Combating Rogue Applications from Malware to Unauthorized Applications

Wes Miller

wmiller@coretrace.com
Director of Product Management
CoreTrace ™

January 2008

Today’s Endpoint Control Challenges

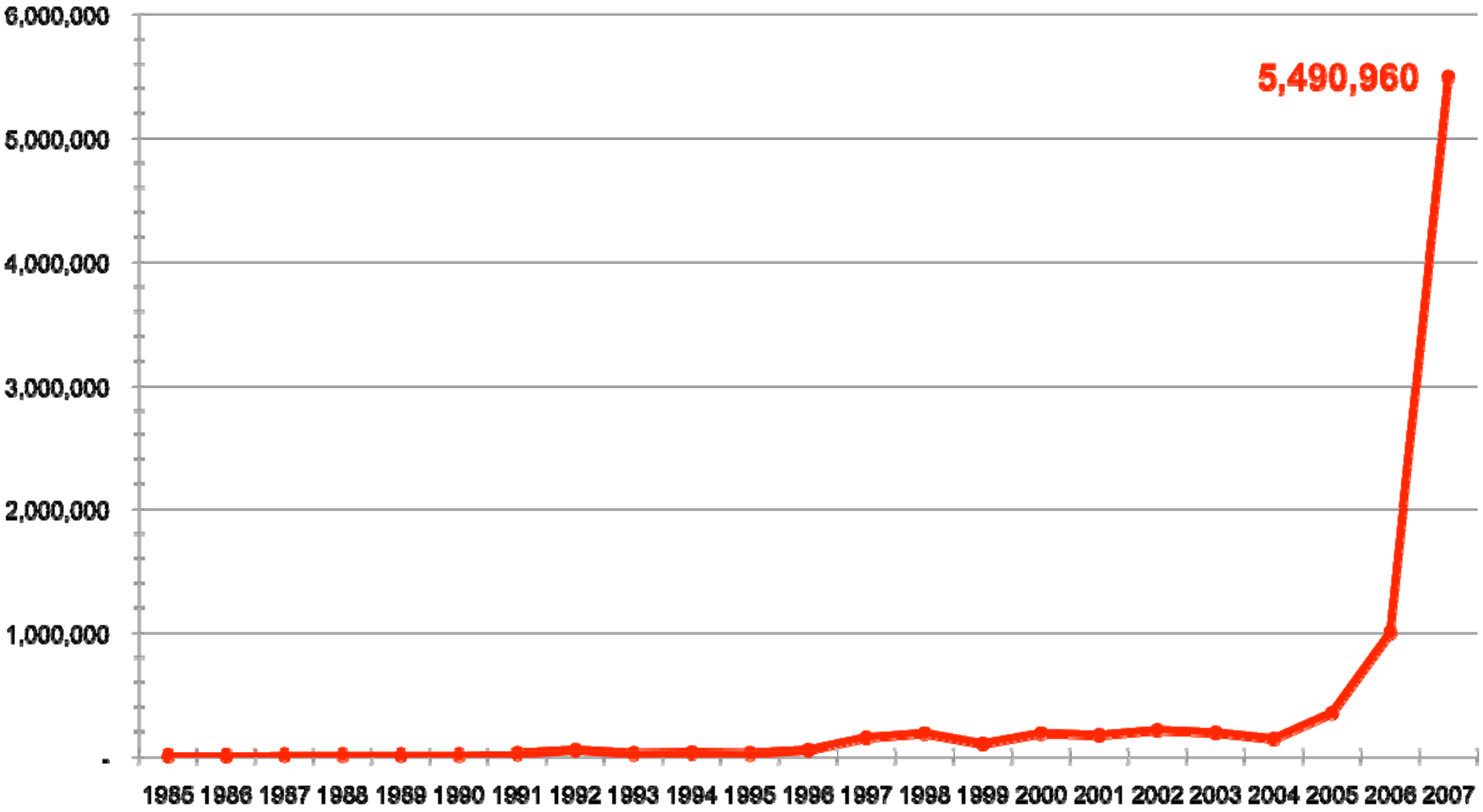
- Current generation endpoint security solutions are no longer effective:
  - Malware is more targeted and increasing in volume and sophistication
  - Blacklisting & heuristics-based solutions are failing to catch zero day attacks
- The Security — IT Operations balancing act
  - Frequent patching
  -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

Overview

- Endpoint Security 1.0
  - Evolution of Malware
  - Malware Cloaking Techniques
  - 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

Malware Is a Booming Business!

www.av-test.org — 2008



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

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

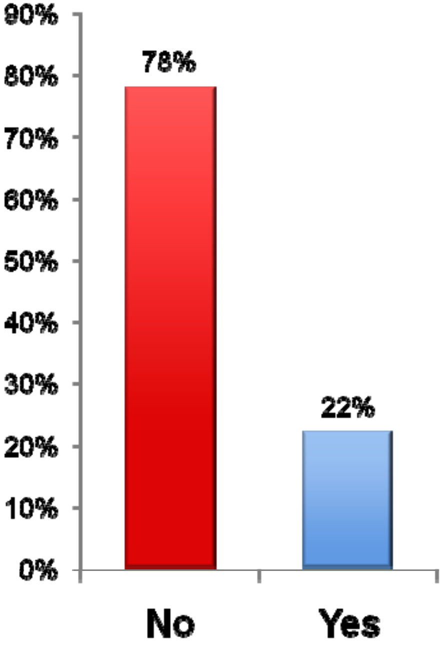
"If the trend continues and bad programs outnumber good ones, then scanning for legitimate applications (whitelisting) makes more sense from both an efficiency and effectiveness perspective."

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

Do you think signature-oriented security suites make your systems secure?



SC Magazine Poll,
Ogren Group Webinar, 2008

Protecting Critical Systems — What Is Needed Today?

Gartner’s Nine Styles of HIPS Framework

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

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.

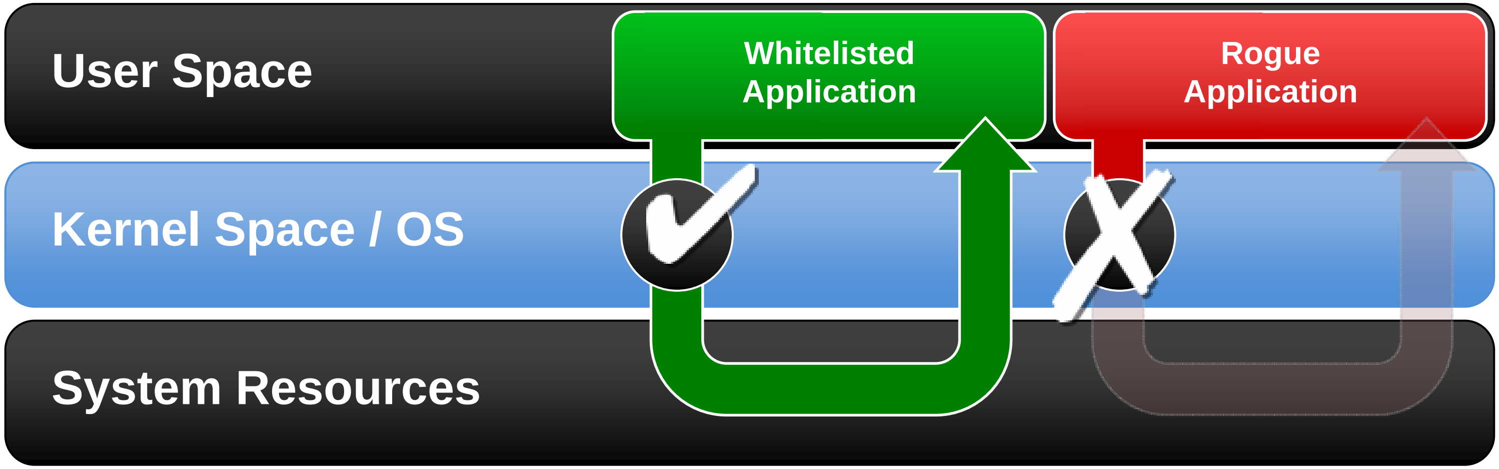
Definition of Application Whitelisting

- 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

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
  - Implement “Trusted Change” to account for new applications and upgrades

Kernel-Level Application Whitelisting



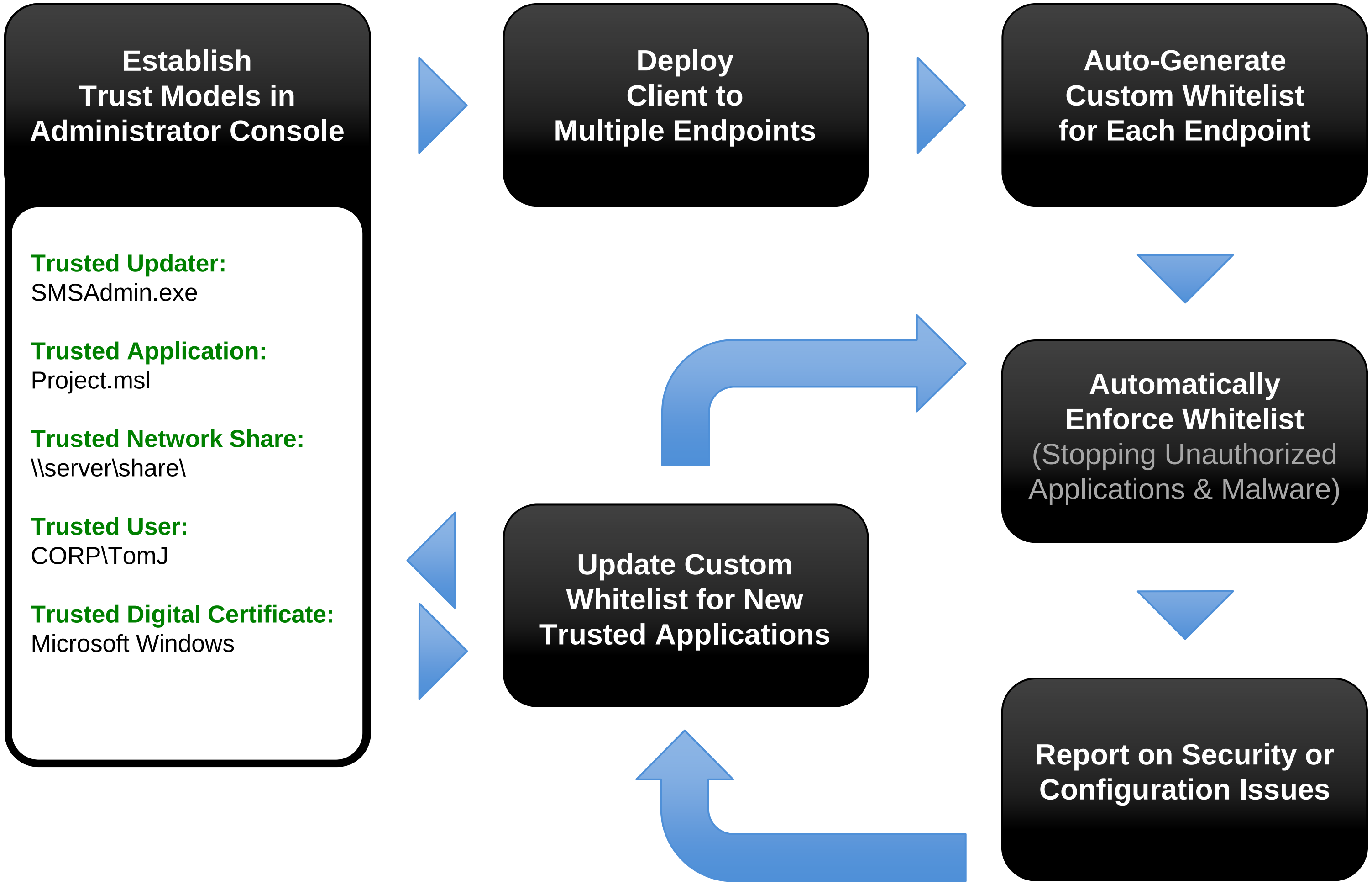
- Protect from within the OS
- Enforce a whitelist of approved applications only
- Provide memory protection
- Provide network filtering
- Utilize minimal system resources

CORETRACE

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
  - East to Enforce, Monitor, and Report for Compliance

How Authorized Change should work:



Establish Trust Models in Administrator Console

Trusted Updater:
SMSAdmin.exe

Trusted Application:
Project.msl

Trusted Network Share:
\\server\share\

Trusted User:
CORP\TomJ

Trusted Digital Certificate:
Microsoft Windows

Deploy Client to Multiple Endpoints

Auto-Generate Custom Whitelist for Each Endpoint

Automatically Enforce Whitelist (Stopping Unauthorized Applications & Malware)

Report on Security or Configuration Issues

Update Custom Whitelist for New Trusted Applications

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

What Does it Do For Me?

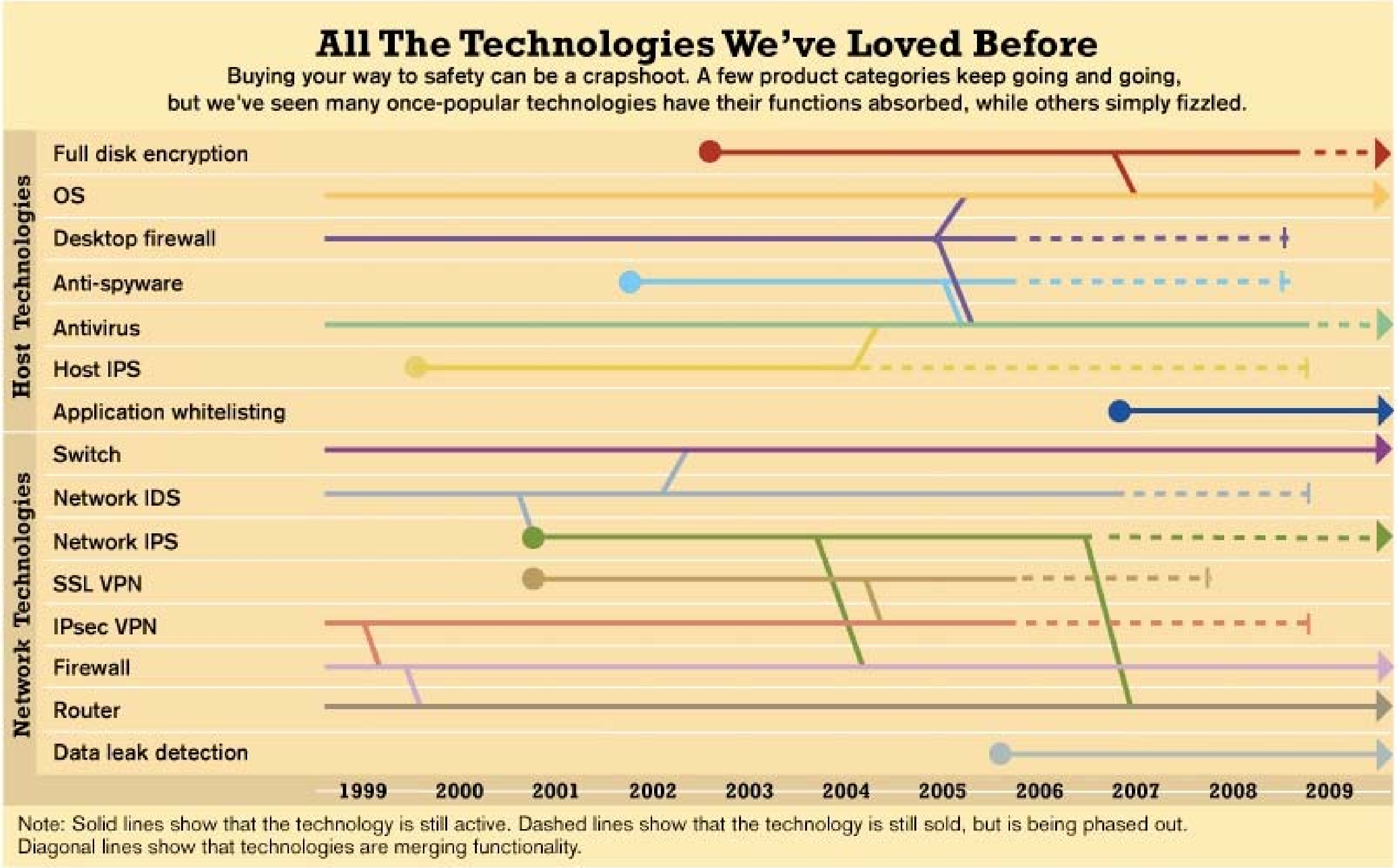
- Only authorized code can execute
  - No zero-day threats
  - No chronic signature updating
  - No paying for chronic signature updating
- Benefits of an Application Whitelisting approach
  - Blocks malware and unlicensed/ unauthorized software from installing and executing
  - Eliminates reactive security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

Press Coverage for Whitelisting is Exploding

- *Security Vendors Embrace Application Whitelisting* eWEEK
- *Antivirus is 'completely wasted money': Cisco CSO* ZDNet
- *Security experts look to 'whitelisting' future* ZDNet.co.uk
- *Coming: A Change in Tactics in Malware Battle* PCWorld
- *Whitelisting and Trust* INTERNET RESEARCH GROUP
- *The Real Dirt on Whitelisting* darkREADING RISKY BUSINESS
- *Black versus White* iTWeb
- *Redefining Anti-Virus Software* washingtonpost.com
- *McAfee CEO: Adware is killing AV blacklisting* ZDNet Australia

CORETRACE

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

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

Thank You!

Wes Miller
wmiller@coretrace.com