Ordr Systems Control Engine Technology

Digital transformation across healthcare, manufacturing, retail, transportation, and logistics is accelerating the hyper-connectedness of enterprise systems powered by IoT and connected OT devices. The enterprise IT network is now the melting pot for a highly eclectic mix of devices that businesses must manage and protect or face immediate security risk.

The Ordr Systems Control Engine allows organizations to rapidly inventory every ***thing*** *in your domain, classify it based on type and business function, and assess it for risk. It learns behaviors and creates device flow genomes, so you'll know what each device should be talking to. It protects using microsegmentation to logically segregate groups of devices from any thing that's non-essential and can rapidly stop active threats and isolate compromised devices. Plus, it is non-disruptive to the device, the network, and the way you run your operations.*

This white paper describes the technology anchors of the Ordr Systems Control Engine and clarifies what sets the product apart from other tools in the market.

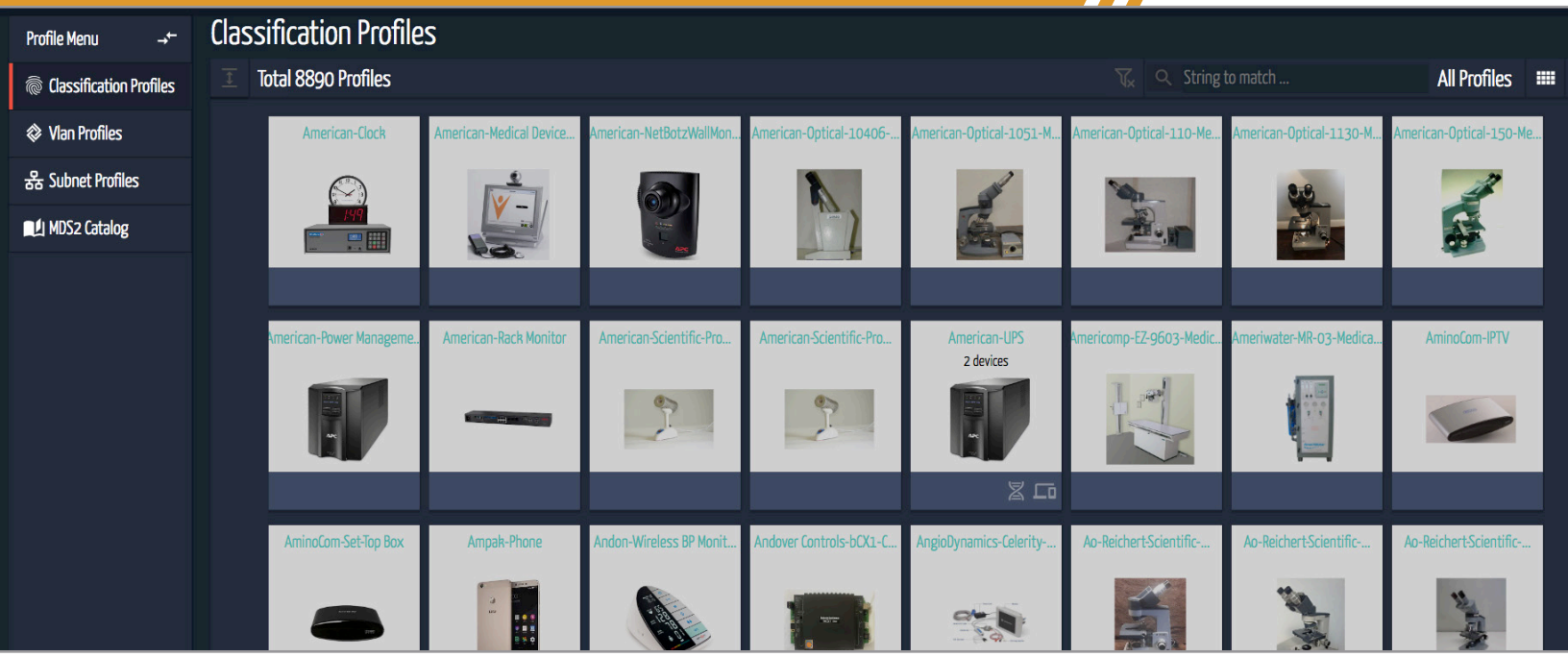
ORDR TECHNOLOGY WHITE PAPER

High-Resolution Device Data & AI-based Classification

The Ordr Systems Control Engine (SCE) rapidly identifies and classifies all connected devices on the network. It has a built-in database of devices, uses protocol decoding and other techniques to discover detailed information about devices, and has an Artificial Intelligence (AI) and Machine Learning (ML) engine to automatically create new profiles for devices it has never seen before. Beyond detailed classification, the product 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 devices that share protected health information (PHI) or payment card information (PCI) are collected.

The system employs various agentless and passive methods of data collection to identify and profile connected devices. Sensors are deployed in the network and start their discovery by inspecting copies of network traffic through a SPAN or tap, and ties this to its extensive device profile library as well as dynamic AI-based classification techniques to begin the process of profiling each observed device. Traffic is analyzed at multiple layers.

DEVICE PROFILES



Beyond basic 5-tuple flow data (source/destination IP/port + protocol), the Ordr Systems Control Engine breaks down traffic at the application layer using protocol decoding to extract the metadata, which reveals details about the endpoint including its identity, manufacturer, model, and often serial number and software version. Over 50 protocols are decoded including DICOM, HL7, POCTX, Med-X, Powerlink, MUD, BACNET,

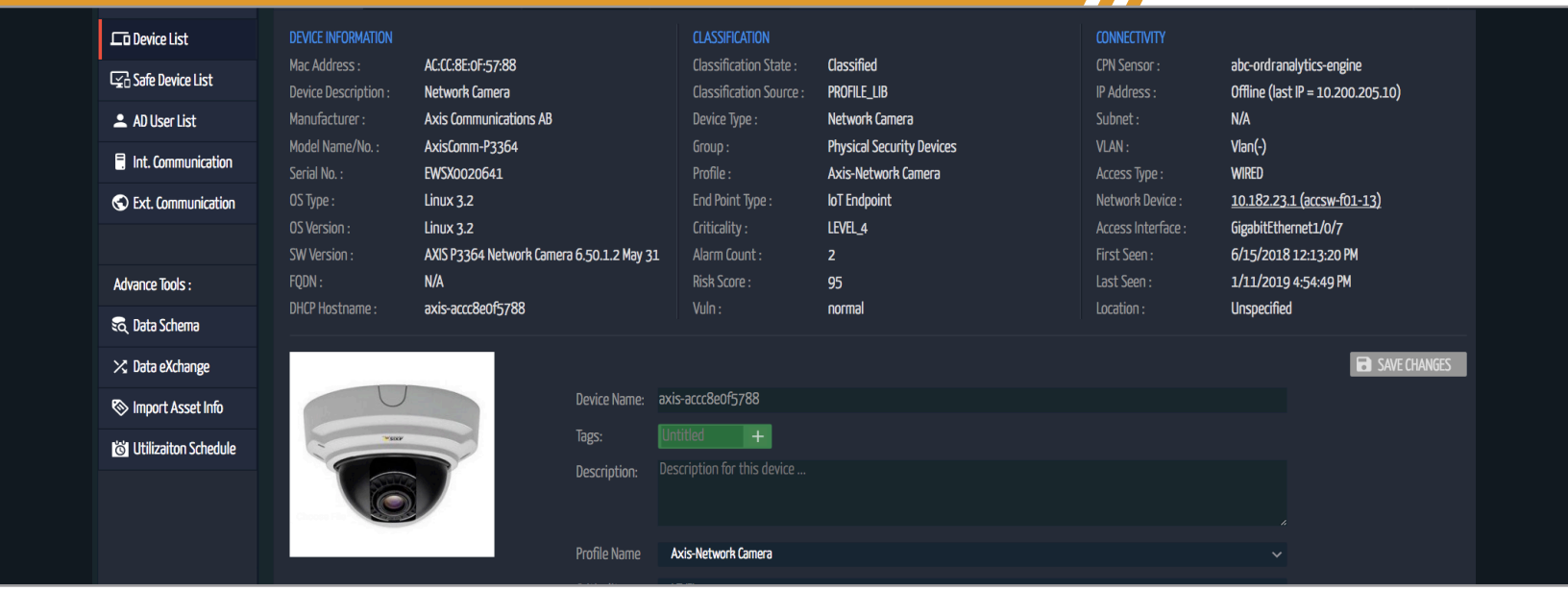
PROFINET, and Modbus. Through this advanced inspection, the product can discriminate between different devices, and even differentiate when a device is directly connected to the network versus if it is connected through a workstation or behind an IoT gateway.

To gather additional intelligence, the Ordr Systems Control Engine discovers and queries network switches to collect details about connected endpoints such as their network properties (MAC/IP address, subnet, interface, VLAN, SSID, etc.), CDP/LLDP data, and other statistics.

The product also learns device details from common services like DNS and Active Directory. For example, it can fetch detailed operating system, patches, hotfixes, application inventory and other details about Windows-based systems using its Windows Remote Management (WinRM) connector. The product retrieves details from the device itself using optional specialized probes including SNMP, UPnP, and mDNS. All non-passive collection methods are configurable to allow administrators to specify which parts of the network to include or exclude; all query methods are disabled by default, but easily enabled with a click of the mouse.

The Ordr Systems Control Engine bidirectionally shares device attribute schema information with popular enterprise tools so organizations can have a common view of all connected assets across every business function. The expanding set of integrations include IT Service Management (ITSM) tools such as ServiceNow, Security Information Event Management (SIEM) tools like Splunk, Network Access Control (NAC) products including Cisco Identity Service Engine, HPE-Aruba ClearPass, and ForeScout CounterACT, network firewalls from vendors including Palo Alto Networks, Fortinet and Cisco, and Enterprise Asset Management (EAM) and Configuration Management Databases (CMDB) tools like Nuvolo. The product offers a RESTful API so new connectors can be quickly implemented. There is a spreadsheet (CSV) import and export option.

HIGH RESOLUTION DEVICE DETAILS



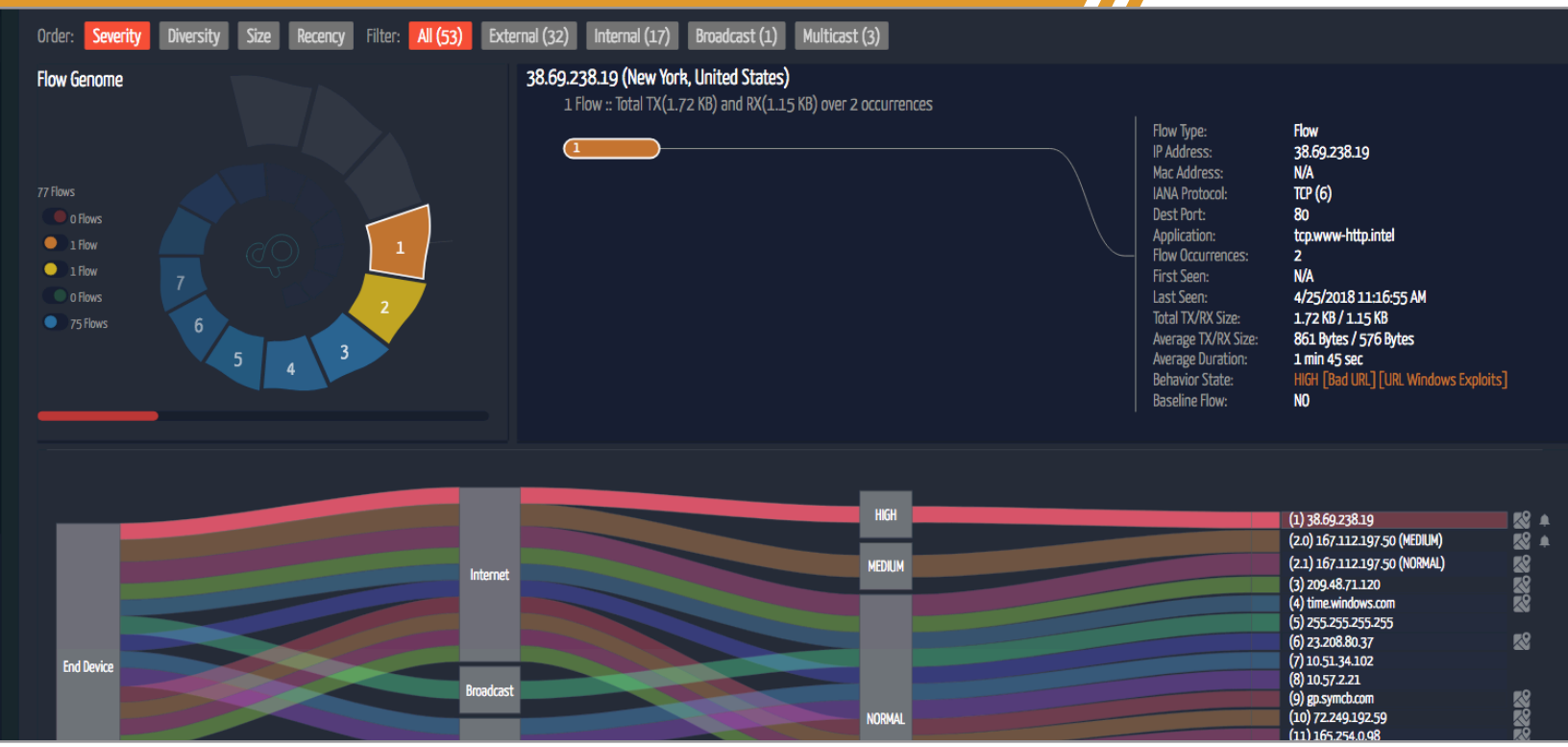
Device Flow Analytics & Baselining

The Ordr Systems Control Engine passively monitors network communications and creates a conversation map, called a flow genome, for every connected device. The product learns the network topology too – the VLANs, subnets, routing, and the access-layer connectivity graph of what is connected to each switch port and wireless AP. The system stores this information in an optimized database inclusive of device, flow, and topology objects. The graphical user interface offers an exceptional presentation layer and workflow to analyze this information and determine 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.

Since the flow analytics is anchored to high-resolution device inventory details, operators can easily learn what every system is actually doing in the network. There are unique views in the product that allow you to:

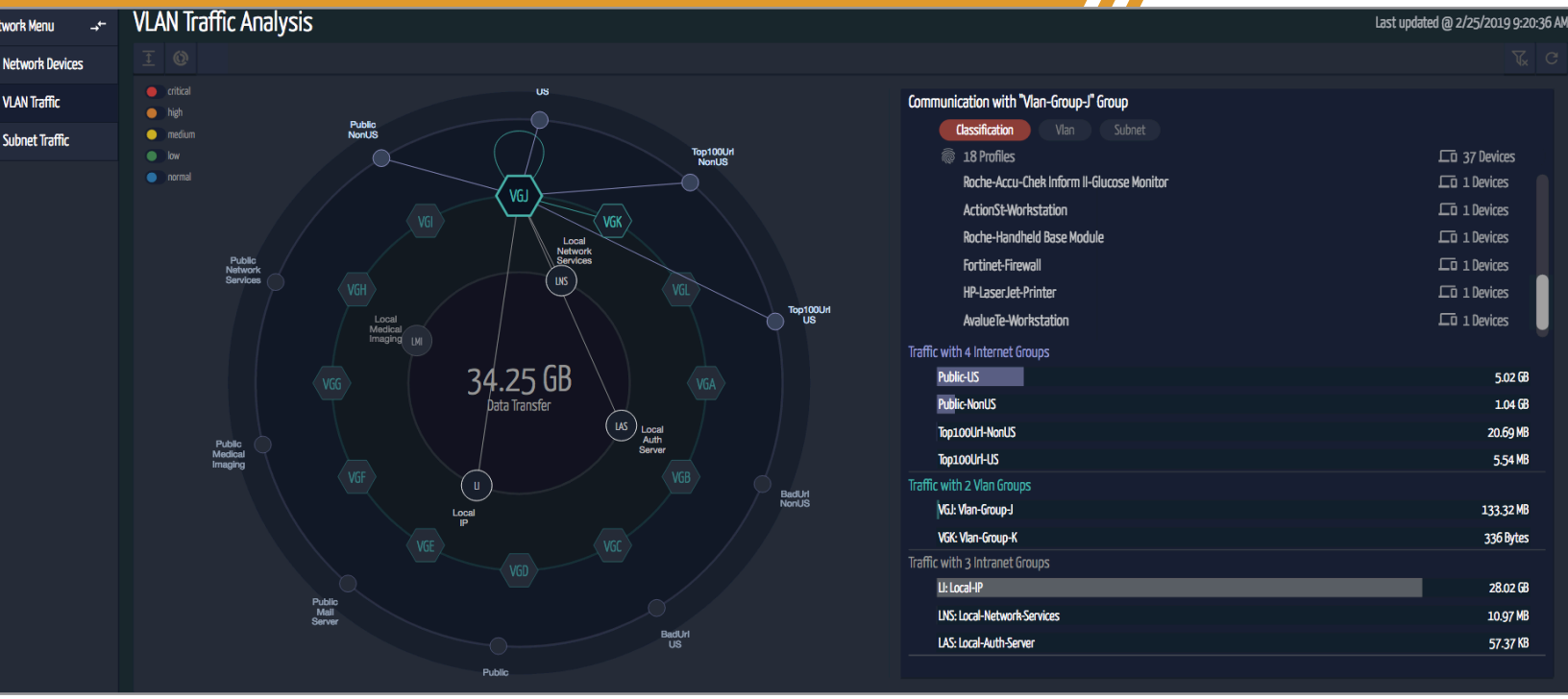
- Audit the communications of every device and see every other system it communicates to inclusive of the IP address, web site/URL, and application protocols used
- View the communication patterns for all devices of the same type, such as Axis surveillance cameras, Rockwell PLCs, and Phillips patient monitoring systems to identify outliers and expedite segmentation efforts

DEVICE FLOW GENOME



- Identify all communications between different VLANs and subnets by device and protocol to streamline firewall and cross-network policy controls
- 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

VLAN DEVICE AND FLOWS VIEW



The product features a proprietary AI/ML-based behavioral analysis engine that baselines normal communications for IoT and OT. The product has automated the process and it requires no manual intervention, however operator confirmation or adjustment is built into the workflow. Pairing a device identity with its correct communication profile is made possible because non-user devices have a narrow and deterministic set of systems they interact with. For example, a video surveillance camera talks to the video storage database and camera management system. Or a medical diagnostic device just communicates with an EMR system and a patch update server.

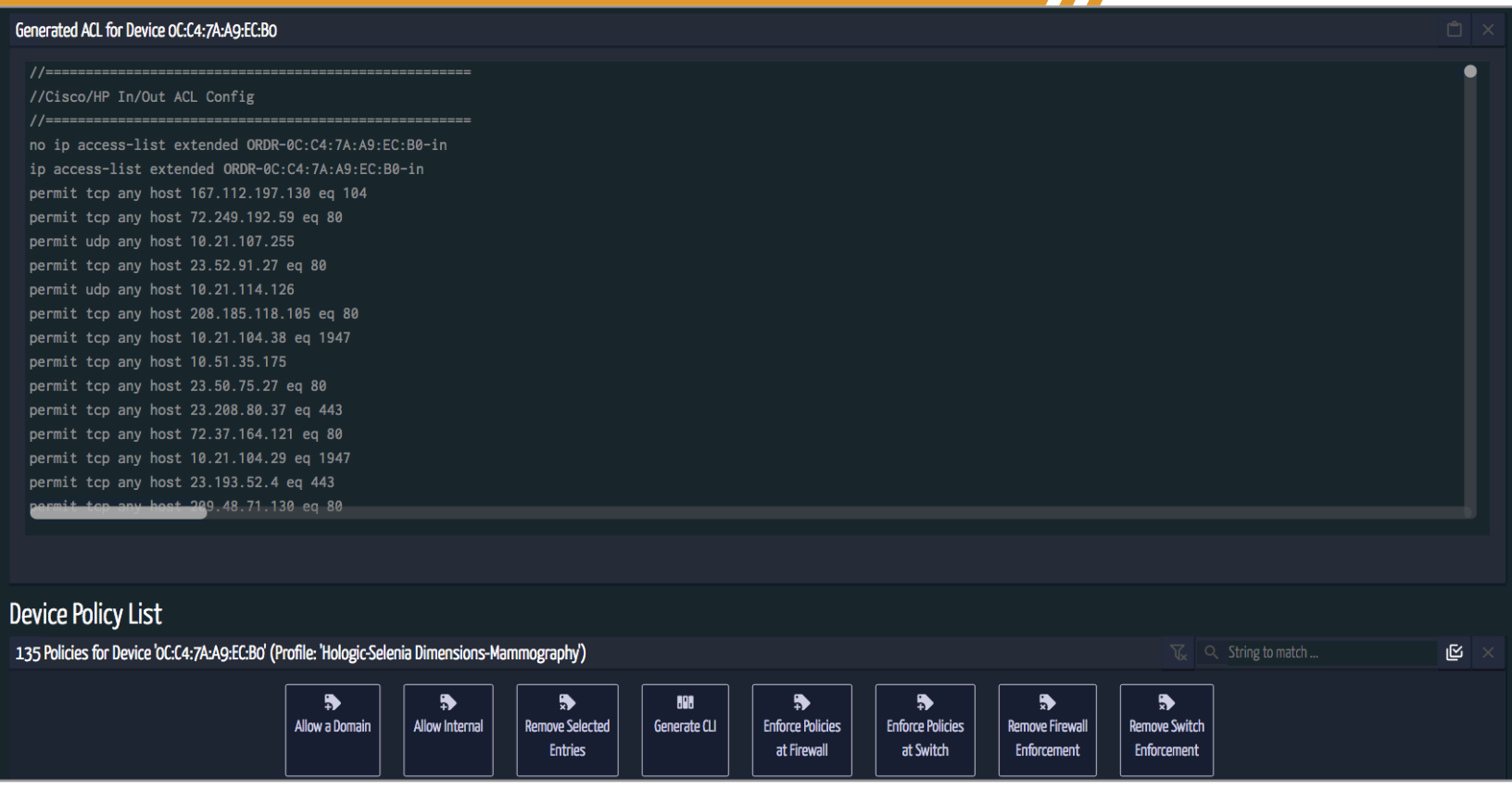
Anomalous communications to and from IoT and OT devices are often indications of attack, compromise, or misconfiguration. The Ordr Systems Control Engine issues security incidents when any anomaly is detected. For example, if a user workstation tries to connect with a manufacturing or medical device using SMB, that indicates the workstation is likely compromised with malware. Or if a non-approved device is conducting ping or port scans, it generates an alert. Notification can be tuned to filter out non-business critical devices.

Protect Devices with Microsegmentation

IoT devices proliferate every company today but are 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 and microsegmentation of IoT/OT enforces a Zero Trust architecture by isolating devices from threats to significantly reduce security risk to the business.

The Ordr Systems Control Engine automates device identification, uses artificial intelligence to baseline normal communication behavior and then translates these behaviors into a device-specific security policy. The policy can be passed via API integration to leading Network Access Control (NAC) tools, or to border Firewalls that control cross-network communications, or pushed to switches and wireless controllers directly. No new technology is required as these precision controls are enforced using the existing network infrastructure. Enabling this capability limits network communications to approved systems only, resulting in a reduced IoT/OT fleet attack surface.

ACL POLICY RULES EXAMPLE

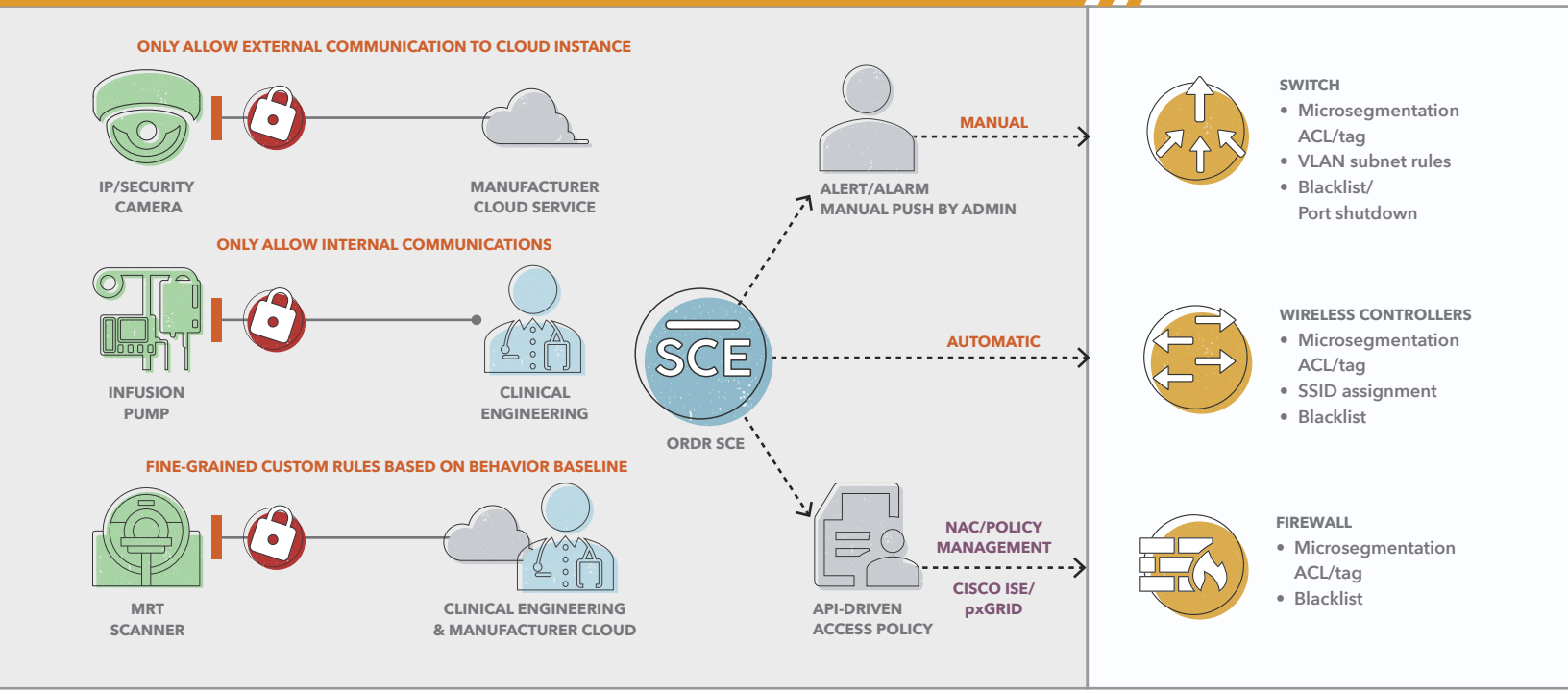


The product has rich integration with leading NAC tools including Cisco Identity Service Engine (ISE), ForeScout CounterACT, and HPE-Aruba ClearPass to be enforced across the infrastructure. While many tools can share device attribute and grouping information with NAC tools, and even trigger blacklist policies to be enforced for compromised or uncontrolled assets, Ordr's solution provides advanced integration so organizations can implement Zero Trust policies to each IoT/OT device in the environment using VLAN assignments, access control lists (ACLS), and even advanced tagging technologies such as Cisco Scalable Group Tags (SGTs).

Many security teams use firewalls to restrict communications between IoT and OT networks, such as the manufacturing line equipment, medical devices, facilities controllers, and physical security systems. The Ordr Systems Control Engine integrates with leading firewall vendor products including Palo Alto Networks, Cisco, CheckPoint, and Fortinet. Using real-time API integration, the product uses high-resolution details about devices to define granular device groups. Then it creates and configures access control policies for them based on ACLs or advanced technologies such as Palo Alto group tags.

For organizations that do not use NAC or firewalls to enforce segmentation, the Ordr Systems Control Engine can still protect at-risk systems, such as those with exposed vulnerabilities and lack a manufacturer patch to fix. The product can build Zero Trust policies to enforce on existing network equipment from vendors such as Cisco, HP, Aruba, Extreme, and Arista. The product is able to 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 native connectors available on the target system, such as CLI or an API.

POLICY ENFORCEMENT



Device Vulnerability & Risk Assessment

The Ordr Systems Control Engine leverages a wide range of security intelligence feeds and AI-based behavioral anomaly detection in order to identify vulnerabilities, detect active threats, and score risk for every device. The suite of security services constantly monitors every device, keeping the risk scores and relevant security issues up-to-date. The suite consists of:

- NVD, the ICS-CERT database (https://nvd.nist.gov/vuln/data-feeds#JSON_FEED)
- ICSA for ICS-CERT advisories (https://ics-cert.us-cert.gov/advisories)
- Medical vulnerability feeds including the FDA recall database, MD-Viper, and support for MDS2 forms
- Behavioral analytics (of communications) to identify attempted attacks or indications of compromise
- Built-in vulnerability scanner, or ingests data information from other vulnerability management tools such as Tenable and Rapid7
- Built-in network intrusion and malware detection system
- Threat intelligence feed from top-tier vendor
- Malware/bad URL/website tracking
- IP reputation and IP/Geo for fraud sites
- Password scanning and weak/open password detection

SECURITY DASHBOARD

Security issues are mapped to the devices they correspond to and provides information about the problem, severity, impact, and remediation recommendations. Often embedded links are included so incident response teams can conduct further research before taking correction action.

The high-definition device data obtained by the solution includes the operating system, hardware/software version, patch level, and in-use applications. This makes it easy to identify outdated or known vulnerable devices so remediation plans can be determined, such as patching, implementing compensating controls like microsegmentation, and prioritizing inventory refreshes.

The Ordr Systems Control Engine combines security intelligence with detailed insight about asset inventory and the network topology. The user interface is optimized to easily pivot between overall risk information for the entire device fleet and drill-in views of specific security incidents or at-risk devices. This results in substantial reduction in the time and resources needed to investigate and respond to incidents. The product integrates with leading security information event management (SIEM) and IT workflow tools used by security operations teams to facilitate ticketing and remediation.

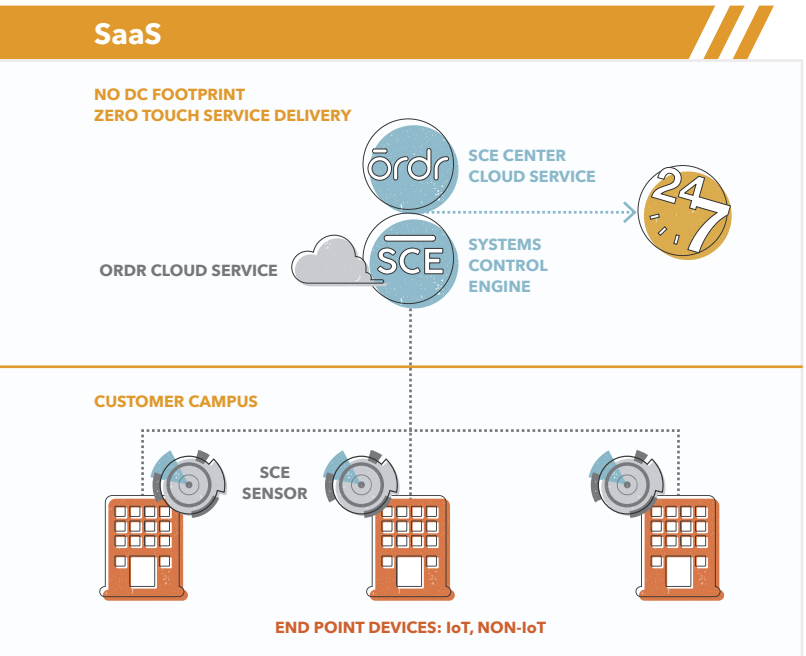
SaaS or On-Premises Deployment Options

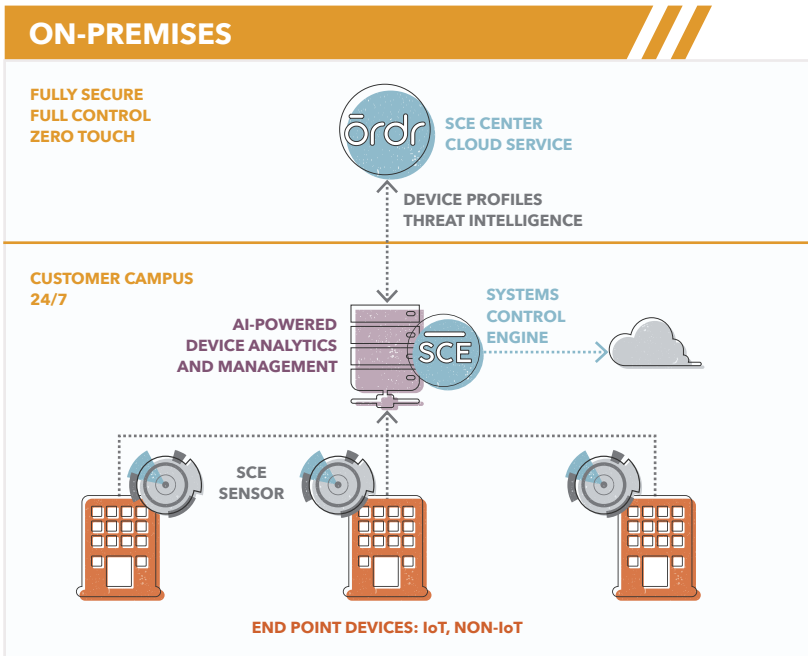
The Ordr Systems Control Engine supports multiple deployment models including Saas delivered, fully on-premises, private cloud, and MSP hosted. There are three key components of the system:

- **Systems Control Engine:** SaaS managed service in the cloud or on-premises/private cloud hosted appliances or virtual machines in the datacenter that perform behavioral analysis, identify anomalies, and act as the solution's management and policy decision point for the organization.
- **SCE Center:** Ordr-operated cloud service that helps in zero-touch provisioning of each deployment and keeps it up-to-date with the latest threat feeds and IoT device profiles.
- **SCE Sensor:** appliances or virtual machines that are deployed at the access, distribution or core layer of the network and receive SPAN, tap, or flow data in order to discover and track IoT devices and monitor communications in a completely passive fashion without any disturbance to operations.

Sensors and on-premises SCE appliances can be delivered as software images or preinstalled on appliances.

Typically, one sensor is needed per major building, and it is installed with a SPAN, RSPAN, or tap from the building core or distribution switch. Setup of a single sensor takes less than an hour, inclusive of racking the device and turning it on. For satellite sites or large distributed deployments, flow export data from NetFlow, IPFIX, or sFlow can be leveraged to gain remote visibility instead of deploying local sensors. With full application flow visibility, all of the product's features are available. Flow-only visibility may limit the ability of the system to glean certain high-resolution device data such as serial numbers and software versions.





ōrdr

take control.

info@ordr.net
www.ordr.net

2445 Augustine Drive Suite 601
Santa Clara, CA 95054