Ordr and Palo Alto Networks® Joint Solution Brief

Take Control of Your Connected IoT and OT Systems

IOT IS EXPANDING FASTER THAN IT CAN BE SECURED

IoT and OT devices present unique challenges to access control. Common traits include:

- No user, No authentication
- Highly vulnerable – Typically run rudimentary or minimized versions of legacy operating systems without basic client protection software
- Closed systems – Minimal or no patching capabilities to defend themselves; installation of posture or other device management agents is rarely an option
- Susceptible to scans – Direct interrogation by profiling and other security assessment tools risky due to the fragile nature of device's OS or network stack

Conclusion: Critical devices are vulnerable to service disruption, data theft, or compromise for ransom or serve as a launchpad for other attacks.

TAKE CONTROL OF YOUR ENTERPRISE

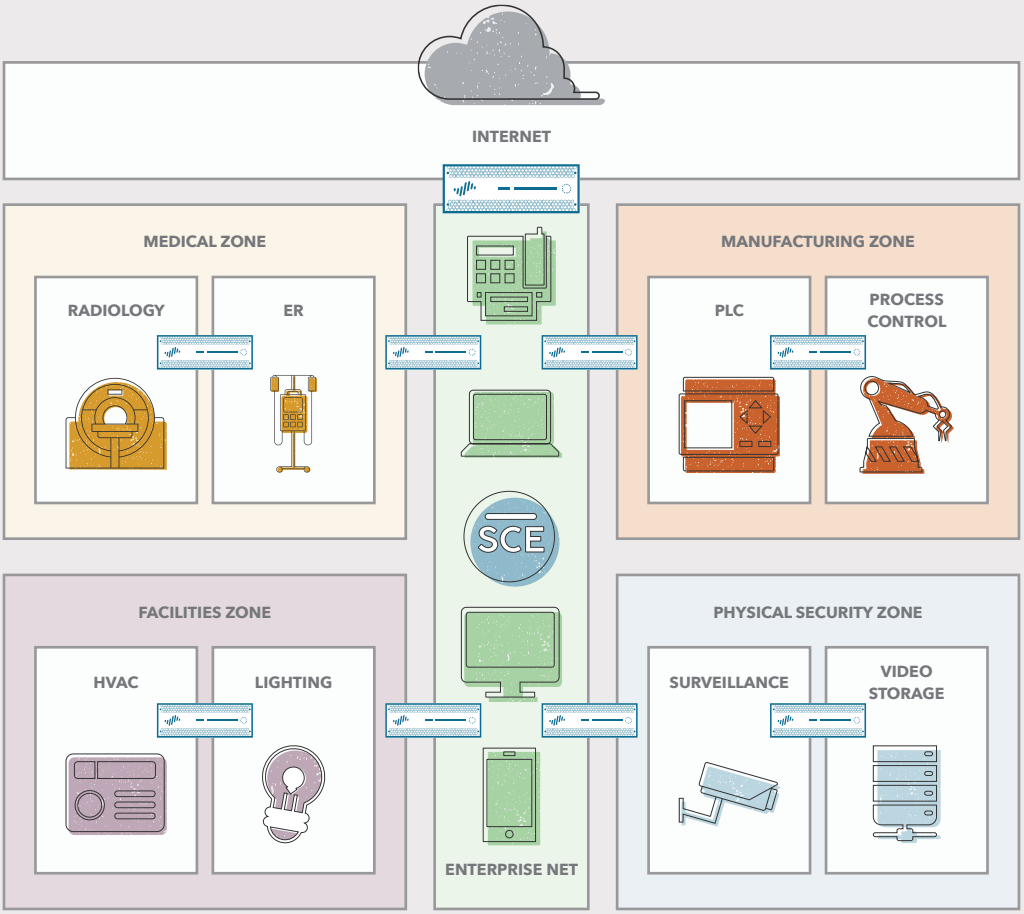
Palo Alto Networks and Ordr have joined forces to provide the most effective solution to identify, classify, and protect IoT and digital OT devices from unauthorized access and cyberattack:

- Passively discovers every connected device with high-definition detail–without the use of agents
- Automatically classifies devices with tags and maintains membership
- Quickly spots vulnerable and compromised devices so they can be quarantined
- Rapidly implements zone-based segmentation per NIST and IEC 62443 with AI-created firewall policies
- Continuously monitors device security risk and behavior
- Verifies segmentation policy is effective using simple, graphical tools

Take Control with Ordr and Palo Alto Networks

Ordr:

1. Identifies devices by zone
2. Groups devices with tags in NGFW
3. Determines minimum communications required across zones
4. Provisions NGFW policies in Panorama
5. NGFWs enforces zone-based policies for enterprise



The most effective means to protect IoT and digital OT devices is through IEC microsegmentation and Zero Trust policy rules. Palo Alto Networks Next-Generation Firewalls (NGFWs) provide scalable policy enforcement and segmentation controls for the enterprise. Ordr Systems Control Engine (SCE) discovers, classifies and groups all devices and automatically maps them into their respective zones, areas, and cells using PAN-OS tags, and then dynamically generates NGFW security policy rules using these tags to deliver streamlined microsegmentation.

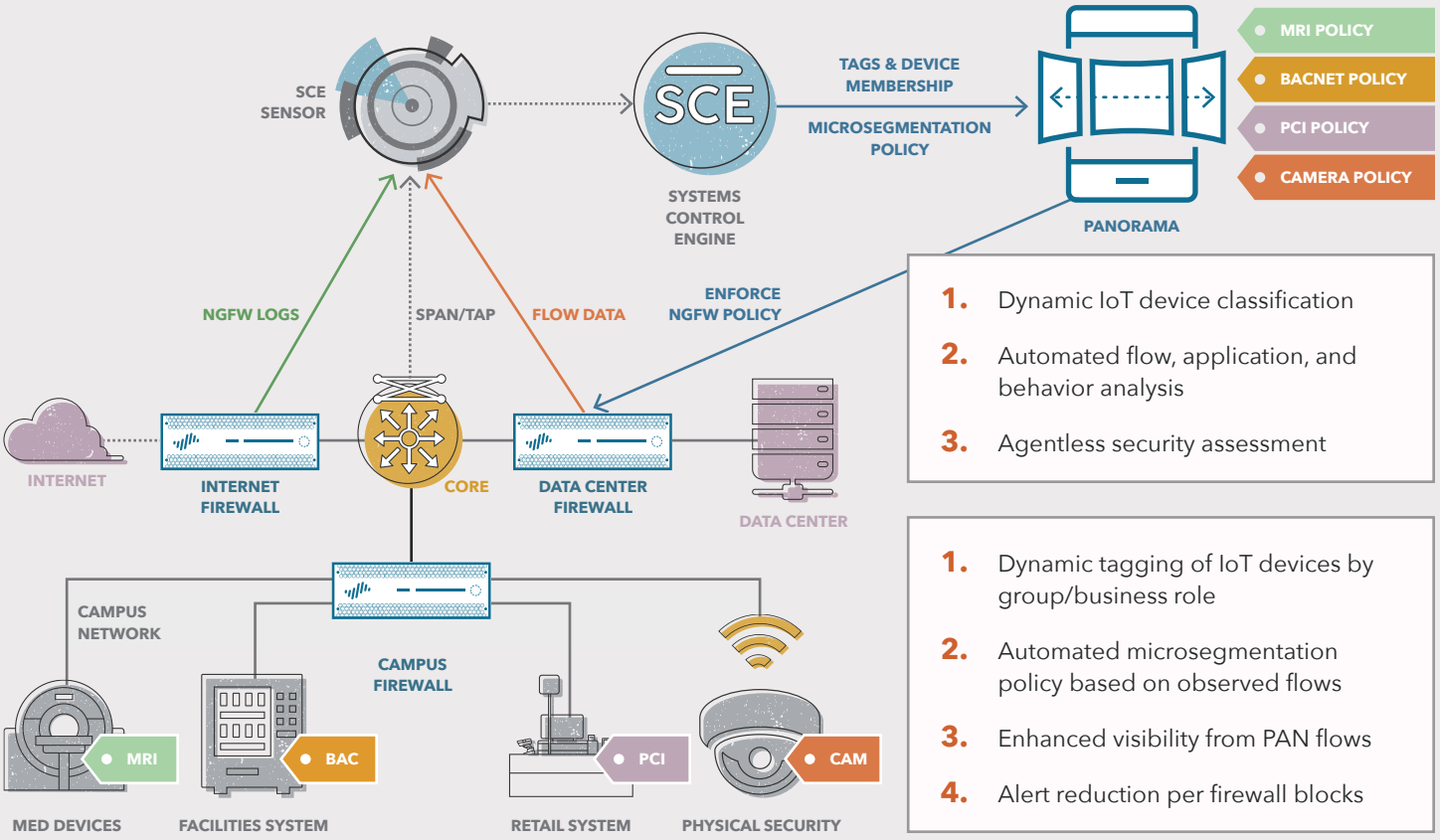
For example, building automation devices are seamlessly mapped to the Facilities Zone and facility devices within this zone are further segmented from each other. Security policy rules are enforced by Palo Alto Networks NGFWs to restrict access between zones, areas, and cells based on the minimum access required to allow devices to properly function while protecting them from insider or outsider attack. An HVAC system can talk with a trusted smart-building controller using approved protocols and applications by App-ID such as BACnet, but blocked from communicating to the Internet or to another HVAC system.

Ordr SCE and Panorama in Action

Ordr SCE integrates directly with the NGFW or Panorama for multi-NGFW tagging and policy enforcement. Ordr SCE Sensors provide agentless, passive data collection which feeds Ordr SCE. Sensors may be centralized or distributed based on collection requirements. NGFWs can also act as sensors by sending rich flow data used to enhance visibility of localized traffic.

Ordr SCE analyzes the data to automatically discover and classify all OT, IoT, and non-IoT devices. It then maps groups of devices to existing PAN-OS tags or new ones auto-generated by Ordr SCE. When new devices are connected to the network, they are automatically classified and updated in Panorama and NGFWs with the proper tag membership. Through its network and device awareness, Ordr SCE maintains current IP address information for tagged devices in NGFWs.

THE PALO ALTO NETWORKS + ORDR POWERED SOLUTION



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

1. Dynamic tagging of IoT devices by group/business role
2. Automated microsegmentation policy based on observed flows
3. Enhanced visibility from PAN flows
4. Alert reduction per firewall blocks

Providing advanced IoT device classification and tagging updates to NGFWs is only one piece of the puzzle. To move to microsegmentation and the enforcement of Zero Trust policy rules, administrators must understand which traffic to allow and deny. Ordr SCE provides this insight to Panorama and fully automates the provisioning of security and segmentation policy. Alternatively, firewall administrators may leverage the auto-generated security policies as a reference to simplify manual update to security policy. Ordr SCE policy rules are translated into the syntax required to directly update NGFWs.

Ordr 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. Here Ordr SCE can reassign at-risk, vulnerable, and compromised devices to quarantine VLANs that map to restricted firewall zones. Attempts to access malware and other malicious sites are detected and correlated against NGFW logs to reduce criticality ratings for mitigated threats.

Together, Ordr and Palo Alto Networks allow you to Take Control of your IOT and OT security by implementing segmentation across your hyper-connected enterprise.

About Ordr

At Ordr, we're energized by the explosive growth in network-connected systems and devices. We recognize the tremendous opportunities that this represents for the hyper-connected enterprise. Improved delivery of care, efficient logistics and operations, quality enhancements in manufacturing, more stable and intelligent business-critical systems. We're energized because we give you the power to take control and realize these myriad opportunities.

Learn more at **www.ordr.net**.

About Palo Alto Networks

We are the global cybersecurity leader, known for always challenging the security status quo. Our mission is to protect our way of life in the digital age by preventing successful cyberattacks. This has given us the privilege of safely enabling tens of thousands of organizations and their customers. Our pioneering Security Operating Platform emboldens their digital transformation with continuous innovation that seizes the latest breakthroughs in security, automation, and analytics. By delivering a true platform and empowering a growing ecosystem of change-makers like us, we provide highly effective and innovative cybersecurity across clouds, networks, and mobile devices.

Find out more at **www.paloaltonetworks.com**.