



Leading Edge OT Cyber Visibility, Detection, and Response
When You Need it Most

Dragos Platform Overview

Sam Wilson
Kimberly Graham

Agenda

1. Dragos Platform Overview
2. What's New in Platform 2.1?
3. Platform Appliance Updates
4. Q&A



DRAGOS

Safeguarding Civilization

The Most Effective OT Security Tech Platform

Expertise integrated into software to reduce OT risk

A Community-Focused Mission

Skills, communications, & resources to strengthen the collective defense

Expert OT Intelligence & Service Resources

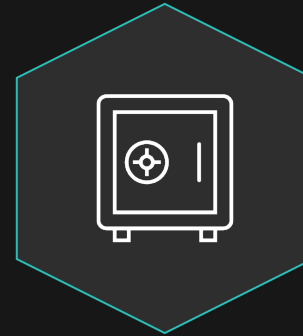
OT expert analysts, threat hunters, & responders to help you win the fight.

Key Challenges Managing OT Cyber Risk



What's running in my OT network?

- Identify crown jewel assets
- Create asset inventory
- Evaluate unusual changes



What should I do with this CVE?

- Simplify compliance
- Prioritize vulnerabilities
- Maximize remediation resources



Am I really compromised?

- See unauthorized IT-OT traffic
- Analyze file downloads
- Detect adversary behaviors



How can I respond in time?

- Analyze changes & forensic records
- Efficiently manage response & recovery
- Leverage prescriptive playbooks

Tell us your thoughts ...

DRAGOS PLATFORM

Expertise Integrated Into Software to Reduce OT Risk

OT THREAT
INTELLIGENCE



OT EXPERT
SERVICES



DRAGOS
PLATFORM



OT WATCH Dragos Managed Vulnerability Response, Hunting, & Incident Triage



VISIBILITY

Assets, Traffic, &
Vulnerabilities



DETECTION

Compromises &
Threat Behaviors



RESPONSE

Investigation Forensics
& Playbooks

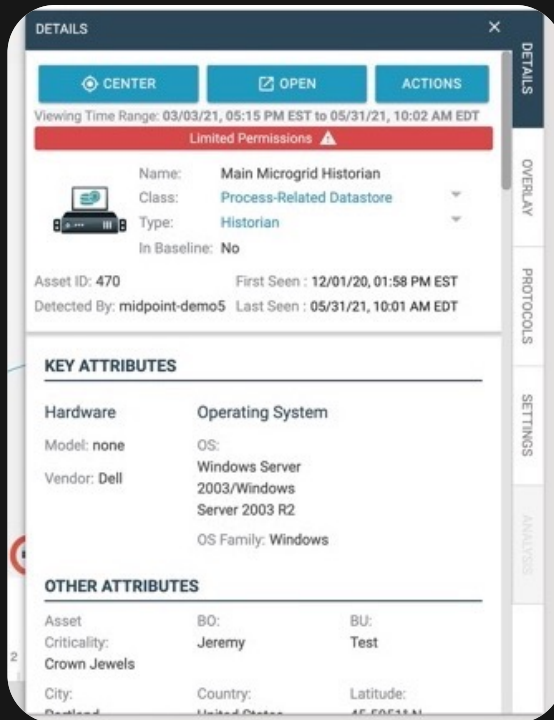


NEIGHBORHOOD KEEPER Community-Wide Threat Visibility & Collective Defense

VISIBILITY – ASSET INVENTORY & PROFILES



A comprehensive inventory is essential for any monitoring, threat correlation and effective vulnerability management



Build **asset inventory depth** through “operations safe” passive collection and **device level detail**

- Establish asset profile baselines for connected integrations with firewall and CMDB systems
- Group assets in a visual map with customizable zones for easier cyber-ops management
- See historical changes with timeline views to spot unexpected activity

VISIBILITY – ICS PROTOCOL & TRAFFIC ANALYSIS



Proper traffic dissection and inspection requires in depth protocol coverage – assets and threats remain hidden until their communications are exposed



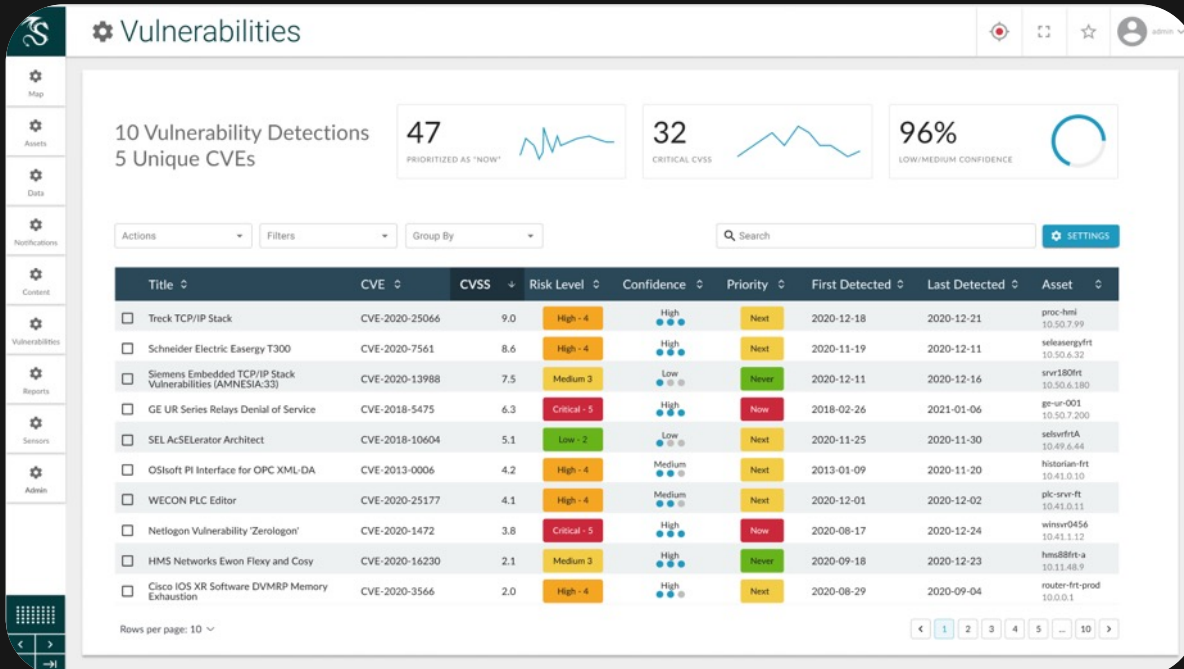
Improve the **accuracy** and **understanding** of devices in your environment

- Full support across most industrial vendors, equipment, and protocols
- Capture, analyze, and investigate device communications
- Monitor for remote connections, search historical activity

VISIBILITY – VULNERABILITY MANAGEMENT



OT cyber teams face impossible numbers of potential vulnerabilities to remediate – without simple, accurate, prioritized guidance they become overwhelmed



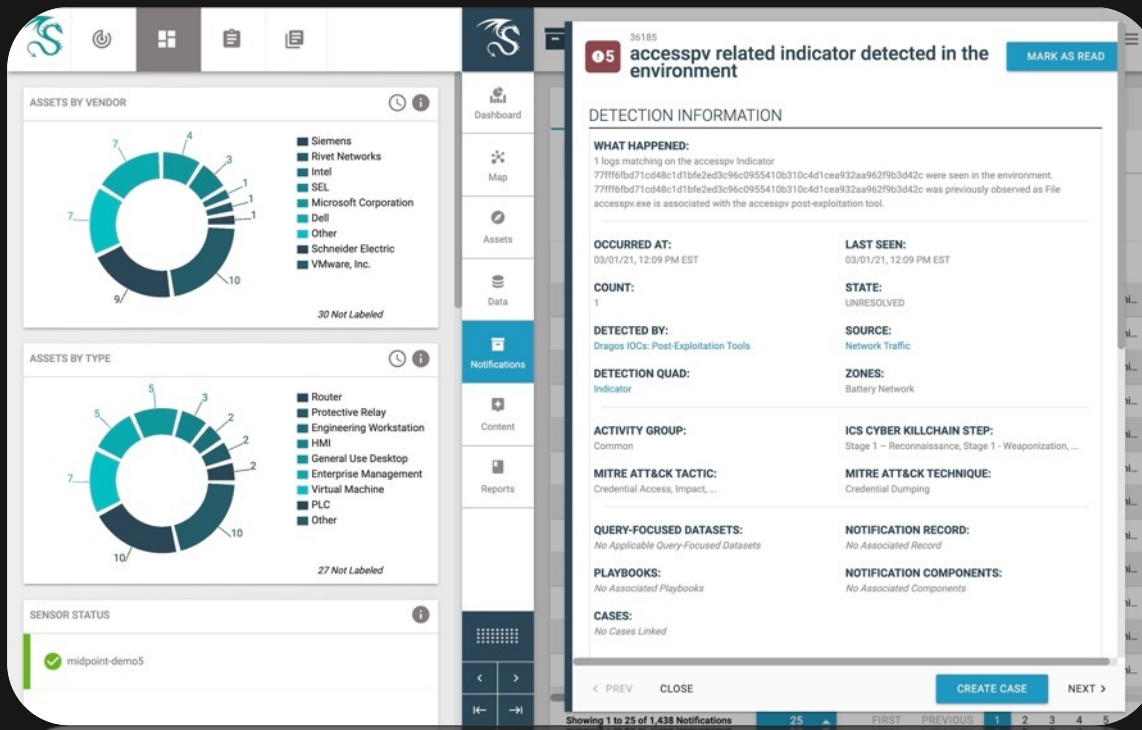
Practical OT vulnerability intelligence and mitigation strategies

- Industry specific analysis, correction, and enrichment of known vulns
- Alternative mitigation advice, prioritized with “Now, Next, Never” guidance
- Disposition tracking for full lifecycle management and to simplify audits

THREAT DETECTION



Adversaries evolve their Tactics, Techniques, and Procedures (TTPs) with subtle behaviors lost in the noise without AI (**Actual** Intelligence) – creating alert fatigue



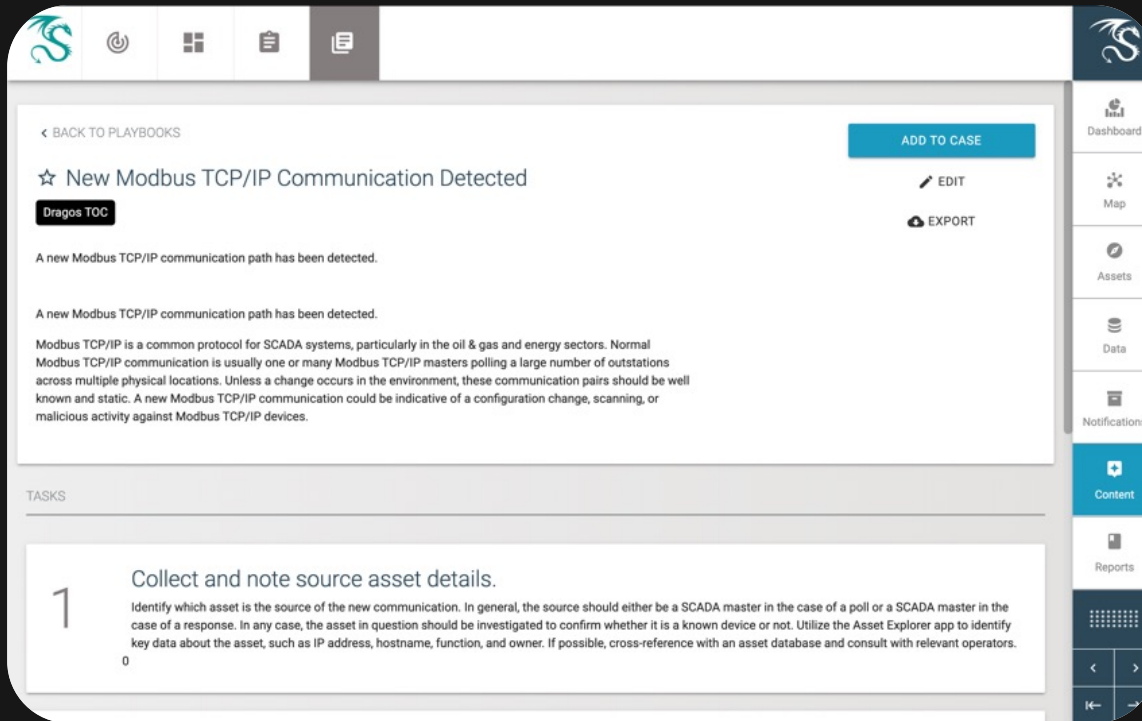
High signal, low noise **intelligence-based detections** mapped against MITRE ATT&CK for ICS :

- Curated Indicators of Compromise (IOCs), malicious IPs, domains, and hashes from Dragos Intelligence
- Anomalous traffic patterns and baseline deviation alerts
- Composite detections from TTP analysis of threat groups and attacks

RESPONSE



When faced with a potential incident, clear and carefully vetted guidance can mean the difference between quickly restoring operations or making the situation worse



Provide responders with the tools to **triage** and **investigate** potential incidents

- Incident response playbooks with OT-centric guidance from industry experts
- Collect evidence and organize by case in the analyst investigation workbench
- Centralized forensics and timeline views to coordinate across OT and IT teams

OT WATCH – OUR TEAM IS YOUR TEAM

Managed Service Quickly Establishes World Class OT Security Controls

**INDUSTRIAL
HUNTERS &
RESPONDERS**



**DRAGOS
PLATFORM**

**CURATED VISIBILITY
OF YOUR OT ENVIRONMENT**

**DETECTION
PROACTIVE THREAT HUNTING**

**RESPONSE
INCIDENT TRIAGE**

NEIGHBORHOOD KEEPER

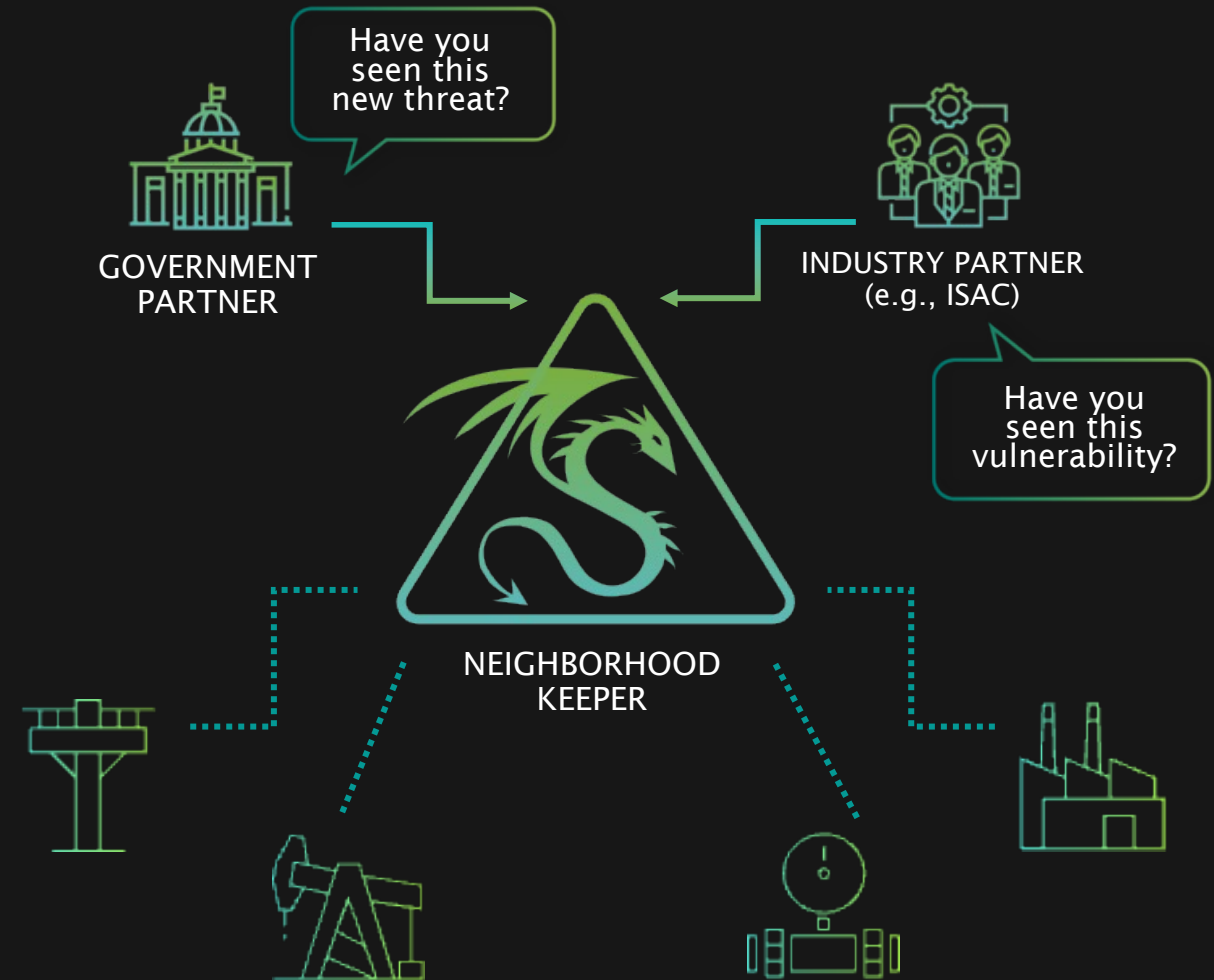
Community Wide Visibility & Collective Defense For OT Threats

A free, opt-in program for
Dragos Platform customers





Collective ICS threat, asset, & vulnerability
intelligence across Dragos Platform

Industry, regional, & system-wide view shared
between asset owners & community defenders

Request for Assistance between participant
peers or Trusted Advisors



DRAGOS PLATFORM Integrations

| SIEM | Network | Firewall | CMDB | Historian | Endpoint | SOAR |
|---|--|--|---|---|---|------|
|  |  <small>SCHWEITZER ENGINEERING LABORATORIES</small> |  |  | AVEVA +  |  *  | |
|  |  |  |  | |  | |
|  |  <small>Stronger Than Firewalls</small> |  | | | | |
|  |  |  | | | | |
|  |  | | | | | |
|  |  | | | | | |

Threat Intelligence Integrations

| | | |
|---|---|---|
|  |  |  |
|  |  |  |
|  |  |  |

* Under active development

DRAGOS PLATFORM PROTOCOL COVERAGE

Support for all
major industrial
vendors

Over 100
protocols
included

Vendors,
product, and
protocol coverage
continuously
expanding

YOKOGAWA

EMERSON

BECKHOFF

Honeywell

Rockwell
Automation

Schneider
Electric

Wonderware
by AVEVA

MITSUBISHI

OSIsoft

AVEVA

ABB

GE

SEL

DRAGOS PLATFORM KNOWLEDGE PACKS

Regular enhancements through content updates including:



Detections - for new or evolving threats

- Activity Groups (e.g., XENOTIME, KOSTOVITE, DYMALLOY)
- Ransomware and malware (e.g., Lockbit, Doppelpaymer, RYUK)
- Targeted exploits (e.g., Log4j, CRASHOVERRIDE, TeamViewer)

Characterizations - to expand protocol dissection

- ICS protocols (e.g., DNP3, FTE, Modbus, OPC-UA)
- Equipment (e.g., Oasys, DeltaV, Cimplicity, Experion, Triconex)
- Vendors (e.g., Emerson, Honeywell, Rockwell, Siemens, Yokogawa)

Playbooks - to guide cyber analysts and responders

- Protocol related (e.g., RDP RCE, IEC 104 violation)
- Behavior related (e.g., Authentication Success/Failure, scan activity)
- Hunt related (e.g., SolarWinds SUNBURST, Rockwell CIP, DeltaV)

What's New in Platform 2.1?

- CentralStore – central view of Assets, Vulns, and Notifications
- Cloud-Hosted Deployment Options
- New Health & Status Dashboard
- Notification and Vuln Overlays in Asset Map
- Notification Manager Workflow Enhancements
- Asset Inventory Usability Improvements



New Health & Status Dashboard

High-level Service Status and Resource Utilization

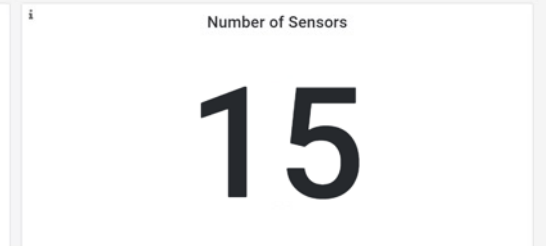
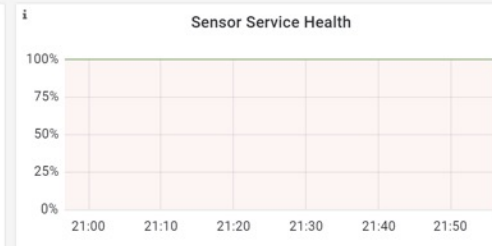


Health and Status

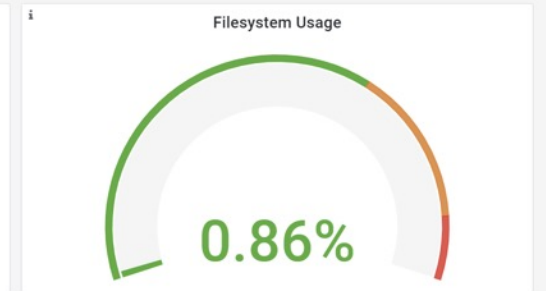
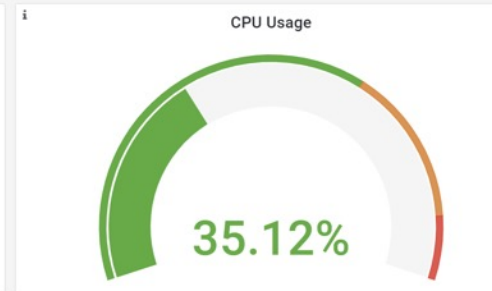
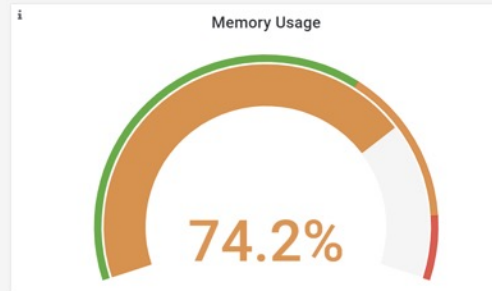
General / Health & Status

Last 1 hour UTC

Overall Health



SiteStore Status - 10.20.3.199:10250



New Health & Status Dashboard



Resource Utilization History



New Health & Status Dashboard



Network Traffic History

Health and Status

General / Health & Status

Last 1 hour UTC



New Health & Status Dashboard

Per-Sensor Health Status and History

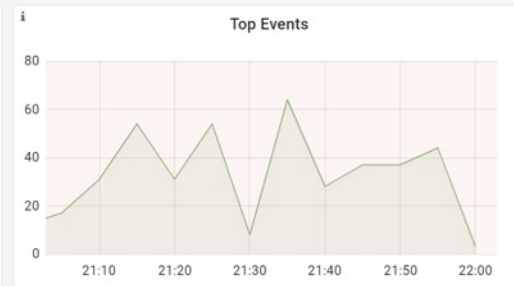
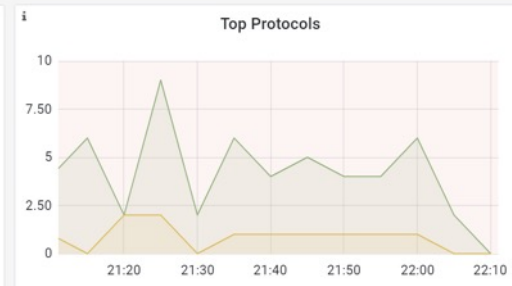
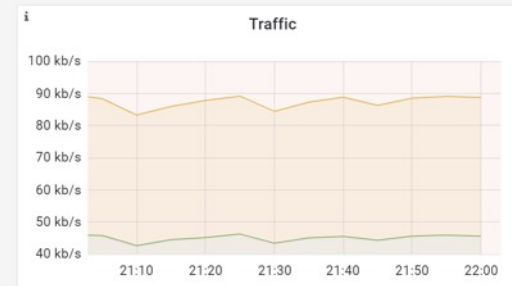
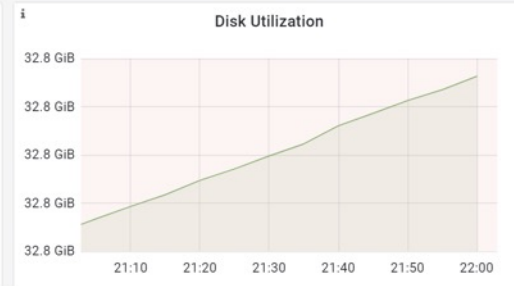
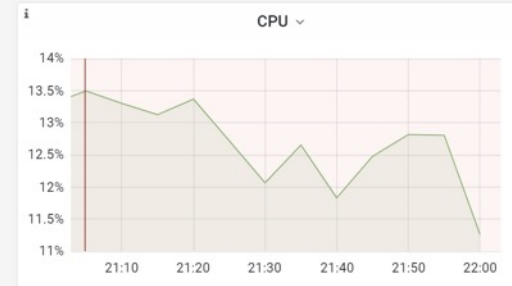


Health and Status

General / Health & Status

Last 1 hour UTC

Sensor Status - 01e66de1-d1f7-42f7-b6c0-6653e803704f



Notification/Vulnerability Overlay in Asset Map

The screenshot displays the 'Interactive Map' application. The main area shows a network diagram with nodes labeled 'General Use Desktop' and 'WebServer' connected by lines. A red circle highlights a specific area. The interface includes a sidebar with navigation options like Dashboard, Map, Assets, Data, Notifications, Content, Vulnerabilities, Reports, and Admin. The top bar shows filtering options and a search bar. The bottom right corner displays a summary of 46 assets, 12 links, and 4 groups.

Notification/Vulnerability Overlay in Asset Map

The screenshot displays the 'Interactive Map' interface. The main map area shows a network diagram with a 'General Use Desktop' node (a cluster of blue circles) and a 'WebServer' node (a single blue circle). They are connected by several lines. A green oval highlights the 'General Use Desktop' node. On the right side, an 'OVERLAY' panel is open, showing options for 'Enable overlay on assets', 'Baselines', 'Notifications', and 'Vulnerabilities'. The 'Notifications' option is selected. Below the overlay settings, a section titled 'Notifications Overlay' shows '40 Assets with Notifications' and a 'SELECT ALL' button. The interface also includes a sidebar with navigation options like Dashboard, Map, Assets, Data, Notifications, Content, Vulnerabilities, Reports, and Admin. The top bar shows filtering options, a date range (08/15/22, 09:45 PM EDT to 08/15/22, 10:00 PM EDT), and an 'UPDATE MAP' button. The bottom bar shows a 'Timebar'.

Dragos Platform Evolution

CENTRAL VIEW OF ASSETS, VULNERABILITIES & NOTIFICATIONS

CentralStore – Consolidated Meta Data & Navigation

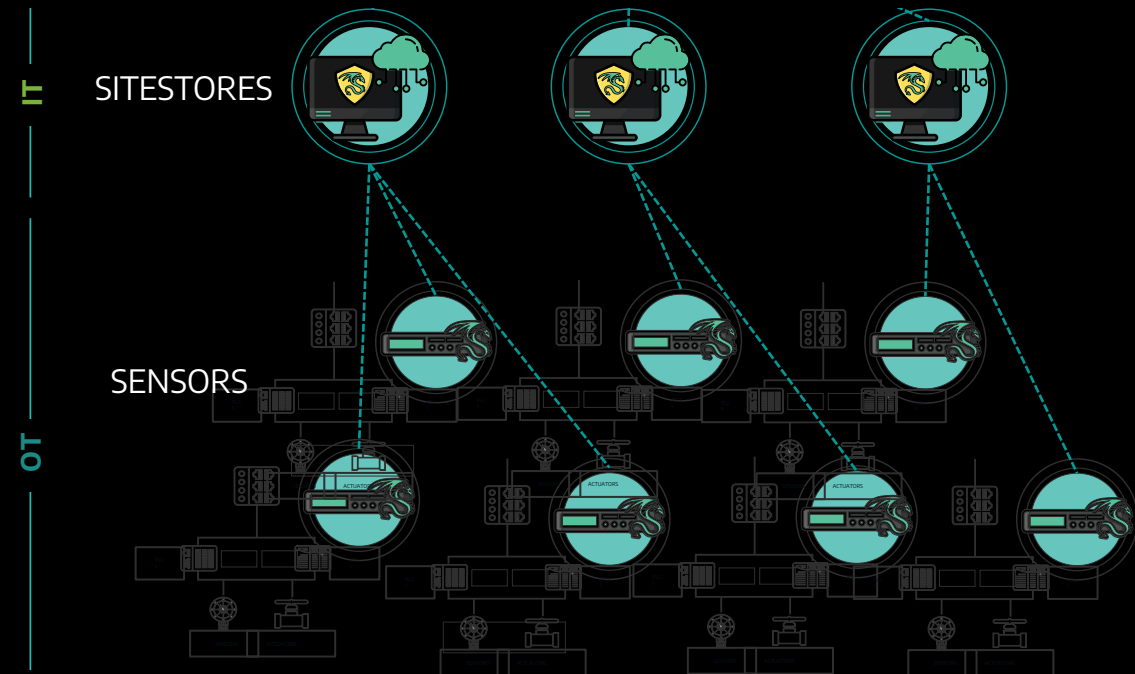
- Central visibility, searching, and reporting
- Role-based data permissions
- Cloud/on-prem, physical/virtual

SiteStore – Distributed Aggregator of Sensor Data

- Stores traffic logs, files, captures, & other forensics
- Cloud/on-prem, physical/virtual

Sensor – Passive Network Data Collection

- On-prem, physical/virtual
- Deployed in L1-L3



CentralStore Function



Enterprise-scale
OT visibility,
detection, and
response



Multi-site,
multi-organization
Dragos Platform
architecture



Consistent,
centralized **risk**
management
and **reporting**

CentralStore Features



View and search all assets, vulnerabilities, and notifications from multiple SiteStores in one location.

Familiar UI, with enhancements to Asset Inventory—such as Group By.



Built-in dynamic and interactive dashboard for Organization-wide overview

With “follow me” filters.



Provides support for SiteStore-level User Scoping

“RBAC for data access.”

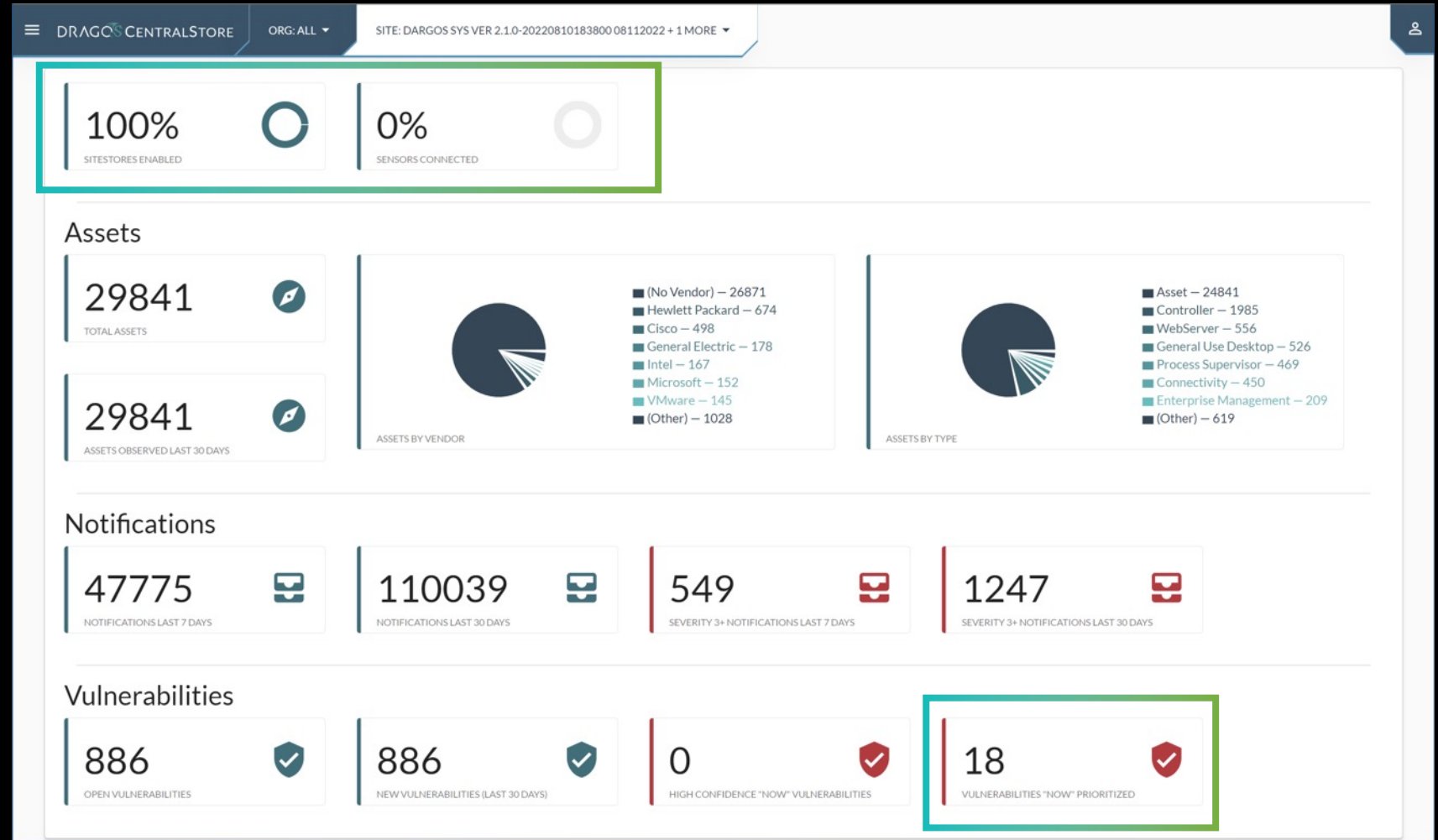


Supports local authentication and OIDC for SSO and MFA

Azure AD, ADFS, Okta, etc.

CentralStore Dashboard

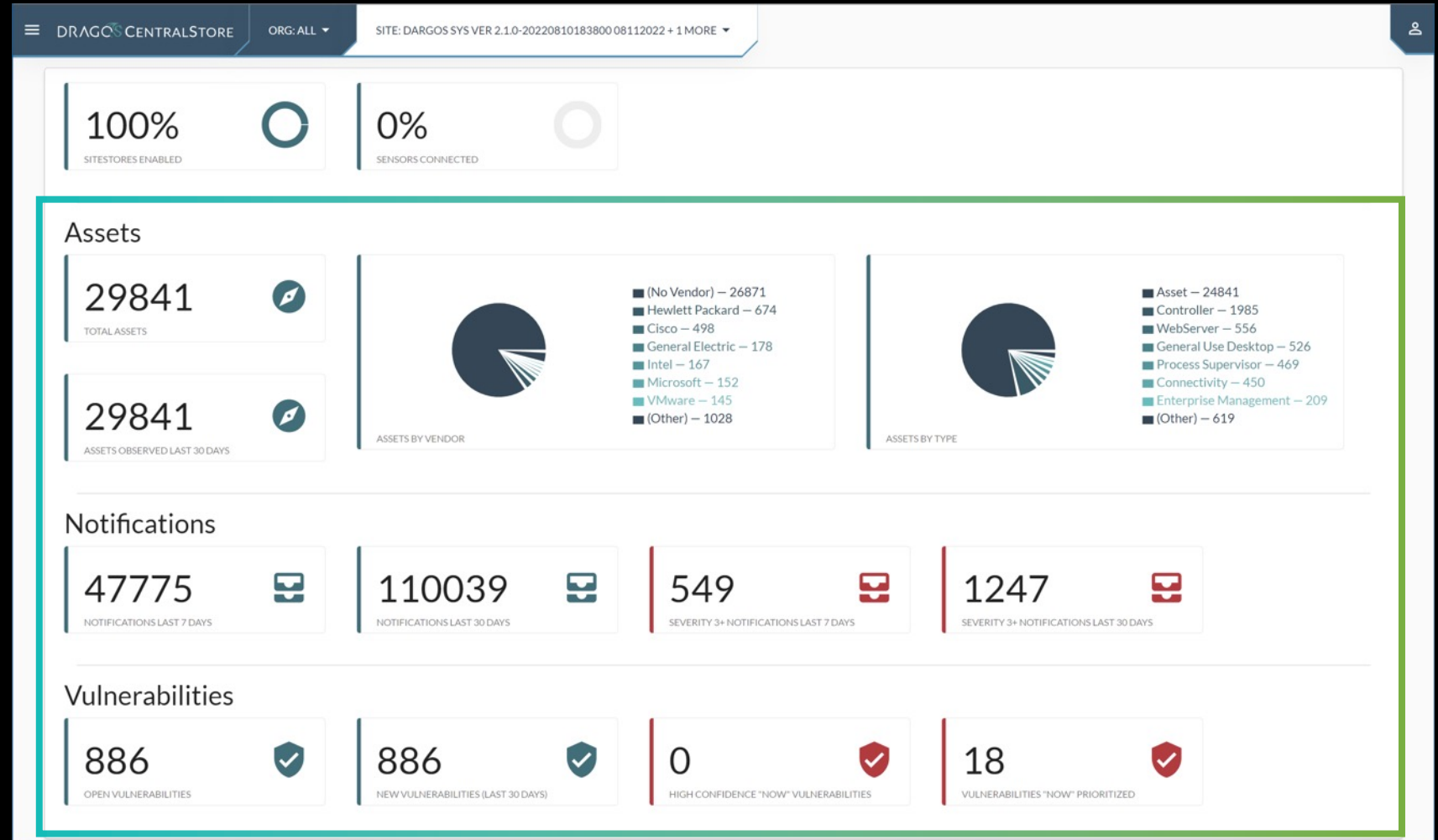
Provides an overview of SiteStore and Sensor connectivity



CentralStore Dashboard

Provides an overview of SiteStore and Sensor connectivity

Quick access to important data points, like number of high-severity Notifications

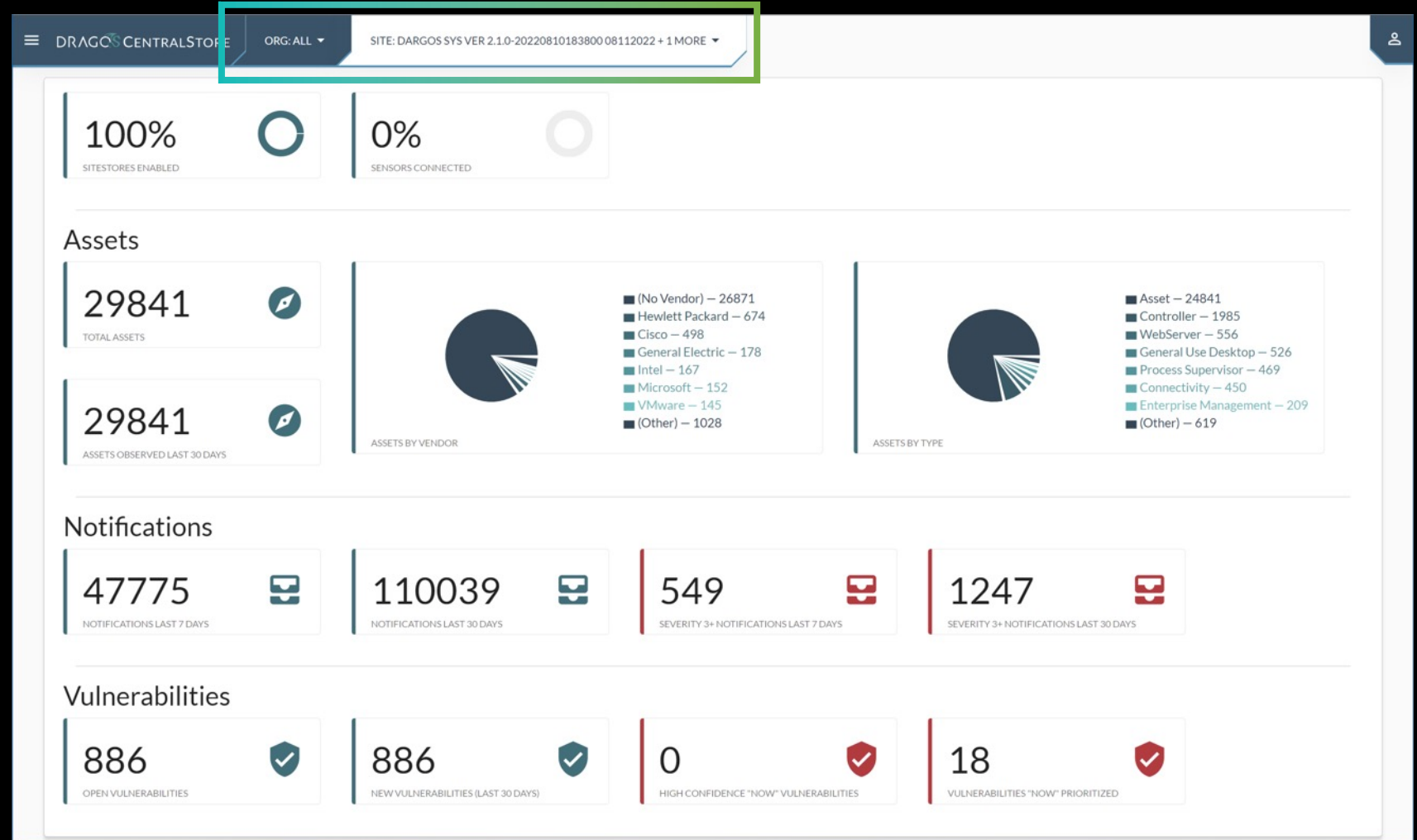


CentralStore Dashboard

Provides an overview of SiteStore and Sensor connectivity

Quick access to important data points, like number of high-severity Notifications

Dynamic – automatically updates with “follow me” filters

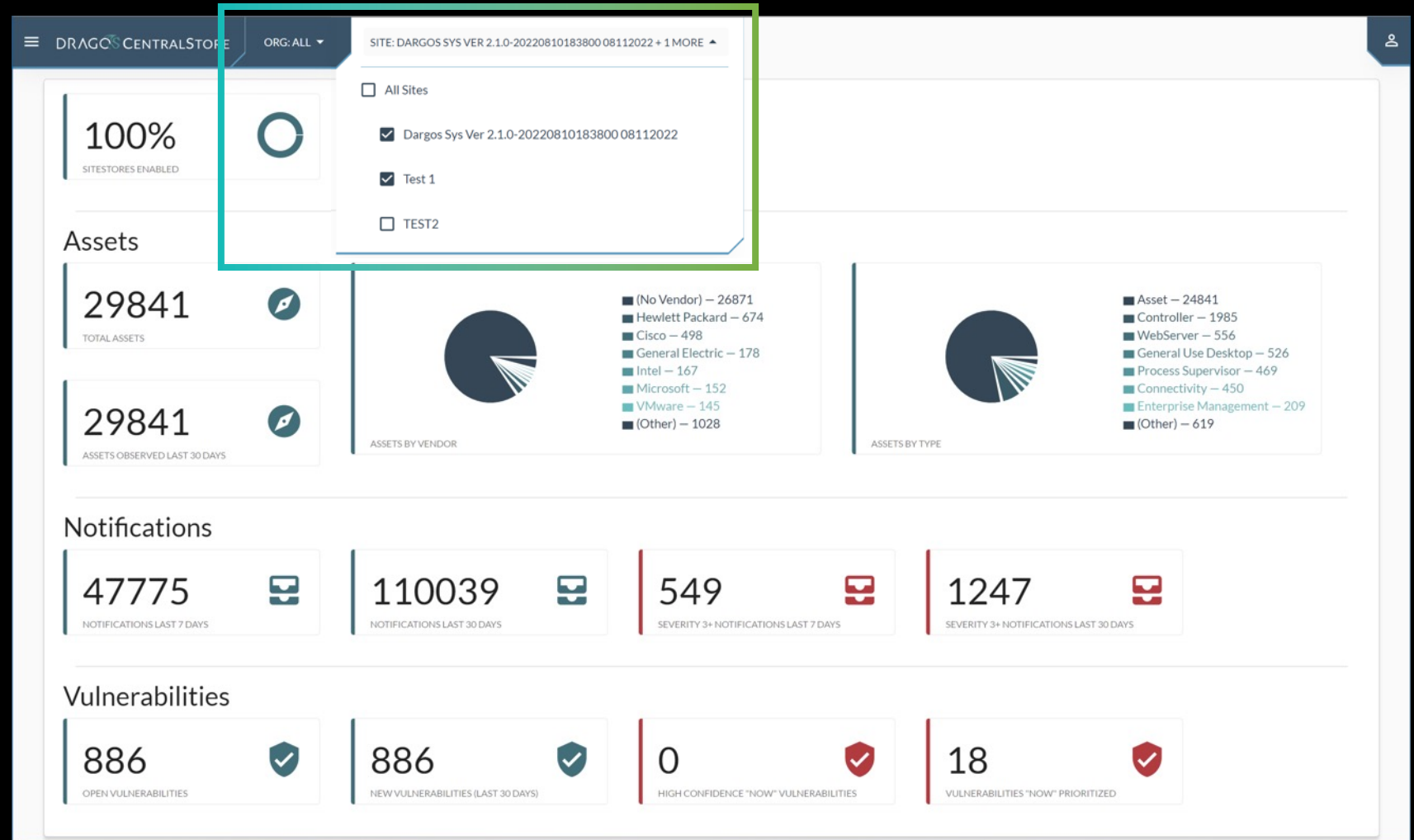


CentralStore Dashboard

Provides an overview of SiteStore and Sensor connectivity

Quick access to important data points, like number of high-severity Notifications

Dynamic – automatically updates with “follow me” filters



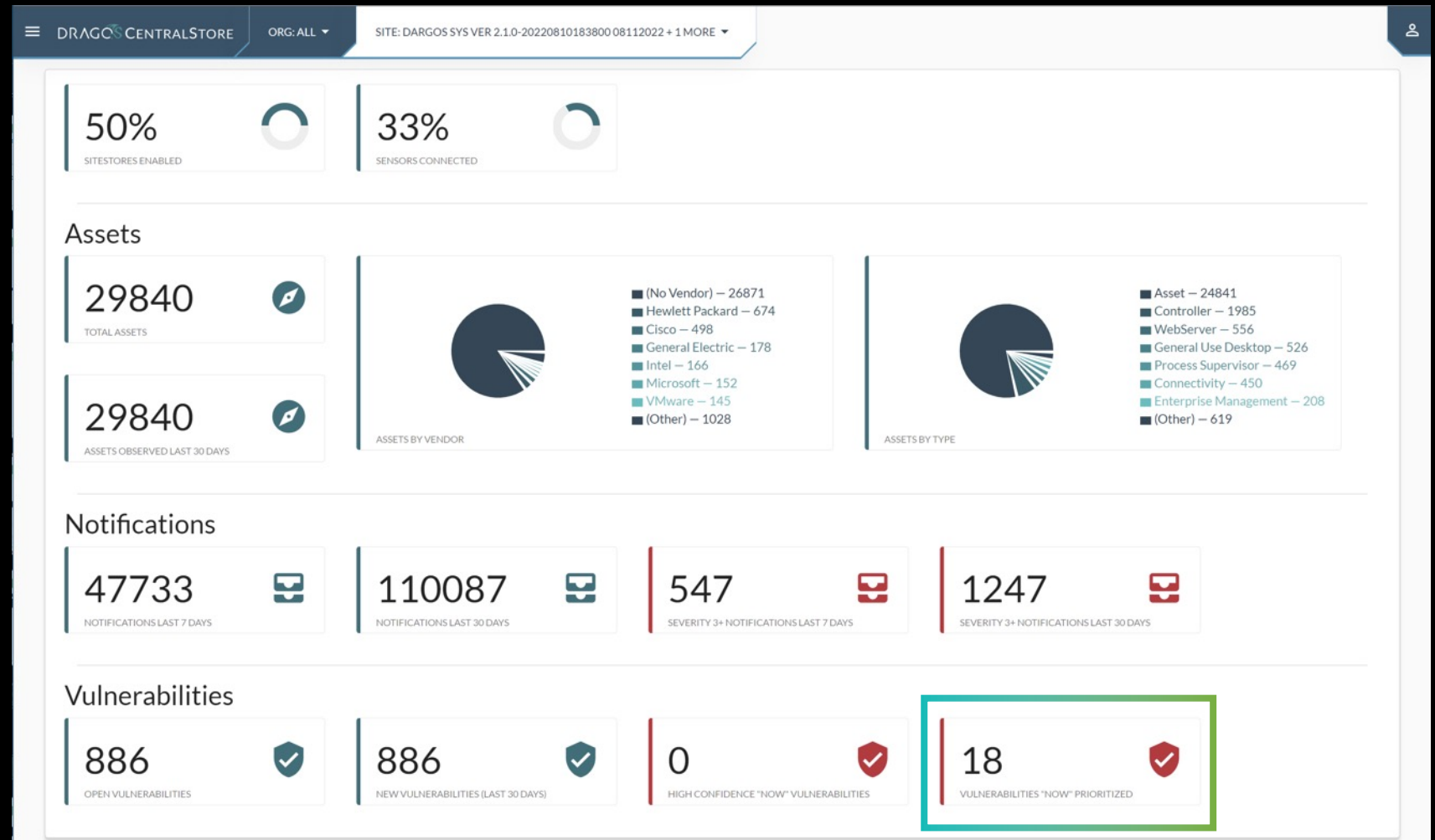
CentralStore Dashboard

Provides an overview of SiteStore and Sensor connectivity

Quick access to important data points, like number of high-severity Notifications

Dynamic – automatically updates with “follow me” filters

Interactive – Everything is clickable



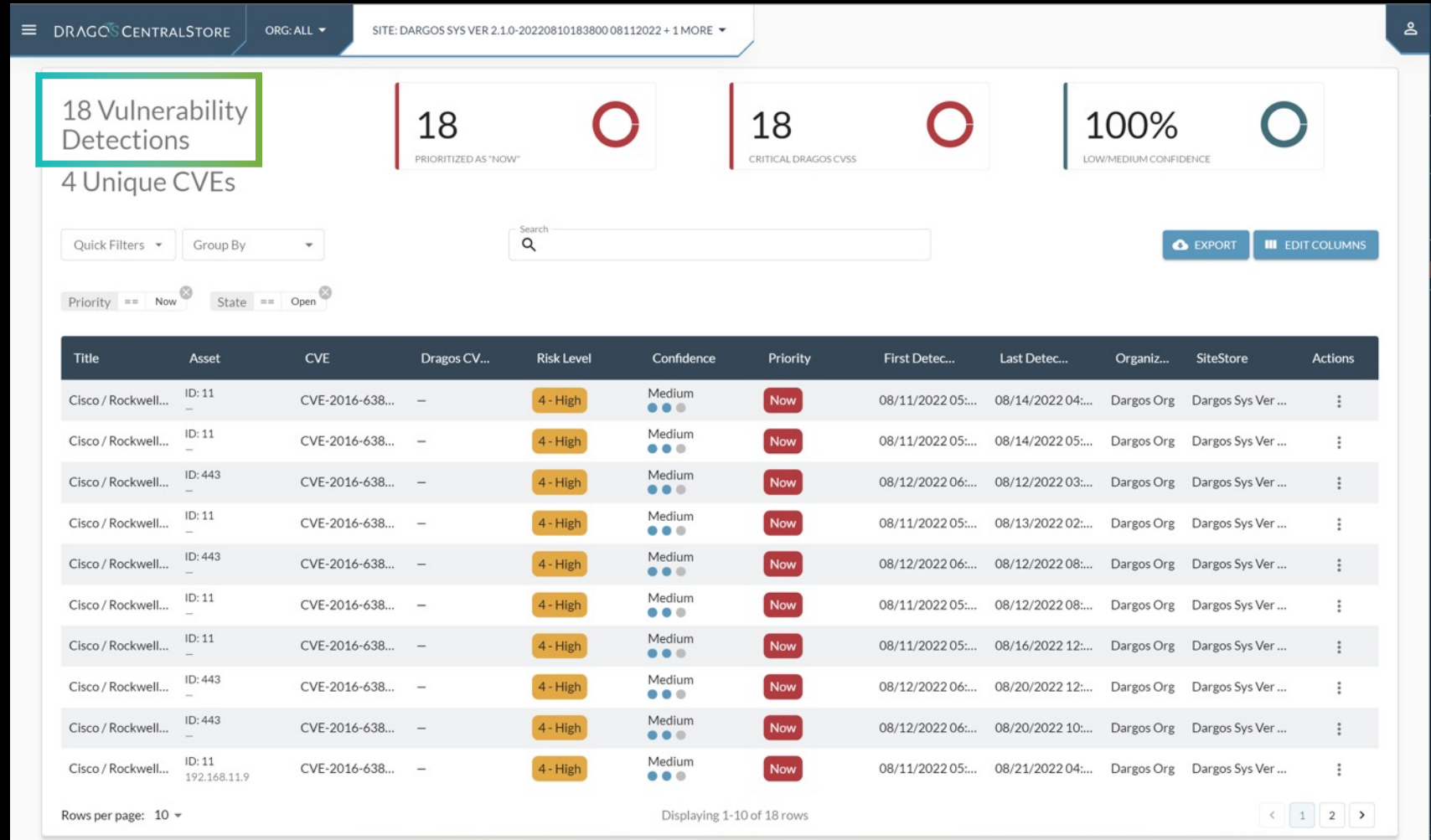
CentralStore Dashboard

Provides an overview of SiteStore and Sensor connectivity

Quick access to important data points, like number of high-severity Notifications

Dynamic – automatically updates with “follow me” filters

Interactive – Everything is clickable



The background features a dark, moody image of a Ferris wheel's structural framework. Overlaid on this are faint, light-colored technical diagrams, including a circular gear-like structure with radial lines and various geometric shapes and lines, suggesting a theme of engineering or technology.

Appliances

CentralStore Appliances

HARDWARE

CS-50-E



Capacity:
Up to 50 connected Dragos SiteStores
(flexible licensing options available)

VIRTUAL (VMWare)

CS-50-VM



SiteStore Appliances

HARDWARE

SS1 (Legacy)



STS-500-E



Capacity with Platform 2.1:
Up to 20 Gbps of aggregated monitored traffic

VIRTUAL (VMWare)

STS-200-VM



Coming Soon!

STS-500-VM



Capacity with Platform 2.1:
Up to 10 Gbps of aggregated monitored traffic

Aggregated Monitored Bandwidth

Sensor Appliances

RUGGEDIZED
INDUSTRIAL

NS-25-DR



25 Mbps
DIN Rail / Wall Mount

NS-100-SEL



100 Mbps
3U Rackmount (SEL-3355)

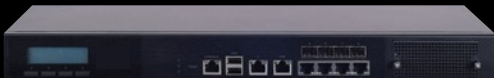
ENTERPRISE
DATACENTER

NS-100-E



100 Mbps
Wall Mount / 1U Rack Mount Kit

NS-500-E



500 Mbps
1U Rackmount

NS-1000-E



1 Gbps
1U Rackmount

VIRTUAL
(VMWare)

NS-25-VM



NS-100-VM



NS-1000-VM

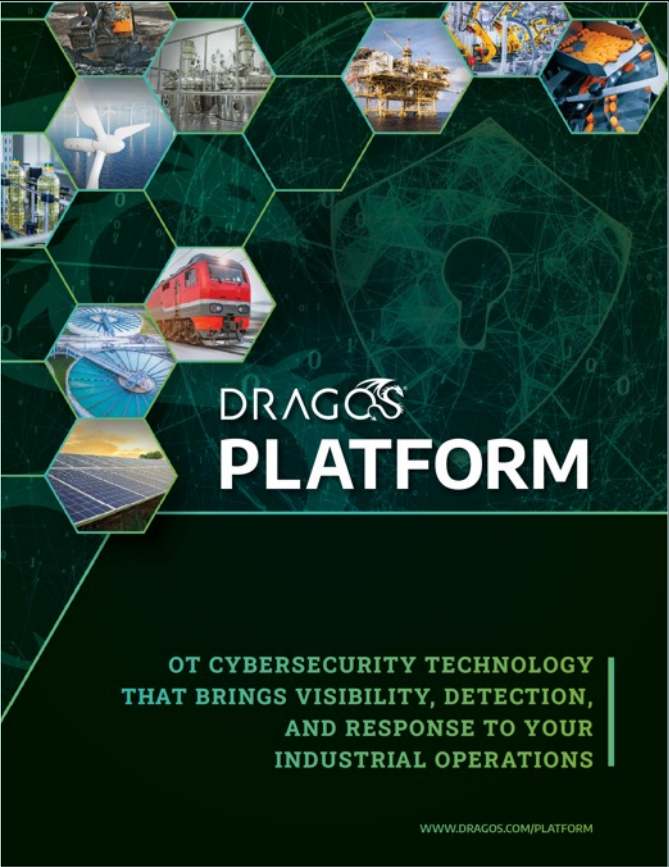


Monitored Network Throughput



Q U E S T I O N S A N D A N S W E R S

Additional Material - dragos.com/platform



DRAGOS
PLATFORM

OT CYBERSECURITY TECHNOLOGY
THAT BRINGS VISIBILITY, DETECTION,
AND RESPONSE TO YOUR
INDUSTRIAL OPERATIONS

[WWW.DRAGOS.COM/PLATFORM](https://www.dragos.com/platform)

Platform Datasheet ([link](#))



Dragos Platform appliances are designed to accommodate a wide variety of industrial environment scenarios. For optimal architecture and sizing, please consult with your account team or contact: sales@dragos.com.

HARDWARE – CENTRALSTORE AND SITESTORE MODELS

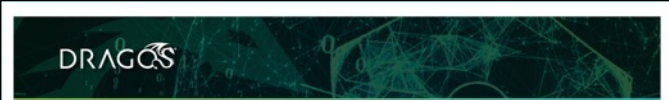


| Model | CS-50-E | STS-500-E |
|-----------------------------|--|--|
| Capacity | Up to 50 connected Dragos SiteStores* | Up to 20 Gbps of traffic monitored by connected Dragos Sensors |
| Management Interfaces** | RJ45 (1-3) | RJ45 (1-3) |
| Local Console | Serial (DB9) Mini-HDMI / USB | Serial (DB9) Mini-HDMI / USB |
| Remote Management*** | Yes | Yes |
| Storage | 24 TB SSD (RAID 5), 22 TB usable | 24 TB SSD (RAID 5), 22 TB usable |
| Form Factor | 2U Rackmount | 2U Rackmount |
| Field Replaceable Parts | Power Supply (2), Disk (24) | Power Supply (2), Disk (24) |
| Power Supply | Dual 800W (100 - 240 VAC), Hot Plug Redundant | Dual 800W (100 - 240 VAC), Hot Plug Redundant |
| Avg/Max Power Consumption | 553 W / 1600 W | 553 W / 1600 W |
| Avg/Max BTU/hr | 1886 / 5459 BTU/hr | 1886 / 5459 BTU/hr |
| Operating Temperature Range | 10C - 35C | 10C - 35C |
| Storage Temperature Range | -30C - 60C | -30C - 60C |
| HxDxW (in/mm) | 3.44 x 28.75 x 17.54 in, 87.6 x 730.3 x 446 mm | 3.44 x 28.75 x 17.54 in, 87.6 x 730.3 x 446 mm |
| Weight | 61 lb / 27.7 kg | 61 lb / 27.7 kg |
| Certifications | CE, FCC Class A, UL, RoHS | CE, FCC Class A, UL, RoHS |

* Multiple subscription options are available with varying terms for connected SiteStores.
** Management interfaces are 10/100/1000BaseT Ethernet.
*** Remote Management is provided by ICD or DRAC (depending on model).

[WWW.DRAGOS.COM/PLATFORM](https://www.dragos.com/platform)

Appliance Datasheet ([link](#))



DRAGOS PLATFORM SUBSCRIPTION MODEL

An Overview of the Dragos Platform Subscription Model

The Dragos Platform is industrial cybersecurity (ICS/OT) technology that arms your organization with the tools and intelligence to stay ahead of cyber attackers and confidently identify and respond to threats in your environment. Designed to accommodate both CAPEX and OPEX expenditures, the Dragos Platform subscription model gives our customers the ultimate in flexibility and immediacy for our content-rich offering.

ALWAYS UP-TO-DATE

A key benefit of the Dragos Platform subscription model is the assurance your company has the latest asset visibility, vulnerability management, threat detection, and incident response capability available. Our technology is developed and maintained by analyst-driven intelligence, ICS-specific practitioner experience, and insight from customer engagements that is codified into Platform updates delivered through Knowledge Packs.

This provides your security team the most up-to-date tools to defend your organization, including: regularly updated adversary tactics, techniques, and procedures (TTPs) based on our latest intelligence; new indicators of compromise to detect threats in their early stages; and investigation playbooks, authored by Dragos's expert threat hunters and incident responders, to provide step-by-step response guidance.

To provide seamless delivery of this critical and rapidly-changing content, the Dragos Platform Subscription Model offers single or multi-year software agreements to your industrial organization via a scalable, consistent platform.

WHAT YOU GET

- Pricing Incentives**
Pay for what you need with discounts and guaranteed SLAs on specific Dragos Platform-enabled Services based on volume tiers
- Scalability**
Start with targeted deployments and expand when the time is right
- Immediacy**
Continuous access to the most current Dragos Platform upgrades
- Practitioner-Driven Content**
The latest analytics and content based on dedicated expert threat intelligence
- Critical Support**
Rapid, convenient support when you need it most
- Ease Of Use**
Newest features and content updates available on demand through the customer portal to deploy when you're ready

[WWW.DRAGOS.COM/PLATFORM](https://www.dragos.com/platform)

Continued >

Subscription Datasheet ([link](#))



Dragos Industrial Security Conference 2022

Join us on November 5, 2022, in-person in Hanover, MD,
for expert research on ICS threats, malware, incidents,
and vulnerabilities.

Register your interest today →

www.dragos.com/disc