Honeywell
THE POWER OF CONNECTED

Industrial Cyber Security

INDUSTRIAL CYBER SECURITY RISK MANAGER

Proactively Measure, Monitor and Manage the Risks that Matter the Most

Industrial Cyber Security is Not Just a Technology Problem

Unlike just a few years ago, leadership teams across today's Industrial organizations are under immense pressure to get ahead of cyber security, or face serious fines or business damage.

Advisory boards are increasingly asking cyber preparedness questions, while legal and risk management teams want proof of cyber security resilience to prevent liability issues. At the CFO level, companies are facing downgrades of debt ratings if their cyber security strategies are not deemed resilient.

Before an outage or attack, industrial companies need:

- Real time access to security posture of their industrial networks
- Aggregated reporting of security risks across all operating sites
- Evergreen alerts and measurements of industrial security posture, relative to selected standard.

At the same time, the Industrial Internet of Things (IIoT) promises new opportunities for cost savings and operational improvements. IT/OT convergence and business models require more remote network access. One result of this dynamic environment is that automation assets are no longer truly isolated, and the availability, reliability and integrity of industrial systems, networks and devices can no longer be taken for granted. Visibility into risk is essential.

How are You Managing Industrial Cyber Security?

Global Cyber Security Challenges:

- Increased risk from IIoT connectivity
- Regulatory cyber standards & requirements
- Limited cyber security expertise
- Operational-business security silos
- Low security visibility across complex multi-vendor control networks.

The Consequences of a Cyber Attack Can Include:

- Unplanned downtime and loss of production
- Costly harm to plant assets
- Reputational damage potentially impacting stock prices
- Negative health, safety and environmental consequences
- Fines due to regulatory compliance issues.

"It is no longer sufficient that organizations should have security in the board; it will increasingly become a legal requirement."

—*Security Week, discussing Cybersecurity Disclosure Act of 2017 new US federal legislation*

Importance of Understanding Risks

Risk-based frameworks have emerged as the most effective approach to achieve continuous cyber security improvement. Working in concert with compliance and policy goals, a risk-based approach helps plants and critical infrastructure sectors manage risk based on the security profile of each site, and select controls determined by informed decision making.

Proactively Measure, Monitor, and Manage Cyber Security Risk

Honeywell's Industrial Cyber Security Risk Manager is the first solution to proactively measure, monitor, and manage cyber security risk across industrial environments, providing users of all levels with real-time visibility, understanding and decision support required for action.

Honeywell developed Risk Manager from the ground-up to translate complex industrial vulnerability, threat and risk data into a consolidated, at-a-glance view for improved site-wide situational awareness.

Risk Manager: first of its kind for industrial environments

Risk Manager Helps Answer Critical Cyber Leadership Questions

- What is my company's exposure to the latest industrial cyber threat?
- Has anything changed in my risk profile? If so, what actions do I need to take?
- Are we improving our cyber resilience over time?
- Are my plants compliant with our corporate cyber security directive?
- Have any "non-sanctioned" devices been added to plant process control networks?
- What happens if I have a malware outbreak in my control network?

Patent-Pending Technologies from People Who Know Industrial Control Systems

Address cyber security challenges in ways not previously possible.

Most cyber security tools detect threats after they've occurred. Risk Manager continuously monitors for indicators of risk, employing powerful proprietary algorithms to constantly identify and analyze cyber vulnerabilities and threats. This proactive detection of risk indicators changes the game, giving you early insight, more offensive control and opportunities to eliminate vulnerabilities before they are exploited.

Risk Manager detects and monitors risk originating from 4 sources:

- Endpoint Security
- Network Security
- Patches
- Backup.

The network and all connected devices—including many controllers—are discovered and monitored by Risk Manager. You're able to develop meaningful metrics for threat management.

With Risk Manager, There's No Need to Be a Cyber Security Expert

Risk Manager understands cyber security so that you don't have to. It also understands industrial control systems, which is why Risk Manager ensures that devices are ready and safe to monitor before doing anything—so that security monitoring won't impact reliability. Through a user-friendly interface, Risk Manager allows all levels of users to accelerate their protection efforts, prioritize, and focus on managing those risks that are most important for reliable plant operations.

Real-Time Monitoring of Devices Throughout the PCN

Control Engineers and operators must have a full view of their infrastructure, its connections and applications to identify changes an attacker might make in the environment. However an abundance of data from disparate point products can quickly overwhelm staff. Risk Manager provides a consolidated view of risk intelligence data generated by various security solutions, maximizing your investments in third-party security solutions.

Risk Manager integrates with leading network and endpoint security controls to accurately measure threats as they occur, and also integrates with enterprise security platforms such as Security Information and Event Management systems (SIEMs).

"Correlating information from multiple sources ranked as the second-biggest challenge for security professionals."

—SANS Survey, "Breaches on the Rise in Control Systems"

"Industrial facilities have clearly become targets for cyber-attacks. Safety and operational continuity demand a clear understanding of these serious, dynamic risks and a program to ensure that they remain within acceptable levels. While most organizations recognize this need, operational people often lack the expertise to properly assess and manage cyber risks," said Sid Snitkin, Vice-President, ARC Advisory Group. **"So, we applaud Honeywell's development of Cyber Security Risk Manager. From what we've seen, it is a comprehensive, yet understandable, solution that should meet the needs of operational, automation, and manufacturing IT personnel."**

Benefits of the Risk Manager Solution

- *Real-time data collection and analytics platform that continuously monitors for indicators of cyber security risk*
- *Proactively identifies vulnerabilities and threats that could impact the Industrial Control System*
- *Provides extensive industrial security visibility by monitoring network and system devices, network traffic, and rogue devices*
- *Reduces reliance on cyber security expertise through easy-to-use interface and actionable remediation guidance*
- *Works with non-Honeywell systems—vendor neutral technology*
- *Designed for industrial operations—low impact technology that won't disrupt plant operations or cause network delays.*

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. Using proprietary algorithms. Risk Manager is able to extrapolate how a specific vulnerability or threat might impact other network zones or devices.

Operate at Peak Performance—Patch Monitoring for Third-party Products

Risk Manager monitors and reports on patches and prescribes a risk value accordingly. You're then able to better address the never ending patch management problem by understanding how missing patches impact overall risk to devices, zones or even the entire site.

The Right Context for Your Environment

Most existing cyber security solutions are designed with enterprise IT in mind. However, plant process control departments require specialized capabilities to collect the correct data points from industrial networks and assess them against criteria important to engineers and operators. Risk Manager focuses primarily on industrial cyber security requirements:

- Evaluates indicators of risk using patented algorithms to generate accurate risk scores in line with industry risk management standards
- Monitors risk continuously, in real-time, to provide immediate notification when unacceptable risk is present
- Translates complex indicators of vulnerabilities and threats into metrics that can be used by control engineers and operators without cyber security experience
- Tracks and inventories assets on the network
- Detects the presence of new or unknown devices on the network, so they can be properly managed
- Performs "low-impact" discovery and monitoring of key assets within the IACS to maintain reliability while monitoring for risk.

Is Your Cyber Security Maturity Level Improving?

Risk Manager generates trending analytics based on the amount and type of risk you are willing to accept in pursuit of your business goals (risk appetite), and the maximum risk you are willing to take regarding each relevant risk (risk tolerance). You can allocate resources based on your particular KPIs and gauge the impact of your decisions over time.

Break Down Communication Silos

Risk Manager allows users to search, sort and filter to get just the right information. When something important happens, automatic notifications are sent to ensure that nothing is missed. Built-in reports mean that site-wide cyber security data can be shared more easily with plant personnel, auditors and executives— without the tech talk.

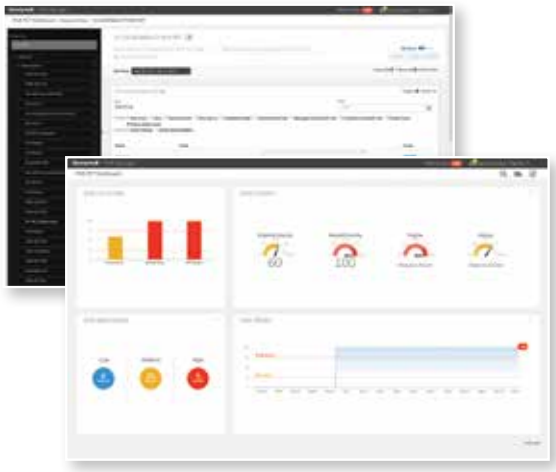
Align with Industry Standards

Several standards and frameworks including ISA99/IEC 62443 and the ISO 27000 series identify continuous monitoring as a critical cyber security program component. Risk Manager simplifies industrial security reporting with less disruption or network delays than manual reporting or IT solution retrofitting.

Reduce the Complexities of Cyber Security

Proactively Address C-Suite Industrial Cyber Security Priorities

Risk Manager provides executives with the ICS status and risk metrics they need to make informed decisions on cyber security compliance, liability and resilience issues.



Realize your Industrial Cyber Security Program

Risk Manager helps expedite the transformation of cyber security strategies into prioritized, measured and managed risk reduction efforts. It is best used as part of an ICS cyber security program that also includes threat remediation activities, counter measure and controls augmentation, and other defense-in-depth practices.

You Don't Have to Go it Alone

Risk Manager monitors, measures and manages cyber risk in a way not previously possible, but nothing replaces human insight. If your staff lacks the expertise and/or time required for Risk Manager Administration and Analysis, Honeywell can help. Our Managed Industrial Cyber Security Services offering includes remote support that helps maximize the benefits of Risk Manager.

How Honeywell Can Help

Recent years have seen a major increase in security incidents related to industrial control systems. As new threats emerge and the industrial security landscape evolves, you need an experienced and trusted partner to help protect the availability, reliability and safety of your plant automation system, as well as safeguard people and processes involved in all facets of your operation.

Honeywell Industrial Cyber Security Solutions are specifically designed to defend your control infrastructure and plant operations. These broad solutions leverage our industry-leading process control and cyber security know-how, recognized expertise and advanced technology, combined with partnerships delivering cutting-edge offerings from leading cyber security partners, including McAfee, Palo Alto Networks and others.

Honeywell is a proven industrial security partner that offers:

- Tailored solutions to efficiently secure industrial controls, without impacting processes
- Global/regional industrial cyber security service hubs close to our customers
- Extensive coverage of industrial control networks
- Ability to support our customers from security assessments to cyber security program development
- Track record of completing over 1,000 global industrial cyber security engagements
- Mature solutions with 300+ managed industrial cyber security sites.

For more information

To learn more about Honeywell's Industrial Cyber Security Risk Manager, visit www.becybersecure.com or contact your Honeywell account manager.

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

BR-17-30-ENG | 05/17

Honeywell