ordr

ENHANCED DEVICE VISIBILITY

FOR CISCO ISE

© 2022 ORDR, INC.

SOLUTION PAPER

NETWORK SEGMENTATION IS THE BEST WAY TO SECURE IOT

HOWEVER IT IS TOO COMPLEX TO BE EFFECTIVE

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:

- *Which devices are in the environment and what is their function or role in the organization?*
- *What is normal versus abnormal communications between devices?*
- *Which devices are high risk, vulnerable or non-compliant and require quarantine and 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 devices be sufficiently segmented to provide protection without service disruption?*
- *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 click on a malicious email can disrupt business operations and seg- mentation projects can be stalled due to the sheer complexity, time, and costs to implement and manage.

WHY IoT SECURITY SHOULD BE A TOP PRIORITY

To the cybercriminal world, unprotected IoT devices represent a back door into your operations. Cyberattacks are launched to ferret weak and vulnerable targets leading to data exfiltration or hijack to solicit ransom. Since IoT devices are often difficult or impossible to individually secure they are easy prey with high financial reward.

There are a growing number of examples where these breaches resulted in debilitating consequences.

- *Target was breached through its HVAC system*
- *WannaCry took medical equipment offline and caused over 65 hospitals to shut down*
- *The Mirai and newer HNS viruses compromised cameras in scale*
- *NotPetya hit a broad set of vulnerable devices that impacted business operations globally*

© 2022 ORDR, INC.

ORDR MAKES SEGMENTATION FOR IOT SECURITY PRETTY DARN EASY

THIS IS A BOLD STATEMENT AND IT IS TRUE

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. 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.

WHAT DOES ORDR DO FOR CISCO ISE?

Cisco Identity Services Engine (ISE) provides endpoint visibility and identity-based access control for the Enterprise. To make these technologies effective for IoT requires additional intelligence and automation. That is where Ordr comes into the picture.

The Ordr Systems Control Engine (SCE) helps you to optimize your Cisco ISE investment to deliver effective IoT security. Its device classification, network awareness, security intelligence, and ability to auto-generate enforcement rules simplifies the process of creating, provisioning, and managing your IoT segmentation policy.

ORDR AND CISCO ISE INTEGRATION

The combination of Ordr and Cisco ISE simplifies the tasks that often overwhelm and stall IoT security initiatives by:

- *Automating IoT inventory discovery, classification, and categorization, and sharing detailed device context with Cisco ISE*
- *Providing rich analytics about the behavior of all devices that guides segmentation design, streamlines the segmentation implementation, and audits the result to assure accuracy and effectiveness*
- *Accelerating Cisco ISE deployments with powerful yet easy-to-use tools that provide accurate information and automate steps that are traditionally error-prone and labor intensive*

Businesses using the Ordr SCE have been able to dramatically reduce FTE hours as well as the time required to move their projects forward.

The Ordr and Cisco ISE integrated solution makes it easy to get rich visibility of IoT devices and simplify segmentation projects. The solution completely automates the process of implementing software defined microsegmentation to provide more precise controls for every IoT device in the network. Continuous, multi-level security monitoring of all devices communications allows Ordr to detect anomalous behavior, as well as control network access based on vulnerability, threat, and risk ratings (Threat-Centric NAC). The Ordr SCE also integrates with Cisco ISE to streamline the process of blacklisting unauthorized devices and flows in the network (Rapid Threat Containment).

Any organization with critical IoT and digital OT systems that is also using or exploring Cisco ISE will dramat- ically benefit by adopting the Ordr SCE.

© 2022 ORDR, INC.

INVENTORIES DEVICES AUTOMATICALLY

The Ordr SCE makes it easy to determine what IoT devices are in an organization and where they are located. Once discovered and classified, the SCE audits the environment to ensure devices are moved to the proper network segments. The Ordr SCE accomplishes this by:

- *Learning device details such as the manufacturer, model number, and software versions of the IoT devices*
- *Deep application inspection and behavior analysis*
- *Dynamic grouping of devices by type and purpose*
- *Identifying which network segment each device is connected and the segments of its communication peers*

The solution uses passive inspection of devices and their communication patterns, providing detailed information about each device and the protocols and applications they speak. This information is augmented with real-time network data (such as the switch or wireless ingress point, or the current VLAN and subnet) and real-time risk scoring based on observed threats and vulnerabilities. The consolidated results are then shared with Cisco ISE so operations staff have comprehensive up-to-date intelligence of every IoT device in the enterprise.

The Ordr SCE classifies devices, placing them into groups based on type, behavior, and business purpose. For example, Alaris Infusion Pumps are grouped together and are classified as Medical Devices. Axis P3364 IP cameras are classified as Physical Security Devices. The Ordr SCE shares the classification information with Cisco ISE making it easier to determine the access policy to apply based on a device's business function. This same function allows easy auditing of the applied access policy.

PROVIDES SEGMENTATION ANALYTICS AUTOMATICALLY

You need to collect and analyze a multitude of data to create segmentation policies. The Ordr SCE automates the labor-intensive work required for network segmentation such as:

- *Identifying and tracking the conversations between devices and networks*
- *Highlighting cross-domain and internal versus external communications*
- *Detecting and blocking anomalous communications between devices*
- *Deploying firewall policies to control traffic between network boundaries*
- *Keeping inventory and policy information consistent across security, IT, and device management stakeholders*

The Ordr SCE tracks all the communications on the network and correlates it with the device inventory. Comprehensive behavioral analytics determines normal versus abnormal communication patterns for each IoT and digital OT device. The solution also learns the network topology of the environment (VLANs, subnets, routing) and the access-layer connectivity graph (switch/port and wireless AP/SSID assignments). All this information is stored in an optimized database inclusive of device, flow, expected behavior, and topology objects. The graphical user interface offers an exceptional presentation layer and workflow process to easily analyze this information and quickly determine communication mappings based on devices, topology, and risk.

© 2022 ORDR, INC.

PROTECTS IOT WITH MICROSEGMENTATION

With technologies such as the SCE you can build effective network segmentation for IoT. Furthermore, the Ordr SCE enables the deployment of more finite and secure microsegmentation—in essence, a very exclusive and secure segment within a segment. Microsegmentation is the most effective approach to protect IoT as it allows enforcement of policies down to the switchport or wireless controller where the device connects to the network. These are precise access controls specific to each device. 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. ***The Ordr SCE makes it easy to implement microsegmentation by:***

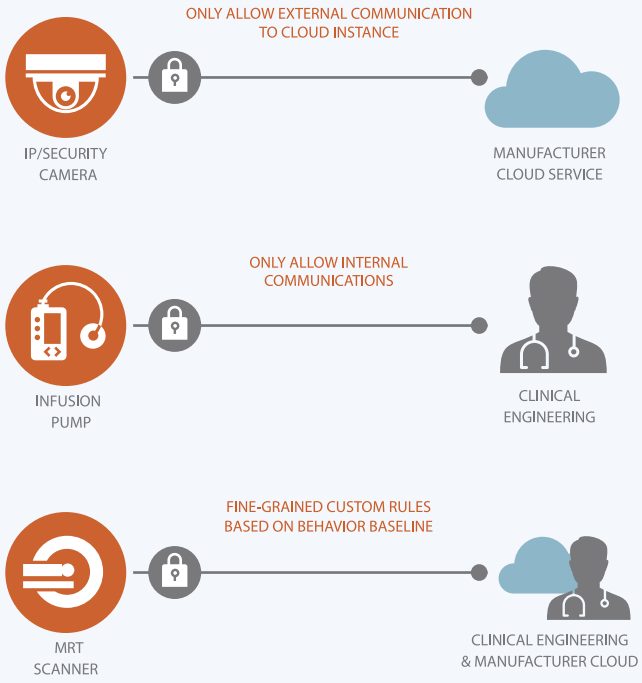
- *Creating precise access policies for each IoT device based on learned, approved communications*
- *Enforcing policies using your existing network where your devices are connected*
- *Supporting a wide range of network and security equipment including Cisco, Meraki, HPE-Aruba, Extreme, Brocade, Palo Alto, and Fortinet*

The policies learned and approved in the Ordr SCE can be used in conjunction with Cisco ISE to allow the enterprise to quickly and proactively reduce the exposed attack surface area for critical and at-risk devices without requiring a network redesign.

SEGMENTATION VS MICROSEGMENTATION

When you protect IoT with network segmentation, devices are segregated based on business purpose by placing them in different network VLANs. For example, there are network VLANs for physical security devices, facilities equipment, guest devices, manufacturing line equipment, and medical devices. Each VLAN is assumed to be secure and firewalls are used to protect each VLAN by controlling inbound and outbound communications.

Microsegmentation takes that notion one step further by protecting devices from other systems in the same network segment in addition to systems outside of their network. It is based on the concept of Zero Trust and is the most effective way to protect devices. IoT hosts are purpose-built devices that adhere to a predefined set of limited communication patterns, so they are well suited to be protected with microsegmentation. Ordr Systems Control Engine is uniquely able to automate microsegmentation provisioning.



© 2022 ORDR, INC.

ORDR AND CISCO ISE IN ACTION

The diagram illustrates the integration of the Ordr SCE 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.

Providing advanced IoT device information to ISE is only one piece of the puzzle. To move to microsegmen- tation and the enforcement of policies, NAC administrators must understand which traffic to allow and deny. The SCE Analytics Server provides this insight to Cisco ISE and facilitates the provisioning of segmentation policy.

The Ordr Systems Control Enging'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. Here the SCE can notify Cisco ISE of at-risk, vulnera- ble, and compromised devices to trigger the necessary quarantine and remediation response.

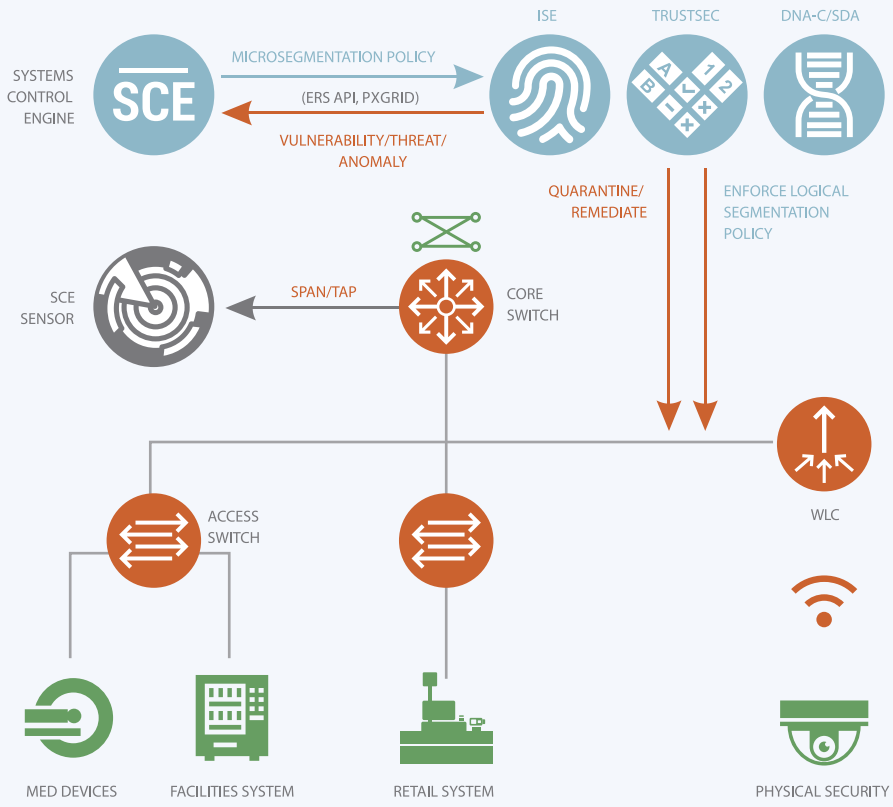
CISCO ISE + ORDR SYSTEMS CONTROL ENGINE

1

1. Dynamic IoT device classification
2. Automated flow, application, and behavior analysis
3. Agentless security assessment

2

1. Increased IoT device visibility
2. Automated generation of access and segmentation policies based on observed flows
3. Blacklist & quarantine infected/ compromised devices



© 2022 ORDR, INC.

SUMMARY

The Ordr Systems Control Engine compliments and advances the power of Cisco ISE solution by providing:

- *Advanced classification of IoT devices to augment ISE visibility and policy creation*
- *Vulnerability, threat assessment and risk ratings for IoT devices to quickly alert ISE of at-risk and vulnerable devices to automate quarantine and remediation functions*
- *Detailed flow analysis to understand normal versus abnormal communication behavior and notify Cisco ISE of compromised endpoints, again automating the process of threat mitigation*
- *Dynamic translation of IoT approved behavior into ISE and group-based network segmentation and microsegmentation policies*

© 2022 ORDR, INC.