Improving Endpoint Security & Control:
An Introduction to Application Whitelisting

Bob Huffman
VP – Business Development
CoreTrace Corporation

CORETRACE

CoreTrace Snapshot

Founded by the inventor of NetRanger (Cisco IDS)

Core Technology: Application Whitelisting

Product Name: BOUNCER by CoreTrace™

Management team with **120+ years of security and enterprise experience**

WheelGroup corporation

WholeSecurity

Trend Micro

SecureLogix We see your voice™

Boeing

MessageOne

mirage networks

netIQ

National Security Agency United States of America

U.S. Air Force

Cisco

symantec.

CoreTrace

Why Are People Looking Into Application Whitelisting?

Inability for existing solutions to address the onslaught of sophisticated, zero-day and targeted attacks, e.g.,

- Advanced Persistent Threats (e.g., Operation Aurora)
- Memory Exploits

Scans have tremendous impact on endpoint performance

Weekly signature updates → daily updates → intra day updates

- Differential updates still consume bandwidth/resources
- Update requirements are proof of solutions' inability to address zero day threats

Periodic bad signature updates further underscores limitations

> *"We are losing a battle based on technology that quite simply has not addressed the issues in over 15 years."*

EMA™

Endpoint Security: Threat Trends

Traditional security under siege

- Explosion in malicious code
  - 116 million new malware samples in H1 09*
  - 75,000 unique “Tier 1” malware threats detected daily**
  - Custom malware increasingly used against high value targets

Shift to targeted attacks

- APWG reports decline in number of phishing sites, BUT…
- Increase in number of targeted attacks at key employees
- “Aurora” attacks target up to 100 IT, pharma and defense firms
- Custom malware tuned to victims’ applications, AV
- Attacks moved laterally within victim networks, pinpointing high value users and assets
- Sophisticated social engineering attacks

* Microsoft Security Intelligence Report

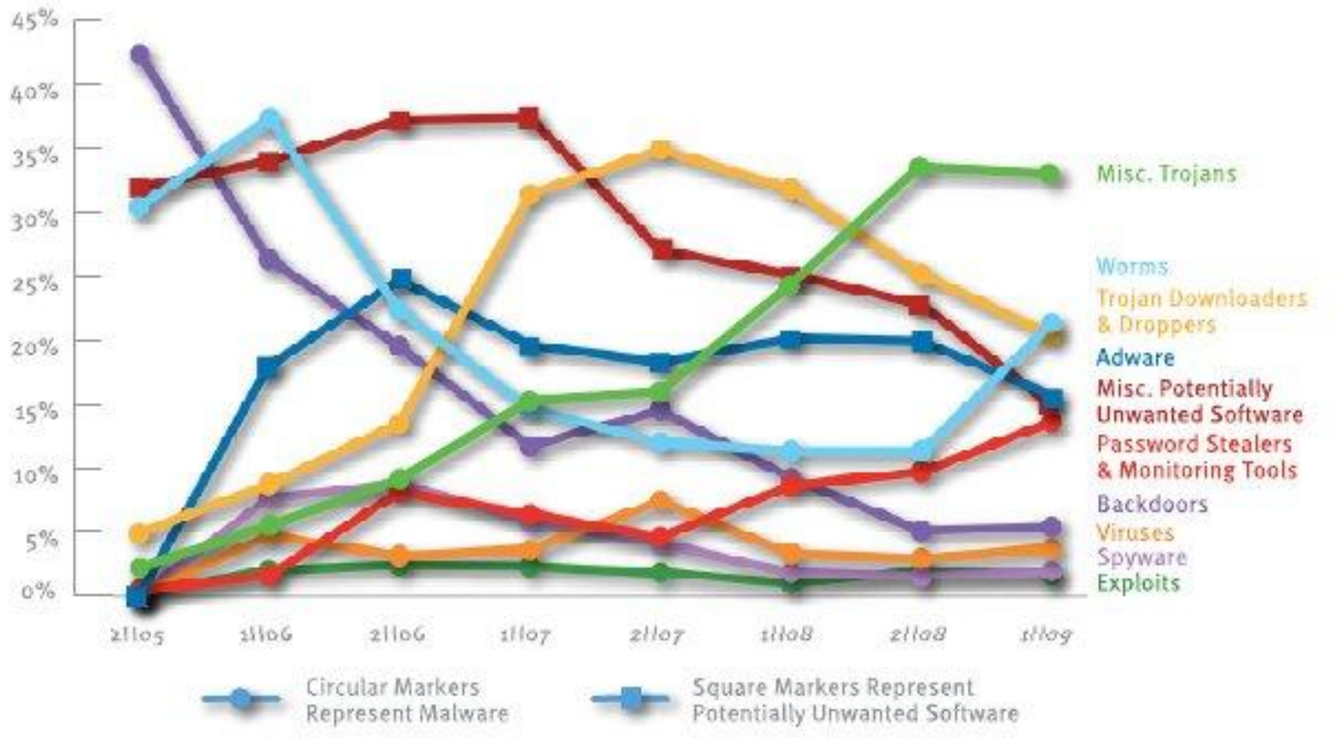
** Sophos PLC

the 451 group

CORETRACE

Endpoint Security: Threat Trends

FIGURE 10. Computers cleaned by threat category, in percentages, 2H05–1H09



* Microsoft Security Intelligence Report

Endpoint Security Rethink: Some Questions

Are you satisfied that your existing endpoint protection software is preventing infection/exploitation?

Are you protected against “Aurora”-style attacks?

- Application-focused
- Employ new/unknown exploits
- Deploy custom malware for data exfiltration, remote control

Do you have non-traditional endpoints to secure?

- VMWare, Mac, Linux, ATMs, POS terminals, mobile devices, etc.

Application whitelisting

Relies on "positive" detection of allowed ("good") applications, rather than blocking of malicious or unknown applications

- Most combine agent with database (client, server or cloud hosted)
- Apps or application components verified with hash or other cryptographically secure signature
- Client enforces policies on endpoint (kernel mode driver to kill offending apps or cut off access to processor, memory, etc.)

Advantages over threat signature based products

- No more "whack a mole" with cybercriminals
- Platform diversity: POS, SCADA in addition to laptop/desktop
- Improved performance on endpoint
- Less infrastructure to maintain, fewer updates
- Answer to "zero day" quandary
- Ability to spot and block "injection" attacks and other attempts to impersonate good applications

the 451 group

Application whitelisting Adoption Hurdles

Manageability

- Plays nice with existing software update, patch and config management platforms?

Flexibility

- Granular policies for different users, roles

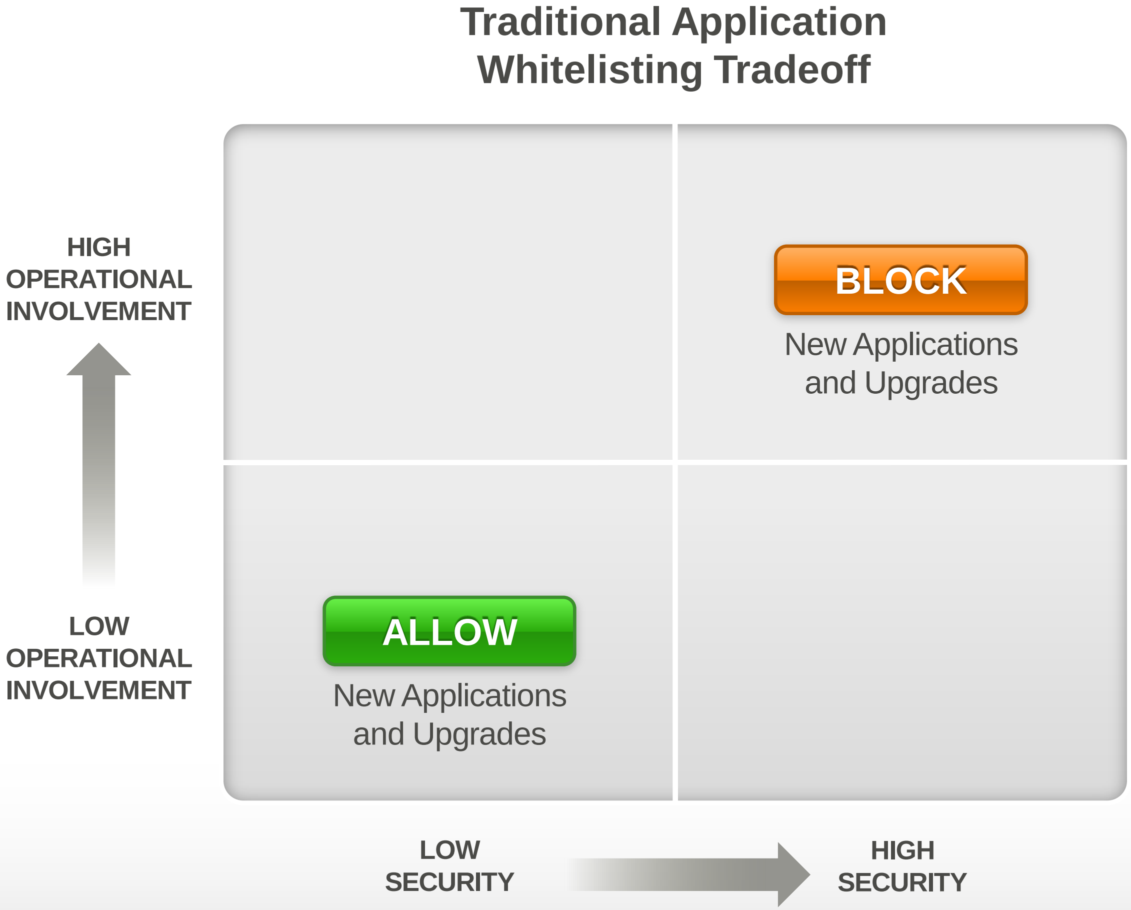
“Friendly Sheets” problem

- Deployment on existing desktops? Are you locking in malware?

Support for the “long tail” of applications

- Transparently handles the installation of new applications—without requiring IT to be in the critical path each time?

What Has Hindered Adoption Historically?



CORETRACE

The Three Pillars of Effective Application Whitelisting

Application Whitelisting

Enforces a whitelist of approved applications at the kernel-level.

+

“Trusted Change”

Transparently add new applications or upgrades to whitelists.

+

“Application Intelligence”

Provides intelligence about authorized and unauthorized applications

CORETRACE

"Trusted Change" Is Critical To Reducing Operational Friction & Overhead

Application Whitelisting

Enforces a whitelist of approved applications at the kernel-level.

+

"Trusted Change"

Transparently add new applications or upgrades to whitelists.

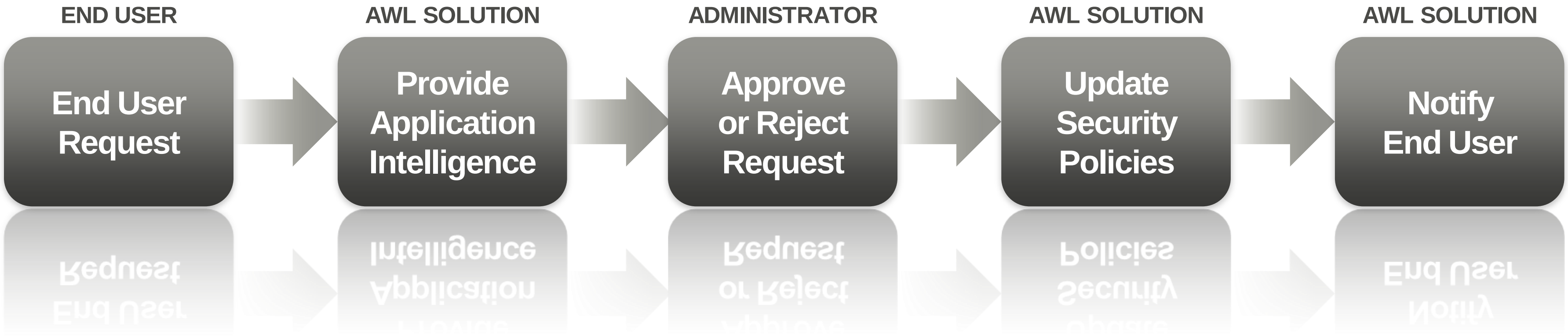
+

"Application Intelligence"

Provides intelligence about authorized and unauthorized applications

- TRUSTED UPDATERS
- TRUSTED NETWORK SHARES
- TRUSTED APPLICATIONS
- TRUSTED DIGITAL SIGNATURES
- TRUSTED USERS

Application Whitelisting Solutions Should Facilitate A Simple, Streamlined Approval/Rejection Workflow



END USER

End User Request

AWL SOLUTION

Provide Application Intelligence

ADMINISTRATOR

Approve or Reject Request

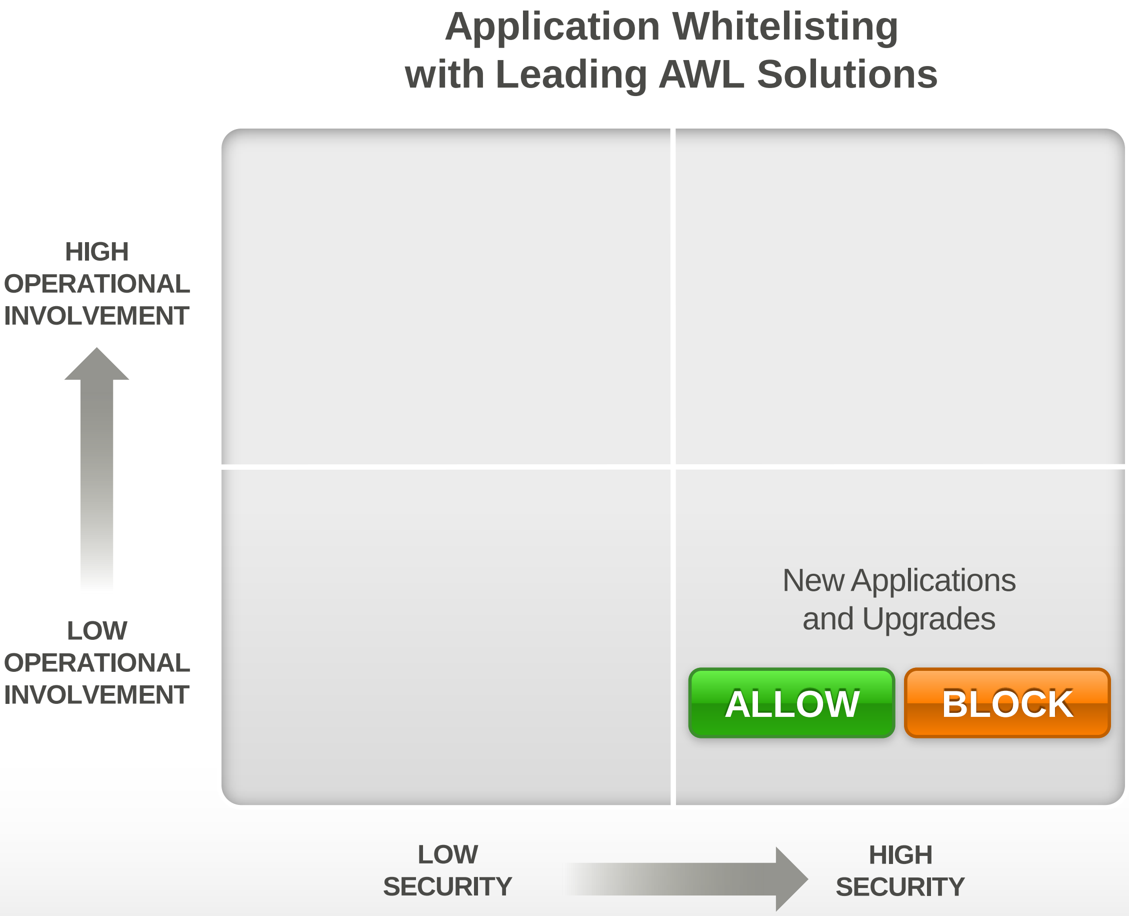
AWL SOLUTION

Update Security Policies

AWL SOLUTION

Notify End User

Today's Leading Application Whitelisting Solutions Increase Security/Control With Minimal Operational Overhead



Application Whitelisting
with Leading AWL Solutions
HIGH OPERATIONAL INVOLVEMENT
LOW OPERATIONAL INVOLVEMENT
New Applications and Upgrades
ALLOW
BLOCK
LOW SECURITY
HIGH SECURITY

CORETRACE

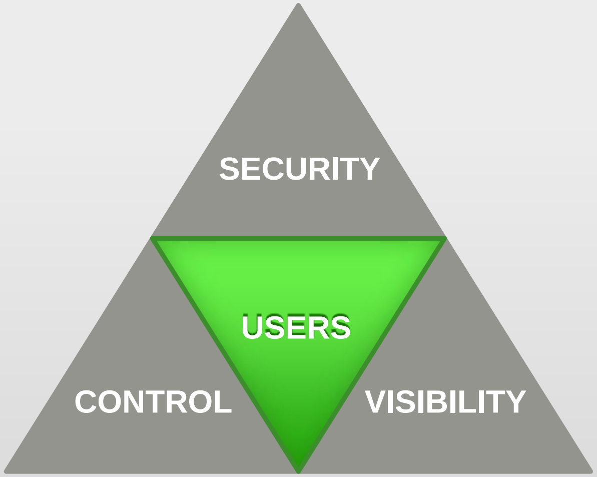
Requirements for Enterprise-Level Application Whitelisting Solutions…

- ✓ **Automatic whitelist generation for each computer**
- ✓ **Prevention of unauthorized application execution**
- ✓ **Support for multiple operating systems**
- ✓ **Advanced protection against sophisticated attacks**
  e.g., memory exploits
- ✓ **Remediation/Removal of unauthorized applications**
- ✓ **Roles-based management**
- ✓ **Self-defending**
  e.g., local admins cannot bypass
- ✓ **Trusted Change**
  Automatic updating for new/upgraded authorized applications
- ✓ **Application Intelligence**
  Intelligence about installed/denied applications
- ✓ **Leverages existing investments**
  e.g., Active Directory,
  patch management systems, SEIM
- ✓ **Centralized administration and reporting**

Summary of Application Whitelisting's Value…

AWL Helps You…

- Increase Security
- Control Your Endpoints
- Gain Application Visibility



Which Enables You To…

- Stop & remove even sophisticated, targeted, zero-day threats
- Enforce approved configurations
- Meet critical compliance mandates
- Understand the prevalence, location and usage of applications
- Reduce unnecessary Help Desk requests & reimaging efforts
- Lower the total cost of ownership (TCO) of each protected system

CORETRACE

Thank You

For More Information Contact:

Bob Huffman

VP – Business Development

rhuffman@coretrace.com

512-592-4140

CORETRACE