Solution Brief

PAS
Ensuring **OT** Integrity

A THREE-STEP APPROACH TO OT CYBERSECURITY

How modular in-product expansion supports organizations as OT security programs mature

Executives and boards in industrial organizations want to understand current risk profiles and whether a recently disclosed vulnerability puts the organization at risk. However, OT cybersecurity is less mature than IT cybersecurity. Most industrial organizations are still in the early stages of improving their OT asset inventories, relying on manual approaches for risk identification, prioritization, and remediation. OT cybersecurity maturity can also vary widely across sites within a larger organization. PAS finds OT cybersecurity can be grouped into three general steps – visibility, vulnerability, and comprehensive OT security and risk management. PAS Cyber Integrity™ provides a modular solution that provides these capabilities and can expand as OT security needs mature.

OT Security Program Maturity Levels

VISIBILITY

- How do I know what OT assets I have?
- How are my OT assets connected?
- What are they communicating with?
- What is this new asset on my PCN?

VULNERABILITY

- Do my OT assets have this vulnerability?
- Where are they?
- Who owns them?
- What is already patched?
- What still needs to be patched?
- Who is patching what when?
- Are OT assets becoming more vulnerable or less vulnerable over time?

COMPREHENSIVE OT SECURITY & RISK MANAGEMENT

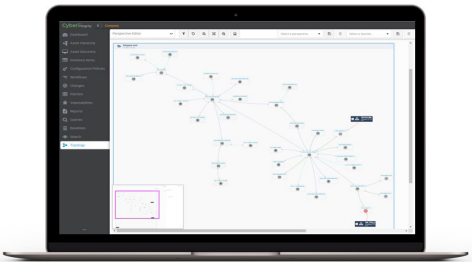
- What is my enterprise-wide OT cyber risk profile?
- Which remediation activities will improve OT security the most?
- How do I measure conformance with corporate OT cybersecurity policies?
- How do I demonstrate compliance with external OT cybersecurity standards?
- How can I prove compliance with industry regulations to auditors?
- How can I streamline efforts required to demonstrate compliance?
- How do I know when the configuration of an OT asset changes?
- How do I know if a change made to an OT cyber assets was authorized?

STEP1: VISIBILITY

Obtaining an accurate and detailed OT asset inventory is foundational for improving OT cybersecurity maturity. It is also a prerequisite for OT cyber vulnerability and risk management, meeting internal and external compliance requirements, understanding potential attack vectors, and investigating incidents.

Cyber Integrity – Inventory provides unmatched industrial control systems discovery and topology mapping — down to Level 0 devices — without passive network detection limitations and active network polling risks.

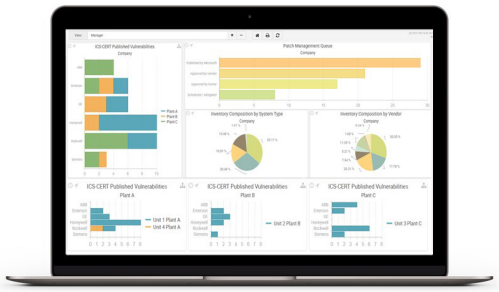
- Automatically discover IT and OT assets (Level 3 – Level 0) for over 120 cross-vendor OT systems
- Maintain a complete inventory of IT and OT system hardware and software, I/O cards, firmware, applications, and any custom data
- Identify compromised endpoints, their relationships and connections with other endpoints, and their role in the process



STEP 2: VULNERABILITY

With a comprehensive OT asset inventory in place, vulnerability management is the next step. Identifying and remediating known vulnerabilities is one of the best ways to reduce critical infrastructure risks. However, despite many known vulnerabilities for industrial control systems, OT teams often struggle to identify vulnerabilities.

Cyber Integrity – Vulnerability Management includes inventory management and also identifies and assesses vulnerabilities hidden in industrial infrastructure.

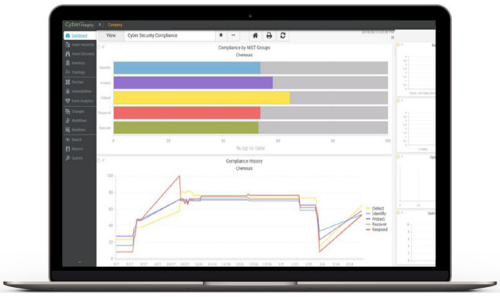


- Automatically compare and assess the latest vulnerability information from the United States National Vulnerability Database (NVD) – and further enriched by PAS cybersecurity analysts – with inventory data to identify OT assets with vulnerabilities that may put production systems at risk
- Obtain a centralize, unified view of current patch levels across all managed cyber assets
- Identify health and security events that may impact the reliability of Windows computers supporting critical industrial processes

STEP 3: COMPREHENSIVE OT SECURITY & RISK MANAGEMENT

With a detailed and accurate OT asset inventory and operational vulnerability and patch management in place, the final stage of maturity is to enable capabilities for comprehensive OT security baselines, configuration management, policy management, and workflows to manage compliance.

Cyber Integrity – Enterprise includes inventory, vulnerability and patch management, and adds in-depth Level 3 to Level 0 OT asset configuration management, comprehensive cybersecurity configuration baselining, unauthorized configuration change detection, workflow-driven vulnerability remediation and incident response, risk analyses, compliance workflows and reporting, and backup and recovery support.



- Track configuration changes against established baselines
- Establish configuration policies to monitor for unauthorized changes to control strategies, device inventory, asset configuration, and logical and graphical files
- Enable workflows and documentation for vulnerability remediation and compliance with NIST, ISA/IEC 62443, NERC CIP, ISO 27001/2, the NIS Directive, and other regulations
- Capture full configuration backups to support in-depth forensic analysis and speed recovery in the event of a worst-case scenario

BUILT FOR TODAY AND TOMORROW

The cyber risk for critical infrastructure and process industries is greater than ever. Digitalization projects and remote work have expanded the attack surface. The modular licensing and deployment capabilities of Cyber Integrity provide flexibility to address current needs and expand to support future needs as sites advance their OT cybersecurity maturity.

About PAS

PAS, the OT Integrity company, delivers software solutions that prevent, detect, & remediate cyber threats; reduce process safety risks and optimize profitability; and enable trusted data for decision-making. For more information, visit www.pas.com.

PAS
Ensuring OT Integrity

PAS Global, LLC
13100 Space Center Blvd. | Suite 500 | Houston, Texas | 77059
T. 281-286-6565 | F. 281-286-6767 | info@pas.com | www.pas.com