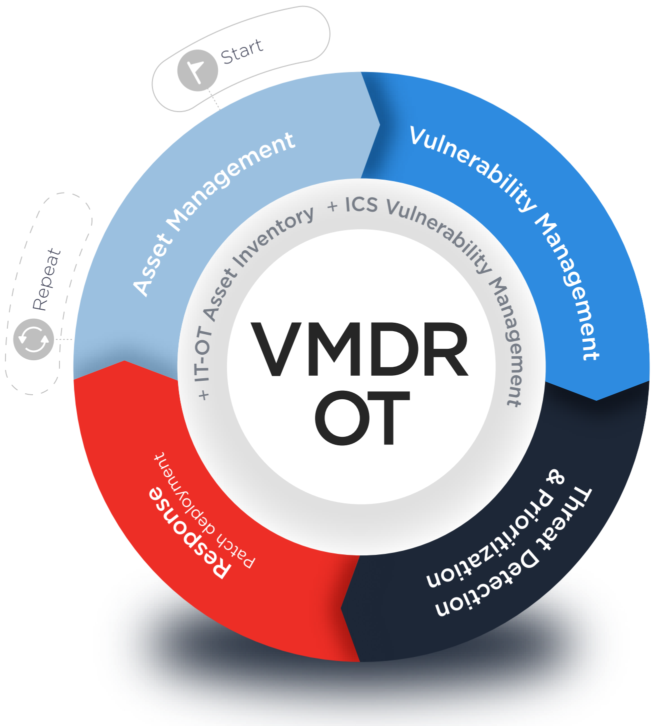
SOLUTION BRIEF

VMDR OT

View Industrial Assets & Manage Industrial Networks, Vulnerabilities & Threats

The interconnectivity between conventional IT networks and Operational Technology (OT) applications has increased productivity in the manufacturing, energy, and transportation sectors. However, this IT-OT convergence has also expanded the attack surface and exposed critical infrastructure to new cyber threats. Security stakeholders are now responsible for a network infrastructure that includes once air-gapped applications comprised of new industrial devices, that include programmable logical controllers (PLCs), remote terminal units (RTU), industrial gateways, and more. These industrial devices run on diverse industrial protocols and are geodistributed, remote, and sometimes mobile.

Vulnerability management technologies need to provide the same asset discovery, and security oversight for OT as they have provided for IT.

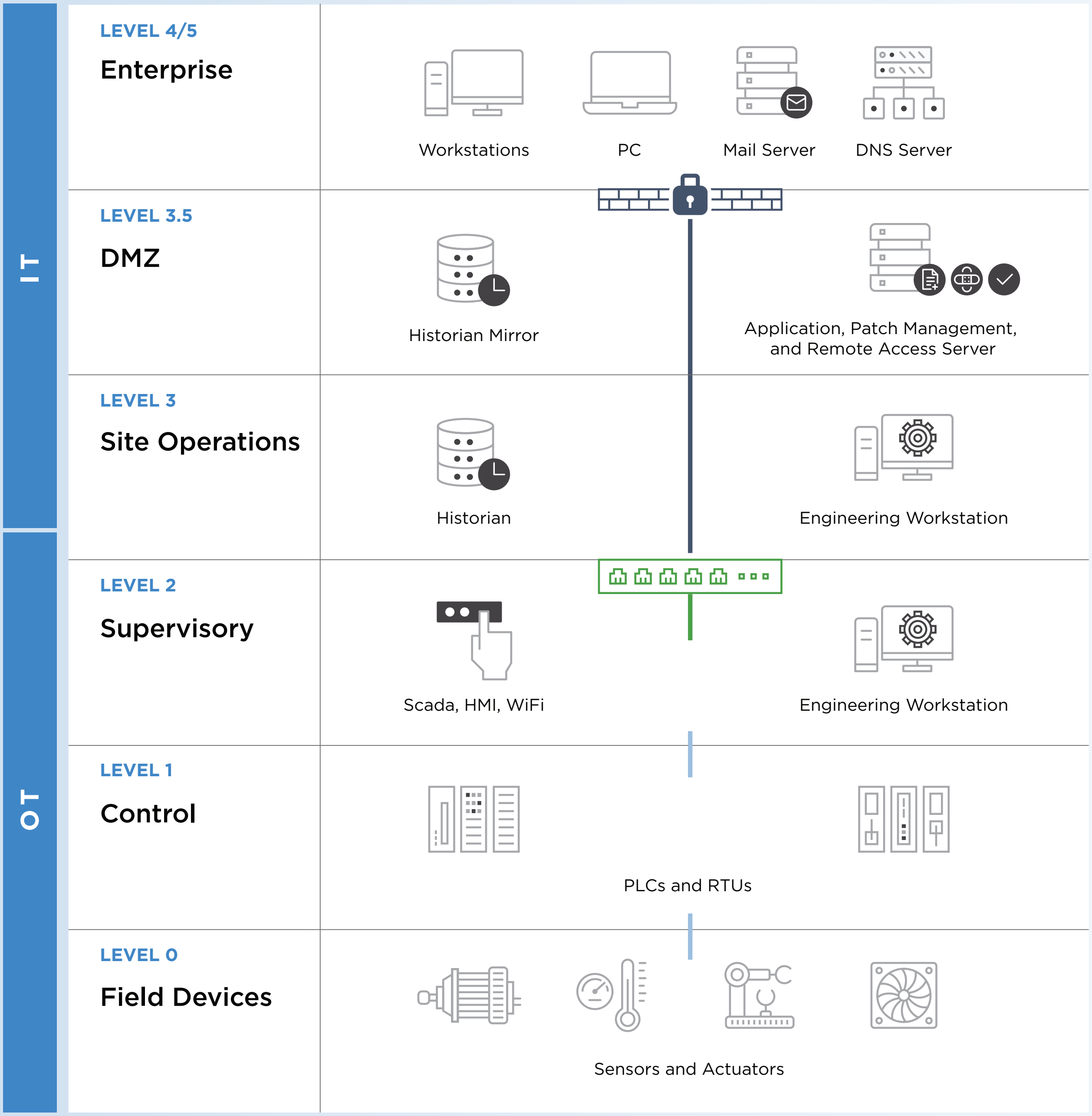


Finally, a single unified cybersecurity discovery, assessment, detection, and response solution for the hybrid IT-OT network environment.

Extend security and accelerate IT-OT convergence with a single agent, single dashboard, and single asset inventory.

Qualys VMDR OT is a cloud platform-based asset inventory and vulnerability management solution for real-time visibility into critical industrial infrastructure.

OT is a Platform Story



IT

OT

LEVEL 4/5
Enterprise
Workstations · PC · Mail Server · DNS Server

LEVEL 3.5
DMZ
Historian Mirror · Application, Patch Management, and Remote Access Server

LEVEL 3
Site Operations
Historian · Engineering Workstation

LEVEL 2
Supervisory
Scada, HMI, WiFi · Engineering Workstation

LEVEL 1
Control
PLCs and RTUs

LEVEL 0
Field Devices
Sensors and Actuators

Qualys VMDR OT Provides

Extensive ICS/OT Protocol Support ffor IT and ICS protocols including S7Comm, Profinet, Ethernet IP, S7comm Plus, BACnet, Modbus TCP, DNP3, MQTT, IEC 104, CIP, OPC UA, IEC 61850 MMS, IEC 61850 GOOSE, SLMP, EtherCAT, Beckhoff ADS, CC Link IE, Niagara Fox, Omron Fins, PCCC, and many more.

Broad Industrial Vendor Support for major distributed control systems (DCS) and industrial automation vendors including Rockwell Automation, Siemens, Schneider Electric, OSI Soft, Mitsubishi, Invensys, Advantech, Aveva, Beckhoff, GE, Yokogawa, Emerson, ABB, Delta Electronics, WAGO and more.

Continuous, Real-time Visibility into your industrial networks via the Qualys Passive Network Sensor by capturing and processing network traffic from mirror ports of managed switches, as well as performing deep packet inspection (DPI) of IT and ICS/OT protocols.

Safe Active ICS On-Demand Scans capture complete asset information non-intrusively within the network environment, automatically mirroring the ICS/OT protocol language of any and all devices within the network via Qualys active scanners.

Multi-site Management optimizes monitoring of distributed plant and applications via a unified central management dashboard for greater simplicity, scalability, management oversight and ROI for security practitioners.

Identification of Vulnerabilities with the Qualys Out-of-Band Configuration Assessment (OCA) function that gathers additional asset inventory and vulnerability detection information, allowing security practitioners to collect metadata and configuration information from devices on how, when, and what data is accessed.

Prioritized Vulnerability Response with Qualys TruRisk™ provides risk-based scoring of vulnerabilities and threat prioritization based on asset criticality and potential business impact for improved MTTR.

Key Use Cases for Qualys VMDR OT

CHALLENGE	SOLUTION	OUTCOMES
Achieving and Maintaining a Complete Asset Inventory of Your ICS/OT Devices ICS/OT devices and applications such as industrial PCs hosting operator stations, SCADA servers, engineering workstations, IT stations hosting manufacturing execution systems (MES), and remote connectivity workstations are often not visible within IT asset inventory solutions, thus leading to blind spots and increased exposure to cyber risk for the enterprise.	Qualys VMDR OT builds a comprehensive real-time asset inventory via multiple inputs including non-intrusive sensors that dissect industrial protocols. Authenticated scans triggered for all industrial endpoints with operating systems like Windows and Linux, as well as OS-based endpoints, provide a detailed asset inventory as well as related software vulnerabilities.	Complete, real-time asset visibility and monitoring capabilities extending device visibility across IT and ICS/OT applications and software, down to Field and Control network layers. Security practitioners receive complete device visibility regardless of location for improved compliance, reduced threat remediation and response time, and improved cybersecurity.
Preventing Lateral Movement of Cyber Threats ICS/OT devices and applications are exposed to a rising number of vulnerabilities and targeted malware that can infect industrial networks via their connectivity to IoT and IT networks. 70% of vulnerabilities can be exploited without needing special privileges. Security practitioners must identify and isolate vulnerabilities faster than ever before to ensure the risk of malware lateral movement is as low as possible.	Qualys VMDR OT provides continuous vulnerability assessments on all industrial assets on a continuous basis. Hardware and firmware-based vulnerabilities impacting PLCs, IOs, Robots, HMIs, drives, etc. as well as software vulnerabilities affecting SCADA servers, MES & ERPs systems and other industrial applications are covered with Quays passive sensors, Qualys scanners, and optional cloud agents enabling security practitioners to formulate zero-trust network access policies within ICS/OT without effecting network performance.	With Qualys VMDR OT, security practitioners are able to identify and manage vulnerabilities at all ICS/OT endpoints, enabling zero-trust segmentation, targeted remediation, and detailed compliance programs that reduce lateral movement of cyber threats between industrial applications, as well as between IT and OT network environments.
Out of Band Vulnerability Monitoring One of the greatest contributors to risk and network downtime comes from the human factor within an ICS/OT environment. For example, misconfigurations may allow attackers to elevate permission to access and exploit critical infrastructure using ransomware for example. Monitoring out-ofband vulnerabilities is key to maintaining compliance and preventing cyber threats.	In addition to the Qualys Passive Sensor, this Out-of-Band Assessment (OCA) function gathers additional asset inventory and vulnerability detection information. With OCA, users can easily collect metadata and configuration information from industrial devices; thus controlling how, when, and what data is accessed — and by whom.	With out-of-band assessment (OCA) metadata, security practitioners can examine vulnerabilities and calculate risk with greater context, thus improving security policy implementation and lowering the potential contribution of human factors to cyber risk and potential downtime.
Integrating Endpoint Security for ICS/OT For ICS/OT security practitioners, legacy perimeter defense technologies have vast limitations for modern ICS/OT networks, leaving security practitioners unable to identify insider threats and over-dependent on industrial firewalls. Therefore, endpoint detection and response (EDR) has become increasingly relevant for ICS/OT, but integrating them is cumbersome, complex, and expensive.	VMDR OT can be combined with Qualys Multi-Vector EDR to provide ICS/OT security practitioners with behavioral detection, threat intelligence, and machine learning within their network environment to help identify important threats and IOCs related to SCADA & HMI Servers, Engineering tools, Historians and other devices at supervisory levels. Qualys Multi-Vector EDR is a separate SKU.	With Qualys Multi-Vector EDR, VMDR OT unifies different context vectors like asset discovery, vulnerabilities and exploits, misconfigurations, in-depth endpoint telemetry, and network coverage with a powerful back end to correlate it all for accurate assessment, detection, and response actions from a single agent, single platform, and single dashboard.
Policy Compliance for Industrial Assets Auditing policy compliance reports, especially within heavily regulated industries such as power transmission and distribution and petrochemicals, is critically important for security and liability reasons. However, it is also complex, time-consuming, and expensive.	VMDR OT is continuously updated to monitor and enforce compliance with the latest government regulations and industry mandates with Qualys Policy Compliance, which includes compliance monitoring for NERC CIP, IEC-62443, and much more. Qualys Policy Compliance is a separate SKU.	Maintaining policy compliance and reporting are faster, more accurate, and less resource-intensive with Qualys VMDR OT. Reduce compliance audit time and costs with Qualys Policy Compliance, allowing security operations to focus on high-value security tasks.