ESSENTIAL ANTIVIRUS PROTECTION AND REMOTE MANAGEMENT

Protect the essentials with basic security

Safeguard your system from cyber threats. As your facility becomes more connected to the Internet of Things (IoT), to the cloud, to your operations it becomes an increasingly sophisticated and vital part of your business.

This means it also becomes increasingly essential to keep your facility and your Operational Technology (OT) network secure by continuously monitoring it to promote optimal uptime and rapid response.

The proactive and prevention centric approach enhances protection, while helping to dramatically reduce costs.

Honeywell Advanced Endpoint Security (HAES) is a pioneering technology that applies deep learning to OT cybersecurity. Deep learning is inspired by the brain's ability to learn. Once the brain learns to identify an object, its identification becomes almost second nature.

As the artificial brain learns to detect certain cyber threats, its prediction capabilities become more instinctive. As a result, zeroday and Advanced Persistent Threats (APT) attacks are more readily detected and thus prevented in near real-time with enhanced accuracy.

Honeywell Remote Management (HRM) platform helps optimize the performance and security of your facility OT systems with regular remote monitoring of health, connectivity, compliance and uptime. The HRM platform continuously monitors and analyzes your critical OT servers, workstations, virtual machines, and applications to help alert you regarding potential issues - proactively.

This level of visibility can help you effectively plan and monitor critical site activities. The platform also provides guidance to help you prioritize maintenance while promoting enhanced value and minimized disruption, while using a powerful scripting engine to support customization and detects missing patches and pushes just the needed patch files for your choice of manual, scheduled, or automated execution.

HONEYWELL ADVANCED ENDPOINT SECURITY (HAES)

- OT Antivirus, built for control-system servers and workstations
- Blocks malware, ransomware, and suspicious files from running on OT machines
- Alerts you when something unsafe is detected on an OT machine

HONEYWELL REMOTE MANAGEMENT (HRM)

- Actively monitors OT Server and workstation system performance
- Shows if patches, antivirus, and system configurations are up to date
- Alerts you if something changes on the machine that shouldn't (new services, firewall changes, etc.)
- Delivers remote patch management as a service

Honeywell

OUR SOLUTION PROVIDES ENHANCED PROTECTION AND IS BASED ON A PREDICTION AND PREVENTION FIRST APPROACH, FOLLOWED BY DETECTION AND RESPONSE, WITH HIGH EFFICACY AGAINST CYBER THREATS TAILORED FOR OT ENVIRONMENTS.

ANTIVIRUS/ENDPOINT SECURITY

	TRADITIONAL	MACHINE LEARNING	HONEYWELL DEEP LEARNING
Accuracy	Low, signature based	Moderate with high false positives	High accuracy with a nearly zero false positive rate
Involvement of domain expert	Required for signatures and heuristics creation	Required for feature engineering and extraction	Not required; virtually autonomous
Amount of Data Analyzed	Analyzes known threat vectors	Analyzes small fraction of entire threat vector	Analyzes the entire threat vector
Type of files	Any	Mostly Portable Executable (PE)	Wide variety of files and fileless

Honeywell Building Solutions
Honeywell House,
Skimped Hill Lane,
Bracknell, Berks,
RG12 1EB
buildings.honeywell.com

HBS-CyberBasics-Sell Sheet | Rev1 | 02/26

THE FUTURE IS WHAT WE MAKE IT

Honeywell