



Dragos Platform Protocol Coverage

Overview

Dragos Sensors use deep packet inspection (DPI) to decode the protocols that run across extended operational technology (xOT) environments, from vendor-specific industrial control system (ICS) protocols and widely used OT standards to building automation, IoT, and IT traffic. That coverage is the foundation for asset visibility, vulnerability management, and threat detection in the Dragos Platform.

Dragos continuously evaluates and expands the breadth and depth of its protocol coverage through Platform releases and Knowledge Packs. Running a protocol you don't see here? Share your requirements with your Dragos account team or sales@dragos.com.

Vendor-Specific OT and ICS Protocols

Proprietary protocols used by automation, control system, and instrumentation vendors.

GROUP	FAMILY	PROTOCOLS
ABB	800xA	CNCP, CSLib, MMS, NIS, PN800, RNRP
	Other	Freelance, TotalFlow
ABICOR BINZEL	EWR / EWR2	BAEWR
Atlas Copco		OpenProtocol
AutomationDirect		CLICK PLUS, C-More HMI, ECOM (HAP)
Bachmann		Bachmann M1 Protocol
Beckhoff Automation		TwinCAT ADS, TwinCAT IO-RAW, TwinCAT NV
Cognex	DataMan and MX	DataMan Control Commands (DMCC)
Cooper Power Systems		SES-92
Digi International		ADDP
Eaton	MTL	MTL8000 Matrix
Emerson	Bristol Babcock	BSAP IP, BSAP Serial
	DeltaV	DOP, RTP, SIS
	Fisher ROC	ROC Plus
	Ovation	Data Highway, DB XMIT, Mgmt, REM, SSQuery, SSRPC, System Reservation, Toolserver, UDP 5230

Continued on next page

Vendor-Specific OT and ICS Protocols (continued)

GROUP	FAMILY	PROTOCOLS
GE		Genisys
	FANUC	EGD, SRTP
	InterSite	ISD
	Multilin UR	Modbus
	Proficy	iFix 2010, iFix Historian
	SDI	Classic SDI, SDI
Honeywell	Experion	Experion DSA, Experion SRP, SDP
	Mercor (Mercury)	Mercor
Johnson Controls		Metasys Private Message
Lantronix		Lantronix Discovery
Mitsubishi Electric		GOT2000, MELSECQ
Motorola		MDLC
NMEA		NMEA 0183
OMRON		FINS
OSIsoft		Pi-connect
Phoenix Contact	PLC	DDI, OPC, PCWorx, ProConOS
RDCCOM		RDCCOM
Red Lion Controls		Crimson Download Protocol
Rockwell Automation		CIP, CISP, CSP, ENIP, PCCC
Schneider Electric		NetManage, UMAS
	AVEVA	OASys DNA
	Foxboro	Comex
	Triconex	FW, P2P, TCM, Tristation, TSAA
	Wonderware	Suitelink
Schweitzer Engineering Laboratories (SEL)		ASCII, FM
Siemens		CAMP, NIPT, S7Comm, S7Comm-Plus, Sinaut ST7, Sinec H1
	Profinet	CBA, DCP, IO, MRP, MRRT, PTCP, RT
TechnipFMC	Smith Meter	SMIP
Yokogawa		Historian
	Centum	Vnet/IP

Widely Used OT Protocols

Open and standards-based protocols common across OT and ICS environments.

GROUP	FAMILY	PROTOCOLS
ASHRAE	BACnet	BACapp, BACnet, BVLC
CLPA	CC-Link	SLMP
CODESYS Group		CODESYS v2.0, CODESYS v3
DNP.org		DNP3
Eclipse Foundation		Sparkplug
EtherCAT Technology Group		EtherCAT
FieldComm Group		Foundation Fieldbus, HART-IP
IEC	IEC 60870	ICCP TASE.2, IEC 101, IEC 104
	IEC 61850	GOOSE, MMS, SV, UCA2 (GSSE)
	IEC 62439	HSR PRP
IEEE		C37.118, PTP, Synchrophasor
Industry Standard	ATG	Veeder-Root TLS
ISO		COTP, TSAP
KNX Association		KNX/IP
LonWorks		LonTalk
Modbus Organization		Modbus RTU, Modbus TCP
OPC Foundation		OPCAE, OPCDA, OPCHDA, OPCUA
Tridium	Niagara	Fox

Building Automation and IoT Protocols

Connected devices with influence over facilities and operations, from building systems to cameras and medical devices.

GROUP	FAMILY	PROTOCOLS
Audio/Video		Crestron
Automotive		SOMEIP
Building Automation		BACapp, BACnet, BVLC, KNX, KNX/IP, LonTalk, Metasys Private Message, Niagara Fox
IP Cameras/Video Surveillance		AXXON Next, Dahua DVR / IP Camera Control Protocol, Dahua IP Camera / IP PBX, DHIP, ONVIF Network Camera Device Discovery
Medical Devices		DICOM, Intellivue
Printers		Appsocket/Jetdirect, BJNP, Canon, LPD, TSPL/TSPL2
Other		CoAP, LANE POS, OneHome, PAX POS, Sparkplug

IT Protocols

IT traffic that crosses into OT networks, decoded for context on the assets and communications with influence over operations.

GROUP	FAMILY	PROTOCOLS
Cisco		CDP, Cflow, Cisco ACS, Cisco Fabric Manager, Cisco UCS alternative, Cisco UCS deployment, Cisco UCS Manager, Cisco VPN, Cisco Wireless LAN Controller, HSRP, NetFlow, UDLD, VTP
IBM		IBM HTTP Server Administration, IBM WebSphere Administration, IBM WebSphere Administrative Console, IBM WebSphere Alternative, IBM WebSphere Alternative HTTP, IBM WebSphere bootstrap, IBM WebSphere Process Server, IBM WebSphere secure channel, IBM WebSphere SOAP Connector, IBM WebSphere Virtual Host, Lotus Notes / Domino, WebSphere, WebSphere control port, WebSphere Node Metadata
IEEE		LLDP, STP
IETF	Application Services	Finger, FTP, IPP, NFS, TFTP
	Authentication & Security	Diameter, DTLS, GSSAPI, IKEv2, Kerberos 5, LDAP, OCSP, RADIUS, SPNEGO, TLS
	Core IP & Routing	ARP, BGP, CAPWAP, EGP, GRE, GRE TEB, ICMP, IGMP, IP in IP, LISP, OSPF, PGM, PIM, RARP, SCTP, TCP, Teredo, TPkt, VRRP
	Email	IMAP, POP3, SMTP
	IPv6	DHCPv6, NDP
	Management	SNMPv1, SNMPv2, SNMPv3, Syslog
	Naming, Time & Discovery	DHCP, DNS, MDNS, NTP, RDNS, SSDP
	Real-time Media	RTCP, RTP, RTSP, STUN
	Remote Access	RFB / VNC, SSH, Telnet
	Web & Proxy	HTTP, HTTP Proxy, HTTP-MGMT, HTTP-RPC-EPMAP, QUIC, SOCKS, WebSocket
Microsoft		BBN IAD / Microsoft RPC, LLMNR, Microsoft Exchange / Interweave, Microsoft Lync/Skype for Business, MSMQ, NTLM, RDP, TDS or MSSQL-TDS, Windows Communication Foundation, Windows Dynamic RPC, Windows Management Instrumentation (WMI), Winrm, WSD, WUDO
	NetBIOS	NetBIOS Browser, NetBIOS Datagram, NetBIOS Name Service, NetBIOS over TCP, NetBIOS Stream Service
	SMB	SMB, SMB Mailslot
Open Group	DCE	DCERPC, DCOM
Oracle		Oracle Application Server, Oracle Cluster File System, Oracle HTTPS Console, Oracle Web-tier / Terraria Server, Oracle WebLogic Server HTTP / BEA WebLogic, Tuxedo Client / Security controls
SAP		SAP Enqueue Replication Server, SAP GUI Communication, SAP Host Control, SAP Router, SAP Solution Manager
VMware		Apex Mesh / VMware Server Authentication, VMware esxi, VMware Host Agent, VMware Server, VMware Server Management Console, VMware vCenter

Continued on next page

IT Protocols (continued)

GROUP	FAMILY	PROTOCOLS
Applications & Services		AccessBuilder / IBM NetBios, ADB, AFP, AMS, Apple iOS Wireless Syncing / lockdownd, ATH, Cadlock Protocol, Cloud Gateway Protocol, EAQ, Ethereum JSON-RPC, FFST, gpsd, HP Loadrunner/Diagnostics, HP VM Group Management, Jamlink, Kontiki, Lwresd, MITML, Multicast FTP, NATO Link 16, OpenSSL / QUIC test configurations, Quagga OSPF daemon, Reserved / First Dynamic Port, RPCbind, rtip, RX, SCADA / Control system applications, SCO-Z-Phone, Secure RPC Alternative, Service Management Protocol, SIF, Sun RPC, Thunder, UPnP, WS-Discovery, Zebra / Quagga routing daemon
	Anonymizers & Malware	Android Emulator console / Sasser worm, Cisco/Linksys Router Backdoor, http-alt/Torpark, Metasploit Default Reverse Shell / I2P HTTP Proxy, NetBus Trojan / Moon Secure Antivirus, TINC, Torpark Onion Routing / Xpress Transport, UltraSurf, VLC Media Player streaming / Sub7 Trojan
	Application Servers	AJP, CORBA, Custom Application Cluster Communication, GlassFish Application Server Administration Console, Java JMX Management, Java RMI Alternative, Java RMI Registry, JBoss / Apache Tomcat Alternative, JGroups Cluster Communication, JRMP, JRun Web Server, Object Request Broker, RMI Activation System, SOAP, Tomcat/Wildfly extreme alternative, Visual Studio/Custom Apps
	Backup & Storage	Amanda Backup / Alternative HTTP, Backup Exec Agent, BackupExec / Commvault, Cluster configuration backup systems, Commvault Communication Service, Commvault Edge, Data mirroring / SAN systems, Data replication services, RSYNC, SAN systems alternative, Veritas Cluster Server, Veritas NetBackup / McAfee ePO, Veritas Storage Foundation, Webadmin/Backupexec
	Database	Apache Cassandra CQL client port, Apache Cassandra Inter-node Communication, Apache Cassandra Thrift API, Apache CouchDB, Apache Derby Database, Apache Hadoop HDFS / Impala StateStore, Apache Hadoop HDFS NameNode Web UI, Apache Hadoop Secondary NameNode Web UI, Apache Spark Master, Elasticsearch, Elasticsearch Transport Port, Firebird / InterBase Database, IBM DB2, InterBase database alternative, InterSystems Caché Web Management, MaxDB Database, Memcached, Microsoft SQL Server, MongoDB Database, MongoDB Routing Service Config Server, MySQL, Neo4j HTTP, Oracle Database Listener, Oracle ISQL, Oracle XDB, Pervasive SQL Transactional interface, Postgresql, Redis, Riak Protocol Buffers, SAP, SAP Sybase IQ Database, Sybase Adaptive Server Anywhere, Vertica Database / PostgreSQL alternative
	DevOps & Containers	Apache ZooKeeper, Atlassian Confluence, Atlassian Crowd API, Cockpit Web Console / Prometheus / WebSphere, CVS pserver, Dapr sidecar HTTP API, distcc distributed compiler, Docker REST API, etcd key-value store client port, Gearman job server, Hashicorp Consul, Kubernetes Nodeport, Octopus Deploy, SonarQube / PHP-FPM / Portainer, SonarQube Server, Subversion

Continued on next page



IT Protocols (continued)

GROUP	FAMILY	PROTOCOLS
Applications & Services (cont.)	Email & Directory	IMAP, IMAPS, Kerio connect, LDAPS, NNTP / Usenet, POP3, POP3S, SMTP, SMTP Alternative, SMTPS, Spamd, Tine 2.0 Webmail, Zimbra Administration Console
	File Sharing	Aimini, AppleJuice, Direct Connect, eDonkey, FastTrack, Gnutella, OpenFT, StealthNet
	Financial	FIX
	Gaming	Blizzard Battle.net games, Quake Server / Id Software games, Sony PlayStation Network Client, Unreal Tournament
	Legacy Services	Character Generator, Common Trace Facility, Daytime Protocol, Discard Protocol, Echo Protocol, Ident, Quote of the Day, Time Protocol
	Messaging	ActiveMQ / Borland Enterprise Server, AMQP, AMQP / RabbitMQ, Apache ActiveMQ Admin Web Console, Apache ActiveMQ OpenWire JMS Broker, Apache Kafka Broker, IBM Lotus Sametime / Replicated UI, IBM Sametime IM, IBM WebSphere MQ, IBM WebSphere Secure MQ, ICQ, imo, IRC Alternative, IRC Default, Messaging, MQTT, MQTT over TLS/SSL, NATS, QQ, RabbitMQ Web Management Interface, Wechat, XMPP, ZeroMQ
	Monitoring & Management	AgentX, Checkmk, collectd, Dell OpenManage, FlexNet / FLEXlm License Manager, HP iLO, HP Insight Manager, IPMI, Kibana Web UI, LANDesk Management Suite, Lantronix Device Installer / Ubiquiti discovery, Novell Zenworks, NRPE, OpenView Network Node Manager, Redfish, SentinelSRM/HASP, sFlow, Splunkd, UBNTAC2, Zabbix, Zabbix Server Monitoring Daemon
	Remote Access	3Com Telnet alternative, Alternative SSH / Custom remote configuration, AnyDesk Alternative / Software management, AS400 Telnet, Citrix ICA, Netop Remote Control, Netop Secure alternative, noVNC HTML5 VNC client / ArcGIS Server, pcAnywhere data, pcAnywhere status, RDP Alternative, rexec, RFB / VNC, rlogin, RSH, SSH, TeamViewer Remote Desktop, Telnet, Telnet SSL, VNC over HTTP / FireShare, X11, XDMCP
	Security	AVASTSecureDNS, CPHA, Metasploit Automation / RPC Daemon, Metasploit Web UI, Nessus Vulnerability Scanner Daemon, Rapid7 Nexpose Security Console, Symantec Antivirus Client, Symantec Endpoint Protection Manager, TACACS+, Tenable Nessus
	Streaming	Adobe Flash Media Server, Flash Media Server administration, Microsoft Media Server, MPEG-DASH, Peercast, QuickTime Streaming Server, RTMP, RTP, RTSP
	Telecom	GPRS Protocol, GTP, GTP Prime, GTP-C, GTP-U, SMPP

Continued on next page

IT Protocols (continued)

GROUP	FAMILY	PROTOCOLS
Applications & Services (cont.)	VoIP	Asterisk Manager Interface, Cisco Unified Communications Manager, H.323, IAX, Megaco, MGCP, NOE, SIP, SIP-TLS, Skinny/SCCP
	VPN	BGMP / Check Point VPN-1, Check Point VPN-1 Firewall-1 Management, ESP, FortiGate SSL VPN / Web UI alternative, IKEv2, IPsec, ISAKMP, NetScreen ScreenOS SSL VPN, OpenVPN, PPTP, SecuRemote, WireGuard
	Web Servers & Proxies	Alternative HTTP proxy/testing, Apache Traffic Server, cPanel, DirectAdmin Web Control Panel / Alternative SSH, FTP Proxy / CCProxy, HTTP Alternative, http-alt, http-alt/HEC, http-alt/WAS, Node.js / React Development Server / Grafana, Osxwebadmin, Sinatra Ruby framework / Tramp, Squid HTTP Proxy, Web Application framework debugging, wwwCrawler

Need coverage for a protocol not listed here?

Dragos adds protocol coverage based on what practitioners run in the field. Share the requirements for your environment with your Dragos account team or contact sales@dragos.com.

About Dragos

Dragos delivers xOT cybersecurity for industrial and critical infrastructure, backed by a decade of frontline incident response experience. The Dragos Platform provides asset visibility, continuous monitoring, vulnerability management, and real-time threat detection, all powered by industry-leading intelligence. Dragos protects OT environments globally, including electric, oil & gas, manufacturing, water, and transportation.

Learn more: dragos.com

