

Strengthen IT/OT Security with QNAP

From Storage to Layered Protection,
Ensuring Uninterrupted Operations



IT/OT security step-by-step, steady and right

In modern enterprises, IT systems and OT (Operational Technology) environments are already inseparable, with cyber threats extending from office networks to production floors. For many manufacturers, practicing OT security is often not a resource issue, but rather a challenge of methods and implementation.

QNAP understands the real-world challenges enterprises face when implementing cybersecurity. That’s why we don’t advocate a “one-shot” approach, but rather building a visible, manageable, and enforceable security foundation from storage to protection. This allows SMBs to steadily take each step toward IT/OT security.



of manufacturing firms experienced a rise in security incidents or



felt adequately equipped to manage these threats



state that OT security complexity was top concern

Data source
<https://www.telstrainternational.com/en/news-research/research/secure-manufacturing-the-challenges-of-IT-OT-convergence>
<https://www.paloaltonetworks.com/blog/network-security/state-of-ot-security-2024/>



QNAP transforms storage technology into cyber defense power, safeguarding enterprise IT/OT security frontlines

QNAP offers a wide range of solutions, including storage, networking, threat detection, offline backup, and remote access.

QNAP solutions align with leading OT cybersecurity frameworks such as NIST CSF and IEC 62443, helping critical industries stay secure and compliant. We empower enterprises to build security architecture that is visible, resilient, and recoverable across IT and OT environments.





Cybersecurity, guided by the right blueprint.

Building IT/OT defense step by step with NIST CSF 2.0

- The NIST Cybersecurity Framework (CSF) has been widely adopted by enterprises, manufacturers, and critical infrastructure. The 2024 update of NIST CSF 2.0 further enhances its practical applicability to OT environments.
- The six core functions (Identify, Protect, Detect, Respond, Recover, Govern) provide enterprises with a clear cybersecurity blueprint.
- The framework emphasizes layered defense, asset visibility, incident response, and recovery capabilities—highly aligned with QNAP's solution architecture.
- For small and medium-sized businesses, NIST CSF is not just a standard but also a practical roadmap for phased implementation.
- QNAP leverages NIST CSF 2.0 as its foundation, integrating NAS, networking devices, and security applications to help enterprises build feasible IT/OT cybersecurity defenses.



From standards to practice

QNAP Solutions fully address the core functions of NIST CSF 2.0

- Supported across all product lines
- Only supported by specific product models; not all series
- Non-support

Function Category	Pain Points	Solution	NAS	QHora Router	ADRA Switch	QSW Managed Switch
Identify	Diverse IT/OT environment devices lacking a unified asset inventory	Centralized device manage	●	●	●	●
		Visualized inventory	●	●	●	●
		Cloud monitoring	●	●	—	●
Protect	Legacy control systems are unable to defend against modern threats	Data encryption	●	●	—	—
		Multi-layer access control	●	●	—	●
		Network segmentation	●	●	●	●
Detect	Lack of real-time monitoring for anomalies in IT/OT environments	Device anomaly detection	●	●	●	●
		Login anomaly detection	●	●	●	●
		Network anomaly detection	●	●	●	●
Respond	No immediate notification/reporting mechanism during incidents	Instant alerts	●	●	●	●
		Remote access	●	●	●	●
		Cloud management	●	●	—	●
Recover	No automated backup mechanism; difficult disaster recovery	Backup mechanisms	●	●	—	●
		Data integrity	●	—	—	—
		Disaster recovery	●	—	—	—



From storage to networking, QNAP strengthens IT/OT Cybersecurity



A black QNAP Network Attached Storage (NAS) device is shown in the upper left corner. It has a textured front panel with a series of horizontal ridges. On the right side of the front panel, there are four green status LEDs and the QNAP logo. The device is sitting on a blue, reflective surface that looks like a modern desk or table. In the background, there are several dark, rectangular blocks stacked on top of each other, creating a sense of depth and a futuristic, tech-oriented environment.

NAS

A key storage, backup, and application integration platform for IT/OT environments

- Supports AI analysis, virtualization, QuFirewall, and AMIZcloud management
- Some models feature industrial-grade design (desktop, rackmount, wall-mount, dual power), suitable for harsh environments

Enterprise-class QuTS hero NAS:

- Reliable file storage and backup (snapshots, immutable backups, WORM)
- High availability (HA) architecture to minimize downtime risk

A silver QNAP QHora Series router is shown in the top left corner of the slide. It has a textured front panel with a grid of ventilation holes and a small display with four colored LEDs (yellow, orange, green, and white). The QNAP logo and 'QHora Series' are visible on the top right of the device. The background is a dark, futuristic-looking surface with blue lighting and architectural lines.

QHora Routers

Enabling IT/OT cross-domain network security and interconnect protection

- Policy-based / microsegmentation routing, L3 - L7 firewall, DPI packet inspection, IPS intrusion prevention
- Supports Qbelt (DTLS + AES-256), WireGuard, OpenVPN for secure end-to-end transmission
- Secure wireless access with WPA/WPA2/WPA3 Wi-Fi

QuWAN SD-WAN:

- Multi-site interconnection and centralized management
- WAN optimization and automated failover ensures stable remote connections

ADRA NDR Switches

Real-time IT/OT network protection against malicious traffic and abnormal behavior

- Supports AI anomaly detection across hundreds of devices, early detection of internal and external threats
- Automated incident response and remediation with advanced traffic analysis for precise attack interception
- Prevents lateral movement, isolates infected devices, blocks suspicious activity
- SOC/SIEM integration; protects NAS, PCs, printers, and PoE devices; building a complete network defense





QSW Managed Switches

Delivering long-distance, high-bandwidth, low-latency backbone connectivity for IT/OT systems

- 2.5GbE / 10GbE / 25GbE / 100GbE fiber & copper connectivity, suitable for enterprise core/edge networks
- VLAN and QoS management to optimize traffic for different applications
- Supports AMIZcloud centralized monitoring and management
- Some models feature PoE for powering devices; designed for harsh environments

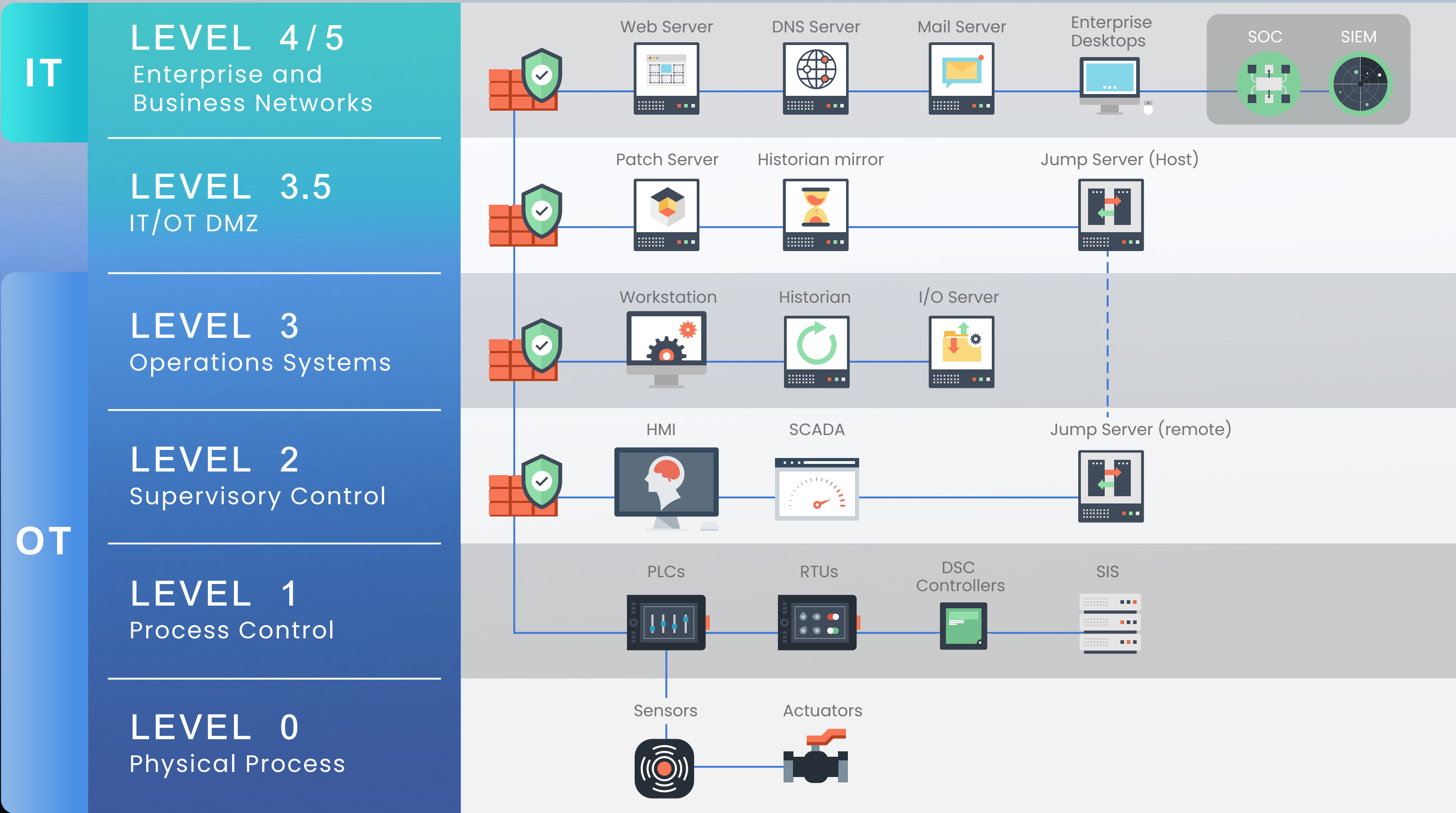
Enterprise-class L3 Switches:

- Built-in MC-LAG HA ensures 24/7 uninterrupted operation
- PTP IEEE ITU-T G.8273.3 Class A <100ns time synchronization, meeting OT/industrial control precision requirements

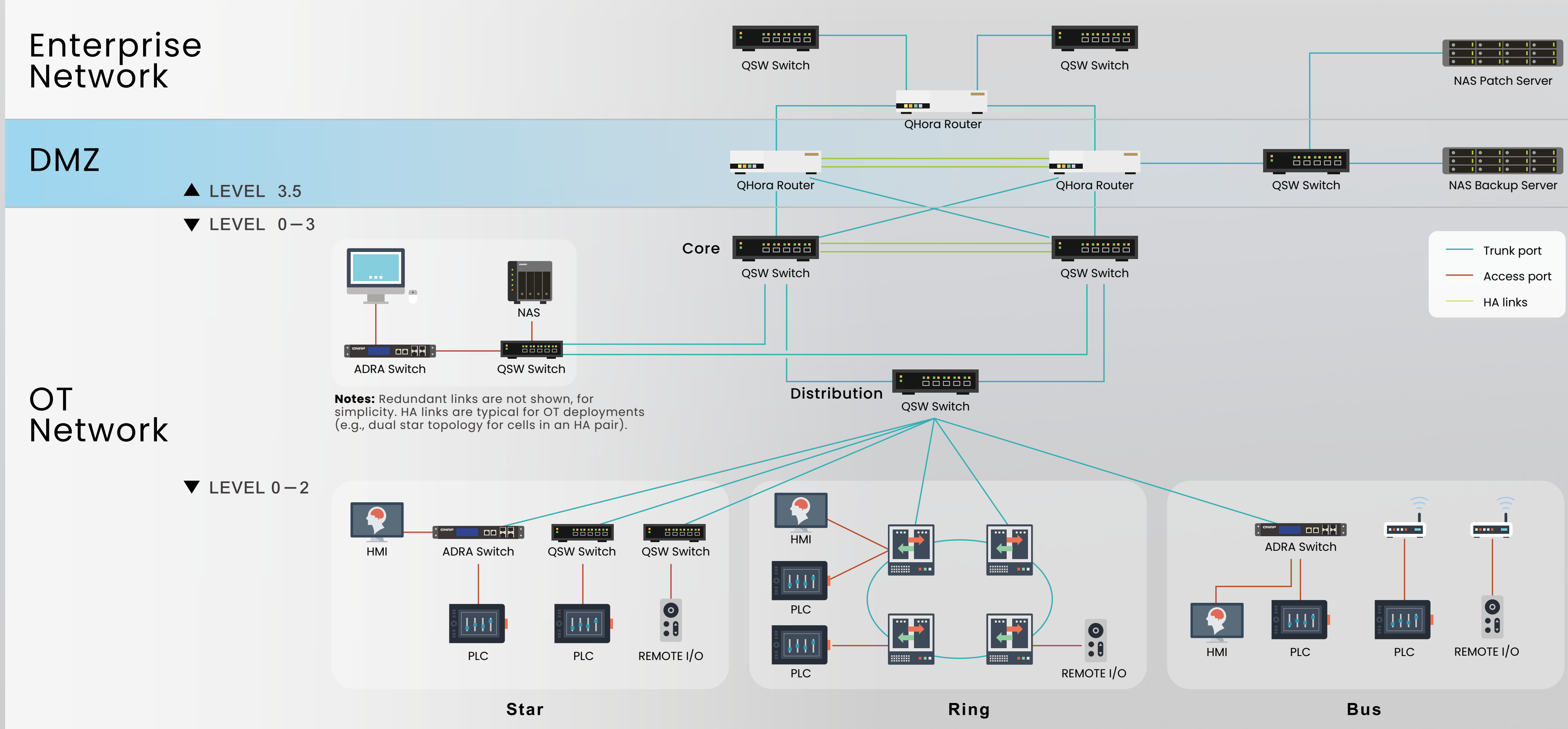
Building on the Purdue Model – Comprehensive protection for IT/OT

Enterprises can adopt the internationally recognized **Purdue Model*** as a layered industrial control network architecture. By clearly defining the roles and boundaries between IT and OT, the model provides a solid foundation for establishing robust cybersecurity defenses and enabling cross-domain collaboration.

* A commonly used framework for layered industrial control networks, widely applied in ISA/IEC 62443 and NIST 800-82 standards.



QNAP safeguards IT/OT Convergence Layer Cybersecurity



Breaking Down the Five Core Functions of NIST CSF 2.0 Building a Practical IT/OT Cybersecurity Defense



Identify

From asset visibility to user awareness — building the foundations of IT/OT security

The first step in cybersecurity is “**knowing what you own.**” In practice, however, many enterprises face challenges such as fragmented asset management, scattered accounts, and complex connectivity. QNAP helps organizations establish an effective risk control foundation by enabling identification and access management across people, devices, networks, and data.

Centralized Asset Inventory & Device Management

- **QuWAN Orchestrator:** The SD-WAN cloud orchestration system enables automatic identification and centralized management of enterprise network segments with QNAP devices, including IP address, model, and device status.
- **ADRA NDR Switch Device Inventory:** Through packet analysis, it automatically identifies connected devices in the network, including MAC address, IP address, hostname, and status.

Disaster Recovery Capability:

- With Snapshots, systems can quickly be restored to normal, minimizing downtime and reducing risks from human error or malicious attacks.

Comprehensive Data Backup & Recovery Solutions:

- QNAP provides all-round backup solutions covering Windows PCs, servers, SaaS cloud data, and virtual machines (VMs) to minimize the risk of data loss and ensure operational continuity.



Protect

Multi-layer defense mechanisms — comprehensive protection for systems, data, and networks

In OT environments, relying on a single defense measure is no longer sufficient to withstand modern attacks. QNAP provides multi-layer protection mechanisms—from systems to data, from internal networks to network management—enhancing infrastructure resilience and ensuring uninterrupted production and operations.

NAS System Protection:

Supports Multi-Factor Authentication (MFA) and built-in firewall to prevent unauthorized access and malicious operations, ensuring NAS stability and availability.

Data Security & Immutable Storage:

Protects data integrity with AES-256 encryption and immutable storage (WORM, Object Lock). Combined with Airgap+ isolated backups, it safeguards against ransomware and prevents backup devices from prolonged network exposure.

Internal Threat Isolation:

ADRA NDR rapidly detects and filters malicious OT network traffic, monitoring for lateral movement and malware propagation, effectively blocking attackers from spreading or exfiltrating sensitive data.

Network Segmentation & Access Control:

QNAP switches leverage VLAN and ACL to segment production, monitoring, and management networks, reducing cross-domain risks and enhancing secure isolation.



Detect

Deploy monitoring systems to analyze network traffic and user behavior

The lack of real-time monitoring for abnormal OT network traffic and behavior allows threats to linger and cause greater damage. QNAP provides comprehensive, real-time monitoring of system, network, and traffic behaviors to quickly detect anomalies, shorten response times, and ensure production and operational safety.

System and Operational Status Monitoring:

NAS continuously monitors system status, file activity, and access logs to quickly identify unauthorized access, abnormal logins, and suspicious actions. Through AMIZcloud centralized management and QuWAN orchestration, administrators gain full visibility into all QNAP devices’ operational states and risks.

Perimeter Network Threat Detection:

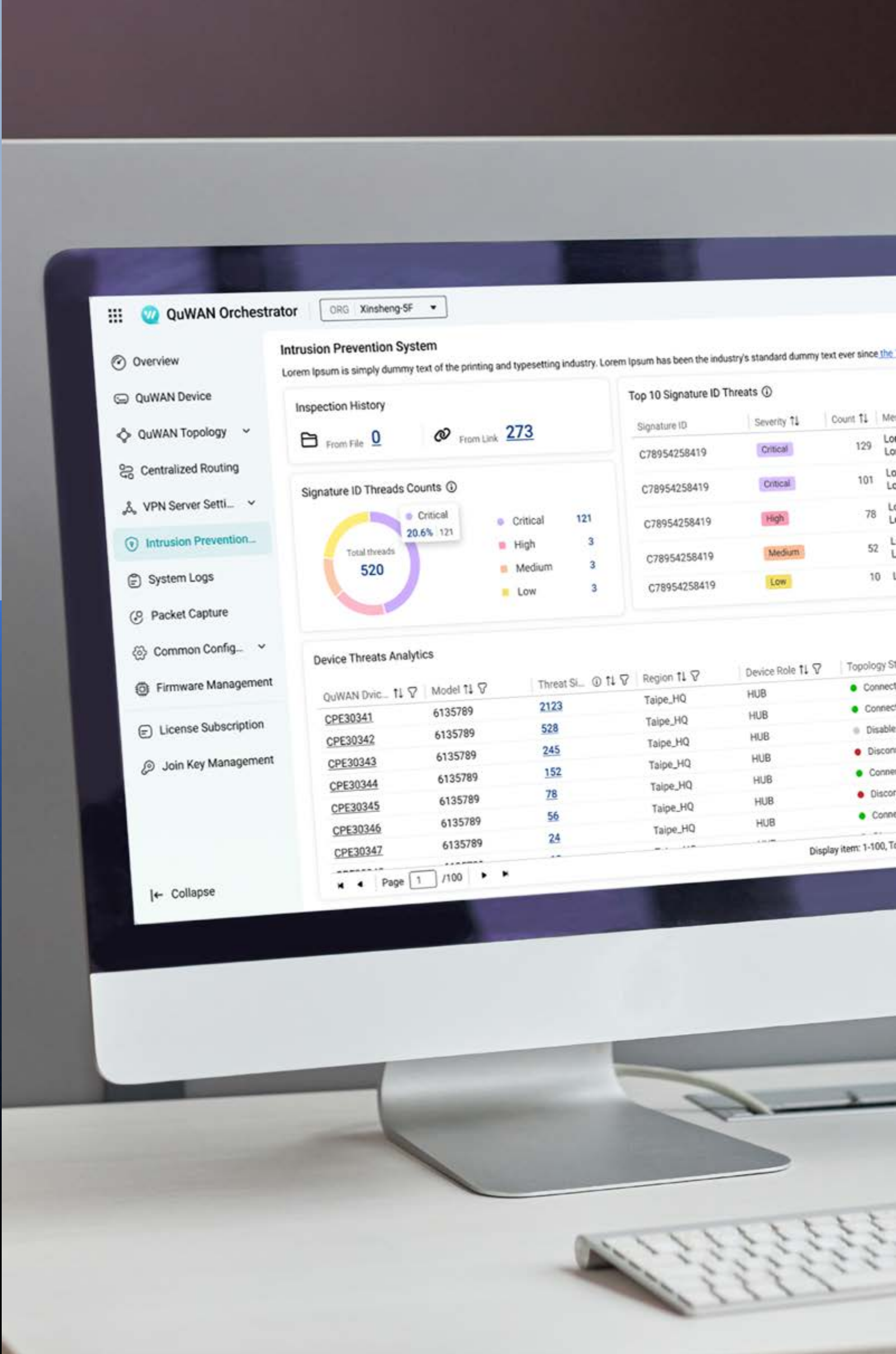
QHora routers offer Intrusion Prevention System (IPS) and deep packet inspection, identifying and blocking malicious traffic to reinforce OT and IT network perimeter security.

Malware Detection and Removal:

Perform scheduled antivirus scans on NAS to detect and eliminate malicious software. QNAP’s regularly updated virus definitions ensure up-to-date protection. In addition, ADRA NDR Trap provides early-stage malware detection and alerts for proactive defense.

Internal Network Behavior Analysis:

ADRA NDR conducts deep analysis of OT traffic and internal behavior, continuously monitoring and automatically flagging suspicious activity to prevent lateral threat propagation.



Respond

Real-time alerts, containment, and remote system updates to effectively stop threats

In OT environments, any delay or mishandling of a security incident can cause production line disruptions or safety accidents. QNAP provides instant notifications and rapid containment to stop threats before they spread.

Real-Time Event Notifications:

With the Notification Center, abnormal events can be simultaneously pushed to multiple channels (including email, SMS, syslog, and webhooks), ensuring security teams and on-site staff are immediately informed.

Rapid Threat Containment:

When an incident occurs, ADRA NDR Switches quickly confirm the threat source and isolate compromised devices to stop malicious traffic from spreading. This ensures other OT systems remain operational and reduces overall impact.

Remote Device Updates:

Using AMIZcloud and QuWAN SD-WAN, administrators can remotely manage QNAP devices, performing operations such as shutdown, reboot, and system updates. This accelerates patch deployment, closes vulnerabilities in time, and reduces the risk of human error.

Malware Removal:

Scheduled malware removal ensures that infected processes are immediately terminated, preventing further damage to systems and data.



Recover

Implement disaster recovery and data integrity backup architectures

The core goal of OT environments is “uninterrupted production.” QNAP focuses on rapid disaster recovery and maintaining data integrity to ensure normal operations can be restored ASAP.

High-Availability Backup Architecture (Servers & Networks):

Through NAS HA (Active/Passive High Availability) and switch MC-LAG, systems can automatically failover to backup equipment during outages, ensuring business continuity and preventing OT control system interruptions.

Disaster Recovery Capability:

With Snapshots, systems can quickly be restored to normal, minimizing downtime and reducing risks from human error or malicious attacks.

High-Availability Backup Architecture (Multi-Site):

QHora routers with QuWAN enable multi-site WAN backup in OT environments. Cross-site failover automatically switches to alternative nodes and routes. Dual-WAN ensures seamless local-to-cloud link failover for uninterrupted remote/cloud services.

Comprehensive Data Backup & Recovery Solutions:

QNAP provides all-round backup solutions covering Windows PCs, servers, SaaS cloud data, and virtual machines (VMs) to minimize the risk of data loss and ensure operational continuity.



Cybersecurity doesn't have to be achieved all at once — but it must begin.

With QNAP solutions, drive IT/OT security transformation with confidence, delivering complete protection from storage to cybersecurity, and ensuring resilient business operations.

From devices to access control
gain full visibility into enterprise assets
and user behaviors.

From deployment to mitigation
effectively integrate security defenses
and operational efficiency.

From prevention to recovery
comprehensively safeguard
operational stability.



Learn More

QNAP helps you take the first step toward IT/OT security, starting with your existing infrastructure.

Want to know which solutions best fit your environment?
Need deployment advice or technical consultation?

Contact Us

QNAP Systems, Inc.
New Taipei City
Email: sales@qnap.com
Tel: +886 2 2641 2000

QNAP Inc. (USA)
Pomona CA
Email: usasales@qnap.com
Tel: +1-909-595-2782

QNAP Inc. (Canada)
Markham, Ontario
Email: canadasales@qnap.com
Tel: +1-905-947-1000

QNAP GmbH (Germany)
Willich
Email: desales@qnap.com
Tel: +49-2154-88428-0

QNAP SRL (Italy)
Roma
Email: eusales@qnap.com
Tel: +39-(0)687-738456

QNAP UK Limited
Swindon
Email: uksales@qnap.com
Tel: +44-(0)333-344-2522

QNAP Japan
Tokyo
Email: jpsales@qnap.com
Tel: +81-3-5901-9735

QNAP Korea
Seoul
Email: krsales@qnap.com

