Supercharge Cisco ISE Deployments with Ordr

Dramatically accelerate deployments and reduce operational costs compared to alternative solutions

Unprotected unmanaged and IoT devices represent a back door into an organization's network. Cyberattacks are launched to ferret weak and vulnerable targets leading to data exfiltration or hijack to solicit ransom. Because these connected devices aren't built with security in mind and often run legacy operating systems that cannot be easily patched, they are easy prey with high financial rewards for cybercriminals.

Cisco Identity Services Engine (ISE), is the market leader in Network Access Control technology, providing endpoint visibility and identity-based access control for the enterprise. Cisco ISE enables customers to secure their network with strong authentication and device authorization mechanisms. Many organizations deploying Cisco ISE want to get to the end goal of network segmentation for better security. However, they face the following challenges in their deployment:

ISE's out-of-box profile lacks important details, such as device model name, OS and software name and versions, protocol in use, for instance. All of these details are important to understand criticality of devices in the organization, and to create a corresponding security policy for both network access and network segmentation

Security and IT teams spend many hours adjusting profiles for existing device as well as new devices onboarding to their network

New device profiles need to be adjusted in their policy, including new ACL, authorization policy, authorization rules.

To ensure Cisco ISE is effective to secure unmanaged, IoT, IoMT and OT devices requires additional intelligence and automation:

- Knowing what the device is and delivering accurate profiling
- Understanding what the device needs to do on the network to operate properly without disruption. For example, what port or protocol the devices are running
- Automation of Segmentation/ISE policies to speed up deployment and reduce operational expenses.

How Ordr Works

The Ordr Systems Control Engine (SCE) helps organizations optimize their Cisco ISE investment. Ordr can maximize Cisco ISE's powerful authentication and authorization features, address challenges with profiling and accelerate operations. In fact, Ordr can cut device profile-oriented tasks by more than half, reducing customers operational costs dramatically.

The Ordr platform offers agentless and passive deployment with options for on-premises or cloud. Within minutes, customers start to see their devices connected in the network with rich context such as manufacturer, model, OS name and version, serial numbers automatically, WITHOUT touching any profile settings (see Figure 1).

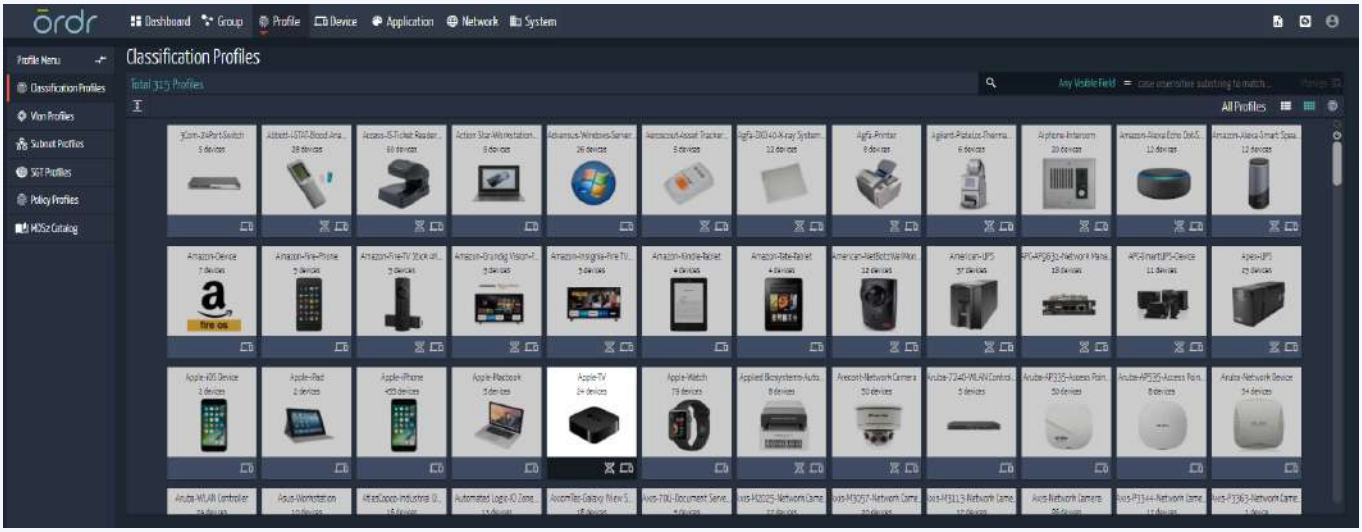

Figure 1: Ordr Device Profiling

Ordr Flow Genome then baselines device communications, showing what systems devices are communicating with detailed network details (Figure 2).

Figure 2: Ordr Flow Genome and device communications map

Ordr complements ISE by automating both device profiling tasks and policy configuration tasks that would otherwise require tremendous customer investment in time and resources. (Figure 3).

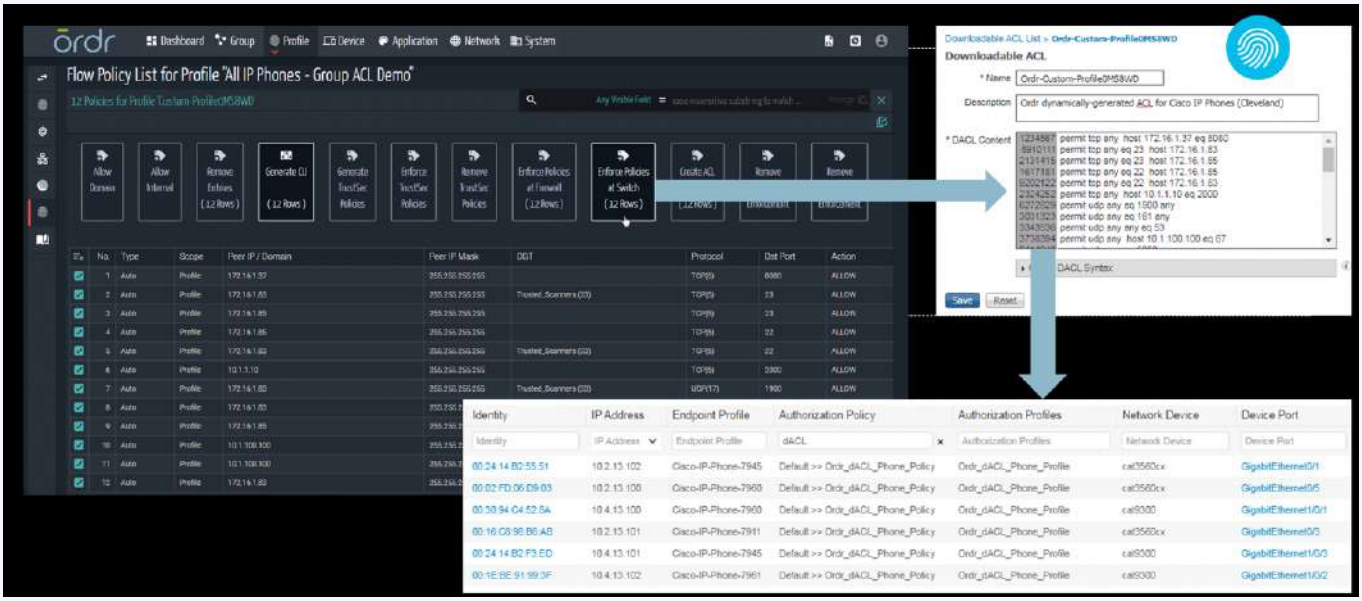

Figure 3: Flexible Grouping and Automated Policy Enforcement

How Ordr Differentiates:

The combination of Ordr and Cisco ISE simplifies the tasks that often overwhelm and stall unmanaged and IoT device security initiatives. Organizations using the Ordr SCE have been able to dramatically reduce Full Time Employee (FTE) hours as well as the time required to move their projects forward. There are three ways that Ordr differentiates against other competitive solutions in its integration with Cisco ISE:

1. Highly granular device context shared with Cisco ISE for access control

Ordr SCE makes it easy to determine what unmanaged and IoT devices are in the network across the ENTIRE organization, not just lines of business. The Ordr platform uses Deep Packet Inspection (DPI) for passive inspection of devices, delivering granular information such as manufacturer, serial number, software versions and the protocols and applications they speak.

Ordr augments Cisco ISE with real-time network connectivity and network location information (such as the switch or wireless ingress point, or the current VLAN and subnet) and real-time risk scoring based on observed threats, known vulnerabilities and recalls. Ordr also monitors IP address changes for devices. All of this rich context is shared with Cisco ISE, and can form the foundation of access control policies.

Many competitive solutions cannot see this info effectively, resulting in duplicate endpoints, unreliable context association, and ultimately false-positive policy generation.

2. Automated translation of Ordr device classification to Cisco ISE policies

Network segmentation is one of the most effective means to secure unmanaged and IoT devices. However, segmentation in practice can be challenging because granular information about devices and their communications patterns is needed to create Cisco ISE segmentation policies. As an example, the policy for an IP camera would only allow communications to a video recorder, the camera management system, and a source for patch updates.

One of the differentiators when deploying Ordr is its ability to automatically translate device profiles and learned, approved, communications, into Cisco ISE policies that can be enforced across a wide range of network and security infrastructure. Cisco ISE policies require specific parameters such as manufacturer, model name, operating systems and more. Ordr understands Cisco ISE nuances and the team's deep background in networking enables this policy automation. Ordr streamlines operations by mapping Ordr profile and ISE policy dynamically, thus eliminating the expensive process of creating ISE device profile and authorization profile and policy, every time a customer sees a new device type. This powerful capability accelerates a process that is traditionally error-prone and labor intensive.

In contrast, competitive solutions require a multi-step process where device profiles need to be modified and customized into Cisco ISE profiles before policy creation can take place. This means that organizations with competitive solutions bear the burden of creating custom Cisco ISE profiles every time a new device is detected.

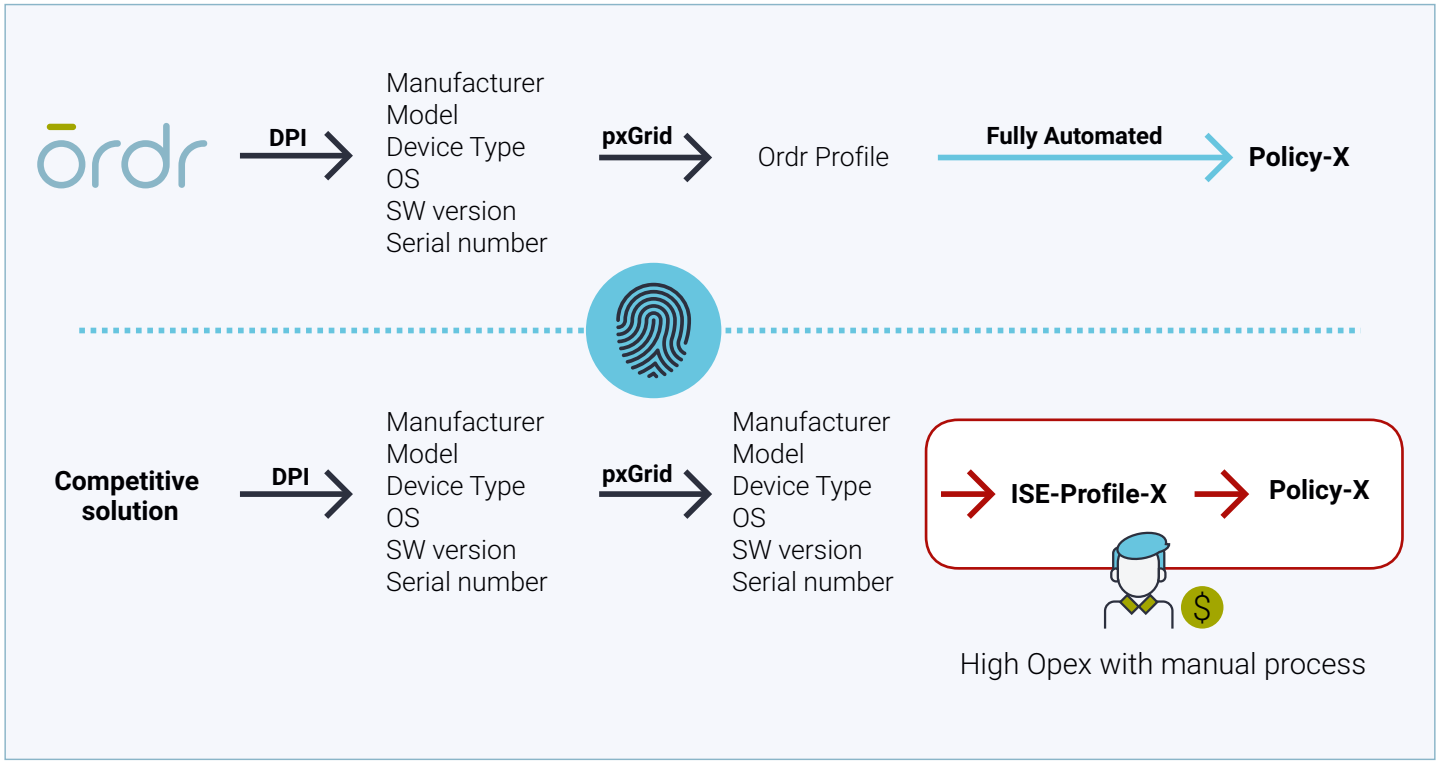

Figure 4: Ordr automatically translates device profiles into Cisco ISE policies

3. Flexible and practical segmentation policy generation

Ordr's Device Profiles are designed to aid segmentation and thus offer detailed grouping structures. Device profiles are based on two primary factors:

- **"what the device is"** - granular details include make, model, software operating system and more
- **"how it normally behaves/communicates"** - in Ordr, we call this the Flow Genome, the behavioral profiling or baseline of device communication patterns within a customer's environment.

Using Ordr, security and networking teams can define flexible and practical Cisco ISE segmentation policies based on type, behavior, location, business purpose and other network, security or device attributes.

For example, Axis P3364 IP cameras are classified as Physical Security Devices. But depending on their attributes, there may be a variety of different profiles of Axis IP Cameras. With Ordr, organizations can define separate policies for an Axis IP camera used in the reception area of an enterprise versus one used in a high-security lab.

Different policies can be applied when the risk association is different, allowing for a meaningful way of doing segmentation, and as alluded to earlier, Ordr automatically generates these Cisco ISE policies.

Competitive IoT security vendors create broad device profiles without any type of group hierarchy, and without context from an organization's actual network. For example, one competitive vendor identifies default behavior and common ports for devices across their customers, and then defines very generic, pre-built ACLs (access control lists) based on these insights. Because this pre-built ACLs needs to work for any customer, the ACL typically does not specify details like destination allowed. For example, if IP cameras were profiled using port HTTP (TCP/80), their suggested policy by competitive vendors would allow this IP camera to communicate with any destination including the Internet, using TCP ports.

In contrast, as described in Figure 5, Ordr segmentation policies are more deterministic, based on the source and destination specific to normal, sanctioned communications for a specific customer.

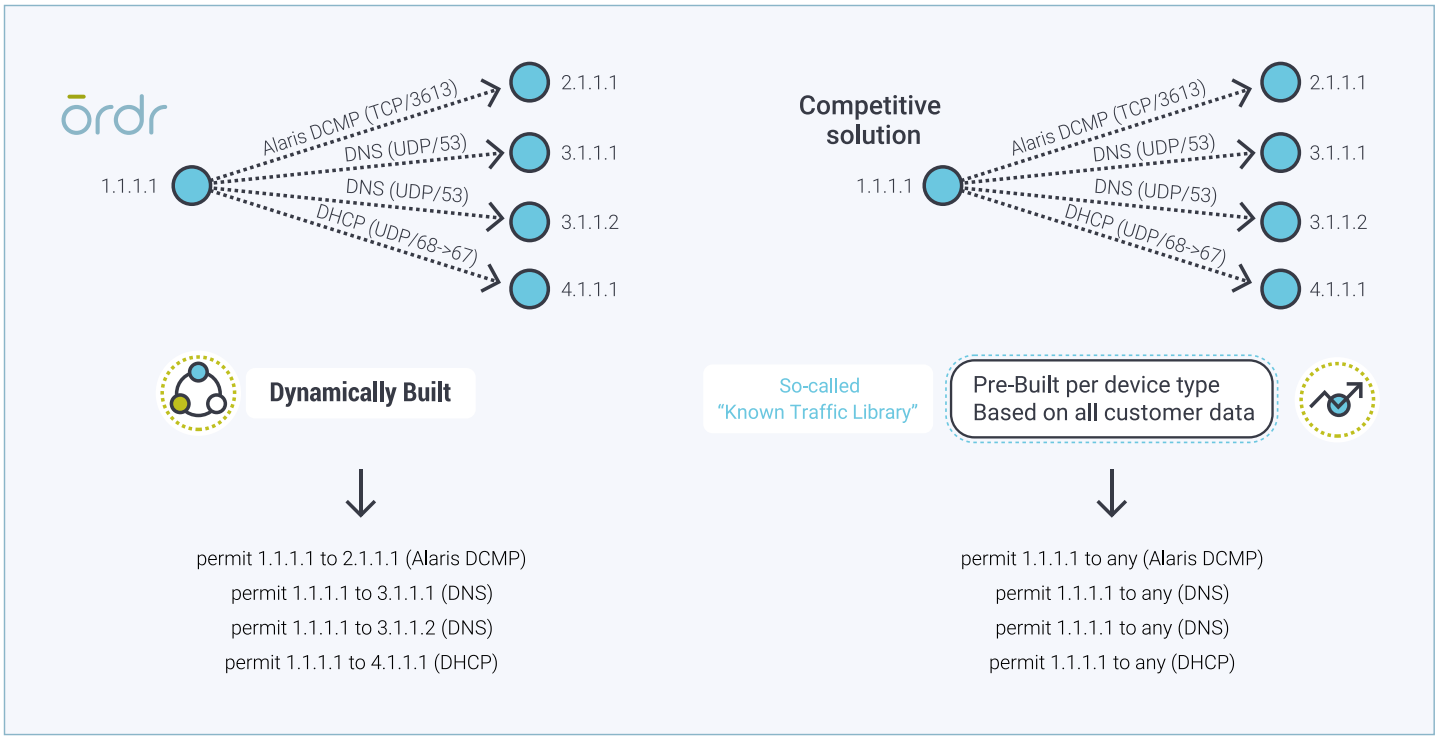

Figure 5: Ordr delivers flexible and practical segmentation policies unlike competitive solutions

In summary, Ordr brings many benefits to Cisco ISE deployments. Ordr provides day 0 return-on investment with its granular visibility of all connected devices, and day 2 operational benefits of opex reduction from continuous profiling and automated policy creation. Any organization with critical IoT and digital OT systems that is using or exploring Cisco ISE will dramatically benefit by adopting the Ordr SCE.

About Ordr

Ordr secures the millions of enterprise IoT and unmanaged devices such as manufacturing machines, building systems, medical equipment, printers, and more that run within global networks. The Ordr Systems Control Engine uses machine learning to automatically discover and classify every IoT and unmanaged device, map all communications, detect and prioritize vulnerabilities, and then proactively secure each device through dynamic policy generation and segmentation. Organizations use Ordr to discover their devices, track usage, achieve proactive protection, and compliance. For more information about Ordr, go to www.ordr.net.