ōrdr

Ordr Systems Control Engine

The Ordr Systems Control Engine (SCE) allows organizations to rapidly inventory every thing in your domain, classify it based on type and business function, and assess it for risk. It learns behaviors and creates device flow genomes, so you'll know what each device should be talking to. It protects using micro-segmentation to logically segregate groups of devices from any thing that's non-essential and can rapidly stop active threats and isolate compromised devices. Plus, it is non-disruptive to the device, the network, and the way you run your operations.

Product Feature Packages

Ordr Systems Control Engine (SCE)

The Ordr Systems Control Engine (SCE) is an IoT device security platform that will discover every connected device, profile device behavior and risks, and automate response. Ordr not only identifies devices with vulnerabilities, weak ciphers, weak certificates, and active threats, but also those that exhibit malicious or suspicious behaviors. Finally, Ordr automates action for security and networking teams, such as dynamically creating and enforcing microsegmentation policies for devices, or alerting and triggering a specific security or operational workflow.

ORDR CORE AND PREMIUM

Ordr offers a foundational and premium software package for organizations:

Ordr Core software delivers foundational device discovery, classification, and behavior analysis as well as risk profiling functionality.

Ordr Premium includes all of Ordr Core features in addition to automated actions to address risks, and advanced integrations with security and networking products.

	SOFTWARE PACKAGE	
	CORE	PREMIUM
What's on the network?		
Device discovery & classification	×	×
What are the devices doing?		
Device flow visibility (Who is speaking to whom?)	×	×
Connectivity analysis (Wired / Wireless / Serial)	×	×
Behavioral analysis (Baselining, Geo-location)	×	×
What is the business risk?		
Risk scoring	×	×
Manufacturing recalls / FDA advisories	×	×
Vulnerabilities (OS, Firmware)	×	×
Active scanning (OpenVas / nMap / Hydra)		×
Segmentation risk assessment	×	×
Endpoint assessment (WinRM / WMI)	×	×
Are there any potential cyber threats?		
IP / URL Threat Intelligence feeds	×	×
Lateral movement (IDS) detections	×	×
Lateral movement (IDS) detections with commercial sig feeds		×
Are assets being utilized efficiently?		
Medical Device Utilization	×	×
How to integrate with existing tools?		
Syslog, SNMP, import/export spreadsheet	×	×
Microsoft Active Directory	×	×
Configuration Management Database (CMDB)	×	×
IP Asset Management	×	×
Network Infrastructure (switches, wireless controllers)	×	×

ōrdr

		SOFTWARE PACKAGE	
BUSINESS OUTCOMES	CORE	PREMIUM	
Security Information Event Management (SIEM)	×	×	
Computerized Maintenance Management Systems (CMMS)		×	
Firewalls		×	
Vulnerability scanners		×	
Network Access Control (NAC)		×	
Network Management System (NMS)		×	
How to protect / harden the organization?			
Segmentation / Policy creation & enforcement (SASE, Network) via CLI & RBACLs		×	
Containment (Quarantine / allow / block)		×	
2 factor authorization		×	

SaaS or On-Premises Deployment Options

The Ordr Systems Control Engine supports multiple deployment models including Saas delivered, fully onpremises, private cloud, and MSP hosted. There are three key components of the system:

Systems Control Engine: SaaS managed service in the cloud or on-premises/ private cloud-hosted hardware ppliances or software appliances in the datacenter that perform behavioral analysis, identify anomalies, and act as the solution's management and policy decision point for the organization. **SCE Center:** Ordr-operated cloud service that helps in zero-touch provisioning of each deployment and keeps it up-to-date with the latest threat feeds and IoT device profiles.

SCE Sensor: Hardware appliances or software appliances that are deployed at the access, distribution or core layer of the network and receive SPAN, tap, or flow data in order to discover and track IoT devices and monitor communications in a completely passive fashion without any disturbance to operations.

Sensors and on-premises appliances can be delivered as software images or preinstalled on appliances.



ōrdr

Systems Control Engine Platforms

SCE is comprised of software running on VMware ESXi 6.0 and later or other hypervisor environments such as KVM that operates on customer-supplied equipment or Ordr supplied hardware appliances.

SCE supports several hardware options for on-premises analytics and sensors. Customers supplying their own hardware should follow similar resource specifications to handle equivalent device counts and packet processing rates. The appliances are big data platforms, optimized to store and process large amounts of information so they have abundant memory. High-availability and maximal scale (over 75,000 devices) can be achieved by deploying the SCE Analytics component in a 5-node cluster configuration consisting of two A2000-4R and three A1000-4R. Please see the table on the following page for detailed specifications of each model number.





ōrdr

	SCE AN		SCE SENSOR			
SPECIFICATIONS	A2000-4R	A1000-4R	S2000-4R	S1000-4R	\$500	S100
FORM FACTOR	1RU, D 20"	1RU, D 20"	1RU, D 20"	1RU, D 20"	H 2.75" x W 7.75" x D 7.75"	H 2.75" x W 7.75" x D 7.75"
CPU	Xeon ES- 2630V4 2.2G, 2 CPUs, 20 Cores, 40 Threads	Xeon ES- 2630V4 2.2G, 2 CPUs, 20 Cores, 40 Threads	Xeon ES- 2630V4 2.2G, 1 CPUs, 10 Cores, 20 Threads	Xeon ES- 2630V4 2.2G,1 CPUs, 10 Cores, 20 Threads	Atom C2550	Celeron
MEMORY	512GB	256GB	64GB	32GB	8GB	8GB
REDUNDANT POWER SUPPLY	Yes	Yes	Yes	Yes	No	No
POWER SUPPLY WATTAGE	Hot Swap 400 Watts AC	Hot Swap 400 Watts AC	Hot Swap 200 Watts AC	Hot Swap 200 Watts AC	60 Watts AC	60 Watts AC
HEAT DISSIPATION	1365 BTU/hr	1365 BTU/hr	682 BTU/hr	682 BTU/hr	205 BTU/hr	205 BTU/hr
SPAN/TAP INTERFACES	NA	NA	4x10/1Gbps SFP+	4x10/1Gbps SFP+	3x1Gbps RJ45	3x1Gbps RJ45
MANAGEMENT INTER- FACES	Redundant RJ45 Ports	Redundant RJ45 Ports	Redundant RJ45 Ports	Redundant RJ45 Ports	Single RJ45 Ports	Single RJ45 Ports
STORAGE CAPACITY	1TB	1TB	64GB	64GB	32GB	16GB
MAX DEVICES	75,000 * (Analytics Total)	NA	10,000 ** (Per Sensor)	10,000 ** (Per Sensor)	3,000 ** (Per Sensor)	500 ** (Per Sensor)
COMMENTS	Analytics appliance	Database appliance for large scale deployments (including 5-node cluster)	Large Sites, Integration Services, and Netflow Aggregation	Large Sites	Mid-sized Sites	Small Sites

* High-availability and greater scale (over 75,000 devices) can be achieved by deploying the SCE Analytics component in a 5-node cluster configuration consisting of two A2000-4R and three A1000-4R.

** Endpoint sizing guidelines are applicable to campus networks. For data center deployments and large TAP Aggregation scenarios it is recommended to use model S2000-4R sensors along with packet broker filtering.

ōrdr

info@ordr.net www.ordr.net

2445 Augustine Drive Suite 601 Santa Clara, CA 95054