ōrdr

Deploying Effective Microsegmentation To Protect Connected Devices

The volume and severity of cybersecurity threats against your network are increasing. Key incentives fueling these attacks include the exfiltration of personal data, trade secrets, valuable research data, and other confidential information that can be sold or traded on the black market. Commandeering systems for ransom or disrupting services to tarnish an organization's reputation to elicit competitive outcomes can also be motivators. Beyond a highly organized framework of cybercriminals, governments have also entered the fray to advance political agendas or inflict cyberterrorism.

Beyond the doom-and-gloom mantra, the fact remains that IoT devices represent prime targets for cyberattack. These devices are not like the common multifunction user device–servers, workstations and mobile devices–that receive constant OS updates and patches, are fortified with the current endpoint security technology, and typically require a credential to connect to the network.

ORDR SOLUTION PAPER

These devices are usually on the opposite end of the spectrum in that they are built for a specific purpose using a lean operating system and connect to the network without user intervention or credentials. IoT devices commonly lack advanced security controls and protections such as anti-malware or continuous threat monitoring. They may go unpatched for their lifetime, or else patched infrequently after long service intervals. The mere act of vulnerability scanning may disrupt their operation.

Organizations that are aware of the deficiencies in connected device security may organize teams to track assets and monitor them for vulnerabilities. These teams may set security standards on new purchases and attempt to enforce regular service intervals or maintenance windows to patch exposed devices, often only after officially declared vulnerable by the manufacturer or other security notification service. Due diligence to reduce exposure is critical, but most organizations concede that these measures are insufficient to shield the devices.

This is where segmentation can provide the needed protections for devices that cannot adequately defend themselves. Segmentation is the concept of placing devices of like type or function into the same physical or logical network segment. Communications between segments is limited, but typically little or no restrictions exist on lateral communications within the segment. Consequently, compromise of one connected device allows infection or compromise of all other IoT devices of same type even when basic segmentation is employed. Examples of widespread attacks impacting IoT devices include the Mirai Botnet, WannaCry, and NotPetya.

Liberal communications within and between segments is a key reason why IoT devices require microsegmentation. Microsegmentation is the concept of segmenting communications to a fine-grained level, ideally to the minimalist communication required for proper operation and management. Segmentation is often useful to separate traffic at a more global level, for example, to separate guest users from internal networks, or to establish PCI zones. Network segmentation can also prove beneficial when users and devices within a segment have a wide range of communication requirements within the group. IoT devices, on the other hand, have very prescriptive communication requirements and lend themselves to microsegmentation.

As a simple example, consider a connected sensor/controller connected to the network. This device requires DHCP and DNS to acquire an address to find and communicate with its “master” server on the network. It does not need to communicate with its peers. It may need to be accessible from a monitoring station that collects data or from a remote station for troubleshooting, but all other communications should be considered foreign and unauthorized. This is an ideal use case for the application of microsegmentation. It would be impractical to force the finite set of destination devices into the same network segment—most are likely in the data center or remote (support vendor, for example). Placing all the IoT sensors/controllers in the same network segment also sounds like a good idea, but then leaves each exposed to the other (compromise one, compromise all). Through microsegmentation, communication can be limited to only the core requirements of the IoT device and the business.

While segmentation or even microsegmentation may be the answer, little has been offered to the industry in the way of tooling to enable organizations to efficiently and effectively implement segmentation.

Why Ordr?

The Ordr Systems Control Engine (SCE) provides the tools needed to protect network-connected devices and systems devices—both from the perspective of "what do I have and is it vulnerable?" as well as "how do I achieve microsegmentation?"

First, Ordr SCE automates the discovery and accurate classification and grouping of all connected devices and systems. The Ordr SCE validates the vulnerability, threat, and risk level of each device through an extensive series of security checks. The embedded security analytics compares the classified endpoints against a suite of industry threat intelligence feeds, network vulnerability databases, ICSA–ICS-CERT advisories, FDA lookups for medical device recalls and alerts, as well as comparison to MDS2 forms for manufacturer-published vulnerability data. Proactive security monitoring detects the use of weak ciphers and non-trustworthy certificates. Results are fed to your security monitoring system, asset management systems are updated, and remediation is triggered through quarantine or service ticketing.

Secondly, the Ordr SCE watches the actual traffic of each device and learns the baseline of the minimal traffic required by the device to properly operate. Communications to other IP/VLAN segments within the organization are easily visualized, as well as communications to external networks. The Ordr SCE automatically categorizes these external and internal communications as foreign and domestic and compares them against known malicious sites through URL/IP reputation analysis. Traffic is constantly monitored for active threats such as attempts to access command and control and other bad actors.

The result of this automated flow and threat analysis is the establishment of prescriptive communication baselines for each device and devices within a device class (for example, AllenBradley-PLC, Hospira-Symbiq Infusion System, or Axis-Network Camera). Once established, the Ordr SCE converts these baselines into microsegmentation policies that can be manually or automatically applied directly to your network and security devices, or via your NAC solution.

Since the Ordr SCE continuously validates all communications, it is able to provide alerts if devices are behaving outside expected and approved baselines. This allows effective, real time detection of compromise as well as an audit of enforced policies to answer the questions:

- Are my connected devices behaving as expected?
- Are my enforcement policies working as expected?

The Ordr Systems Control Engine is the only solution of its kind to provide automated provisioning of microsegmentation policy across wired switches, wireless controllers and access points, firewalls, and network access control (NAC) solutions from all leading vendors. It is highly network-aware, so not only does it understand which policies to apply, but where and how to apply them. In summary, the Ordr SCE quickly determines which devices are on the network and what they should be allowed to do, and then automatically translates this knowledge to a language your network understands to provide effective microsegmentation.

ACL-BASED MICROSEGMENTATION

In the following simple example, Baxter 35700BAX Sigma Spectrum Infusion Pumps have been accurately classified by the Ordr SCE and permissible traffic policy learned through proactive monitoring. The derived ACL establishes a zero-trust boundary at the point of network entry and communications restricted to specific monitoring and data collection servers located elsewhere in the network. The Ordr SCE automatically generates ACLs in the "language" understood by the target system (switches, wireless controllers/access points, firewalls, NAC policy servers, etc.).

```
ip access-list extended CPN-Baxter-35700BAX-SpectrumInfusionPump-in
  permit tcp any host 10.0.60.28
  permit tcp any host 10.0.60.29
  permit tcp any host 10.254.13.52
  permit udp any host 10.254.13.52
  permit tcp any host 192.168.101.181 eq 80
  permit icmp any any
  permit udp any eq bootpc any
  permit udp any eq bootps any
  deny ip any any

ip access-list extended CPN-Baxter-35700BAX-SpectrumInfusionPump-out
  permit tcp host 10.0.60.28 any
  permit tcp host 10.0.60.29 any
  permit tcp host 10.254.13.52 any
  permit udp host 10.254.13.52 any
  permit tcp host 192.168.101.181 eq 80 any
  permit icmp any any
  permit udp any eq bootpc any
  permit udp any eq bootps any
  deny ip any any
```

TAG-BASED MICROSEGMENTATION

This is an example of the same policy, but for use with group-based enforcement devices or microsegmentation services. Typical solutions that employ group-based policy include firewalls and NAC policy servers. Again, the Ordr SCE auto-generates the policy in the language understood by the target system. Enforcement policy can be applied to a single target or multiple targets using the same or different enforcement method based on an organization's requirements.

Source Group
Group Name:
Baxter-35700BAX-Spectrum Infusion Pump
Group Value: 257
IP Address List:
192.168.106.18, 192.168.106.19,
192.168.106.20, 192.168.106.21

Target Group 1
Group Value: 258
IP Address List: 10.0.60.28, 10.0.60.29

Target Group 2
Group Value: 260
IP Address List: 192.168.101.181

Group-based ACLs

- CPN-257-To-258:
  - permit tcp
- CPN-257-To-259:
  - permit tcp dst
  - permit udp
- CPN-257-To-260:
  - permit tcp dst eq 80
- CPN-260-To-257:
  - permit tcp src eq 80

ōrdr

take control.

info@ordr.net
www.ordr.net

2445 Augustine Drive Suite 601
Santa Clara, CA 95054