DRAGOS
PUBLIC SECTOR

SOLUTION BRIEF

OT Cybersecurity for Federal Agencies

Technology, intelligence, and expertise that keep mission-critical operations running. Dragos protects the operational technology behind federal civilian, defense, and intelligence missions.



Updated November 2026

The Challenge Federal Missions Face

Federal civilian, defense, and intelligence missions run on operational technology (OT): power distribution, water and wastewater, fuel systems, building automation, and the industrial control systems (ICS) behind them. Adversaries target these systems because disrupting them disrupts the mission.

OT environments run different systems, protocols, adversaries, and vulnerabilities than IT, and the consequences of getting it wrong are physical. As facilities modernize, the boundary between IT and OT keeps moving, and control systems carry strict latency and safety requirements that demand process-level expertise.

ICS and xOT: Both Matter

- **ICS** names the systems that monitor and control physical processes.
- **xOT** (extended operational technology) names everything with influence over them: building management systems, remote access gateways, IoT and IIoT devices, edge devices, and cloud-connected systems.
- Federal facilities depend on both.

OT Expertise for Your Mission

Qualified OT security practitioners are scarce, and agencies compete with industry to hire them. Dragos puts OT threat hunters, intelligence analysts, and incident responders alongside your team. Dragos EmberAI puts that expertise inside every analyst workflow, so less-experienced staff can work OT problems with methods built and validated by Dragos experts.

Collective Defense Across Government and Industry

Dragos connects government, civilian agencies, and commercial operators of critical infrastructure. Government and intelligence community partnerships surface early signals beyond what any single organization can observe. Neighborhood Keeper shares anonymized insights across participants, so a threat seen in one environment surfaces in others before it strikes.

American-Developed, Headquartered in Maryland

Dragos is privately held and headquartered in Hanover, Maryland, with over a decade of OT-specific incident response experience. Dragos analysts produced the definitive analysis of CRASHOVERRIDE, TRISIS, and PIPEDREAM, the most significant ICS malware ever discovered.

Federal Agency & DOD Partners

Recognition

- Named a Leader in the 2026 Gartner® Magic Quadrant™ for CPS Protection Platforms
- Leader in the Omdia Market Radar: OT Cybersecurity Platforms, 2026
- Leader and no. 1 in Innovation in Frost & Sullivan's Frost Radar™: OT Cybersecurity Solutions, 2025
- Dragos Platform earns highest score in Strategy, 5/5 Vision in The Forrester Wave Q3 2026 for OT cybersecurity solutions

© 2026 Dragos, Inc. All Rights Reserved.

How Dragos Helps Federal Agencies

Dragos protects the systems federal missions depend on, from power grids and fuel depots to manufacturing plants and facility control systems. That supports mission readiness and resilience, enables secure modernization, and makes compliance easier to demonstrate. Dragos helps your team answer:

01
What is on my network, and what can affect the mission?

02
Who and what is communicating, and what is permitted to?

03
Which vulnerabilities need action now, which can wait, and which never will?

04
Is an adversary already here, and what do we do next?

The Dragos Platform

The Dragos Platform is purpose-built for OT cybersecurity and delivers complete visibility into industrial networks, so security teams can identify assets, manage vulnerabilities, and detect threats before they impact operations. Powered by industry-leading cyber threat intelligence, the Platform continuously incorporates real-world threat research and collective defense insights through its Intelligence Fabric, ensuring organizations stay ahead of an evolving threat landscape. Named a Leader in the 2026 Gartner® Magic Quadrant™ for CPS Protection Platforms, Dragos offers unmatched OT-native capabilities including deep packet inspection, risk-based vulnerability management with “Now, Next, Never” prioritization, and segmentation policy validation.

One Platform, Backed by Intelligence and Expertise

The Platform’s Insights Hub unifies alerts, asset data, and AI-powered recommendations in a single dashboard, accelerating investigations and reducing risk. With flexible deployment options and integrations across leading SIEMs, firewalls, and endpoint tools, the Dragos Platform meets organizations wherever they are in their OT security journey.



© 2026 Dragos, Inc. All Rights Reserved.

Platform Use Cases for Federal Environments

Asset Visibility and Inventory

Passive monitoring across 600+ industrial protocols, the Dragos Agent for firmware, OS, and patch detail, and project-file import. Find crown jewel assets, unknown devices, and every asset a new advisory affects.

Vulnerability Management

Only 3 to 6% of OT vulnerabilities require immediate action. OT-corrected scoring and “Now, Next, Never” prioritization show which ones, with alternative mitigations when patching is not viable.

Threat Detection

Modeling, configuration, IOC, and threat behavioral detections, correlated into composite detections. Weekly Knowledge Packs keep them current, mapped to MITRE ATT&CK for ICS.

Compliance and ATO Support

Continuous, audit-ready asset, vulnerability, and network evidence supports RMF and ATO documentation, NIST SP 800-82 guidance, and leadership reporting.

Extending Coverage Across the Enterprise

Agencies that start with OT visibility can extend the same intelligence across every connected asset and the software inside it.

Dragos Exposure Management

See everything, regardless of what you have deployed.

Dragos Exposure Management integrates with the tools already deployed across your tech stack to produce a single, continuously updated exposure view across IT, OT, IoT, and cloud environments. It combines safe active discovery, always-on passive discovery, and pre-built integrations to build a complete asset inventory without agents, credentials, or appliances. Every asset is fingerprinted against thousands of device attributes and enriched by the Dragos Intelligence Fabric, connecting more than a decade of xOT-specific telemetry, adversary research, and frontline incident response to every exposure. Context-based prioritization surfaces the risks adversaries would use first, so teams act on what matters rather than what’s loudest.

Dragos Device Remediation

Reach and remediate what you find.

Dragos Device Remediation extends Dragos asset discovery with deeper safe active querying and richer device-level profiling, then closes the gap between finding a risk and fixing it. Teams can rotate credentials, update firmware, manage certificates, and control configuration changes across the xOT environment, so exposures identified in the inventory get remediated rather than only reported.

Dragos Software and Supply Chain

Know your application risk before it becomes an incident.

Dragos Software and Supply Chain analyzes compiled binary code in firmware, xOT devices, containers, and applications to generate a verified software bill of materials for every device, identifying embedded vulnerabilities, exposed credentials, and open-source components the vendor may not even know are present. Reachability analysis then identifies which vulnerable code executes at startup, cutting through thousands of CVEs to surface what is exploitable, and a single query can scope the blast radius of a compromised component across an entire device fleet in under a minute.

© 2026 Dragos, Inc. All Rights Reserved.

Dragos Platform

Investigation and Response.

When something happens, a slow or wrong response is measured in downtime and safety risk. The Insights Hub, case management, timeline views, and response playbooks written by Dragos OT experts let analysts tell a misconfiguration from adversary activity and investigate without disrupting operations.

Dragos Segmentation

Segmentation Validation.

Dragos Segmentation proves your segmentation holds, validated against your own network configurations. It reads firewall, router, and switch configurations offline, with no agents, no scans, and no traffic on the OT network, and reveals every access path they permit, so teams can validate segmentation, catch misconfigurations, and generate audit evidence.

The Dragos Intelligence Fabric

The Dragos Intelligence Fabric is the living knowledge engine behind the Dragos Platform. It codifies over a decade of OT-specific telemetry, asset and protocol research, adversary research, vulnerability data, and frontline practitioner expertise into a continuously updating loop. Agencies receive it through the content the Platform delivers and can query it directly through Dragos EmberAI.

Data

5+ PB of daily OT telemetry and a decade of research

People

Hunters, analysts, and responders on one model

Partnerships

Government and intelligence community signals

Systems

Platform, OT Watch, and Neighborhood Keeper feed it back

AI

Dragos EmberAI surfaces new insights faster

DRAGOS EmberAI

The AI That Actually Knows OT.

Dragos EmberAI is an xOT-native AI agent built on the Dragos Intelligence Fabric and grounded in each customer's environment. It applies Dragos intelligence and expert methods to the work analysts already do: it activates expert Skills to guide complex tasks, returns structured findings instead of raw output, and turns approved decisions into changes to Platform asset data. The goal is to reduce the manual work between analysis and action. Analysts direct the work and approve every write, and Dragos EmberAI never acts on xOT devices directly.

© 2026 Dragos, Inc. All Rights Reserved.

DRAGOS EMBERAI SKILLS

Built and Validated By Dragos Analysts

Less experienced teams can work at the level of seasoned specialists.

Crown Jewel Analysis

From identifying operational, pathway, and interdependency assets to tagging the ones that matter most.

Structured Threat Hunts

From scoping the search to a final report with findings and coverage gaps.

Data handling. Your data is not trained on or shared with third parties. Dragos EmberAI processes data in-region for US, EU, and Australia customers.

Dragos xOT Threat Intelligence

Finished intelligence built exclusively for OT, from the team that tracks more ICS adversaries than anyone else.

Dragos xOT Threat Intelligence delivers finished OT threat intelligence, including adversary research, vulnerability analysis, IOCs, and strategic reporting, produced by the largest private ICS/OT cyber threat intelligence team in the industry. It is the intelligence layer of the Dragos Intelligence Fabric, fed by Dragos threat hunters, malware analysts, vulnerability researchers, and detection engineers working exclusively in operational environments.

01

Adversary Research

Tracking of 26+ OT-specific threat groups, with TTPs and victimology mapped to MITRE ATT&CK for ICS.

02

Vulnerability Research

ICS vulnerabilities tested on physical devices, with corrected CVSS scores and alternative mitigations.

03

Malware Analysis

Definitive analysis of CRASHOVERRIDE, TRISIS, and PIPEDREAM.

04

IOCs for the SOC

Attributed indicators with OT impact context for existing SIEM, TIP, and SOAR platforms.

05

Strategic Reporting

Industry-specific threat landscapes and finished reporting for leadership briefings.

06

RFI and Concierge

On-demand access to Dragos analysts for research specific to your mission.

© 2026 Dragos, Inc. All Rights Reserved.

Dragos Expert Services

OT Cybersecurity Assessments

Four options, from Compromise Assessment to the full OT Cybersecurity Assessment, evaluating architecture, crown jewel protection, and detection and response capability.

Red Team Services

Network Vulnerability Assessment, Network Penetration Testing, and Purple Team Exercises that find hidden attack paths and validate controls without disrupting operations.

Threat Baselines and Tabletop Exercises

Workshops built on real adversary TTPs and industry-specific scenarios to test response plans and strengthen coordination across teams.

Neighborhood Keeper

Threats seen in one OT environment are surfaced in others before they strike.

Neighborhood Keeper is an opt-in capability, available at no additional cost to Dragos Platform customers, that shares anonymized telemetry across participants. When OT-relevant behaviors are validated in one environment, they surface in peer environments through Trusted Insight Alerts, enabling earlier detection with higher confidence. Government organizations can participate as trusted advisors, gaining visibility into downstream risk to key locations and sharing information with the private sector safely.

01

Opt in

Dragos Platform customers opt in. When detections fire, data stays on premises and only anonymized insights are shared.

02

Share

Neighborhood Keeper shares detections and insights across the community: what is happening elsewhere and which adversary methods and risks are prevalent.

03

Request Help

Participants can make an anonymous, encrypted request for assistance. Responders identify themselves so the requestor can coordinate directly.

© 2026 Dragos, Inc. All Rights Reserved.

WHY DRAGOS

Outcomes for Your Mission

Cyber incidents can stop a mission, threaten the health and safety of the community, and shake public trust. Put Dragos researchers, hunters, and responders to work on your mission.

01

Reduce Cost and Wasted Effort

- Assessments and threat hunting scoped to your mission and maturity
- Continuously collected data that reduces repeat site visits
- Prioritized vulnerability guidance for defensible resource requests
- Faster identification of malfunctioning components

02

Save Time

- Continuous, automated asset inventory
- Live data without lengthy site interactions
- Data collection that starts during the assessment
- Guided workflows with Dragos EmberAI Skills

03

Simplify Compliance and Reporting

- Support for NDAA requirements, CDM goals, and component cyber objectives, including cyber terrain mapping, continuous monitoring of critical assets, OT zero trust, and OT asset visibility across facilities
- Tabletop exercises, baselines, and tracked progress
- Executive-ready reporting for leadership

04

Reduce Risk, Improve Resilience

- “Now, Next, Never” prioritization so the exploitable 3 to 6% is addressed first
- Detection based on the adversaries Dragos tracks
- Segmentation validated against actual configurations

Contract Vehicles and Certifications

Dragos makes it easy to work with us through multiple contract vehicles and certifications.

- UESC/UMCS (OEM partnerships)
- GSA
- SEWP (multiple partners)
- Army ITES-3H / ITES-3S
- DLA Tailored Logistics Support Program (TLSP)
- SBA 8(a); Alaska Native, Native Hawaiian, and SDVOSB partners

Talk to an OT Security Specialist

Learn how Dragos technology, intelligence, and services support your mission.

Contact Sales

sales@dragos.com

© 2026 Dragos, Inc. All Rights Reserved.

About Dragos Public Sector

Dragos Public Sector LLC is the federal subsidiary of Dragos, Inc., delivering xOT cybersecurity technology, intelligence, and services to U.S. federal civilian and defense organizations. Operating with U.S.-based engineering and capable of supporting cleared contract work, DPS provides asset visibility, continuous monitoring, exposure and vulnerability management, threat detection, and incident response for the extended operational environment that federal missions depend on. The Dragos Platform is supported by a DISA-published Security Technical Implementation Guide and is available through multiple federal contract vehicles. Visit dragosgov.com.



© 2026 Dragos, Inc. All Rights Reserved.