Power and Water Cybersecurity Suite – Rogue System Detection

Features

- Detects and remediates rogue systems through McAfee® ePolicy Orchestrator®
- Provides full visibility of all assets on the network
- Converts identified rogue systems into managed clients

Overview

All network-integrated devices must be identified as network assets so they can be properly monitored and controlled. Unprotected or rogue systems are often a weakness within security strategies, creating entry points that viruses and other potentially harmful programs can use to access a network.

Networks are connecting to an increased number of devices or systems, collectively known as the Internet of Things (IoT). Most IoT devices or systems have limited processing and memory to support identifying agents; thus, only a small fraction of IoT components are managed. The rest fall outside of the network and security management tools and are considered ‘rouge’.

Security software focuses on assets that are known and permitted within the network environment; often, they are not designed to detect and control network-connected rogue systems or devices.

Consequently, rogue systems pose a unique threat to organizations by presenting vulnerabilities and allowing sensitive data to be exposed or stolen. Since rogue devices are external to the security management framework, they are not part of any standards, policies, security controls or patch updates. Unmanaged assets are vulnerable to attack, not only to the specific system but to other systems on the network. Furthermore, unprotected systems or systems with an undetermined protection level that join the network can also create compliance issues.

Attackers can use the assets’ legitimate data and access rights to extract sensitive information or to distribute malware.

Rogue systems that are detected on the network can indicate physical malicious activity within the corporate network and can create unprotected wireless access points that bypass firewalls.
Security risks increase as more undetected and unmanaged systems or devices are connected to a network.

**Solution**

The Power and Water Cybersecurity Suite rogue system detection module provides near real-time discovery of rogue systems by using sensors installed throughout a network. The sensors employ passive discovery techniques to detect network-connected systems. New systems identified by the sensors are checked by the dashboard for installed active agents. If the detected system is unknown to the server, the rogue system detection module provides information to the dashboard for immediate action. Remediation steps include alerting administrators to deploy an agent to the rogue system for conversion into a managed system.

**Dashboard**

The rogue system detection module provides expanded reporting and monitoring capabilities through a dashboard powered by McAfee ePolicy Orchestrator (ePO). An overall system status monitor shows the system’s condition as a percentage of compliant systems. Systems are separated into the following categories:

- **Exceptions** – Systems that do not need an agent, including routers and printers, as well as those systems that do not need to be monitored and reported anymore. A system can be marked as an exception only when it does not represent a vulnerability in the environment.
- **Inactive** – Systems that have gone dormant for a certain time are considered inactive. These are systems that are likely shut down or disconnected from the network such as a laptop, or retired system or another device.
- **Managed** – Managed systems have an active McAfee agent that has communicated with the McAfee ePO server in a specified time
- **Rogue** – There are three types of rogue systems:
  - An alien agent is a device with an agent not in the local database
  - An inactive agent is a system with a local agent that is quiet or dormant
  - A rogue system is a device without an agent

The Power and Water Cybersecurity Suite rogue system detection module is included with the suite’s McAfee antivirus protection module.

**Compliance Summary**

<table>
<thead>
<tr>
<th>NERC Standard</th>
<th>Requirement</th>
<th>Emerson Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP-002 R3</td>
<td>Critical cyber asset identification</td>
<td>Identifies critical assets and critical cyber assets</td>
</tr>
<tr>
<td>CIP-005 R1 and R4</td>
<td>Electronic security perimeter</td>
<td>Electronic security perimeter (R1) and cyber vulnerability assessment (R4)</td>
</tr>
<tr>
<td>CIP-007 R4 and R8</td>
<td>Systems security management</td>
<td>Malicious software prevention (R4) and cyber vulnerability assessment (R8)</td>
</tr>
</tbody>
</table>

©2017-2018 Emerson. All rights reserved. The Emerson logo is a trademark and service mark of Emerson Electric Co. Ovation™ is a mark of one of the Emerson Automation Solutions family of business units. All other marks are the property of their respective owners. The contents of this publication are presented for information purposes only, and while effort has been made to ensure their accuracy, they are not to be construed as warranties or guarantees, express or implied, regarding the products or services described herein or their use or applicability. All sales are governed by our terms and conditions, which are available on request. We reserve the right to modify or improve the designs or specifications of our products at any time without notice.