0p2.abchealthf	OUT	10.21.139.210	suite107.abchealthcare.c	TCP (6)	139	tcp.netbios-ssn	4/20/2018 7:43:44 AM	● medium	-
2	Internal	10.21.139.210	suite107.abchealthcare.c	IN	10.21.138.202	philips-qpby0p2.abchealthf	UDP (17)	138	udp.netbios-dgm	4/20/2018 7:43:41 AM	● medium	-
3	Internal	10.21.138.202	philips-qpby0p2.abchealthf	OUT	10.57.2.19	10.57.2.19	UDP (17)	137	udp.netbios-ns	5/2/2018 11:01:39 AM	● normal	● Baseline
4	Internal	10.21.138.202	philips-qpby0p2.abchealthf	OUT	10.57.2.19	10.57.2.19	TCP (6)	104	tcp.acr-nema	5/2/2018 11:01:16 AM	● medium	-
5	Internal	10.21.138.202	philips-qpby0p2.abchealthf	OUT	10.21.139.197	station11.abchealthcare.c	TCP (6)	139	tcp.netbios-ssn	5/2/2018 11:29:09 AM	● normal	● Baseline
6	Internal	10.21.139.197	station11.abchealthcare.c	IN	10.21.138.202	philips-qpby0p2.abchealthf	UDP (17)	138	udp.netbios-dgm	5/2/2018 11:29:34 AM	● normal	● Baseline
7	Internal	10.21.138.202	philips-qpby0p2.abchealthf	OUT	10.21.139.255	10.21.139.255	UDP (17)	138	udp.netbios-dgm	5/2/2018 11:29:34 AM	● normal	● Baseline
8	Internal	10.21.138.202	philips-qpby0p2.abchealthf	OUT	10.21.139.255	10.21.139.255	UDP (17)	137	udp.netbios-ns	5/2/2018 11:29:34 AM	● normal	● Baseline


When baselines are enforced, the SCE will alert administrators of all communications outside the established and approved communication pattern. When ready to enforce policy through network access control (switch, wireless, firewall ACLs), segmentation (VLANs), or microsegmentation (Group/Tag) policy, The Ordr SCE will generate the policy in the language understood by the target enforcement system. Administrators can choose to copy the policy for manual update into the policy server or enforcement device, or else "push" policy through the native connectors available on the target system (for example, CLI, API, pxGrid, etc.).


Rapid Threat Containment


Some devices on the network may pose a significant risk and their communications must be contained as rapidly as possible to stop an attack or contain an infection. Such incidents often go undetected, and if discovered, the remediation process can be time consuming. The Ordr SCE behavioral and security monitoring quickly detects high-risk devices and communications. The Blacklist function provides administrators with the “big red” button needed to quarantine or shut down network access. For example, blocking a rogue device that enters the wireless network, or protecting a compromised or vulnerable device by moving it into a quarantine VLAN to contain the spread of malware.


BLACKLIST EXAMPLE



 Add to Blacklist
 (4 Rows)



 Blacklist & Port Shut
 (4 Rows)



 Remove Blacklist
 (0 Rows)





























 Remove Blacklist & Enable Ports
 (0 Rows)


 Generate Blacklist CLI


 Change VLAN (enforce)
 (4 Rows)


 Copy CSV
 (4 Rows)


 Analyze App Usage
 (4 Rows)

No.	Mac Address	IP Address	Device Name	Group	Profile	Risk	Vuln	Info
<input checked="" type="checkbox"/>	AC:CC:8E:0F:57:88	10.200.205.10	axis-acc8e0f5788	Physical Security Devices	Axis-P3364-Network Camera	high	normal	   
<input checked="" type="checkbox"/>	AC:CC:8E:2B:A5:E4	10.200.205.14	axis-acc8e2ba5e4	Physical Security Devices	Axis-P3214-Network Camera	high	normal	   
<input checked="" type="checkbox"/>	00:1A:07:10:B8:AF	10.200.205.7	AV10B8AF	Physical Security Devices	Arecont-Network Camera	high	normal	   
<input checked="" type="checkbox"/>	00:04:7D:3D:B9:4B	10.200.205.9	IME219-AEFKQ75	Physical Security Devices	Pelco-Sarix IME219-Network Camera	high	normal	   
<input type="checkbox"/>	EC:71:DB:A8:7D:70	10.200.205.4	Shenzhen-1	Physical Security Devices	Shenzhen-Network Camera	medium	normal	   
<input type="checkbox"/>	EC:71:DB:D3:AF:DE	10.200.205.3	Shenzhen-2	Physical Security Devices	Shenzhen-Network Camera	medium	normal	   
<input type="checkbox"/>	54:53:ED:E5:6F:61	10.200.201.204	SONY1	Physical Security Devices	Sony-Network Camera	normal	normal	  

If a network access device is not yet integrated with ISE, the SCE can perform quarantine and VLAN changes directly to the device. When integrated with ISE, the SCE leverages the Adaptive Network Control (ANC) policy feature in Cisco ISE to initiate Rapid Threat Containment (RTC). This allows Cisco ISE to maintain ultimate control over policy assignment and enforcement. Once flagged with the new ANC policy assignment by the Ordr SCE, ISE triggers Change of Authorization (CoA) to the network access device, thus instantiating the desired ISE Authorization Policy Rule on the infected/compromised endpoint. Example actions include terminating network connections, restricting network access, shutting down switch ports, changing VLAN assignments, and other blacklisting operations.

Endpoints are dynamically added to the assigned ANC policy through SCE Blacklisting.

BLACKLISTING EXAMPLE

Refresh + Add Trash Edit EPS unquarantine

MAC Address	Policy Name	Policy Actions
00:16:C8:98:B6:AB	ANC_Quarantine	[QUARANTINE]
00:1F:6C:7E:E6:A2	ANC_Quarantine	[QUARANTINE]

The below ISE Authorization Policy Rule example matches all endpoints with an ANC Policy assignment of ANC_Quarantine and assigns them a Deny_All_Traffic access policy with a Quarantine SGT.

AUTHORIZATION POLICY RULE EXAMPLE

Status	Rule Name	Conditions	Results	Profiles	Security Groups
✔	Quarantine Policy	Session-ANCPolicy EQUALS ANC_Quarantine	× Deny_All_Traffic +	Quarantine × +	

ISE administrators can modify the policy results as needed based on the device type. For example, a compromised workstation or camera may be locked down completely, whereas a medical or other critical device may be restricted from all external communications or simply set to “permit and investigate”.

Unparalleled Visibility

When rich device information from the Ordr SCE is married with ISE Context Visibility Services, ISE administrators are provided with unparalleled visibility into all connected endpoints.

CONTEXT VISIBILITY

The screenshot shows the Cisco ISE Context Visibility interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. Below this, there are tabs for 'Authentication', 'BYOD', 'Compliance', 'Compromised Endpoints', 'Endpoint Classification' (which is active), 'Guest', 'Vulnerable Endpoints', 'Hardware', and 'CloudPost'. The main area displays a table of endpoint classification data with columns for MAC Address, OUI, IPv4 Address, Endpoint Profile, CloudPost Profile, CloudPost Category, Criticality, Alarm Count, Incidence Score, Risk Score, Vulnerability, VLAN Num, and VLAN Name. The table contains 20 rows of data, including entries for Philips Patient Monitoring, Xensource, Inc., Smiths Medical, DigiBoard, and VMware, Inc. with various medical devices and their associated network details.

MAC Address	OUI	IPv4 Address	Endpoint Profile	CloudPost Profile	CloudPost Category	Criticality	Alarm Count	Incidence Score	Risk Score	Vulnerability	VLAN Num	VLAN Name
00:09:FB:47:9C:49	Philips Patient Monitoring	192.168.104.113	Philips-Device	Philips-Patient Monitoring	Medical Devices	LEVEL_3	0	0	0	NORMAL	4	Vlan-4
00:16:3E:1C:98:9A	Xensource, Inc.	192.168.104.31	Unknown	Hospira-Lifecare PCA-Infusion Pump	Medical Devices	LEVEL_3	0	0	0	NORMAL	4	Vlan-4
00:16:3E:6D:36:02	Xensource, Inc.	192.168.104.88	Unknown	Hospira-Lifecare PCA-Infusion Pump	Medical Devices	LEVEL_3	0	0	0	NORMAL	4	Vlan-4
00:1A:01:00:11:11	Smiths Medical	192.168.104.201	Unknown	Smiths-Medfusion 4000-Infusion Pump	Medical Devices	LEVEL_3	0	0	0	NORMAL	4	Vlan-4
00:1A:01:00:11:12	Smiths Medical	192.168.104.184	Unknown	Smiths-Medfusion 4000-Infusion Pump	Medical Devices	LEVEL_3	4123	0	60	NORMAL	4	Vlan-4
00:40:9D:59:4B:BB	DigiBoard	192.168.106.18	Unknown	Baxter-35700BAX-Spectrum Infusion ...	Medical Devices	LEVEL_3	0	0	0	NORMAL	6	Vlan-6
00:40:9D:59:4B:BC	DigiBoard	192.168.104.16	Unknown	Baxter-35700BAX-Spectrum Infusion ...	Medical Devices	LEVEL_3	0	0	0	NORMAL	4	Vlan-4
00:50:56:07:DB:E4	VMware, Inc.	10.200.204.9	VMWare-Device	GE-LOGIQ700-Ultrasound	Medical Devices	LEVEL_3	0	0	0	NORMAL	204	VLAN0204
00:50:56:1F:7D:7E	VMware, Inc.	10.200.204.22	VMWare-Device	Fujifilm-9000-CR Reader	Medical Devices	LEVEL_3	0	0	0	NORMAL	204	VLAN0204
00:50:56:35:52:12	VMware, Inc.	10.200.204.15	VMWare-Device	GE-LOGIQ700-Ultrasound	Medical Devices	LEVEL_3	0	0	0	NORMAL	204	VLAN0204
00:50:56:40:F6:E4	VMware, Inc.	10.200.204.13	VMWare-Device	Philips-MRI	Medical Devices	LEVEL_3	0	0	0	NORMAL	204	VLAN0204
00:50:56:4A:08:43	VMware, Inc.	10.200.204.5	VMWare-Device	Picker-PQ5000-CT Scanner	Medical Devices	LEVEL_3	0	0	0	NORMAL	204	VLAN0204
00:50:56:54:57:F0	VMware, Inc.	10.200.204.8	VMWare-Device	Picker-PQ5000-CT Scanner	Medical Devices	LEVEL_3	0	0	0	NORMAL	204	VLAN0204
00:50:56:64:60:CB	VMware, Inc.	10.200.204.20	VMWare-Device	Fujifilm-9000-CR Reader	Medical Devices	LEVEL_3	0	0	0	NORMAL	204	VLAN0204
00:50:56:64:E3:93	VMware, Inc.	10.200.204.25	VMWare-Device	Picker-PQ5000-CT Scanner	Medical Devices	LEVEL_3	0	0	0	NORMAL	204	VLAN0204
00:50:56:6A:42:46	VMware, Inc.	10.200.204.16	VMWare-Device	GE-LOGIQ700-Ultrasound	Medical Devices	LEVEL_3	0	0	0	NORMAL	204	VLAN0204
00:50:56:70:95:2C	VMware, Inc.	10.200.204.21	VMWare-Device	Fujifilm-9000-CR Reader	Medical Devices	LEVEL_3	0	0	0	NORMAL	204	VLAN0204
00:50:56:7A:21:AE	VMware, Inc.	10.200.204.7	VMWare-Device	Picker-PQ5000-CT Scanner	Medical Devices	LEVEL_3	0	0	0	NORMAL	204	VLAN0204
00:50:56:7D:90:31	VMware, Inc.	10.200.204.24	VMWare-Device	VmWare-PACS Server	Medical Workstations	LEVEL_3	0	0	0	NORMAL	204	VLAN0204
00:50:56:82:39:C9	VMware, Inc.	10.200.204.19	VMWare-Device	Fujifilm-9000-CR Reader	Medical Devices	LEVEL_3	0	0	0	NORMAL	204	VLAN0204

Without effective classification, many customers find they are unable to make any policy decision for many of their critical devices without incorporating some manual whitelisting process. The SCE's accurate device inventory and classification also enables network access control, especially for IoT endpoints that lack the ability to identify or authenticate themselves to the network. Visibility into network communications (as established through the SCE baselining and flow genomes) enables the definition of network access policy as well as microsegmentation policy.

Protecting IoT through Network Segmentation

IoT devices proliferate virtually every company today but are virtually impossible to individually secure. These devices often run legacy operating systems with minimal or no patching capabilities to defend themselves. Network convergence and cross-domain communication demands that IoT devices share the same infrastructure and physical communications paths. Consequently, network segmentation is proving to be the most effective means to protect IoT. Executed properly, network segmentation can isolate devices from threats and significantly reduce security risk to the business.

Organizations face these challenges when attempting to deploy network segmentation:

- What devices are in the environment and what is their function or role in the organization?
- Which segments are devices currently in and which segments do they belong in?
- How verify new devices and device types are properly onboarded and placed in the right segments?
- What communications need to be allowed across segments?
- Which devices are high risk, vulnerable or non-compliant and may require quarantine or remediation?
- How can different teams such as IT, Security, Asset and Facilities Management work together to prevent confusion around problem-ownership and streamline operational workflows?
- How can segmentation policies be provisioned in a heterogenous network?
- How can policies be implemented fast and efficiently to reduce or remove threats?

Often segmentation policies are too broad to be effective where business critical devices are intermingled with employee workstations. A single user clicking on a malicious email can disrupt business operations and segmentation projects can be stalled due to the sheer complexity, time, and costs to implement and manage.

Ordr Makes Policy Provisioning and Segmentation using Cisco ISE Easy

Without effective classification, many customers find they are unable to make any policy decision for most of their critical IoT devices without incorporating some manual whitelisting process. In addition to accurate device inventory and classification for all endpoints, the Ordr SCE enables Cisco ISE customers to confidently and quickly move from visibility-only to Zero Trust enforcement and segmentation. Both user and non-authenticating IoT endpoints can be secured from external and unauthorized communications while limiting access to that required for the device or user to perform its intended function (principal of least privileges).

The determination of access control and segmentation policy is ordinarily a complex and tedious task. The process may be simpler for user devices (desktop and mobile endpoints) where access to resources is based on group assignments (as determined through a user's identity via authentication) and the application services associated to a group. However, the majority of IoT endpoints do not identify nor authenticate themselves to the network, and while the communication patterns for IoT devices tend to be more specific compared to a multi-function user device, the understanding of actual policy or segmentation grouping for IoT endpoints is often a mystery. Rarely is there any prescriptive guidance on what an IoT endpoint should and should not do on the network, leaving the burden to the customer to manually inspect traffic flows through packet capture, logs, or other sources. This is a daunting task considering the hundreds if not thousands of different IoT endpoint types on the network. Consequently, enforcement of policy grinds to a halt and customers are left with the impression that NAC enforcement is neither cost-effective nor achievable.

The Ordr SCE simplifies this once-daunting and time-consuming process. Visibility into network communications, as established through Ordr SCE baselining and flow genomes, automates the definition of network access policy as well as microsegmentation policy. Whether at the group or individual device level, the SCE learns what each group and individual device should have access to and automates network segmentation (for example, VLAN assignments), microsegmentation (for example, SGT assignments), and ACLs for automated provisioning to switches, wireless controllers, firewalls, and SGACLs for TrustSec, as well as auto-population of the TrustSec matrix. While possible to enforce policy directly to targeted enforcement devices from Cisco and other vendors, the SCE's unique integration with Cisco ISE simplifies and super-scales the deployment of network access and segmentation policy like no other solution on the market.

What Does Ordr do for Cisco Identity Services Engine?

Ordr SCE:

- Extends Cisco ISE Profiling to cover all IoT including Medical, Manufacturing, Finance, Building Automation, and takes device context to new levels of visibility.
- Extends Compliance and Security Risk assessment and monitoring to all endpoints including IoT devices.
- Extends data exchange services through direct integration with existing asset management systems as well as service/ticketing solutions such as ServiceNow.
- Adds network statistics and availability tracking for all devices as well as detailed utilization tracking for imaging and fleet devices in the healthcare industry.
- Provides advanced Anomaly Behavior Detection based on actual device communication/traffic behavior, not spoofable endpoint attributes.
- Automates policy authoring and provisioning to accelerate policy enforcement, and the application of segmentation and microsegmentation policy, reducing deployment times from months or years down to days or weeks.
- Super-scales policy provisioning through advanced Cisco ISE integration and policy logic to support hundreds of thousands of devices.

The Combined Ordr + Cisco Solution



AAA	✓		
Guest Services	✓		
General Profiling Services	✓		✓
Advanced IoT Device Profiling			✓
Asset Details (make, model/serial number, HW/SW versions)			✓
Device Onboarding	User BYOD		IoT Devices
Compliance/Posture	User Devices Only		IoT Devices + Windows Workstations
Anomaly Behavior Detection/Detection of MAC spoofing	Limited	Limited	✓
Vulnerability Assessment & Threat Monitoring		Limited	✓
Traffic/Flow Analysis		✓	✓
Policy Enforcement using ACLs, VLAN assignment, and SGTs/Group-based tags	✓		✓
Dynamic Policy Learning and Authoring			✓

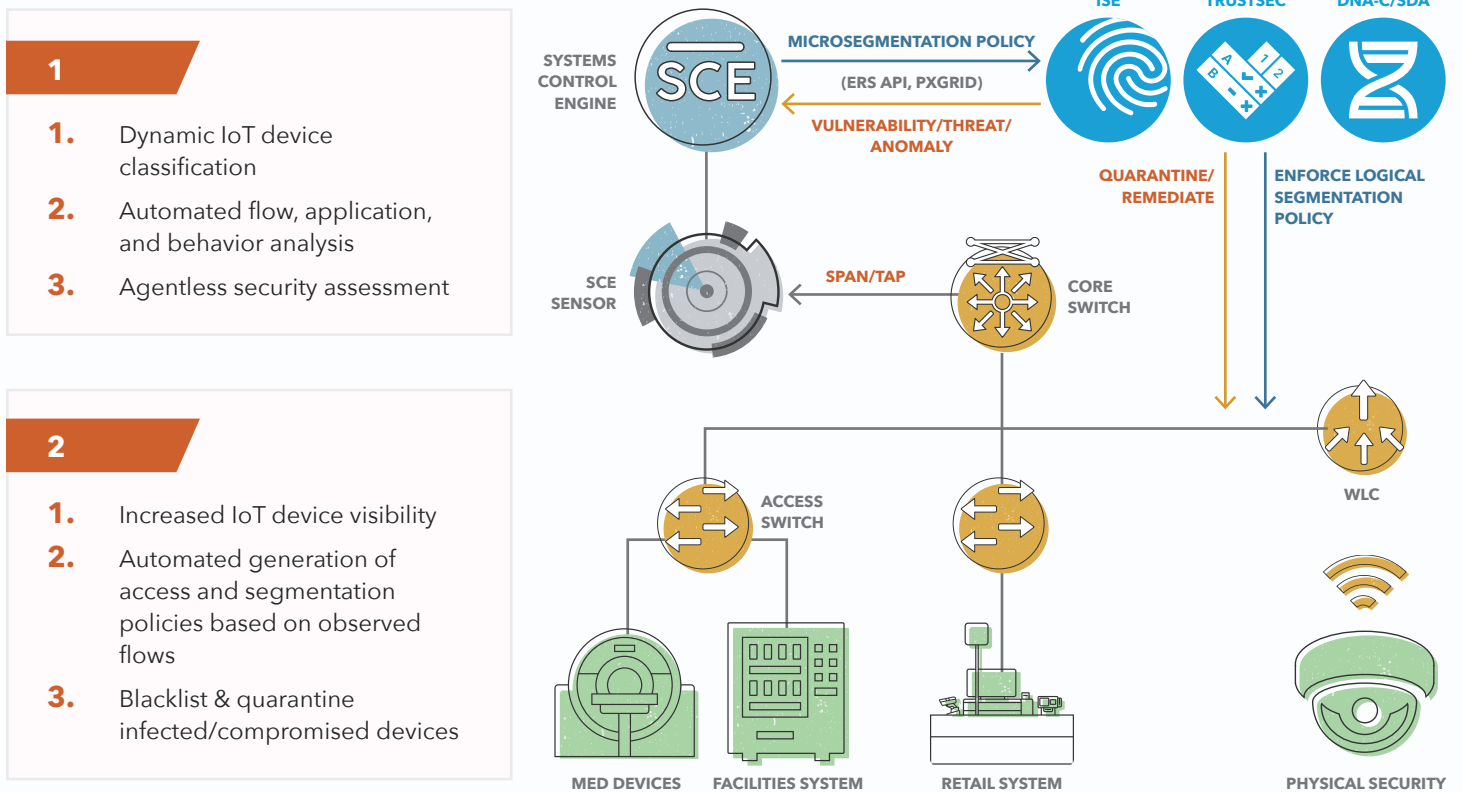
Ordr and Cisco ISE in Action

The diagram illustrates the integration of Ordr with Cisco ISE. SCE Sensors provide agentless, passive data collection which feeds the SCE Analytics Server. Sensors may be centralized or distributed based on collection requirements. The SCE Analytics Server analyzes the data to automatically discover and classify all IoT and non-IoT devices. It then feeds the rich contextual data to Cisco ISE.

To move to microsegmentation and the enforcement of policies, NAC administrators must understand which traffic to allow and deny. SCE Analytics Server provides this insight to Cisco ISE and facilitates the provisioning of segmentation policy.

The SCE's job is still not done. While monitoring all devices for known threats and vulnerabilities, it is also keeping close watch on communication flows and anomalous traffic. The Ordr SCE can notify Cisco ISE of at-risk, vulnerable, and compromised devices to trigger the necessary quarantine and remediation response.

CISCO ISE + ORDR SYSTEMS CONTROL ENGINE



Why Ordr?

The Ordr engineering team led development for major wired and wireless networking companies such as Cisco and HPE/Aruba. Ordr understands hybrid networking and the challenges customers have securing IoT. The team also consists of industry leaders in Cisco NAC solutions and microsegmentation. It is this intimate technical understanding of networking and NAC technologies that has allowed Ordr to deliver a next generation solution for dynamic device classification and automated policy enforcement through segmentation.

Using our experience and knowledge we set out to create a solution that abstracts you from the complex underpinnings of the network so you can focus on your objectives to run a secure IoT operation.

Summary

Without Ordr, customers can struggle for months or years to achieve a comprehensive inventory and device visibility. Often the topic of real enforcement and microsegmentation is just a distant vision as the classification of endpoints with confidence becomes the all-consuming task. With Ordr Systems Control Engine integration, the ability to accurately identify endpoints—IoT and non-IoT—is drastically accelerated allowing customers to finally broach the topic of policy enforcement and segmentation. Ordr's AI-driven analysis engine automates these difficult and time-consuming tasks without the use of agents. The Ordr SCE can be deployed passively in minutes within your existing environment without risk to existing operations. Contact Ordr today to learn how we can help simplify and accelerate your IoT security deployment.



ōrdr

take control.

info@odr.net
www.odr.net



2445 Augustine Drive Suite 601
Santa Clara, CA 95054

