HONEYWELL FORGE for Buildings

# HONEYWELL FORGE CYBERSECURITY+ FOR BUILDINGS

## | CYBER INSIGHTS

# HONEYWELL FORGE CYBERSECURITY+ FOR BUILDINGS | CYBER INSIGHTS

**Knowledge is power when it comes to protecting operational technology (OT) assets from cyberattacks. Turning data into information and that information into knowledge is an ongoing challenge, especially if information technology (IT) solutions are the only tools. What's needed are OT-specific solutions.**

Honeywell Forge Cybersecurity+ for Buildings | Cyber Insights is designed to provide protection for the unique challenges of OT environments. It's an on-premise, vendor-neutral solution designed to provide building and asset owners with real-time data on assets, threats and vulnerabilities to help reduce cyber risks and maintain normal operations.

## KNOW WHAT'S CONNECTED TO YOUR NETWORK

Knowing what assets are on the network is a fundamental starting point for any cybersecurity program. This can be done manually, but it may not be effective with detecting newly added devices without a delay. With its OT-specific network monitoring capabilities, Cyber Insights is designed to provide a comprehensive and accurate inventory of all the assets in the network when first run and then to detect new additions to the network and to provide an alert for further investigation. If the newly added node was malicious, being able to quickly address the intrusion can significantly help reduce the risk of negative impact on safety and operations.

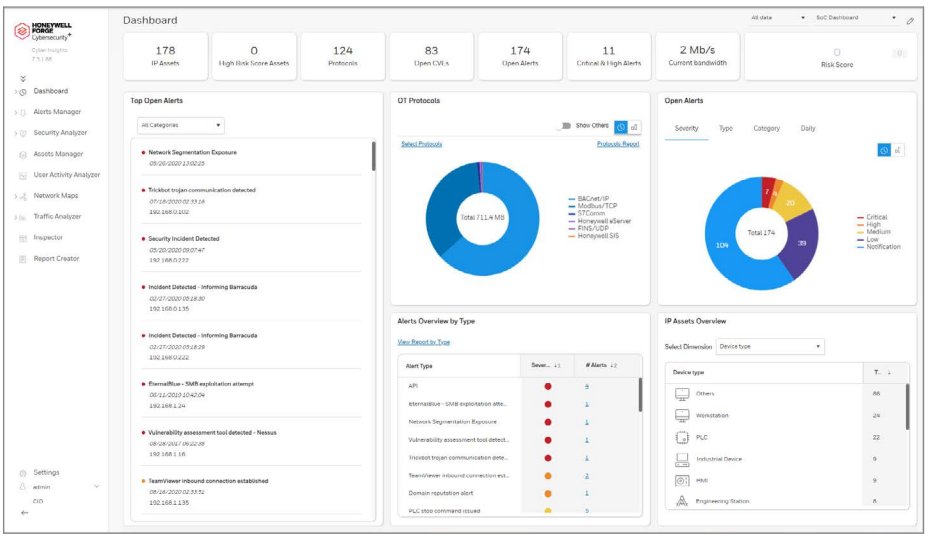
Another common challenge for building OT is the ability to keep track of assets that are getting close to their end-of-life. Cyber Insights is designed to help with this task by showing the assets' current lifecycle status and end-of-life date based on vendor-provided information to help sites better plan their upgrades and migrations.

## DETECT THREATS FASTER, MANAGE VULNERABILITIES BETTER

Information on lower-level assets such as controllers and PLCs can be hard to get in OT environments without disrupting the building automation process. Cyber Insights is designed to use passive network monitoring or, if preferred, active polling using native protocols to collect details on these assets and compare against the known vulnerabilities in the National Vulnerability Database (NVD). To provide even more useful information to help prioritize remediation work orders, Cyber Insights allows the identified vulnerabilities to be further filtered to only show known exploited vulnerabilities (KEV). This feature together with the CVSS scoring from the NVD are designed to help the OT cybersecurity team to focus on addressing the weaknesses that need the most urgent attention and leave the lesser concerns for later.

## GET BETTER VISIBILITY OF AN OT SYSTEM'S CYBERSECURITY STATUS

Cyber Insights is one of the most comprehensive cybersecurity solutions for OT and IoT networks. It is designed to discover and inventory all the assets in the network, provide comprehensive information about the site's cybersecurity posture – including known exploited vulnerabilities and active threats relevant to the site - and help investigate suspicious activity. It's capable of providing vital insights into a site's assets, vulnerabilities, cybersecurity threats and operational failures.



Cyber Insights is also designed to compare the data it collects against the MITRE ATT&CK for ICS framework. Seeing a site's current security data mapped against attack tactics and techniques observed in the real world can be useful when trying to decipher whether an individual event is just that, an isolated event - or part of a malicious chain of events in progress. When investigating an alert, Cyber Insights can allow a site's OT cybersecurity team to trace the alert to the user whose actions caused it to occur – and to see what else the user had been up to.

In addition, Honeywell threat researchers continuously investigate reported cyber threats and exploits against specific industries, locations and assets to help sites better protect themselves against targeted cyberattacks. This intelligence is fed into Cyber Insights that can provide curated information to the site's OT cybersecurity team on threats that should be top of mind.

## AN ON-PREMISES AND VENDOR-NEUTRAL SOLUTION

Cyber Insights is deployed on the OT network to provide cybersecurity information even at sites with limited or no connectivity to the corporate network. It is designed to monitor network traffic to capture a wealth of information from Honeywell and non-Honeywell assets unobtrusively and transform it into valuable intelligence without the collected data having to leave the premises. As such, Cyber Insights is well suited for on-premises use at individual sites. For organizations that need the information from the individual sites to be shown in a single view, Honeywell Forge Cybersecurity+ for Buildings | Cyber Watch can be added. This complementary solution can provide an aggregated view from a central location, making it easier for a multi-site organization to have a comprehensive view into their cybersecurity posture.

## PROTECT OPERATIONS IN AN EVER-CHANGING THREAT LANDSCAPE

As potential cyber threats increase with more specific attacks on OT, companies that can best identify threats and vulnerabilities earlier can reduce the likelihood of an unplanned shutdown or safety incident caused by a malicious actor. Knowing your site's current cybersecurity posture is vital to reducing cyber risk. Cyber Insights is designed to be used in building OT environments to provide crucial information on your site's assets, vulnerabilities and threats to give your OT cybersecurity team the insights needed to better protect operations. Cyber Insights is designed to be a readily accessible resource with up-to-date information empowering you to focus on improving a facility's overall cybersecurity posture.

## HONEYWELL FORGE CYBERSECURITY+ FOR BUILDINGS | CYBER WATCH IS DESIGNED TO PROVIDE

### BETTER ASSET MANAGEMENT

Designed to provide fully automated asset discovery and inventory for comprehensive visibility into OT networks and IoT devices, including their lifecycle status and end-of-life (EOL) information.

### COMPREHENSIVE VISIBILITY

Designed to deliver visibility into OT networks, communication patterns, and attack vectors at a single site.

### IMPROVED RISK MANAGEMENT

Designed to support better cybersecurity risk management and improved cyber hygiene with detailed security information and existing vulnerabilities based on the NVD.

### NEAR REAL-TIME DETECTION OF THREATS AND ANOMALIES

Designed to passively identify indicators of compromise (IOCs), providing early attack detection. It is also designed to monitor user activity inside a site's OT network, looking for and alerting to any signs of potential cybersecurity threats.

### MITRE ATT&CK FRAMEWORK

Designed to map security events to the MITRE ATT&CK for ICS framework for better analysis.

### TAILORED THREAT INTELLIGENCE

Designed to provide curated threat intelligence on reported malicious activities and their relevancy to specific locations, industries, and equipment.

### VENDOR NEUTRAL

Vendor-neutral, on-premise solution, designed by OT cybersecurity professionals for OT environments.

### DEPLOYMENT FLEXIBILITY

Ease of deployment, designed to integrate into a site's existing security architecture.

Honeywell has more than a century of experience in building automation, with more than 20 years in industrial and building OT cybersecurity, deploying thousands of solutions worldwide. We provide cybersecurity solutions that protect the availability, safety and reliability of OT assets worldwide. Honeywell's complete portfolio includes cybersecurity software, managed security services, building security consulting and integrated security solutions. We provide the premier cybersecurity solutions for an operational technology environment.

**For More Information**
buildings.honeywell.com

**Honeywell Building Technologies**
715 Peachtree St NE
Atlanta, Georgia 30308
www.honeywell.com



Honeywell Forge
Cybersecuruty+ for Buildings | Cyber Insights I 12/23


THE FUTURE IS WHAT WE MAKE IT

Honeywell