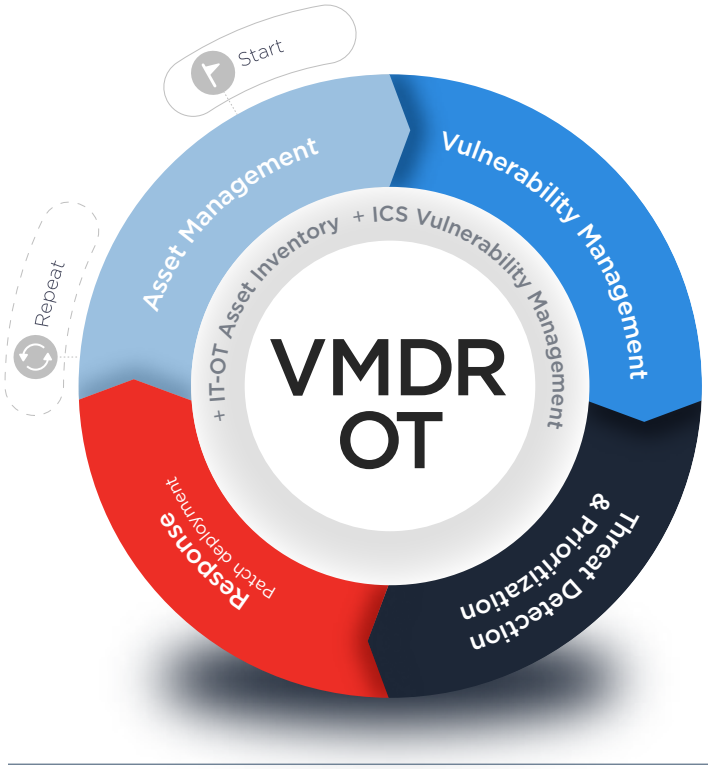
Qualys.

# VMDR OT

## Real-time visibility into critical Industrial Networks, Assets and Manage Vulnerabilities & Threats

The interconnectivity between conventional IT networks and Operational Technology (OT) applications has increased productivity in manufacturing, energy, and transportation sectors. However, this IT-OT convergence has also expanded the attack surface and exposed critical infrastructure to new cyber threats. Cybersecurity 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 geo-distributed, remote, and sometimes mobile.



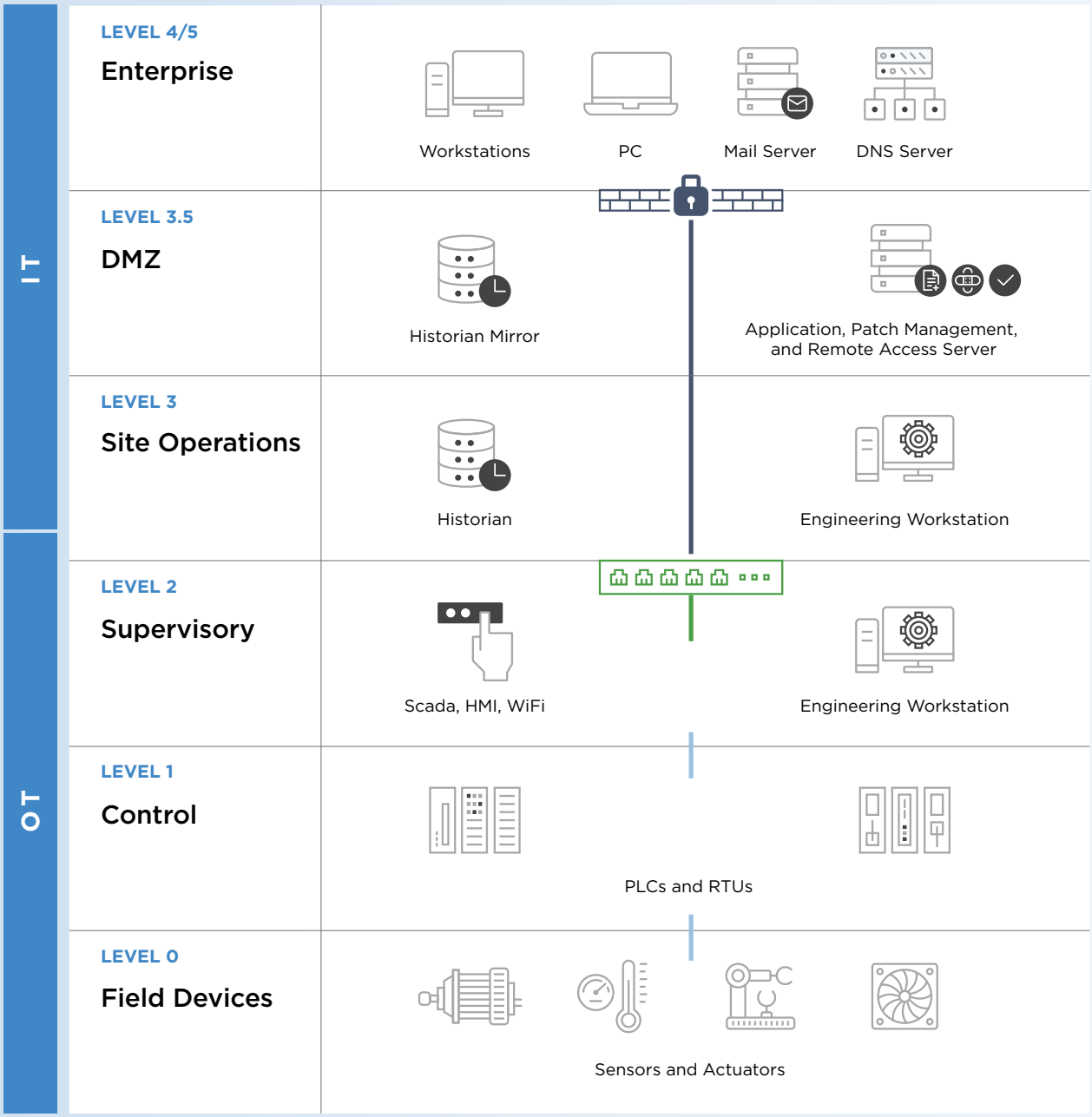

Finally, a single unified cybersecurity discovery, assessment, detection, and response solution for the hybrid IT-OT network environment.

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

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

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

## OT is a Platform Story



## Qualys VMDR OT Provides

**Extensive ICS/OT Protocol Support** for 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 DCS and industrial automation vendors like 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** inside your industrial network via the Qualys Passive Network Sensor, capturing and processing network traffic from mirror ports of managed switches and does deep packet inspection (DPI) of IT and ICS/OT protocols.

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

**Multi-site Management**
to support multi-fleet application and geo-distributed plant monitoring via a central management dashboard provided without additional deployments for greater simplicity, scalability, management oversight and ROI for security practitioners.

**Misconfiguration Identification** with the Qualys Out-of-Band Configuration Assessment (OCA) function 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 Management** with Qualys TruRisk™, VMDR OT provides risk-based scoring that identifies vulnerabilities and prioritizes threats according to asset criticality and potential business impact for improved remediation efforts.

# Key Use Cases for Qualys VMDR OT

| USE CASE CHALLENGE | SOLUTION | OUTCOMES |
|---|---|---|
| **Achieving and Maintaining a Complete Asset Inventory of Your ICS/OT Devices**<br>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 enterprise 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 engines that include non-intrusive sensors that dissect industrial protocols.<br>Authenticated scans triggered for all industrial endpoints with operating systems like Windows, Linux and OS-based endpoints provide detailed asset inventories 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 can accomplish complete device visibility regardless of location for improved compliance, reduced threat remediation and response time and improved cybersecurity. |
| **Preventing Lateral Movement Containment**<br>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.<br>Security practitioners must identify and isolate vulnerabilities faster than ever before to ensure the risk lateral movement of malware is a low as possible | Qualys ICS provides continuous and robust 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 a passive sensor, Qualys scanner, and optional Cloud agent, enabling security practitioners to formulate zero-trust network access (ZTNA) policies within ICS/OT without effecting network performance. | With Qualys VMDR OT, security partitioners are able to identify and manage vulnerabilities at all ICS/OT endpoints, enabling zero-trust segmentation, targeted remediation and compliance programs to reduce lateral movement of cyber threats between industrial applications, as well as between IT and OT network environments. |
| **Out of Band Vulnerability Monitoring**<br>One of the greatest contributions to risk and network downtime comes from the human factor within an ICS/OT environment. Misconfigurations may allow attackers elevate permission access and exploit critical infrastructure to ransomware for example. Monitoring Out of Band vulnerabilities are key to maintaining compliance and preventing cyber threats. | In addition to Qualys Passive Sensor, this Out-of-Band Assessment (OCA) functionality gathers additional asset inventory and vulnerability detection information. With OCA, customers can easily collect metadata and configuration information from devices, controlling how, when, and what data is accessed — and by whom. | One of the greatest contributions to risk and network downtime comes from the human factor within an ICS/OT environment. Misconfigurations may allow attackers elevate permission access and exploit critical infrastructure to ransomware for example. Monitoring Out of Band Configurations are key to maintaining compliance and preventing cyber threats. |
| **Integrated Endpoint Security for ICS/OT**<br>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 leverage behavioral detection, threat intelligence, and machine learning within their network environment to helps identify important threats and IOCs related to SCADA & HMI Servers, Engineering tools, Historians and other devices at supervisory levels. It is important to note that Qualys Multi-Vector EDR is a separate SKU. | With Multi-Vector EDR, VMDR OT unifies different context vectors like asset discovery, vulnerabilities and exploits, misconfiguration, in-depth endpoint telemetry, and network reachability with a powerful backend to correlate it all for accurate assessment, detection, and response actions from a single agent, single vendor and single dashboard. |
| **Policy Compliance for Industrial Assets**<br>Auditing and reporting policy compliance reports, especially within heavily regulated industries such as power transmission and distribution (PT&D) and petrochemicals is critically important for security and liability reasons, but also complex and expensive. | VMDR OT is continuously updated to monitor and enforce compliance with latest in compliance requirement with the Qualys Policy Compliance functionality, which includes compliance monitoring for NERC CIP, IEC-62443 and more. It is important to note that 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 more on high-value security tasks. |