Honeywell | OT Cybersecurity

CYBER APP CONTROL FOR BETTER INDUSTRIAL CONTROL SYSTEM DEFENSE

SERVICE NOTE

> Constantly defending industrial control systems against cyber threats is challenging, yet essential for protecting assets and processes against today's malicious actors. Honeywell's Cyber App Control adds an important capability to help industrial operators reduce the risk of targeted attacks and endpoint malware infiltration.

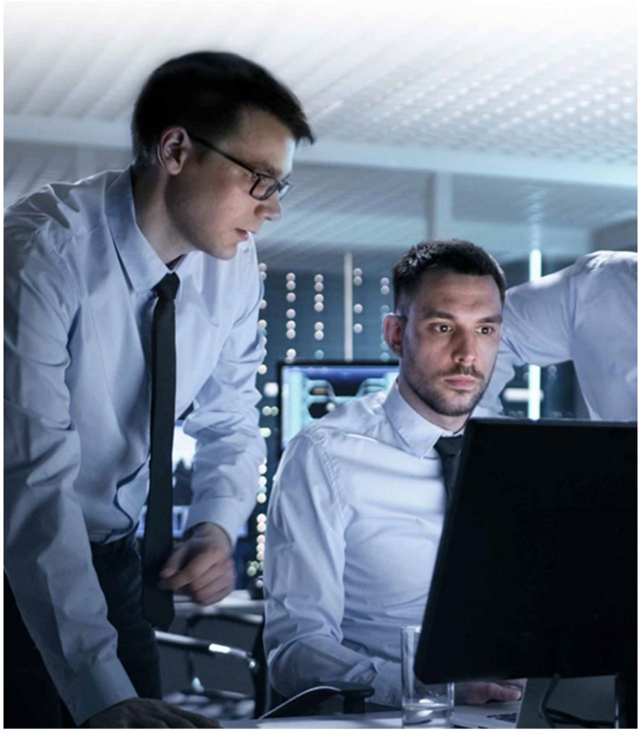
Process control networks, industrial assets and otherwise well-intentioned people represent an expansive attack surface that sophisticated hackers seek to exploit. Attacks against industrial operators are constantly increasing in frequency, and companies must balance allowing legitimate activity while stopping malicious attack behavior. Unnecessary activities or disruptive technologies can also interfere with process operations. Managing such activities through application control can help improve security, ease routine operations and support asset availability.

Complementary to anti-virus technologies, application control offers an additional layer of security through defense in depth, an approach recommended by cybersecurity guidelines such NIST's Guide to Operational Technology (OT) Security.

Permissions for the Known and the Trusted

Application control permits only known and trusted applications to run, helping prevent zero-day and targeted attacks as well as endpoint malware infiltration. By specifying what activities are allowed through allowlisting, and denying all other activities, companies gain greater control over their control system activities.

Honeywell's Cyber App Control solution uses software from security specialist Carbon Black, deployed by Honeywell's experienced and certified OT cybersecurity engineers. The engineers design, implement and configure Cyber App Control by applying Honeywell's rich industrial-specific experience to save time-to-operations. The solution is vendor-agnostic and suitable for any industrial systems.



Honeywell's Cyber App Control solution is deployed by experienced and certified OT cybersecurity engineers to help improve advanced endpoint protection and to reduce risk of targeted cyber-attacks on industrial control systems.

Optimized to Improve Configuration Efficiency

Running in monitor mode, the application control software can scan and monitor the system, helping uncover formerly invisible activity, and allow administrators to list what files, applications and connections should be allowed. Day-to-day, depending on the mode selected, such activities can be automatically monitored and blocked based on the allowlisting policies.

To simplify configuration and management, Honeywell's OT Cybersecurity Center of Excellence and Innovation specialists have created various configuration templates with thoroughly vetted rules that enable faster and better-tested site deployments. One example of these rules includes permitting installation and execution of software only from manufacturers for which Honeywell can confirm a valid digital certificate is present. The specialists at the OT Cybersecurity Center of Excellence and Innovation regularly update the templates to stay current with Honeywell's latest systems releases.

Architecture and Set-Up

The Carbon Black App Control software used in Honeywell's Cyber App Control solution consists of two major components, server and agents. The server acts as a console to the product and interfaces with Microsoft SQL server database to store information. The agents are installed on end nodes, where they maintain a live inventory and enforce the policies supplied by the server.

The Cyber App Control solution is deployed with care at the site by Honeywell's OT cybersecurity engineers. After the software is installed, monitoring of the endpoints is initiated to allow the engineer and the site staff observe the activity over time and to then customize the rules to meet the site-specific need.

Cyber Care for Cyber App Control

To help ensure the continued benefits of Cyber App Control in the long run, Honeywell offers annual, proactive maintenance through the Honeywell Cyber Care service program. This includes the services of a Honeywell OT cybersecurity engineer auditing the site's existing allowlisting and denylisting rules and examining the logs to see if changes are required. After installing the latest Honeywell-qualified version of Cyber App Control, the engineer then updates the settings as required, to better suit the site's as-is environment. With Cyber Care, organizations are able to maintain their endpoint protection at optimal levels, even as their process control network environment continues to evolve.

Practice Defense in Depth

Application allowlisting is commonly recommended by experts as one of the key tools for effective endpoint protection in industrial control system environments, as these often have static systems and may also rely on more vulnerable legacy operating systems. While anti-virus blocks malware it knows about, application allowlisting blocks unknown and untrusted applications from running on protected nodes.

Unlike anti-virus solutions, application control with its allowlisting capabilities does not require frequent updates, making it suitable for environments where regular maintenance is a challenge. Due to its nature, application control has an excellent reputation for protecting against zero-day attacks.

Application control tools such as Honeywell's Cyber App Control is not intended to replace existing antivirus solutions. No single cybersecurity solution protects against determined actors and defense in depth is always the best approach. With cybercrime becoming big business, it is even more imperative that industrial companies continue to improve their defenses against attacks through additional layers of protection.

FEATURES AND BENEFITS

- An essential tool in OT cybersecurity, helping reduce risk of targeted and zero-day attacks by denying unknown or untrusted applications from executing
- Deployed by experienced Honeywell OT cybersecurity engineers to meet site-specific needs

- Vendor-agnostic solution suitable for Honeywell and non-Honeywell systems
- Pre-tested on Honeywell systems, including Experion® PKS, to enable faster deployments when compared to off-the-shelf app control solutions
- Supports compliance with standards requiring up-to-date inventory of approved-to-run applications

- Allows for different levels of node control within the network to best suit specific security requirements
- Well-suited for environments where the ability to update the systems is limited

About Honeywell’s Professional Cybersecurity Services

Honeywell’s Professional Cybersecurity Services provide over 30 specialized OT cybersecurity offerings and custom consulting to help process control industries safely operate and connect. Honeywell consultants are versed in both industrial operations and cybersecurity to help companies best assess their risks, design robust architectures, better protect networks and endpoints, and improve situational awareness and incident response. Companies can leverage Honeywell OT Cybersecurity Centers of Excellence and Innovation to safely simulate, validate and accelerate their cross-vendor industrial cybersecurity solutions in state-of-the-art facilities staffed by highly skilled professionals.

Why Honeywell?

Honeywell has more than 100 years of industrial experience and over 20 years of industrial cybersecurity domain expertise. We are the leading provider of cybersecurity solutions, protecting the availability, safety and reliability of industrial facilities worldwide. Honeywell’s complete portfolio includes cybersecurity software, managed security services, industrial security consulting, and integrated security solutions. We combine industry-leading expertise in cybersecurity and decades of experience in process control, for the best solutions in an operational technology environment.

This document is a non-binding, confidential document that contains valuable proprietary and confidential information of Honeywell and must not be disclosed to any third party without our consent. It does not create any binding obligations on us to develop or sell any product, service or offering. Content provided herein cannot be altered or modified and must remain in the format as originally presented by Honeywell. The quantified product benefits referenced are based upon several customers’ use cases and product results may vary. Any descriptions of future product direction, intended updates or new or improved features or functions are intended for informational purposes only and are not binding commitments on us and the sale, development, release or timing of any such products, updates, features or functions is at our sole discretion.

For More Information

To learn more about how Honeywell’s OT cybersecurity solutions can help you, visit www.becybersecure.com or contact your Honeywell Account Manager.

Honeywell Connected Enterprise

715 Peachtree Street NE
Atlanta, Georgia 30308

www.honeywellforge.ai

SV-21-04-ENG
June 2024

Honeywell