



CORETRACE

Cyber Security and NERC Compliance With Application Whitelisting

A New Approach to Anti-Virus

August 2009



Traditional Endpoint Security Strategies

- Anonymity
- Controlling physical access
- Anti-virus
 - Blocking known bad applications
- Frequent, unplanned operating system and application patching
 - “Patch Tuesday”
- Host Intrusion Protection Systems
 - Behavior technologies



Today's Endpoint Control Challenges





Traditional Endpoint Security: Challenges

- **Reactive** response to new malware
- **Reactive** discovery of unauthorized applications
- **Reactive and rushed** patching of new vulnerabilities
- **Reactive** recovery from malicious or accidental user actions
- **Reactive** efforts to meet compliance requirements



● Examples in Cyber Security: “Responsible entity shall:”

- Limit ports and services to those required
- Document implementation of security patches or have compensating control
- Prevent malicious software
- Monitor events, preventing unauthorized change to systems

● Challenges

- Feasibility
- Cost
- True benefit to security of critical infrastructure

NERC



A New Approach to Cyber Security is Required

- Proactive in nature
- Prevents malicious AND unauthorized applications
- Protects at the operating system level
- Enables stability and availability
- Minimizes changes to SCADA environments
- Addresses security challenges while:
 - Understanding real time environment
 - Minimizing management overhead for staff
 - Balancing security with operational requirements





Whitelisting 101

● What is whitelisting

- A method for locking down the applications and operating systems so no other unauthorized software can run.

● What security risks does whitelisting address

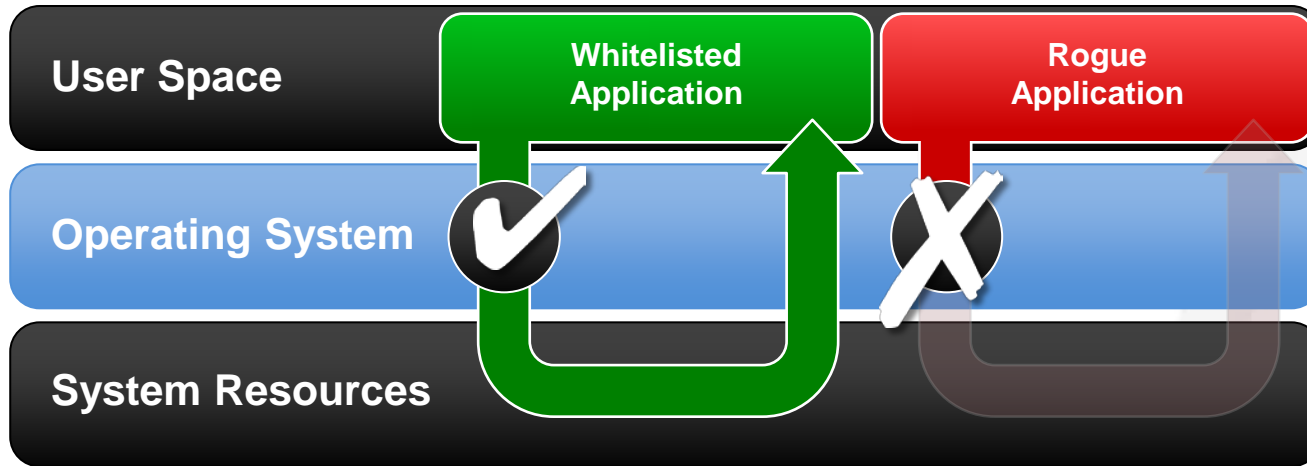
- Prevents malware ***including memory based attacks (CoreTrace Only)***
- Stops day zero attacks
- Neutralizes the risk of existing vulnerabilities
- Eliminates unauthorized software (e.g. games, peer to peer sharing...)

● Other benefits

- Guaranteed configuration control, you know exactly what is on the system at all times
- Prevents CPU degradation from malware
- Integrated logging
- LOW CPU overhead – less than 10% of a typical antivirus scan during normal operations
- NO signatures to update



Application Whitelisting: Key Considerations



“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

- Enforce a whitelist of approved applications only
- Enable dynamic updates to whitelist from trusted sources
- Provide memory protection
- Utilize minimal system resources



Application Whitelisting: Minimizing Overhead

Application Whitelisting

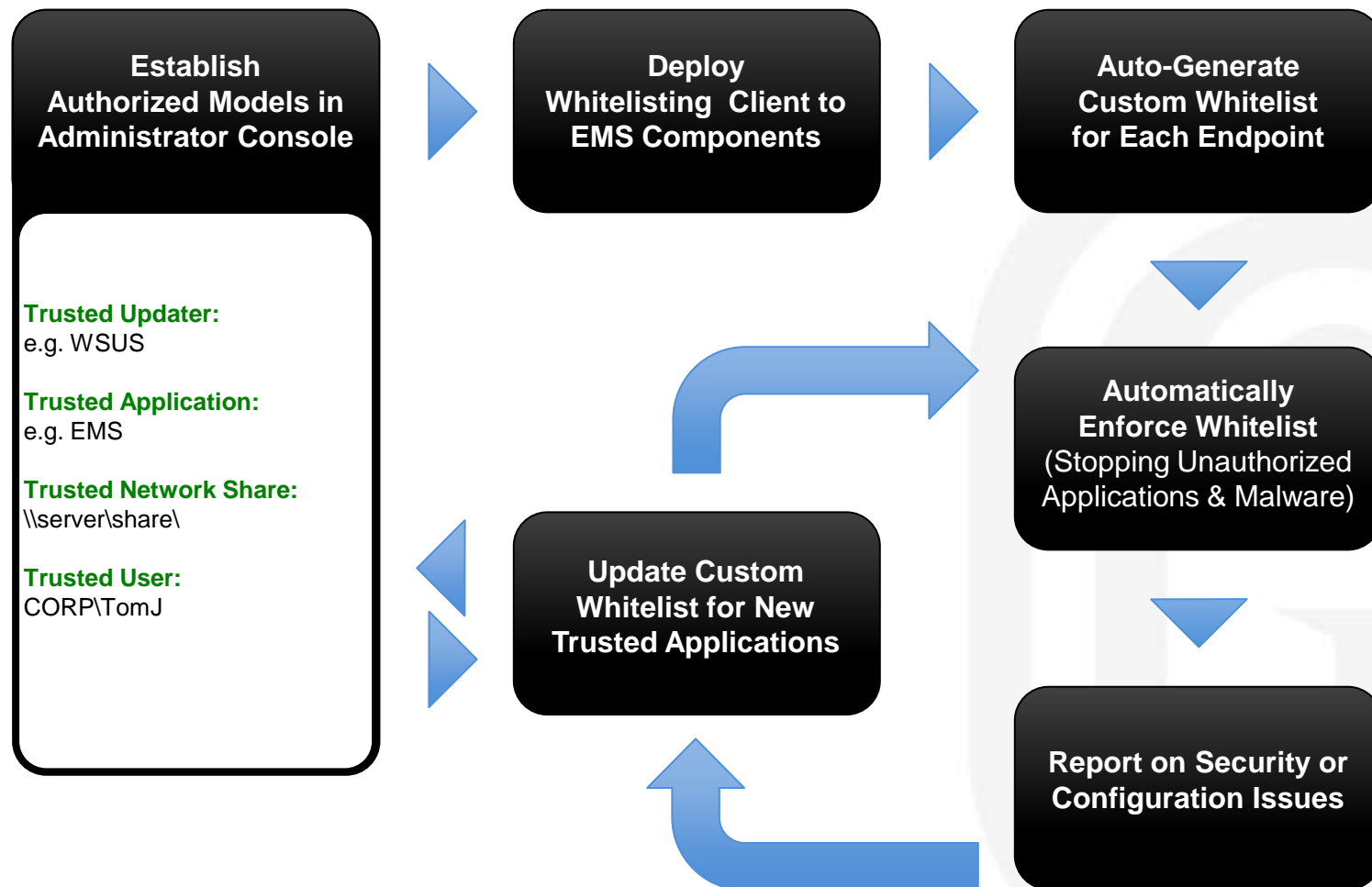
Only allow **KNOWN**
and approved applications
to execute.



“Authorized Change”

Transparently add
new applications or upgrades
to whitelists.

“Authorized Change”: Easy, Immediate, and Ongoing Endpoint Control



How Application Whitelisting enables CIP 3,7 and 9 Compliance



- Document implementation of security patches or have compensating control
 - ✓ **Whitelisting** provides compensating control for systems where patching is not possible, practical, or affordable and protects systems in legacy environments.
- Prevent malicious software
 - ✓ **Whitelisting** prevents all unauthorized change, including all malware — such as zero-day attacks, rootkits, buffer overflows, etc.
- Monitor events and prevent unauthorized change to systems
 - ✓ **Whitelisting** provides monitoring and reporting of events and attack attempts.
 - ✓ **Whitelisting** ensures only authorized application changes occur on the system.
- Track and log security incidents
 - ✓ **Whitelisting** logs unauthorized change attempts and malicious or unauthorized application access .



Best Path to Compliance – Whitelisting vs. AV

Key Consideration	Whitelisting	Anti-Virus
Increased security	Yes	Limited
Prevents false positives	Yes	No
Low CPU overhead	Yes	No
Platform coverage for legacy environments	Yes	No
Mitigates vulnerabilities between patch cycles	Yes	No
Reduces cost for ongoing support; no frequent signature updates	Yes	No
Increases overall stability and reliability	Yes	No
Enables configuration control CIP-007	Yes	No
Provides log data for CIP-008	Yes	No



Case Study: Municipal Owned 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 system

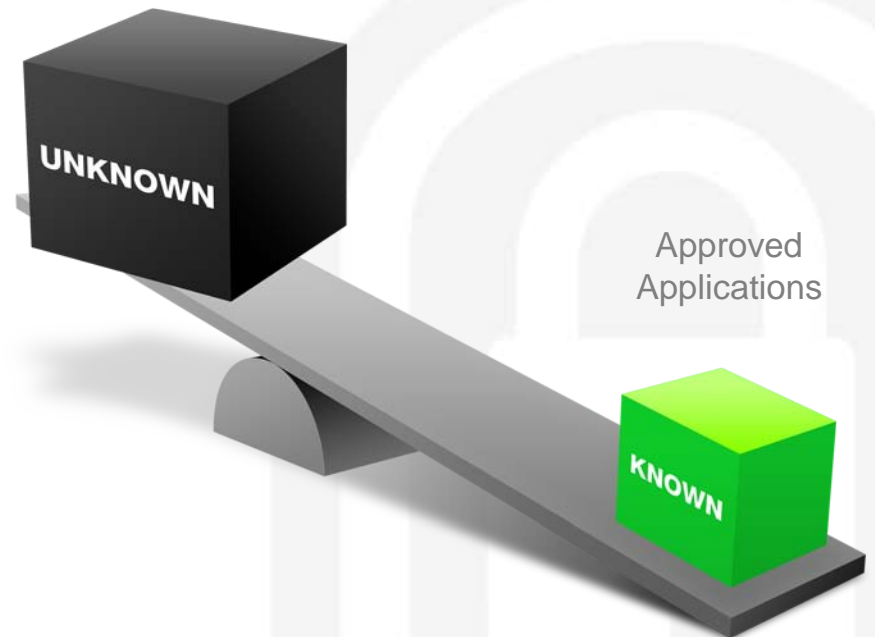
Benefits

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



The Benefits of Shifting the Focus

- **Proactive** elimination of all malware
- **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



- **BOUNCER directly addresses three major endpoint challenges:**
 - Security
 - Manageability
 - Compliance
- **BOUNCER simplifies endpoint control by:**
 - Ensuring that only approved applications can execute
 - Enabling transparent additions of new applications or upgrades to the whitelist
- **BOUNCER provides significant benefits:**
 - Proactively eliminates malware & unauthorized applications
 - Enables measured and well-tested patching
 - Proactively eliminates malicious or accidental user actions
 - Reduce Help Desk requests and reimaging efforts
 - Helps automatically meet compliance requirements