

Prohibited Device Detection and Response

Find and Disable Risky Devices Banned by the U.S. Government

Adversarial, state-sponsored cyber operations have matured into instruments of geopolitical leverage. These intrusions are deliberate pre-positioning efforts, designed to enable surveillance, disruption, or escalation during periods of heightened tension.

The Growing Threat

One of the most urgent risks is untrusted or banned foreign technology operating across enterprise and extended operational technology (xOT) networks. Equipment from companies such as Huawei, Dahua, Hikvision, ZTE, and Hytera, and devices derived from their components or firmware, can appear under white-label brands or obscure manufacturers with little or no identifiable vendor, likely intended to evade bans and compliance controls.

At the same time, attackers increasingly exploit unmanaged connected devices: systems with default credentials, vulnerable firmware, insecure configurations, or end-of-support software that fall outside traditional IT visibility. A compromised IP camera, badge reader, or building management system can provide the same foothold as a vulnerable router. Removing untrusted technology from operational environments is essential to protecting infrastructure, mission continuity, and national resilience.

Discover All Devices, Alert on Banned Ones

Dragos flags devices prohibited under National Defense Authorization Act (NDAA) Section 889 restrictions on certain foreign-manufactured technologies, helping organizations enforce compliance while reducing risk. This includes:

- ✓ Devices manufactured by Huawei, Dahua, Hikvision, ZTE, and Hytera
- ✓ Devices with firmware that was OEMed from the above companies, regardless of device hardware manufacturer or labeling

Banned devices extend far beyond the explicitly listed manufacturers, encompassing those concealed through OEM arrangements, disguised branding, and other evasion tactics. Unlike conventional tools that rely on low-fidelity OUI lookups and MAC address registries, Dragos interacts directly with devices in their native protocols, uncovering the true origin of a device, whether it carries an overtly banned brand, is OEMed by a known or seemingly Western brand, is disguised behind an unknown brand, or is unbranded, to reveal what conventional lookups miss.

Deep Device Visibility

Dragos identifies device type, manufacturer, model, IP and MAC addresses, firmware versions, active protocols, open ports, running services including Telnet, SSH, and FTP, as well as other device metadata. This is enriched with device-specific attributes, such as white balance settings on IP cameras, humidity control parameters on HVAC controllers, and power thresholds on PDUs.

Risk Assessment

Source: CISA, "BOD 26-02: Mitigating Risk from End-of-Support Edge Devices"

In addition to detecting banned devices, Dragos surfaces default passwords in use, outdated or available firmware updates, and historic firmware versions still present in the environment, correlates firmware with known CVEs with KEV and EPSS context, and evaluates end-of-life or end-of-support status, now mandated under CISA's Binding Operational Directive BOD 26-02. Dragos also detects insecure configurations, exposed or expired certificates, self-signed certificates, and weak or deprecated ciphers.

Discovery Built to Be Trusted

01

Safe, Native Communication

No reckless scanning. Only safe, intelligent active discovery using native device protocols.

02

Evidence-Based Analysis

No guesswork. Device identification with certainty, the first time.

Contain and Disable High-Risk Devices

Once a high-risk device, such as one running banned or unverifiable firmware, is identified, Dragos can disable it remotely.

Automate Risk Remediation

In addition to detecting and disabling banned devices, Dragos continuously identifies vulnerabilities, misconfigurations, and outdated firmware, then remediates them through policy-driven workflows without disrupting operations:

- ✓ Rotate weak or default credentials across entire device fleets on an automated schedule
- ✓ Patch, upgrade, or downgrade vulnerable or outdated firmware
- ✓ Disable unnecessary or insecure protocols, such as Telnet, SSH, and FTP
- ✓ Replace expired or self-signed certificates with trusted ones

Monitor Continuously, Detect Drift

Dragos even monitors devices continuously for state changes, including configuration changes, firmware tampering, or credential resets, that indicate compromise, enabling immediate response.

Why It Matters Now

Adversarial threat actors are no longer simply stealing data. They are laying the groundwork for disruption, embedding within critical xOT environments. The presence of banned devices, combined with unmanaged connected-device risk, offers adversaries a reliable foothold.

With Prohibited Device Detection and Response, organizations can:

- ✓ Eliminate blind spots across millions of unmanaged devices
- ✓ Comply with NDAA and other mandates by finding and removing banned assets
- ✓ Deny adversaries persistence by hardening every connected device against default credentials, vulnerable firmware, and insecure configurations

The Path Forward

Dragos equips organizations to discover and assess, harden and remediate, and monitor and manage connected devices at scale. By bringing banned devices and hidden vulnerabilities out of the shadows, organizations can protect critical infrastructure from adversaries exploiting the devices meant to connect and enable it.

Next Steps

Schedule a demo to see how Dragos can help your organization identify, contain, and remove dangerous devices before they are weaponized.

About Dragos

Dragos is the world's leading OT cybersecurity firm headquartered in Washington DC, USA area with offices around the world. It provides the most effective OT cybersecurity technology for industrial and critical infrastructure to deliver on our global mission: safeguarding civilization. The Dragos Platform provides visibility and monitoring of OT environments for asset identification, vulnerability management, and threat detection with continuous insights generated by the industry's most experienced OT threat intelligence and services team. Dragos protects customers across the range of operational sectors, including electric, oil & gas, data centers, manufacturing, water, transportation, mining, and government.

Learn more: dragos.com

