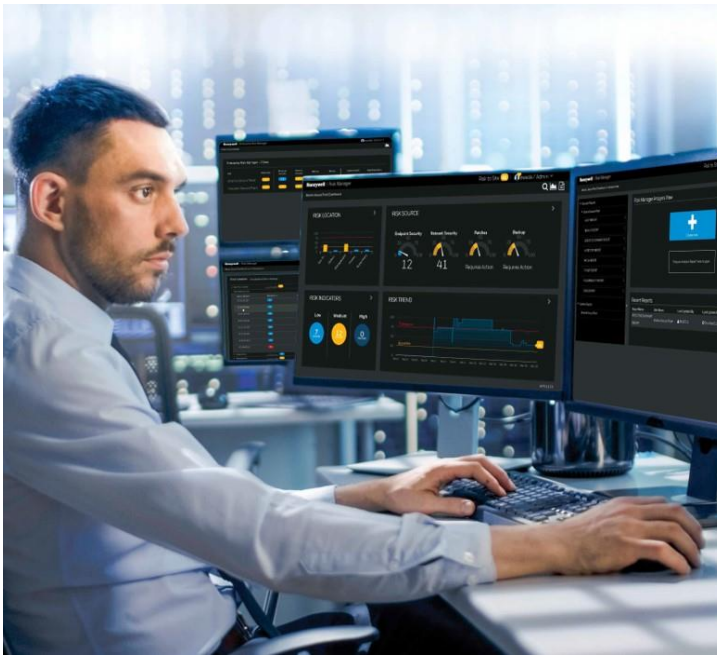
Honeywell | Industrial Cybersecurity

Industrial Cybersecurity Risk Manager and Enterprise Risk Manager

Product Information Note

Honeywell's Industrial Cybersecurity Risk Manager offers a single view for operations, IT and leadership teams to measure and manage the industrial cybersecurity risks that matter most to protecting operational uptime. Enterprise Risk Manager provides multi-site visibility of Risk Manager data, all in a single Level 4 integrated dashboard view.

Industrial cybersecurity has risen to the list of top five enterprise risk concerns for critical infrastructure companies. With more knowledgeable corporate boards and executive leadership teams, these companies are building industrial security programs that require capabilities to continuously measure and manage cybersecurity risks. At the plant operations level, managers must contend with the urgency to resolve cybersecurity issues more efficiently, before they impact safety or production.



Honeywell's Risk Manager solution automates and standardizes proactive risk monitoring, measuring and management of industrial control system (ICS) cybersecurity risk 24/7. The solution continually provides a safely generated, understandable and actionable view of cybersecurity posture. With Risk Manager, companies can improve threat mitigation, simplify compliance and keep teams productively at work on the greatest risk-impacting issues specific to their unique organization and ICS environment. Organizations gain the visibility, automation, reporting and guidance needed to find and resolve cybersecurity and performance issues efficiently and effectively.

FEATURES & BENEFITS

Risk Manager

- Translates complex network data into easy-to-understand risk impact on plants using patented Honeywell analytics
- Standardizes risk measurement and monitoring with Risk Indicators based on industry standards including ISA99/ IEC 62443 and ISO 27000 series
- Alerts users automatically through e-mail alerts whenever risk issues arise
- Provides power users the analytics to understand and act on cybersecurity risks
- Allows creation of custom rules that search for specific threat patterns

Enterprise Risk Manager

- Rolls up multi-site Risk Manager data into a single Level 4 integrated dashboard
- Facilitates additional analysis and correlation of multi-site threats and events, providing broader risk visibility across remote sites
- Standardizes cybersecurity risk policies across all plants
- Enables Risk Manager to securely deliver syslogs from network and security devices to an upstream SIEM

Mitigate ICS Risks with Less Effort and Higher Accuracy

Risk Manager improves compliance results and protects high priority assets based on the company's designated cybersecurity thresholds. Risk Manager helps to:

- Safely gain visibility into process control network (PCN) security status
- Automate the prioritization of risks
- Easily identify required actions to improve ICS security posture
- Speed and simplify PCN cybersecurity information reporting

Safely Gain Visibility into PCN Security Status

Risk Manager understands that in an industrial control system, networks and devices are interconnected to form systems that are greater than the sum of their parts. Understanding these relationships, Risk Manager is able to determine how risks to one area might impact other areas. It provides a clear indication of where risk originates by aggregating risk items in categories including endpoint, network, backup and patching. Whenever risk issues arise, staff can be automatically notified through e-mail alerts.

Risk Manager provides a consolidated view of cybersecurity risk intelligence from multiple point products for a true understanding of the site-wide security posture. Risk Manager can be provided as a purpose-built server or hosted in a virtual environment. It is deployed at Level 3 and accessed via a web-based interface.

Risk Manager translates complex cybersecurity data into an easily-understandable risk impact view, using patented Honeywell analytics. It continually measures and monitors risk in a standardized approach that Enterprise Risk Manager leverages to provide powerful multi-site comparisons. The solution's Risk Indicators are based on industry standards including ISA99 / IEC 62443 and ISO 27000 series.

Easily Identify and Resolve Risk-Impacting Issues

Risk Manager's Dynamic Rules allow creation of custom rules that search for specific threat patterns by registry values, data strings and installed files and applications. They help discover specific Indicators of Compromise (IoCs) and can pinpoint where attacks have bypassed defenses and identify infected systems.

Risk Manager itself is also monitored. The system health summary and detailed pages provide the status of Risk Manager internal services. Users always know if there are issues that might affect the operational performance or the accuracy of risk calculations.

Speed and Simplify OT Cybersecurity Reporting

Risk Manager's Analysis View provides analytics for power users to understand and act on cybersecurity risks. The drag-and-drop feature requires no configuration or coding, simplifying analytics and allowing staff to easily generate and save custom report types.

Risks are tracked over time and reports generated for various user needs. For example, detailed data exports are available for engineers and other power users to leverage, and concise reports of the most important trends and indicators are useful for managers and executives.

Automate and Prioritize Risk Mitigation

Risk Manager automates data collection and risk scoring calculations, providing a single view into cybersecurity posture that would otherwise require months and heavy staffing to compile. At any time, staff can view the dashboard to verify, for example, that security patches and AV signatures have been applied. As shifts change, incoming staff can readily understand status and work priorities by viewing Risk Manager's dashboard. Based on the company's risk appetite and risk thresholds, together with priorities of assets, Risk Manager prioritizes and articulates the core tasks that will most efficiently and effectively impact risk. Guidance for non-security personnel is included, to simplify and expedite tasks that reduce risk.

Risk Manager includes guidance for non-security ICS personnel to act on risk improvements.

Enterprise Risk Manager

Enterprise Risk Manager rolls up Risk Manager data from multiple sites into a single Level 4 integrated dashboard. It enables corporate security teams to conduct further analysis and correlation of multi-site threats and events, providing broader risk visibility across remote sites. Using Enterprise Risk Manager makes it easier for the corporation to standardize on cybersecurity risk policies across all plant locations, and understand what actions are necessary to improve overall cybersecurity resilience.

In addition, the Syslog Forwarding capability enables Risk Manager to securely deliver syslogs from network and security devices at a process control network level to a Level 4 SIEM via Enterprise Risk Manager. This allows for further analysis into risk causes and correlations.

Risk Manager supports:

Control System Nodes

- Experion® PKS R410.x – R51x.x
- Non-Experion systems running on Windows 7 and 10, Windows Server 2008, 2012 and 2016

Risk Manager monitors:

Endpoint Security

- Antivirus: McAfee Virus Scan Enterprise, Symantec Endpoint Protection
- Windows security events and auditing settings
- Honeywell C200/C300 controllers
- Secure Media Exchange (SMX)

Network Security

- SNMP v1/v2 network devices

Patches

- Core Windows operating system, expanded Microsoft and 3rd party
- McAfee and Symantec
- Adobe Reader

Backup

- Experion Backup and Restore (EBR) R4xx, R500.1
- Windows Backup and Restore

Installation, Maintenance and Support Services

During installation, Honeywell experts collaborate with customers on site to identify all assets to be monitored. This is followed by a baseline assessment (included with the initial installation) to address known vulnerabilities and assign ratings to all risks. Re-tuning services re-establish baselines and account for changes in the threat environment.

Why Honeywell?

Honeywell Industrial Cybersecurity is the leading provider of cybersecurity solutions that protect the availability, safety and reliability of industrial facilities and help securely deploy IIoT technologies. Honeywell's complete portfolio includes cybersecurity software, managed security services, industrial security consulting services and integrated security solutions. The portfolio leverages the company's industry-leading expertise and experience in process control.

Businesses all over the world partner with Honeywell to address cybersecurity holistically and improve their cybersecurity posture with advanced technology, backed by continuous innovation and investment.

For More Information

To know more about Honeywell's Industrial Cybersecurity Risk Manager, visit www.becybersecure.com or contact your Honeywell Account Manager, Distributor or System Integrator.

Honeywell Process Solutions

1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Skimped Hill Lane Bracknell,
Berkshire, England RG12 1EB UK

Building #1, 555 Huanke Road, Zhangjiang Hi-Tech Industrial Park, Pudong New Area,
Shanghai 201203

www.honeywellprocess.com

PIN-19-03-ENG
April 2019

Honeywell