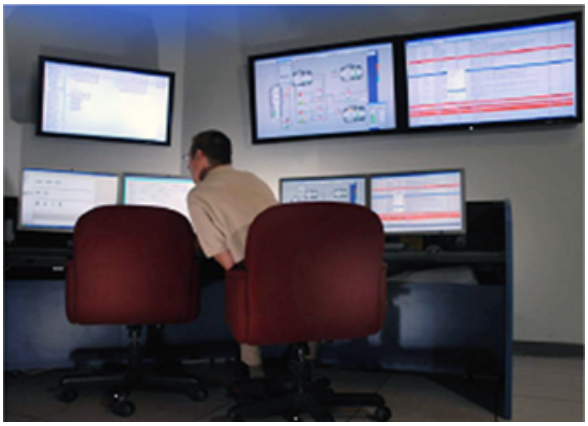
Mark* VIe Control Whitelisting

fact sheet
GEA-S1276A



Whitelisting is a security technique that allows only pre-authorized applications to run on a computer for protection against attacks.

Whitelisting neutralizes malware (malicious software in the form of code, scripts, active content, and such) by preventing its execution. Even if an intruder manages to plant malicious code on a device within the information security perimeter, it is blocked from running unless it is whitelisted.

Conversely, blacklisting blocks only listed applications from running and allows all others to run. Therefore, there is no inherent protection against zero-day threats (threats prior to the awareness and deployment of a security fix) that are not yet known to be undesirable. Also, blacklisting tends to require more server updates to keep pace with the proliferation of malware.

Security Server Whitelisting

The whitelisting service consists of two components. A whitelisting client runs on every protected Windows-based Human Machine Interface (HMI) to provide individual real-time monitoring and protection with all functions. The clients are supported by a whitelisting server with a centralized management solution and simplified single-point management of whitelisting databases and rule sets. In addition, the server provides centralized monitoring. Each whitelisting client sends server performance data such as executable activity, blocked executable attempts, and Windows registry and configuration file activity.

Controller Whitelisting

GE has developed a proprietary whitelisting mechanism to determine the validity of software processes running in an embedded control system. This method ensures that only the genuine released software is allowed to run on a Mark VIe controller. This allows for easy and convenient automatic updating of the whitelist definitions with every new ControlST* installation or upgrade.

This prevents the execution of malicious programs, malware, or other software processes deemed to be a security risk. This functionality is performed as part of the background security maintenance operations inside the controller, and handled with the constructs of a real-time operating system.

Benefits

- Prevents malicious code or malware from being allowed to execute
- Secures server and controllers against attacks for which no patch or antivirus signature exists
- Ensures that only genuine firmware code, provided by GE, is capable of running on the secured controller platforms
- Protects servers from zero-day attacks
- Protects against data theft and leakage by auditing and controlling the transfer of sensitive data to personal storage devices

For further assistance or technical information, contact the nearest GE Sales or Service Office, or an authorized GE Sales Representative.

GEA-S1276A Issued: Aug 2013 Revised: Aug 2014