Solution Brief
Security and Manageability

Intel and McAfee Show How to Secure and Manage Industrial Systems

Solutions help protect against malicious attacks, increase equipment uptime, and improve cost efficiency

McAfee®
An Intel Company

Challenges

- **Cyber attacks and other security concerns are an increasingly critical consideration** as automated industrial systems grow more connected.
- **Aging assets, such as programmable logic controllers (PLCs), predate the Internet of Things**, and are particularly vulnerable and unable to report malicious activity.
- **Hackers have grown more dangerous**, increasing the need to improve situational awareness of industrial IT to more quickly defuse zero-day attacks.
- **Manufacturing is rapidly evolving, stretching industrial organizations** to address growing operational complexity and aging infrastructure, while striving for faster time to market.
- **Standard IT products can't see what's happening within an industrial infrastructure**, and don't understand the unique lexicon of that infrastructure.
- **When a device fails, a costly "truck roll" response may be needed** to fix the issue.

Solutions

The Intel® and McAfee solution, which can be deployed on an Intel®-based industrial PC (IPC) equipped with an Intel® processor with Intel® vPro™ technology,[1] includes the following:

- **Intel® Trusted Execution Technology (Intel® TXT) enhances security** by preventing any node from executing malicious software.
- **Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) enables faster, more affordable data protection** and greater security.
- **Intel® Active Management Technology (Intel® AMT)[2] enhances device management** by enabling network operators to gain full control of an attacked device.
- **McAfee Endpoint Encryption* reduces the risk of device and data theft**, utilizing faster encryption technologies built into Intel AES-NI.
- **McAfee Deep Defender* reduces software risks** around ring 0 malware attacks.
- **McAfee ePolicy Orchestrator* (McAfee ePO*) + McAfee ePO Deep Command* remotely deploy, manage, and update security** and devices software on disabled or powered-off endpoints.
- **McAfee Enterprise Security Manager* accesses actionable intelligence** via a contextual view that helps identify and isolate attacks.

Intel and McAfee help manage and protect industrial systems

Intel® Core™ processor-based platforms with Intel® vPro™ technology, used in tandem with McAfee security solutions, create a powerful end-to-end security solution with advanced remote management to help you safeguard your critical industrial infrastructure.

Once operated as closed and proprietary systems, traditional industrial automation networks were largely protected from outside threats. But as the devices on today's factory floors grow more connected to each other and the network as part of the Internet of Things, security and manageability are becoming increasingly critical requirements.

Those tasked with securing today's factory automation systems face a big job. Multiple zones must be addressed, from corporate IT, to native supervisory control and data acquisition (SCADA), to device networks, and each has its own unique technical challenges. Moreover, because these infrastructures comprise a diverse set of networks, they cannot be effectively secured by simply "bolting on" technologies designed for enterprise IT.

A comprehensive solution requires multiple products to create layers of security that operate together without introducing undue complexity, degrading performance, or impacting availability.

Complete Protection through Hardware and Software

Intel provides a broad spectrum of hardware- and software-based manageability solutions, while the Intel® Core™ vPro™ processor family also provides integrated hardware support for intelligent management functions, virtualization, and platform security. Providing a significant remote management breakthrough, Intel AMT implements a special circuit in the Intel vPro technology-enabled chipset that can access and control the system, even when it is using standby power or the software is corrupted.

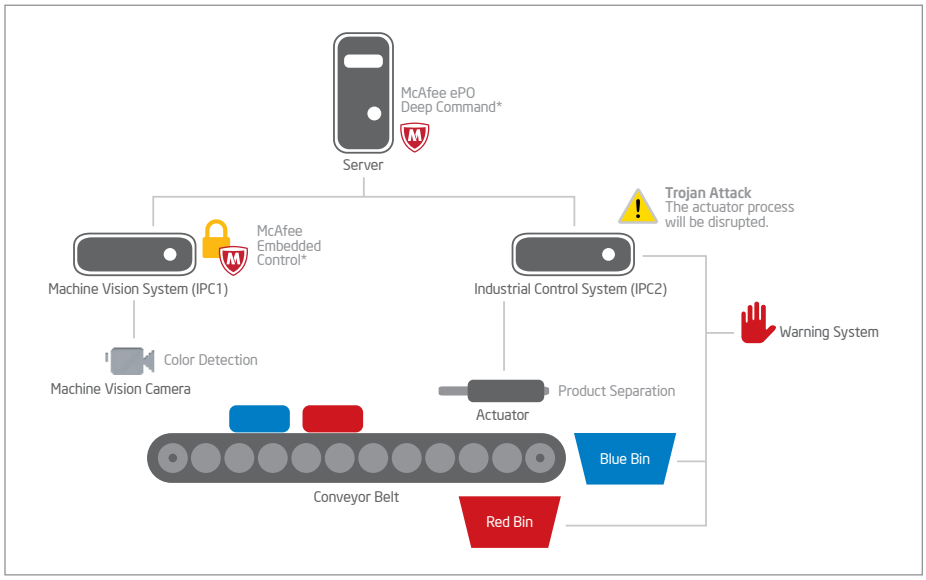
By employing an Intel AMT technology-based management solution, factories can remotely fix a wide assortment of system defects; track inventory, including warranty and software license information; and track intermittent failures. Using the keyboard-video-mouse (KVM) feature, technicians can manage the remote device with out-of-band manageability as if they were sitting right in front of it using normal input devices and not only through command-line instructions.

Intel, in combination with McAfee, provides security solutions to ensure intelligent systems, applications, and data are protected, even minimizing the infection vectors of a Stuxnet-class attack (see related sidebar). The solutions comprise a nearly impenetrable shield against most types of security threats, while also helping increase uptime and lower the cost to service endpoints across your factory.

Intel and McAfee incorporate seamless multizone protection, situational awareness, SCADA support, and remote device management. McAfee ePO software, the foundation of the McAfee Security Management solution, unifies management of endpoints, networks, data, and compliance solutions. The software enables factory operations to centrally manage security and achieve dramatic efficiencies.

McAfee ePO Deep Command runs on Intel Core vPro processor technology, which establishes an out-of-band connection used to take control of the device regardless of the hardware or software state—even, potentially, a rogue device. Intel AMT is a key component of McAfee ePO Deep Command. When untrusted software attempts to run and gets blocked, the whitelisting application alerts McAfee ePO, prompting potential corrective action.

McAfee Enterprise Security Manager incorporates security information and event data for processing logs from all of an organization's sources and organizing them in a central place in near real time. The result is a contextual view that helps identify and isolate attacks produced by unknown malware.



The Intel and McAfee demo uses two IPCs and one remote server to illustrate how different security features can protect industrial operations.

Intel and McAfee Demonstrate a Comprehensive Solution

In an effort to help industrial organizations better secure and manage their devices and systems, Intel and McAfee have shown how a comprehensive security and manageability solution can protect factory operations.

In a recent simulation, Intel and McAfee demonstrate the importance of embedded security and remote manageability on a product separation industrial machine. This demo uses both a security shield and a recovery device to illustrate how different security features can protect operations. There are two IPCs and one remote server in the demo:

Security demo (Trojan attack):

- IPC 1, a machine vision system simulation, has McAfee Embedded Control* (whitelisting) installed and Intel AMT provisioned as part of the Intel vPro platform. A thumb drive is plugged in with a Trojan virus that runs automatically. Because of the security features, the Trojan does not execute, and the machine vision works perfectly.
- IPC 2 simulates an industrial control system with AMT provisioned but does not have McAfee Embedded Control* protection. The Trojan runs automatically, when the same thumb drive is plugged into the IPC2 system. When the database is attacked, the actuator process is disrupted, forcing the conveyer belt to stop and triggering a warning light/ buzzer to indicate a line is down.

Remote management demo (System recovery):

- Through a remote server, McAfee ePO Deep Command makes use of Intel AMT out-of-band remote management to remotely diagnose and repair the problem. The Trojan is removed, the actuator control system is recovered remotely, and the product separation process runs properly again.

Stuxnet highlights vulnerability of the factory floor

Stuxnet raised awareness for the need to provide system security, forever changing the scope and context of control system cyber security. Stuxnet combined stolen certificates and multiple zero-day exploits to deliver a payload that was designed to find and disrupt a specific industrial control process. A sophisticated cyber weapon, it targeted the automated uranium enrichment facilities in Iran by reaching assets thought to be untouchable due to their isolation, obscurity, and specialized functions.

Because threats like Stuxnet are adaptive and sophisticated, defending against them requires improved protection at three levels:

1. Better network protection to secure the initial attack vectors of the worm
2. Better host security to block the worm's ability to infect SCADA system and the PLCs that those systems control
3. Better situational awareness to detect any incidents that do occur

While Stuxnet targeted a particular SCADA system, it proved to be a use case that puts all industrial control systems at risk. The knowledge that these systems are vulnerable underscores the need for improved cyber security measures to deter Stuxnet-class threats.

Secure Your Industrial Systems Today

Protecting industrial infrastructures can be challenging, complicated by network diversity, data overload, complex endpoint management, and tools that lack the right security context.

Using Intel Core processor-based platforms with Intel vPro technology, in combination with McAfee security solutions, you can enhance your situational awareness, manageability, and multizone protection by using purpose-built, compliance-oriented solutions. Such an end-to-end security solution features advanced remote management using Intel AMT, with out-of-band software solutions. The result is a comprehensive solution for securing critical infrastructure, designed to protect against malicious attacks, increase equipment uptime, and lower costs.

Learn more about Intel® solutions

For more information about manageability and security offerings from Intel, visit:
www.intel.com/industrial
www.intel.com/vpro

Learn more about McAfee products

To find additional details about McAfee security products, visit
http://www.mcafee.com/us/.

Solution Provided By:

intel®

McAfee®
An Intel Company

1. Intel® vPro™ Technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software, and IT environment. To learn more visit: http://www.intel.com/technology/vpro.

2. Requires activation and a system with a corporate network connection, an Intel® AMT-enabled chipset, network hardware, and software. For notebooks, Intel AMT may be unavailable or limited over a host OS-based VPN, when connecting wirelessly, on battery power, sleeping, hibernating or powered off. Results dependent upon hardware, setup, and configuration. For more information, visit: http://www.intel.com/content/www/us/en/architecture-and-technology/intel-active-management-technology.html.

Printed in USA 1013/RH/CMD/PDF ♻ Please Recycle 329690-001US