SOLUTION SHEET

Octave Cyber Integrity

Identify, detect and recover from industrial cyber threats

Key benefits

- Hardens OT assets against cyber threats
- Identifies critical endpoint vulnerabilities and risks
- Manages across all major control system manufacturers
- Accelerates forensic analysis and incident response
- Prevents unplanned shutdowns
- Enables rapid recovery

Challenge

Securing Operational Technology (OT) systems for critical infrastructure requires identifying and tracking a complete inventory of all OT and IT endpoints. Only with a comprehensive inventory that includes configuration data can companies protect against unauthorized change, achieve compliance, mitigate risk and ultimately secure OT assets and improve process safety.

Centralized monitoring and management of proprietary, multi-vendor OT systems in a facility is a complicated process. Control system inventory and configurations are typically gathered manually, a time-intensive process requiring expensive engineering resources. In addition, using IT-centric network monitoring tools to identify and manage OT system inventory is insufficient. Traditional IT-based security tools have limited visibility to Level 1 and Level 0 devices, and most importantly, do not collect the deep proprietary configuration data required to manage configuration changes.

Lack of a comprehensive, evergreen inventory exposes OT systems to cyber attacks and makes it difficult to detect unauthorized change, identify vulnerabilities and risks or maintain compliance with regulatory and corporate standards.

Solution

Cyber Integrity delivers comprehensive inventory, vulnerability, configuration, compliance, backup and recovery and risk management for OT assets:

- Discovers and automatically maintains a complete inventory of OT assets (Level 3.5 – Level 0)
- Provides continuous vulnerability management with patch level assessments
- Identify, evaluate, and prioritize OT cybersecurity risk across multiple domains.
- Tracks configuration changes against established baselines
- Enables workflows and documentation for vulnerability remediation and compliance with NIST, ISA/IEC 62443, NERC CIP, ISO 27001/2, the NIS Directive and other regulations
- Accelerates recovery with backups of critical control system data and supports in-depth forensic analysis
- Integrates with Security Information and Event Management (SIEM), Intrusion Detection Systems/Intrusion Protection Systems (IDS/IPS) and IT Service Management (ITSM) tools

Cyber Integrity supports multi-vendor, multi-generational OT assets, providing enterprise scalability, performance and platform independence.

Cyber Integrity capabilities

Inventory management

Maintains a complete inventory of OT and IT system hardware and software, including configuration data, control strategies, I/O cards, firmware, applications and any custom data.

Vulnerability management

Automates vulnerability assessment and includes impact factors to further evaluate and prioritize the OT cybersecurity risk that matter most to your environment. Assesses applicability and impact of Microsoft patches and automation system vendor bulletins. Provides enterprise-wide holistic image of vulnerability risk and enhances risk-based decision making. Maintains situational awareness of attack surface and vulnerability severity, aging and propagation paths as they relate to known weaknesses in your infrastructure.

Configuration management

Monitors for unauthorized changes to control strategies, device inventory, asset configuration and logical and graphical files. Automates remediation actions via workflows based on asset value and risk, guiding operations, compliance and cybersecurity responses. Establishes configuration baselines for ICS cybersecurity, compliance, governance and operations change monitoring.

Compliance management

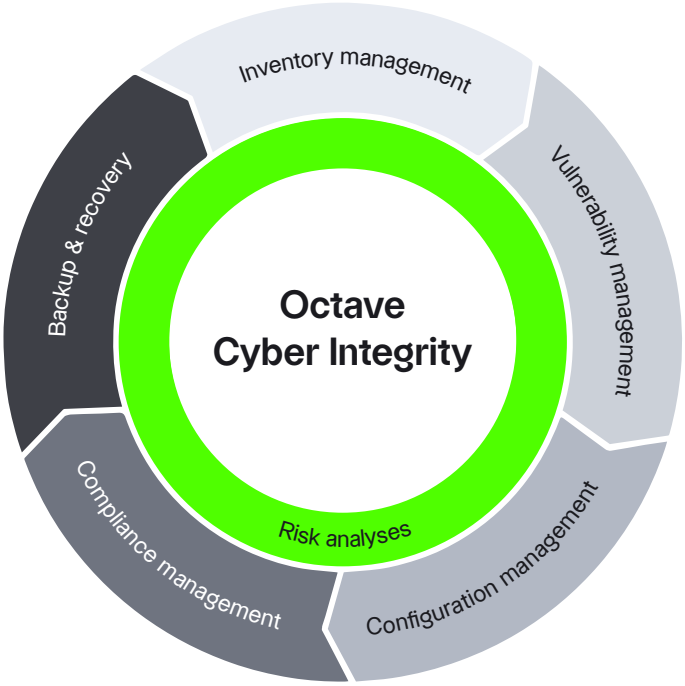
Audits and delivers reports to meet internal and regulatory compliance requirements. Provides relevant and actionable information to the right people at the right time – including inventory, alerts, user authentication events, configuration details and change history.

Workflows

Facilitates remediation, mitigation, policy and regulatory compliance activities and enables action documentation and reporting.

Backup and recovery

Enables rapid restoration of control system operations in the event of a worst-case scenario. Supports in-depth forensic analysis. Captures full configuration backups to speed recovery.



Risk analyses

Identifies cybersecurity risks to both OT and IT endpoints, continuously measures multi-vendor system security posture and visualizes risk propagation.

Asset models

Support for more than 120 control systems enables Cyber Integrity to deliver value to industrial companies who must maintain and secure multi-vendor, multi-generational OT systems. Cyber Integrity is a highly scalable, enterprise-class solution deployed at hundreds of sites globally.

Cyber Integrity is a powerful and scalable OT/ICS risk and endpoint management solution that provides OT operators and cybersecurity personnel with the critical data and insight needed to make their industrial operations safer and more resilient.

About Octave

Octave is a leader in enterprise software, turning data into decisive action and intelligence into your edge. Our software solves for and simplifies complexity, from the design and build to operations and protection of people, property, and assets– for any scope, at any scale. For decades, we've partnered with customers to sharpen performance, elevate efficiency, and amplify results. From factory floors to entire cities, our solutions are tuned to scale up what's possible from day one onward.