
Securing Control Systems With Application Whitelisting: Why All the Hype?

Greg Valentine
Director of Technical Sales & Service
CoreTrace Corporation
gvalentine@coretrace.com

April 2010

Agenda

- Overview of the operational realities that make control systems unique—and make the use of traditional security solutions impractical.
- Discussion of the new approach to fight malware on control systems, application whitelisting.
 - Preventing unauthorized applications from executing
 - Painlessly handling the addition / upgrading of authorized applications
 - Control systems case studies
- Live demonstration showing how an application whitelisting solution secures a control system human machine interface (HMI).

Control Systems Are Unique

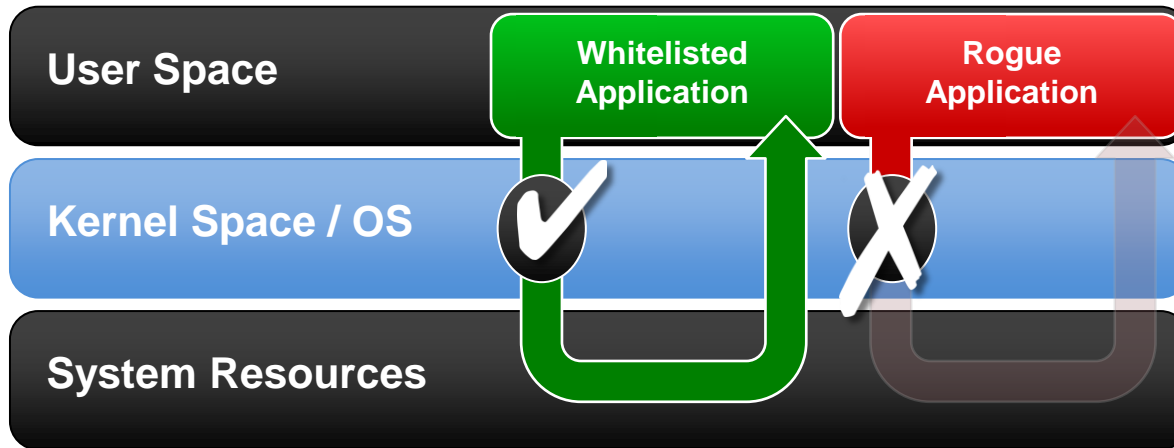
- Reality #1: Many control systems are isolated and not always connected to the Internet.
 - Ramification: the systems are unable to consistently download the latest antivirus signatures or patches, leaving them vulnerable even to known attacks.

- Reality #2: Most control systems cannot be rebooted or can only be rebooted at specific times in very tight maintenance windows.
 - Ramification: Unplanned installations of operating system or application patches are infeasible.

Control Systems Are Unique

- Reality #3: Control systems generally have limited memory and hardware resources.
 - Ramification: Systems cannot handle the performance impacts of resource-hungry security applications, including blacklist-based antivirus.
- Reality #4: Many systems today are on older operating systems that are no longer supported and for which patches are no longer created.
 - Ramification: Teams must find solutions that stop the execution of vulnerability-leveraging unauthorized applications.

The Future of Endpoint Protection: *Application Whitelisting*



"[Application Whitelisting] stopped **100%** of the entered viruses while traditional blacklist-based antivirus solutions detected an average of **60%**."

Simon Howard
DEFCON 16
"Race to Zero"
Organizer

- Based on looking for "known GOOD"
- Enforce a "Whitelist" of approved applications only
 - NOTHING else can run
- Utilizes minimal system resources
- Leading solutions extend protection to memory (e.g., DLL injections, writing to kernel memory)

Key Feature for Control Systems: *Memory Protection—Beyond the Payload*



		Patches	Antivirus	Application Whitelisting
Malicious Payloads		N/A	✓*	✓
Memory -based Exploits	DLL Injections	N/A	✗	✓
	Writing to Kernel Memory	N/A	✗	✓
	Buffer Overflows	✓**	✗	✗

** If payload is known*

*** If available & properly implemented*

Application Whitelisting: *Minimizing Overhead*



Application Whitelisting

Only allow **KNOWN**
and approved applications
to execute.



“Trusted Change”

Transparently add
new applications or upgrades
to whitelists.

- Enable dynamic updates to system/whitelist from Trusted Sources based on your existing operations environment
- Whitelisting without Trusted Change isn't practical
- Trusted Change allows you to:
 - Define boundaries of trust in advance
 - Specify what can modify your systems
 - Control systems and keep them secure without hampering user productivity

Application Whitelisting Lifecycle

Step 1: Who to Trust

Establish Trust Models in Administrator Console

Trusted Updater:
SMSAdmin.exe

Trusted Application:
Project.msi

Trusted Network Share:
\\server\share\

Trusted User:
Corp\JoeEngineer

Trusted Digital Certificate:
Emerson, ABB, Siemens,
OSI, Rockwell, Telvent, etc

Step 2: Rapid Deployment

Turnkey Application Whitelisting Solution

- Deploy hardened appliance
- Deploy AW client to multiple endpoints (desktops, laptops, and servers) via SMS, Group Policy, integrated AD push or manual deployment
- AW client automatically generates custom whitelist for each endpoint

Step 3: Ease of Management

Automatically Enforce/Update Whitelist

- AW Client stops all unauthorized applications & malware
- Protect existing applications from accidental or malicious modification
- Report on security or configuration issues including integration with SIEM
- AW solution transparently updates custom whitelist for new Trusted Applications or changes made by Trusted Sources.

Case Study: Large Utility

Problem

- ✗ Difficulty in running and updating antivirus
- ✗ Unable to patch consistently due to legacy systems
- ✗ Need to enforce configuration control
- ✗ Need to protect and control systems for NERC-CIP compliance

Solution

- ✓ Protect all Windows systems in SCADA control environments
- ✓ Provide compensating control for regulatory and audit requirements
- ✓ Ensure security between patching opportunities and on legacy systems

Benefits

- Increase system reliability
- Compliance with applicable NERC-CIP requirements
- Able to use a single solution across platforms and requirements

Case Study: Municipal Owned Utility

Problem

- ✗ Need to protect and control systems for NERC-CIP compliance
- ✗ Need to enforce configuration control
- ✗ Need additional anti-malware protection
- ✗ Need solution that could not be disabled by local users

Solution

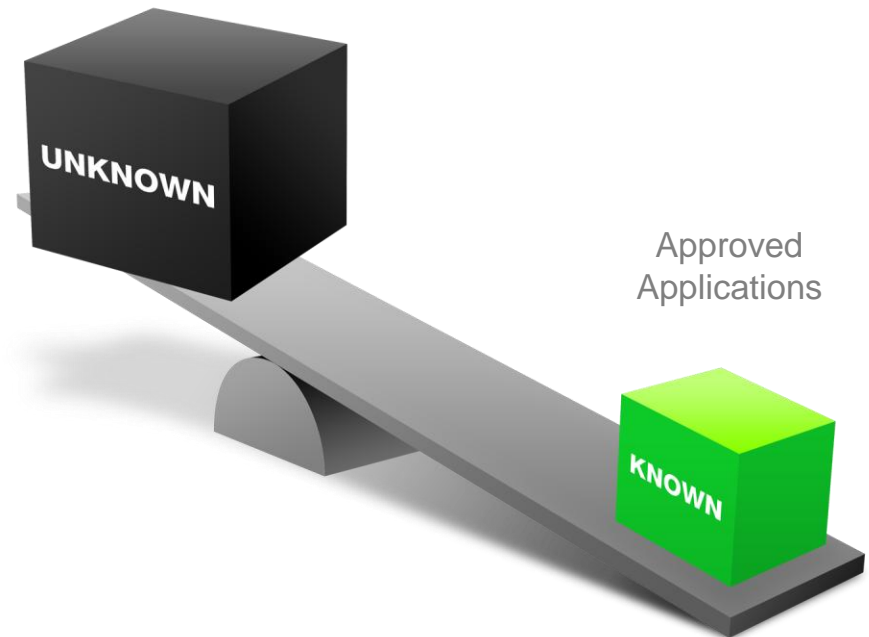
- ✓ Protect all Windows systems in SCADA control environments
- ✓ Provide reporting & audit trail to demonstrate compliance
- ✓ Lower management friction by trusting certain entities (e.g., Windows Update Server)
- ✓ Remain hidden to all users not designated as “Trusted Users”

Benefits

- Ensure, and document, that only authorized applications can execute
- Compliance with applicable NERC-CIP requirements
- Transparent protection, with minimal management overhead

The Benefits of Shifting the Focus

- **Proactive** elimination of all malware
(including memory attacks inside whitelisted applications)
- **Proactive** elimination of unauthorized applications
- **Measured and well-tested** patching
- **Proactive** elimination of malicious or accidental user actions
- **Reduction** of Help Desk requests and reimaging efforts
- **Automatically** meet compliance requirements



Industry Reference – Enterprise Products

- Dan Crandell (CCNA Security, PMP) – Specialist, Controls and Cyber Security
 - Reasons for choosing Application Whitelisting
 - Simplify the Environment,
 - Reduce Change Introduced through Patching, AV Updates
 - Reduce System Resource Utilization on Key Systems
 - Feedback - Best Practices, Planning
 - Know your Network
 - Know your Environment
 - Software Updaters (LanDesk, SMS/SCCM, etc)
 - Patching Mechanisms (WSUS, etc)
 - Questions?

Thank You!



CORETRACE

www.coretrace.com