



Confidence in a connected world.



# Application Control Solution

Distributed by Codework – ALTIMATE UK

[sales@codework.com](mailto:sales@codework.com)

- Application Security Concerns
- Problems Solved
- Key Features and Benefits
- Demonstration
- Questions and Answers

## Compromised Systems

“Can I combat stealth applications and malware?”

## Regulatory Compliance

“How can I prove compliance with regulations if I can’t control application rights?”



## Rising Support Costs

“How can I effectively support users if I can’t keep track of the applications installed?”

## Human Error

“When did the user install unsupported applications?”



# Reasons to Implement Application Control



## Advanced Application Inventory

Track applications the moment they are installed or modified

## Zero-Day Threat Protection

Neutralize malware by preventing the execution of any unknown code

## Application Authorization

Allow users to install and run only authorized applications

## Privilege and Rights Management

Centrally demote or elevate application rights and privileges

- Unique tracking of application installations
  - Accurate identification of unique executables by calculating a specific hash
- Determine when applications are modified
  - Automatic change detection of executables, such as application of a patch, by differences in the hash
- Streamline helpdesk support
  - Instantaneous identification of executables and locations in real-time
- Review reports for compliance purposes
  - Roll-up summaries by machine or across systems

- Control rights and execution of unknown applications
  - Automatic client-side graylist of locally discovered applications with administrator defined actions, such as limit rights or deny execution
- Contain threats from infection base system
  - Run applications and contain all changes in a Software Virtualization layer
  - Captured changes can be stored in an isolation layer visible to only that application or in global layer visible to the entire system

- **Classify known applications as allowed or disallowed**
  - Allow or prevent their execution
  - Classification can be based upon discovery date, administrator security rating, digital code signing, etc.
- **Protection from spyware, adware and keyloggers**
  - Deny Windows hooking to limit access to the keyboard or to persist on the system

# Privilege and Rights Management



- Lock down systems and preserve legacy application functions
  - Elevated rights can be assigned to specific legacy applications allowing them to run successfully
- Reduce chances that malicious code can be installed or executed
  - Reduce rights on internet facing applications or any specified application thereby reducing your “attack footprint”
- Control application behavior
  - Automatic encryption enforcement through EFS
  - Limit an application’s ability to read or write certain types of files – either by file extension or file path
  - Deny windows hooking to prevent shadow attacks through privilege escalation
- Automatic “graylist” of locally discovered applications

- Protect your most valuable information assets from unwitting attack
- Prevent unknowledgeable or malicious employees from compromising your security
- Comply with industry regulations by implementing least privilege best practices
- Gain visibility and control over the applications in the environment



Confidence in a connected world.

# Thank You!

For more information please contact us at  
[sales@codework.com](mailto:sales@codework.com) or call **0161 474 0444**

Copyright © 2009 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.