HONEYWELL APPLICATION WHITELISTING SOLUTION

North American Offshore Operator Safeguards Its ICS Using Honeywell's Solution

Case Study

Honeywell

Outdated, unsupported operating systems create a serious vulnerability for an industrial control system. A robust endpoint security solution is needed to protect critical assets.

Today's integrated business and production systems require careful design and robust infrastructure to ensure selective access and control. The increasing complexity and volume of applications is resulting in the requirement for new and improved security tools. Legacy Operating Systems (OS), such as Windows XP or Windows Server 2003, can put an Industrial Control System (ICS) at risk from multiple cybersecurity threats. Attackers continually change tactics, leveraging different application types and vulnerabilities to cause industrial system outages.

In one case, a major offshore oil and gas operator in the United States was running critical ICS applications based on a Microsoft legacy OS on its offshore platforms. The company wanted to apply an endpoint security solution to protect its control systems from zero-day threats and malware.

HONEYWELL SOLUTION

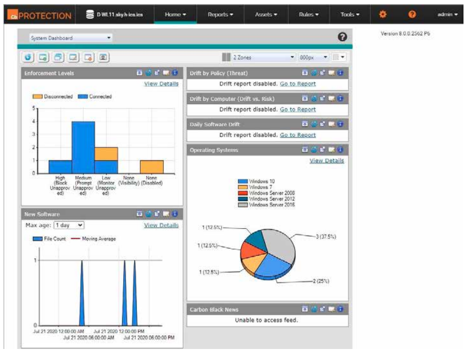
The offshore oil and gas operator chose the Honeywell Application Whitelisting (AWL) – Carbon Black Protection solution to safeguard its crucial control system infrastructure. The Honeywell solution provides high-performance, low-touch application control, utilizing out-of-the-box templates based on Honeywell best practices. AWL blocks the "unknown" and allows the "trusted" without interrupting daily operations.

Honeywell AWL – Carbon Black Protection also bolsters security through defense-in-depth - an approach recommended by cyber security frameworks such as the National Institute of Standards and Technology (NIST). The Honeywell AWL solution is intended to accelerate compliance with regulatory standards and frameworks. It enables users to meet the key requirements of regulatory standards, such as NERC CIP and NIST 800-53.

Honeywell AWL – Carbon Black Protection is part of Honeywell's endpoint protection solutions. In addition to being more effective than antivirus, it is the only solution receiving a 100% effectiveness score by independent NSS Labs. Honeywell AWL - Carbon Black Protection has been qualified for use with Experion® software and is delivered with specialized Honeywell Security Consulting Services for successful configuration and implementation. This solution comprises a modern architecture with AWL Server and Agent and includes multiple enforcement levels which can accommodate special cases on a per node basis. It provides the highest levels of protection against malware, such as WannaCry or Petya.

Essentially, the Honeywell application whitelisting approach flips the antivirus model from a "default allow" to a "default deny" for all executable files (e.g., binaries and scripts). Running in monitor mode, Honeywell AWL can scan and monitor the system, uncovering formerly invisible activities and helping administrators auto populate applications that are allowed to be run. Day-to-day activities can be automatically monitored and blocked based on the AWL policies.

To simplify configuration and management, Honeywell AWL allows for publisher approval rules that permit installation and execution of software from manufacturers for which a valid digital certificate is present. As part of Honeywell AWL, experts from Honeywell Security Consulting Services deliver proper design, implementation and configuration of the solution. This saves time for operations, while applying rich Honeywell industrial-specific expertise to solving your challenges.

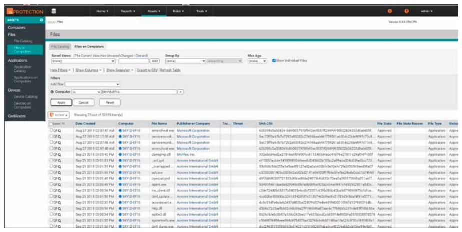


Drift report disabled. Go to Report

Drift report disabled. Go to Report

Drift report disabled. Go to Report

Unable to access feed.



CUSTOMER BENEFITS

As a global leader in industrial cybersecurity, Honeywell offers an endpoint security solution with an agent combining application whitelisting, file integrity monitoring, device control, and memory/tamper protection. Honeywell's approach to application control and whitelisting is an excellent safeguard against zero-day intrusions – where defenders have no prior awareness of that malware and can enable better change management and protection against unauthorized alterations to the system configuration.

With application whitelisting, malware is blocked from entering and executing on endpoints within a network. By specifying allowable applications through whitelisting and denying all other applications from executing, companies gain greater control over their network. Whitelisting provides greater visibility into the applications running as part of an ICS and then enables administrators to allow only their specified index of apps to run. Unlike traditional antivirus solutions, AWL does not require constant updates or frequent maintenance. antivirus definitions are often out of date on ICS networks, and time gaps leave the network vulnerable until the next antivirus definition update is implemented. Complementary to antivirus, whitelisting offers layers of security for ICS assets.

Honeywell AWL – Carbon Black helps industrial organizations gain visibility of the applications running on their ICS network and enables administrators to limit their specified index of applications to run. This reduces the presence of unauthorized applications on the network. The specific benefits of this approach include:

- **Lower security risk** – Reduces targeted attacks, zero-day attacks and endpoint malware infiltration
- **Greater control and visibility** –Allow default-deny policy setting to control undesirable activities and provides visibility into what's running on your network
- **Increased compliance** – Accelerates compliance with regulatory bodies, such as NIST and others
- **Granular security** – Adds a defense-in-depth layer to industrial-specific applications for granular whitelisting control
- **Improved network migrations** – provides migration path to newer versions while ensuring compatibility with Experion systems

By deploying the Honeywell AWL – Carbon Black Protection solution, a major offshore oil and gas producer, operating in the U.S., was able to meet regulatory requirements by following NIST guidelines throughout its facilities. During this engagement, the operating company's requirements were diligently integrated while prioritizing plant safety and ensuring uptime.

Honeywell is dedicated to protecting control and safety systems running on unsupported operating systems, such as Windows XP and Windows Server 2003. In this case, comprehensive security consulting services helped the end user lower the risk and possible impact of security incidents while improving its industrial cybersecurity maturity level.

For More Information

Learn more about how Honeywell Forge for Cybersecurity can improve performance, visit www.becybersecure.com or contact your Honeywell Account Manager, Distributor or System Integrator.

Honeywell Process Solutions
1250 West Sam Houston Parkway
S. Houston, TX 77042, USA

Honeywell House, Arlington Business Park
Bracknell, Berkshire, England RG12 1EB UK

Shanghai City Centre, 100 Zunyi Road
Shanghai, China 200051

www.honeywellprocess.com

SS-20-8 ENG I 08/20

THE
FUTURE
IS
WHAT
WE
MAKE IT

Honeywell