Ordr SCE App for Cortex™ by Palo Alto Networks

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

The Ordr Systems Control Engine (SCE) app on Cortex provides the most effective solution to identify, classify, regulate, and secure IoT and digital OT devices from unauthorized access and cyberattack:

- Passively discovers every connected device with high-definition detail and without agents
- Automatically classifies devices with tags and maintains membership
- Quickly spots vulnerable and compromised devices so they can be quarantined
- Rapidly deploys zone-based segmentation per NIST and IEC 62443 with AI-created next-generation firewall policies
- Continuously monitors device security risk, application, and behavior with data from Cortex Data Lake
- Verifies segmentation policy is effective using simple, graphical tools

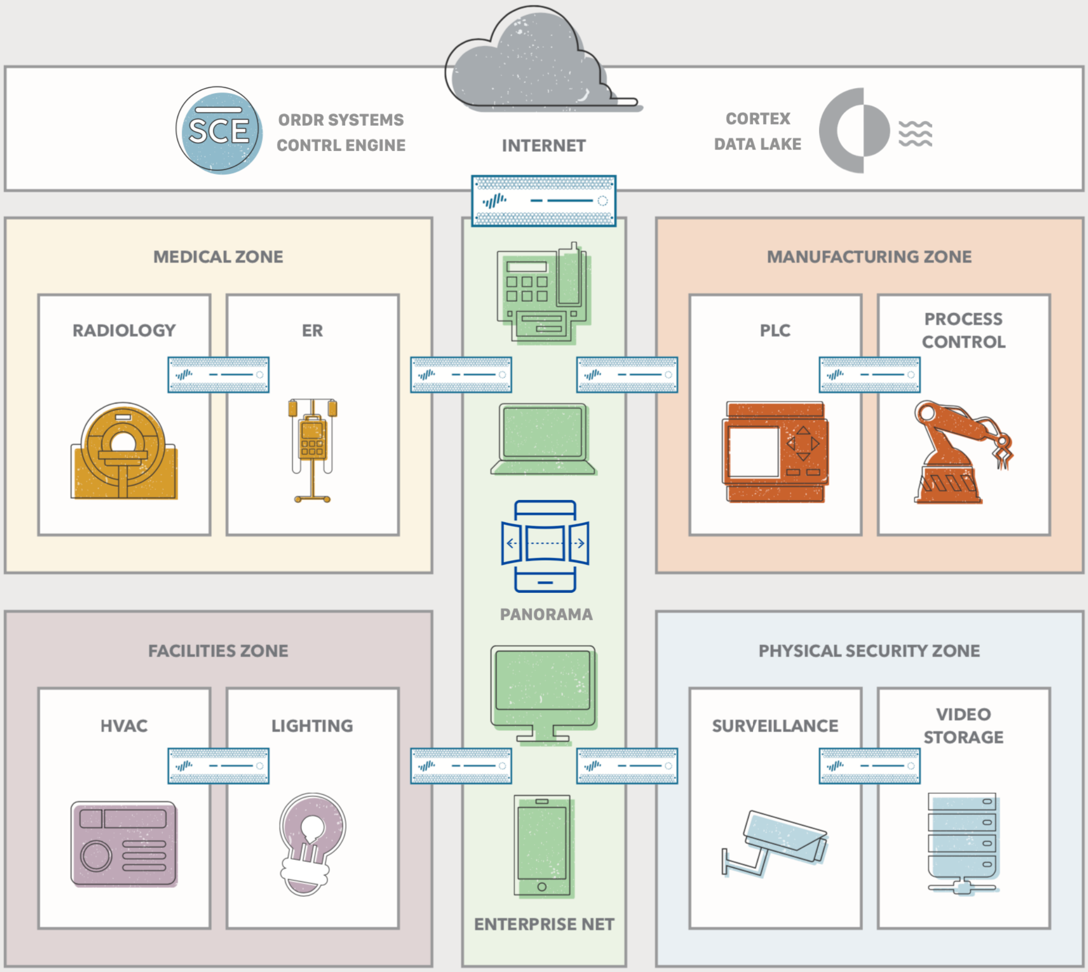
Ordr and Cortex Closed-Loop Security

Cortex:

1. Receives rich data analytics from NGFWs
2. Feeds Ordr SCE with Ordr-enhanced app-ids

Ordr:

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



The most effective means to protect IoT and digital OT devices is through IEC 62443 zone-based segmentation and Zero Trust policy rules. Palo Alto Networks next-generation firewalls provide scalable policy enforcement and zone controls for the enterprise. Ordr Systems Control Engine 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 firewall security policy rules using these tags to deliver streamlined microsegmentation.

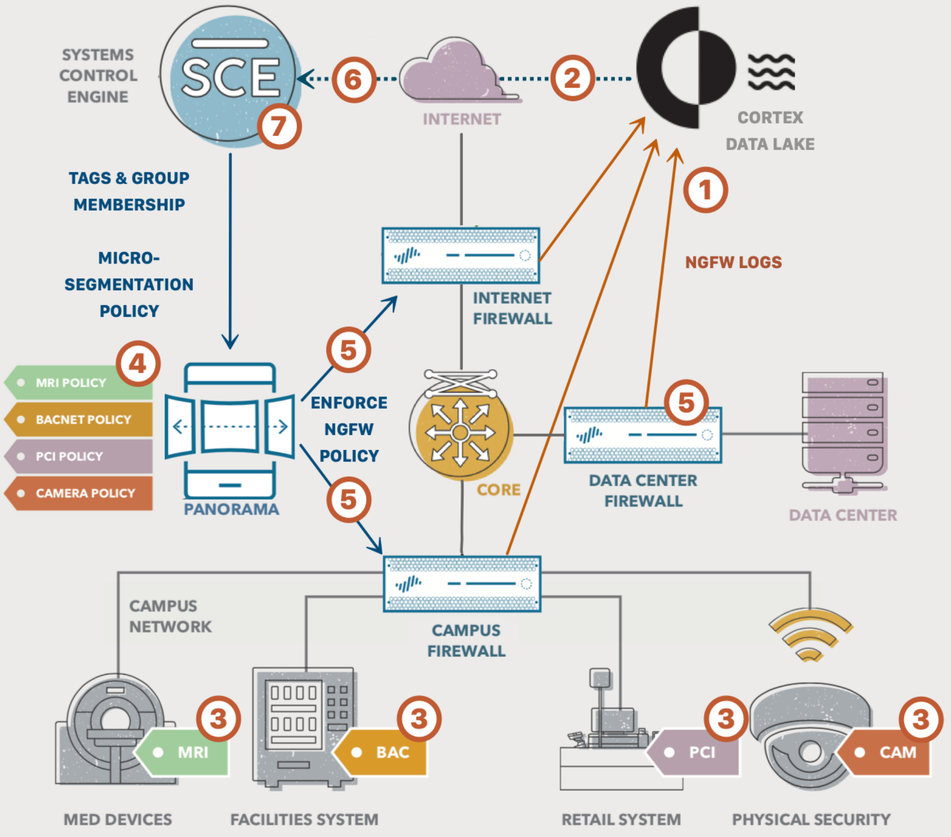
For example, building automation devices are seamlessly mapped to the Facilities Zone and facility devices within this zone are further segmented from each other. Security policy rules are enforced by Palo Alto Networks next-generation firewalls to restrict access between zones, areas, and cells based 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 Cortex in Action

Ordr SCE integrates natively with Palo Alto Networks next-generation firewall (NGFW) or Panorama for multi-NGFW tagging and policy enforcement. Next-generation firewalls collect rich traffic and security analytics into Cortex Data Lake. Next-generation firewalls also enforce zone-based segmentation policy to protect all devices inclusive of IoT and digital OT in the enterprise campus or manufacturing plant, the data center, as well as securing communications traversing the Internet edge.

Ordr SCE analyzes data in Cortex Data Lake 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 next-generation firewalls with the proper tag membership. Through its network and device awareness, Ordr SCE maintains current IP addressing for tagged devices in next-generation firewalls.

THE ORDR SCE APP FOR CORTEX



1. NGFWs DPI and traffic flows logged to Cortex Data Lake
2. Ordr SCE receives rich device and security analytics from Cortex Data Lake
3. Ordr SCE automates IoT/OT device classification, grouping and behavioral baselining
4. Dynamic tagging of devices by group/business role
5. Streamlined microsegmentation policy based on observed, approved flows
6. Enhanced security visibility from Cortex ecosystem
7. Alert reduction per firewall blocks

Providing advanced IoT device classification and tagging updates to next-generation firewalls 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 fully automate 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 Palo Alto Networks next-generation firewalls.

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 received from next-generation firewall logs in Cortex Data Lake. 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 next-generation firewall 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 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.

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.