Multi-zone protection and situational awareness brings Simplified endpoint management
- Centrally manage corporate, SCADA and device networks
- Increase visibility across management activities

Better protection
- Lock down devices to stop unknown threats
- Help prevent zero-day attacks with situational awareness

Lower support cost
- Remotely manage endpoints and their security posture
- Automate the process of demonstrating compliance

A comprehensive end-to-end security solution for industrial and utility infrastructure based on leading Intel® and McAfee® technologies

Securing Different Network Environments
The complexity and diversity of industrial equipment and electric power delivery systems makes it ever more difficult to protect them against a cyber attack such as a zero-day threat. Utility infrastructure comprises a diverse set of networks, illustrated in Figure 1, that cannot be effectively secured by simply “bolting on” technologies designed for enterprise IT. Aging grid assets, such as PLCs, power meters and digital relays, predate the Internet revolution, and therefore are particularly vulnerable to attack and unable to report malicious activity up the chain.

Layered Security Solution
To provide a comprehensive solution, multiple products are needed to create layers of security that operate together without introducing great complexity or impacting availability. Intel and McAfee* demonstrated such a solution with a reference implementation that incorporated seamless multi-zone protection, situational awareness, native supervisory control and data acquisition (SCADA) support, and remote device management. The reference implementation runs on Intel® Core™ vPro™ processors, which enables the network operators to gain full control of an attacked device regardless of its hardware or software state.

Security Solutions for Industrial and Utility Infrastructure
Factory and utility IT departments need products that help protect against both zero-day and known attacks in a manageable way. Intel and McAfee address this with a select group of products and technologies that are highly applicable to critical infrastructures, as described below.

Multi-zone Protection
Centrally manage assets. McAfee ePolicy Orchestrator* (McAfee ePO*) software, the foundation of the McAfee Security Management* solution, unifies management of endpoints, networks, data and compliance solutions. The software enables factory and utility IT organizations or substation network operation centers (NOCs) to centrally manage security and achieve dramatic efficiencies.
Layered Security Solution

McAfee® ePolicy Orchestrator® (McAfee® ePO®) is a scalable solution for centralized protection and security policy management and enforcement.

McAfee ePO Deep Command* with Intel® vPro™ technology enables security administrators to deploy, manage and update security on endpoints, even those that are powered-off or disabled.

McAfee Enterprise Security Manager (McAfee ESM) is based on security information and event management (SIEM) that connects evolving threat data with a real-time understanding of the risk, asset importance and security posture throughout the enterprise.

McAfee Intrusion Prevention System (McAfee IPS) protects systems by monitoring and blocking unwanted activity with a comprehensive three-part threat defense — signature analysis, behavioral analysis and system firewall.

McAfee Integrity Control allows the execution of permitted code – registered on a carefully controlled list – while unknown software is prevented from running, thus making this solution particularly effective against zero-day attacks.

Protecting critical infrastructure is about a comprehensive solution – not a single product

Lower operational costs. Used on nearly 65 million nodes, McAfee ePO provides end-to-end visibility and powerful automations that slash incident response times. McAfee ePO software dramatically strengthens protection to protect energy assets and drives down the cost and complexity of managing risk and security.

Remotely manage. Security administrators can remotely deploy, manage and update security and device software on disabled or powered-off endpoints, thus minimizing expensive onsite visits. McAfee ePO Deep Command employs Intel vPro technology, which establishes an out-of-band (OOB) connection used to take control of the device regardless of the hardware or software state.

Automate compliance. Complying with regulatory mandates, including NERC CIP, typically entails a slow and costly manual effort. McAfee helps by automating the process of reporting and demonstrating compliance with multiple regulatory mandates across enterprise IT, SCADA and device networks, thereby addressing auditor requirements in minutes instead of hours or days.

Situational Awareness

In order to stop zero-day attacks, factory and utility IT departments need actionable intelligence, not just security data. This is the role of the McAfee Enterprise Security Manager (ESM), which incorporates security information and event data for processing logs from all the organization’s sources and organizing them in a central place in near-real-time.

Handle large numbers of security logs. The McAfee ESM parses valuable information from the logs, normalizes the data and correlates the information into a common taxonomy that is understandable to humans. The result is a contextual view that helps identify and isolate attacks produced by unknown malware.

Improve security visibility. The McAfee ESM stitches the distinct events together, looking for patterns in order to answer questions such as: What and how big is the threat? Where is it coming from? What is my exposure? How can I best react to this threat? One of the ways McAfee ESM answers these questions is by calculating a risk score and notifying security administrators when a threshold has been exceeded, as depicted in Figure 2. It answers these questions using multiple advanced event correlation and threat detection techniques—even for sophisticated attacks that originate or target protected SCADA and process control systems.

For More Information

This paper briefly covers technologies offered by Intel and McAfee to address the security needs for industrial and utility infrastructure networks. More details are available in the whitepaper at www.intel.com/content/www/us/en/energy/energy-intel-mcafee-utility-security-brief.html.

To learn more about substations and other assets can use Intel vPro technology to improve the security posture of the industrial and utility infrastructure, visit www.intel.com/vpro and www.intel.com/industrial.

---

Lower operational costs. Used on nearly 65 million nodes, McAfee ePO provides end-to-end visibility and powerful automations that slash incident response times. McAfee ePO software dramatically strengthens protection to protect energy assets and drives down the cost and complexity of managing risk and security.

Remotely manage. Security administrators can remotely deploy, manage and update security and device software on disabled or powered-off endpoints, thus minimizing expensive onsite visits. McAfee ePO Deep Command employs Intel vPro technology, which establishes an out-of-band (OOB) connection used to take control of the device regardless of the hardware or software state.

Automate compliance. Complying with regulatory mandates, including NERC CIP, typically entails a slow and costly manual effort. McAfee helps by automating the process of reporting and demonstrating compliance with multiple regulatory mandates across enterprise IT, SCADA and device networks, thereby addressing auditor requirements in minutes instead of hours or days.

Situational Awareness

In order to stop zero-day attacks, factory and utility IT departments need actionable intelligence, not just security data. This is the role of the McAfee Enterprise Security Manager (ESM), which incorporates security information and event data for processing logs from all the organization’s sources and organizing them in a central place in near-real-time.

Handle large numbers of security logs. The McAfee ESM parses valuable information from the logs, normalizes the data and correlates the information into a common taxonomy that is understandable to humans. The result is a contextual view that helps identify and isolate attacks produced by unknown malware.

Improve security visibility. The McAfee ESM stitches the distinct events together, looking for patterns in order to answer questions such as: What and how big is the threat? Where is it coming from? What is my exposure? How can I best react to this threat? One of the ways McAfee ESM answers these questions is by calculating a risk score and notifying security administrators when a threshold has been exceeded, as depicted in Figure 2. It answers these questions using multiple advanced event correlation and threat detection techniques—even for sophisticated attacks that originate or target protected SCADA and process control systems.

For More Information

This paper briefly covers technologies offered by Intel and McAfee to address the security needs for industrial and utility infrastructure networks. More details are available in the whitepaper at www.intel.com/content/www/us/en/energy/energy-intel-mcafee-utility-security-brief.html.

To learn more about substations and other assets can use Intel vPro technology to improve the security posture of the industrial and utility infrastructure, visit www.intel.com/vpro and www.intel.com/industrial.

---

1 NERC CIP: North American Electric Reliability Corporation’s Critical Infrastructure Protection

Copyright © 2012 Intel Corporation. All rights reserved. Intel, the Intel logo, Intel vPro and Intel Core are trademarks of Intel Corporation in the United States and/or other countries.

*Other names and brands may be claimed as the property of others.

Printed in USA 0612/LS/TM/PDF Please Recycle 327698-002US