



# ***Endpoint Security 2.0: The Emerging Role of Application Whitelisting Solutions***

Todd Schell

[tschell@coretrace.com](mailto:tschell@coretrace.com)

Director, Product Engineering  
CoreTrace™

December 2008

CORETRACE

©2008 CoreTrace Corporation. All rights reserved.

# Today's Endpoint Control Challenges



- Current generation endpoint security solutions are no longer effective:
  - Malware is more targeted and increasing in volume and sophistication
  - Blacklisting & heuristics-based solutions are failing to catch zero day attacks
- The Security — IT Operations balancing act
  - Frequent patching
  - Configuration control
  - Preventing UNAUTHORIZED change & rapidly allowing AUTHORIZED change
  - Help Desk burden
- Compliance & Governance

CORETRACE

©2008 CoreTrace Corporation. All rights reserved.

# Overview



- Endpoint Security 1.0
  - Anti-malware Technology
  - Evolution of Rootkits
  - Shortfalls of Endpoint Security 1.0
- A Broad Look at Security Technologies
- Endpoint Security 2.0
  - Definition of Application Whitelisting
  - Implementation Philosophies
  - Concept of Authorized Change
  - Some Shortfalls
- What the Press is Saying
- Summary

CORETRACE

©2008 CoreTrace Corporation. All rights reserved.

# Antimalware Technology



- Scans files for malware
- Several Components
  - A malware signature database
  - A remediation database
  - A kernel driver
  - One or more user mode applications
- Two Important Modes
  - Traditional disk scan
  - On-access scanning
- Limitations
  - Only as good as the database
  - Consumes system resources
  - Intrusive

CORETRACE

©2008 CoreTrace Corporation. All rights reserved.

# Evolution of Malware

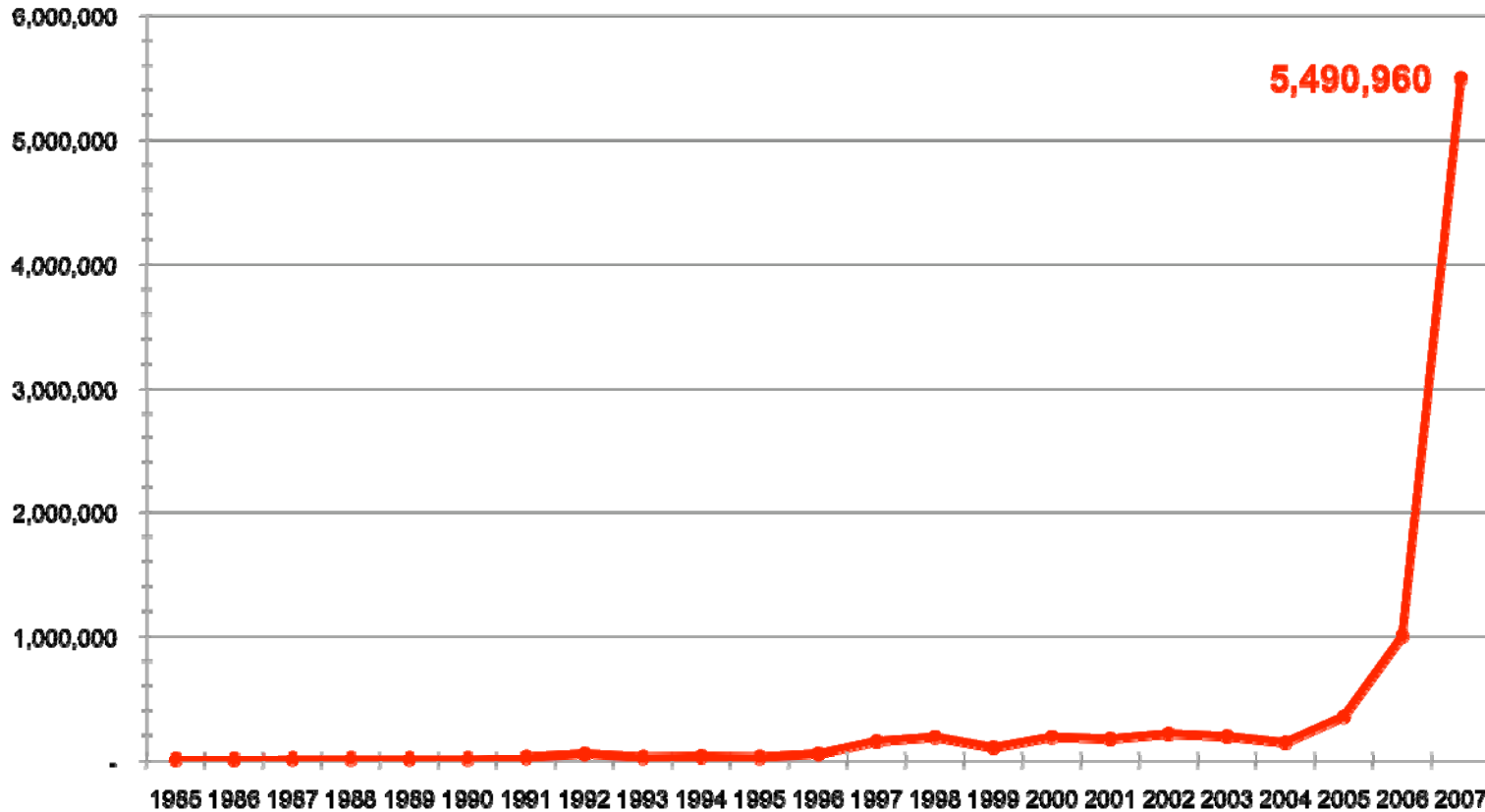


- Malware, including spyware, adware and viruses want to be hard to detect and hard to remove
- Rootkits are a fast evolving technology to achieve these goals
  - Cloaking technology applied to malware
  - Not malware by itself
  - Example rootkit-based viruses: [W32.Maslan.A@mm](#), [W32.Opasa@mm](#)
- Rootkit history
  - Appeared as stealth viruses
  - One of the first known PC viruses, Brain, was stealth
  - First “rootkit” appeared on SunOS in 1994
  - Replacement of core system utilities (ls, ps, etc.) to hide malware processes

# Malware Is a Booming Business!



www.av-test.org — 2008



CORETRACE

©2008 CoreTrace Corporation. All rights reserved.

# “Larger Prey are Targets of Phishing” (April 16, 2008)



1 User baited with false subpoena e-mail



2 User opens document



3 Downloads keylogger or remote access Trojan



- More than 2000 executives infected
- Detected by fewer than 40% of current AV products

CORETRACE

©2008 CoreTrace Corporation. All rights reserved.

# Even Blacklist-based Vendors Agree — A New Approach Is Needed!



“The relationship between signature-based antivirus companies and the virus writers is almost comical. One releases something and then the other reacts, and they go back and forth. It's a silly little arms race that has no end.”

Greg Shipley • CTO, Neohapsis

“If the trend continues and bad programs outnumber good ones, then scanning for legitimate applications (whitelisting) makes more sense from both an efficiency and effectiveness perspective.”

Mark Bregman • CTO, Symantec Corp.

“Authenticate software that is allowed to run and let nothing else run. Anti-virus is a poor IT Security solution because it doesn't do that. Instead it tries to spot software it thinks is bad. Anti-virus comes from a bygone era and that is where it belongs.”

Robin Bloor • Partner, Hurwitz & Associates

CORETRACE

©2008 CoreTrace Corporation. All rights reserved.

# Protecting Critical Systems — What Is Needed Today?



## Gartner's Nine Styles of HIPS Framework

	<b>Allow Known Good</b> (Block All Else)	<b>Block Known Bad</b> (Allow All Else)	<b>Unknown</b>
<b>Execution Level</b>	<b>Application Control</b>	<b>Resource Shielding</b>	<b>Behavioral Containment</b>
<b>Application Level</b>	<b>Application and System Hardening</b>	<b>Antivirus</b>	<b>Application Inspection</b>
<b>Network Level</b>	<b>Host Firewall</b>	<b>Attack-Facing Network Inspection</b>	<b>Vulnerability-Facing Network Inspection</b>

CORETRACE

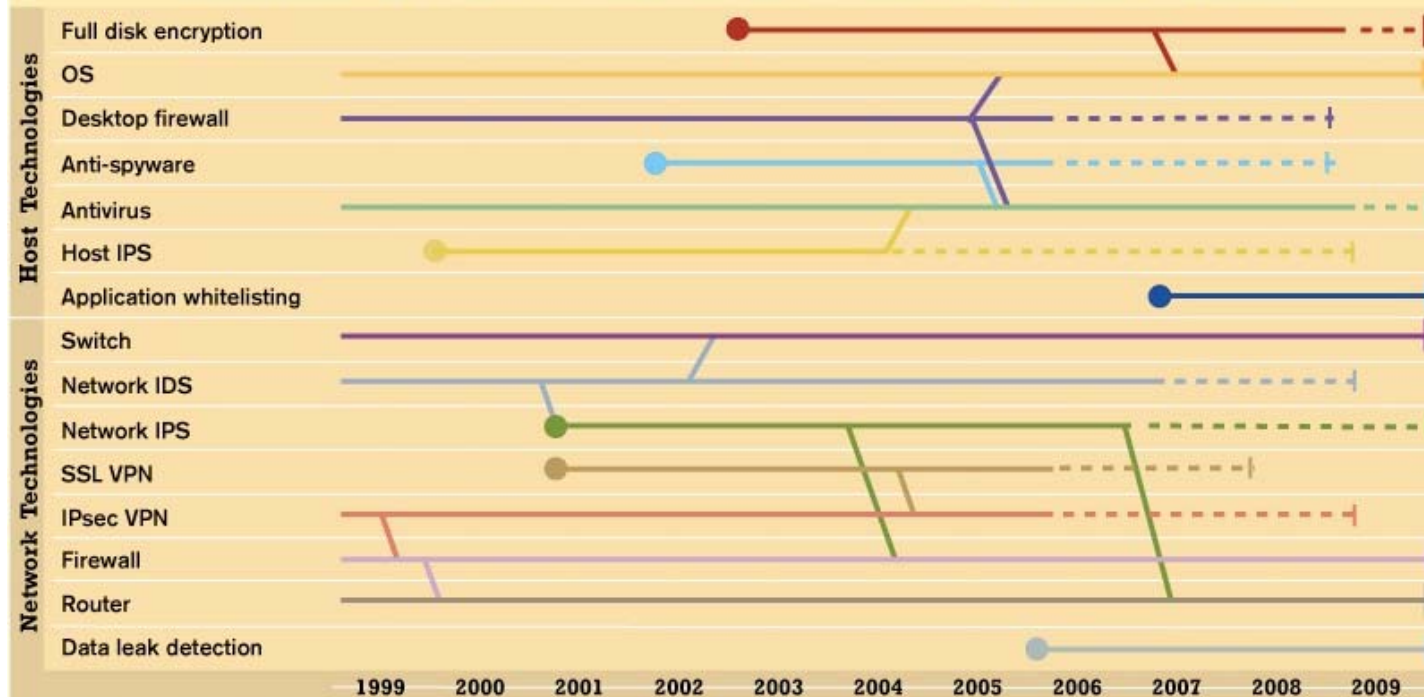
©2008 CoreTrace Corporation. All rights reserved.

# Evolution of Security Technology



## All The Technologies We've Loved Before

Buying your way to safety can be a crapshoot. A few product categories keep going and going, but we've seen many once-popular technologies have their functions absorbed, while others simply fizzled.



Note: Solid lines show that the technology is still active. Dashed lines show that the technology is still sold, but is being phased out. Diagonal lines show that technologies are merging functionality.

Information Week, March 2008

CORETRACE

©2008 CoreTrace Corporation. All rights reserved.

# Ogren Group: The Three Tenets of Endpoint Security



1. Control what you know
  - Easier to control what is known than try to control unknown attacks.
2. Control at the lowest possible level
  - Only security software that functions in the kernel can reliably deliver the controls that IT requires.
3. Control transparently
  - Security must be transparent to end-users and not create administrative burden to operational staff.

CORETRACE

©2008 CoreTrace Corporation. All rights reserved.

# Definition of Application Whitelisting



- What is Whitelisting?
  - List of 'Good' Applications
- Objectives
  - Tracking Applications
  - Only Listed Applications Run
  - Listed Applications are 'Good'
- Some Currently Used List Attributes
  - Signed Binaries
  - Microsoft Group Policy Objects
  - Hashed Executables
  - Simple Executable Names w/Release Dates
  - Combinations of the These

CORETRACE

©2008 CoreTrace Corporation. All rights reserved.

# Philosophy of 'Good'

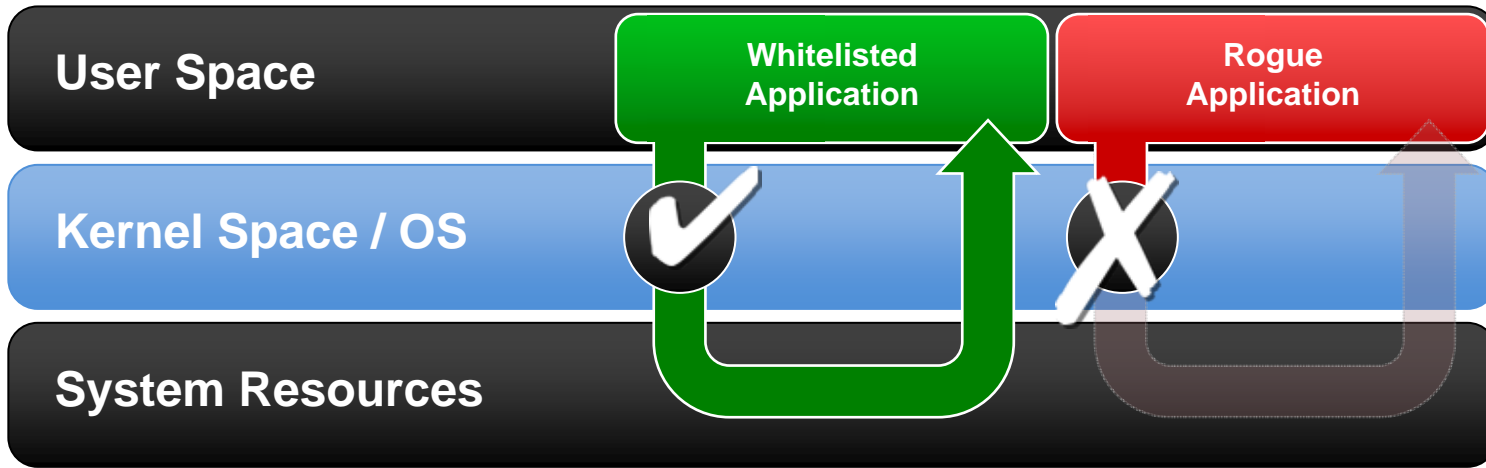


- How do you Determine Good?
  - Trusted Source
  - Signed Binary
  - Mega-whitelist Database
- What do you do with Unknowns?
  - Recently Released Applications
  - Proprietary Applications
  - Miscellaneous dlls, drivers, etc.
- CoreTrace Position
  - Build Whitelist from the Systems Themselves
  - Ideally Start with a New, Clean System
  - If its Working Properly, Its Good Enough (for now)

CORETRACE

©2008 CoreTrace Corporation. All rights reserved.

# Kernel-Level Application Whitelisting



- Protect from within the kernel of the OS
- Enforce a whitelist of approved applications only
- Extend the whitelist to include memory protection
- Utilize minimal system resources

# Enhance IT Operations

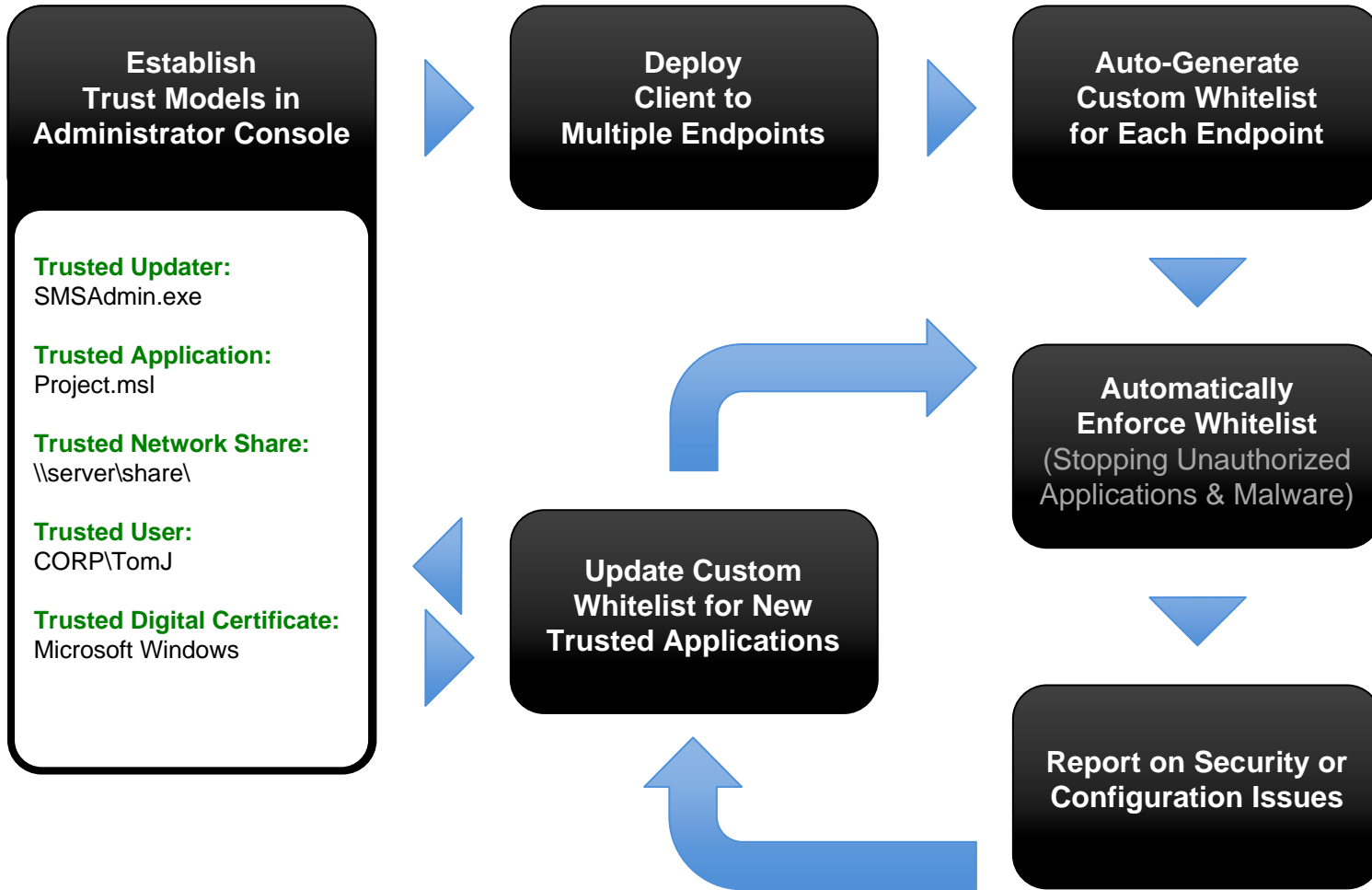


- Security - IT Operations Balancing Act
  - Frequent Patching
  - Image Management
  - Preventing UNAUTHORIZED change & rapidly allowing AUTHORIZED change
- Application Whitelisting must Allow Authorized Change
  - Periodic Application and Operating System Updates
  - Applications Available from Internal Server
  - Ad-hoc Application Installation by Authorized Users
- Application Whitelisting can Enhance Operations
  - Patch on a Controlled Schedule
  - Allow Users Access to Approved Applications
  - Control Authorized Applications on Every Endpoint
  - Easy to Enforce, Monitor, and Report for Compliance

CORETRACE

©2008 CoreTrace Corporation. All rights reserved.

# How Authorized Change should work:



# Positive Environment for Users



- User Expectations are Already Set
  - Company Policies
  - Compliance Requirements
  - Daily Business Operations
- What can the User do on the Personal Computer?
- Whitelist Policy can Match Up
  - Power User Allowing Regular Changes
  - Regular User Allowing Updates for Approved Software
  - Single Purpose System in Lockdown Configuration
- Control and Monitor Change
  - Oversee Problem Users
  - Reporting for Compliance
  - Redirect Corporate Culture as Required

CORETRACE

©2008 CoreTrace Corporation. All rights reserved.

# What Does it Do For Me?





- Only authorized code can execute
  - No zero-day threats
  - No chronic signature updating
  - No paying for chronic signature updating
- Benefits of an Application Whitelisting approach
  - Blocks malware and unlicensed/ unauthorized software from installing and executing
  - Eliminates reactive security patching
  - Eliminates unplanned or unmanaged configuration drift

CORETRACE

©2008 CoreTrace Corporation. All rights reserved.

# Press Coverage for Whitelisting is Exploding



- *Security Vendors Embrace Application Whitelisting* 
- *Antivirus is 'completely wasted money': Cisco CSO* 
- *Security experts look to 'whitelisting' future* 
- *Coming: A Change in Tactics in Malware Battle* 
- *Whitelisting and Trust* 
- *The Real Dirt on Whitelisting* 
- *Black versus White* 
- *Redefining Anti-Virus Software* 
- *McAfee CEO: Adware is killing AV blacklisting* 

# Summary



- Application Whitelisting is the new foundation of endpoint control
- Application whitelisting solutions must be able to easily and immediately handle change
- Application Whitelisting dramatically lowers endpoint TCO
  - Automatically prevents unauthorized and unplanned change
  - Easily allows authorized and planned change
  - Automatically meets compliance requirements for control and visibility
  - Dramatically improves security — with significantly less effort

CORETRACE

©2008 CoreTrace Corporation. All rights reserved.

**Thank You!**

Todd Schell  
tschell@coretrace.com



**CORETRACE**

©2008 CoreTrace Corporation. All rights reserved.