Honeywell | HCE Cybersecurity

APPLICATION WHITELISTING FOR BETTER INDUSTRIAL CONTROL SYSTEM DEFENSE

SERVICE NOTE

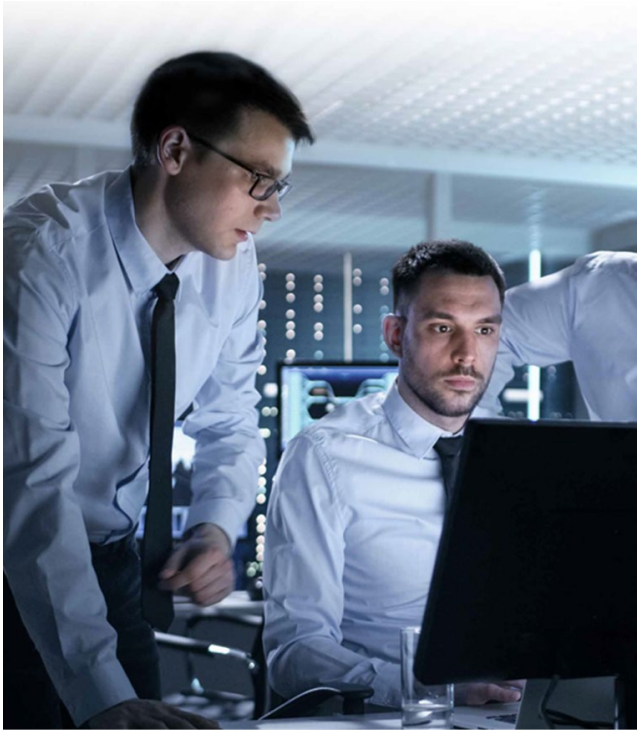
Constantly defending industrial control systems against cyber threats is challenging, yet essential for protecting assets and processes against today's malicious actors. Honeywell's Application Whitelisting adds an important capability to help industrial operators reduce the risk of targeted attacks 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. Controlling such activities through application whitelisting can help improve security, ease routine operations and support asset availability.

Complementary to anti-virus technologies, whitelisting offers an additional layer of security through defense-in-depth, an approach recommended by cybersecurity guidelines such NIST's Guide to Industrial Control Systems (ICS) Security.

Permissions for the Known and the Trusted

Application whitelisting 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 whitelisting, and denying all other activities, companies gain greater control over their control system activities.



Honeywell's Application Whitelisting 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.

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

Optimized to Improve Configuration Efficiency

Running in monitor mode, the application whitelisting software can scan and monitor the system, helping uncover formerly invisible activity, and allow administrators to auto populate 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 whitelisting policies.

To simplify configuration and management, Honeywell's Cybersecurity Center of Excellence experts 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 experts at the Center of Excellence regularly update the templates to stay current with Honeywell's latest systems releases.

Architecture and Set-Up

The VMware Carbon Black software used in Honeywell's Application Whitelisting solution consists of two major components, VMware Carbon Black App Control Server and VMware Carbon Black App Control Agent.

The App Control Server acts as a console to the product and interfaces with Microsoft SQL server database to store information. Honeywell recommends installing the server on Level 3. The App Control Agents are installed on end nodes, where they maintain a live inventory and enforce the policies supplied by App Control Server.

Practice Defense in Depth

Application whitelisting is commonly recommended by experts as one of the key tools for effective endpoint protection in ICS 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 whitelisting blocks unknown and untrusted applications from running on protected nodes.

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

Application whitelisting 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

- Deployed by experienced and certified Honeywell OT cybersecurity engineers to meet specific customer needs
- Uses industry-proven and scalable VMWare Carbon Black App Control technology
- Vendor-agnostic solution suitable for Honeywell and non-Honeywell systems

- Pre-tested on Honeywell systems, including Experion® PKS, to enable faster deployments
- Allows for different levels of node control within the network to best suit specific security requirements
- Supports compliance with standards requiring up-to-date inventory of approved-to-run applications

- Essential component in OT defense-in-depth strategy, complements anti-virus solutions
- Helps reduce risk of targeted and zero-day attacks by denying unknown or untrusted applications from executing
- Well-suited for environments where the ability to update the systems is limited

About Honeywell Security Consulting Services

Honeywell Security Consulting Services provide over 30 specialized industrial 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. Customers can leverage Honeywell Centers of Excellence to safely simulate, validate and accelerate their cross-vendor industrial cybersecurity solutions in state-of-the-art facilities staffed by Honeywell experts.

Why Honeywell?

Honeywell has more than 100 years of industrial experience and over 15 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.

For More Information

To learn more about how Honeywell's Cybersecurity Consulting Services, visit www.becybersecure.com or contact your Honeywell Account Manager.

Honeywell Connected Enterprise

715 Peachtree Street NE
Atlanta, Georgia 30308

www.honeywell.com

SV-21-04-ENG
August 2021

Honeywell