Ivanti Application Control Features & Benefits

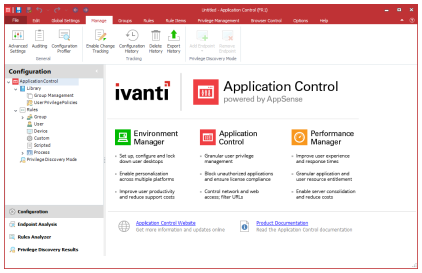
AN IVANTI WHITE PAPER

Contents

Introduction

This document provides a quick overview of the features and associated benefits of Ivanti® Application Control.

The information contained herein is to assist our field sales teams in identifying opportunities and understanding where Application Control can help IT teams.



Features & Benefits

Trusted Ownership™ Checking

Business benefits: Ivanti Application Control protects endpoints automatically without the need for complex configurations and constant management.

Block ransomware, spyware, malicious mobile code, and other web-based threats, including executable-borne viruses, Trojan horses, worms, key logging, script attacks, and rogue internet code.

Trusted Ownership checking provides enterprise-wide desktop/laptop protection both inside and outside of the corporate network, providing a valuable layer of security for a mobile workforce.

It prevents user-introduced, unauthorized applications, preserves the integrity of gold-build images, and increases user productivity by refocusing resources back on business applications.

Additionally, it protects existing anti-malware and antivirus investments by preventing standard users from accessing applications associated with these solutions and extends their capabilities by preventing unknown Trojan and worms from propagating out-of-the-box.

It alleviates the IT burden associated with other application control solutions that require ongoing maintenance of whitelists, such as Microsoft AppLocker.

What it does: Trusted Ownership checking is the default, out-of-the-box security method used by Application Control.

It relies on examining the NTFS owner of an application. If an application is introduced on to an endpoint, and hence owned by a 'Trusted Owner', e.g. an administrator or a software deployment system such as Microsoft SCCM, then everyone can execute the application unless otherwise stated. If the application was introduced, and hence owned, by a non-Trusted owner, e.g. a standard user, then no one can execute the application.

A pre-determined list of 'Trusted Owners' quickly determines which accounts are trusted and hence any applications owned by these users can be successfully installed or executed.

By default, only Administrators and the SYSTEM account are trusted, which ensures only applications installed by an Administrator, or as part of the operating system, can run.

The default list of Trusted Owners can be edited to include other trusted users or groups.

Windows Privilege Management

Business benefits: IT & System administrators prefer their users not have full administrative rights, as this can open up endpoints to security vulnerabilities.

Giving users full admin privileges introduces several costly IT challenges, when the original reason for providing admin rights may be trivial. By providing users with full administrative privileges, IT effectively gives the user the keys to the endpoint. This makes endpoint management incredibly difficult, as the user now has complete control over their own system.

This can significantly increase security costs, manageability costs, decrease productivity, create legal and liability issues, and make compliance with guidelines such as Sarbanes-Oxley, HIPAA COSO, and FERPA very difficult to achieve.

By making sure that users have only elevated privileges for the applications/processes/tasks that need them and nothing more, organizations can reduce their TCO. Managing endpoints becomes easier thanks to fewer support calls, because users still have the ability to perform the tasks they need to—without having excessive privileges that can introduce security vulnerabilities.

Elevate user privileges for running specific applications

What it does: This functionality allows IT admins to specify which applications can run with admin privileges for specific users. Full admin privileges can then be removed from the user, yet the user can continue to perform needed tasks, with elevated privileges only where required.

Use Case: Barclays Bank historically provided users with administrative privileges so they could install printer drivers on their own endpoints. Windows Privilege Management enabled Barclays to remove full admin rights from users, and instead elevate their privileges on an 'as-needed' basis for specific tasks.

Elevate user privileges for running specific Control Panel applets

What it does: Windows Privilege Management allows Control Panel applets to run with elevated privileges. This means that in instances where full admin rights may have been given previously, the user's privileges can now be elevated so that task. For example, stopping or starting a service can still be carried out without users being Admins.

Use Case: Citi Group USA once provided full admin rights to users so they could install Active X components and to allow Development staff to install applications.

Use Case: Morgan Stanley needed to allow its development team to run Visual Studio with admin rights.

Reducing privileges to restrict the rights that applications can run with

What it does: There are two schools of thought when it comes to Windows privilege management. The first is obviously to elevate a process, which is an approach Ivanti takes. The other is to reduce privileges so an administrator can retain the rights they have currently, however the system admin can make sure that certain applications don't run with admin credentials. Reducing privileges can be a better option to removing admin rights across the board and can help with a phased rollout.

Use Case: DSM implemented this functionality to allow users to install ActiveX controls.

Reducing privileges to restrict access to system settings that may be undesirable

What it does: Being able to prevent an administrator from carrying out certain tasks can be advantageous. Windows privilege management can enable IT to stop administrative users from altering settings that the system administrator doesn't want them to change. This could include firewall settings or preventing specific services, such as AV solutions, from being stopped.

Application Control can enable IT to take a user that has administrative privileges and reduce those privileges for certain processes, meaning the user has admin rights to the tasks they require, while IT retains control of the environment.

Use Case: Administrative privileges are needed to allow users to configure their firewall settings. Just giving out the permissions to enable this means that the user has more rights than they need. Application Control can allow IT to give the appropriate privileges without compromising security.

On-Demand Change Request Management

Business benefits: For mobile users or users who spend time working offline, it may often be required for them to access specific applications that may not currently be on an approved, corporate list. Preventing access to these applications can slow down productivity and lead to a poor user experience.

Enabling offline or mobile users to request access to non-standard applications – either via email or telephone – eliminates the need for 'over-the shoulder' support for office-based IT admins, and provides audited application control, improving user productivity and satisfaction.

What it does: End users can request emergency privilege elevation or application access in situations where productivity is blocked. Users can initiate the request right from the application dialogue box. Fulfilment of urgent change requests can be delegated to Level 1 helpdesk analysts using a simple fulfilment portal. Privilege elevation can be fulfilled on either a permanent or time-limited basis.

Application Network Access Control (ANAC)

Business benefits: Prevent employees or contractors from accessing network resources they're not entitled to access, without having to employ complex controls such as routers, switches and firewalls.

What it does: ANAC intercepts and blocks requests made to prohibited network resources and controls outbound network connections by IP, Host Name, URL, UNC, or Ports, based on the outcome of rules processing.

Process Rules

Business benefits: The introduction of process rules to Application Network Access Control (ANAC) means outbound network access can determined by the specific process itself, i.e. different applications can have different restrictions. implementing process rules allows IT to determine what processes (children) can be run by the application (the parent).

Controlling network access per application

What it does: With the introduction of the process rules within the existing rule set, an administrator can decide what network resources an application can access so different applications can have different restrictions placed upon them.

Control what an application can run or not

What it does: It's possible that applications or scripts call other applications or scripts. This functionality allows an administrator to specify what an application can run. For example, although an application maybe prohibited from being run by a user, if this application is called by another, elevated application, IT can configure Application Control to either allow it to run or specify for it not to run if called by a specific process.

Application Termination

Business benefits: If a user disconnects from a multi-user environment, such as RDSH or Citrix XenApp, with certain MS Office applications running and then re-connects to that same session from an endpoint that is not licensed, the MS Office applications will still be running and the company is no longer compliant with Microsoft licensing rules. However, with Application Control, IT can ensure that in such a scenario, either the user is warned that after a specified amount of time the application will be shut down, or it will be terminated immediately and prevented from running again from within that session.

What it does: Application Control has always been able to stop unauthorized applications from running. But what of applications that are currently running and are now, through a change of configuration or an environmental change, prohibited? This has a big impact when it comes to licensing. If a user were to disconnect from their session with MS Project or MS Visio still running, when the user goes home and then re-connects to the same, open session using a different endpoint device that doesn't have a license, those applications will still be running and the company is no longer license compliant. Application Termination will shut down the application should it now be prohibited, either allowing the user to save

their work before closing the application or just terminating the app with no warning.

Application Groups

Business benefits: This aids in making configurations simpler and more quickly.

What it does: Although Application Control generally needs very little configuration, if an organization moves away from the default Trusted Ownership model, they may be required to enforce a whitelist- and blacklist scenario and, due to the amount of applications in typical Windows environments, these lists can get very large and difficult to maintain. Application Groups provide the ability to assemble all rule items together, allowing for a far more organized configuration.

Digital Signatures

Business benefits: Digital Signatures, or Digital Hash Checking, provides IT with peace of mind knowing that applications and files installed on a system remain unaltered, maintaining system integrity and lowering maintenance costs.

Digital signatures provide the ultimate security control as they enable a way of identifying an individual file very easily. Consider it like the digital fingerprint of a file. If one small part of a file is changed, then the digital signature also changes.Creating digital signature groups allows for simplified management of larger and more complex configurations.

What it does: Digital Signatures check the cryptographic hash (think electronic fingerprint) of files against blacklists or whitelists for advanced security and assign SHA-1, SHA-2, or Adler32 digital signatures to applications and files to ensure application integrity. Modified or spoofed applications are prevented from executing. However, digital signatures introduce high management overhead as new signatures need to be taken each time a file is updated by means of a service pack or patch, or when the operating system is patched. Digital signatures are independent of the file system and can be used on local, network, and removable media.

Passive Monitoring

Business benefits: Provides an extremely useful tool to accurately track user behavior prior to full implementation, or to understand application usage for software license management.

What it does: Monitors unauthorized execution attempts without preventing users from running the applications. Passive monitoring can be enabled or disabled on a per-user, group, or per-computer basis.

Application Limits & Time Restrictions

Business benefits: Application limits can be used to enforce corporate license policies, ensuring only authorized users can run business applications and only during certain time periods.

What it does: Limits the number of instances allowed to run on a per-user, per-device, or per-application basis. A further level of control over application access can be achieved by applying time restrictions so users can only run programs during certain hours and for a certain length of time.

Zip Files & Windows Installer Packages

Business benefits: Restrict access to Windows Installer packages by specifying rules governing which packages can run, thus preventing hidden Trojans, worms, or other unauthorized executables.

What it does: Safely opens Self-Extracting Zip files using a built-in Zip Extractor.

Whitelist & Blacklist Configurations

Business benefits: Provides an alternate application control method to Ivanti's out-of-the-box Trusted Ownership Checking to ensure a rigid, locked-down environment for highly secure environments.

What it does: Define blacklists to protect against known threats and problem applications, or create whitelists to guarantee only known and trusted applications can execute on a system.

A 'whitelist' defines a set of applications that are allowed, preventing all other unknown executables. Combined with Digital Signature hashing, this can be a very secure method of application control, yet introduces admin overhead.

A 'blacklist' defines a set of applications that are not allowed to be executed. These is less secure as all applications that need to be prevented from running must be specified, so this does not cater to the unknown.

VBScripts & Batch File Control

Business benefits: Prevents attacks from malicious code and viruses by ensuring users can only invoke scripts that have been authorized by the Administrator.

What it does: Scripts such as Windows Script Host files and DOS Batch scripts are validated against rules to see if they're permitted to run. Added security can be achieved by applying Digital Signature checks to ensure that script content remains unaltered.

Rules Analyzer Console

Business benefits: Allows IT to identify and resolve security vulnerabilities or over-excessive lockdown of user environments quickly and simply.

What it does: The Rules Analyzer allows administrators to troubleshoot any issues resulting from a deployed configuration. Log files provide simplified access to information detailing why an application was or wasn't allowed to run.

Trusted Vendors

Business benefits: Provides a simple mechanism for allowing any application to be executed from a specific, trusted software vendor.

What it does: Checks the digital signature associated with a specific vendor to ensure the file came from that vendor and has not been altered.

Per-Device License Enforcement

Business benefits: Ivanti Application Control is recognized by Microsoft for enforcing device-based software license control.

Ivanti customers have saved over $2,000 per user over a three-year period and have seen a return on investment in just a few months.

What it does: Microsoft Licensing is based on the client access (CAL) model, and thus this licensing is independent of the user. A Microsoft CAL is required for every device that can connect to a Remote Desktop Server Host (RDSH). Ivanti Application Control allows IT to define software access based on the connecting device, rather than just the user.

Self-Authorization

Business benefits: In some environments it's necessary for users to add new executables to a computer, for example, developers who constantly update or test internal software, or power users who require access to new or unknown applications. Self-Authorization allows nominated power users to execute applications they have introduced into the system. These power users can add applications to a

secured endpoint while outside the office without relying on IT support. This provides development teams, power users, and administrators the flexibility to install and test software while still offering a high level of protection against hidden malware and executables.

What it does: Any user configured as self-authorizing will have the option of allowing an untrusted executable to run, either once, every time during the current session, or always. Comprehensive auditing details information such as application name, time and date of execution, and device. What's more, a copy of the application can be taken and stored centrally for examination.

Trusted Applications

Business benefits: Ensures that business applications that rely on personalized, on-the-fly content needed to run or install can continue to function as required.

What it does: Content such as child executables and DLLs may be allowed only if called by a specific parent application. This is useful when applications write executables out to areas of the user's profile during operation.

Archiving

Business benefits: Allows IT to identify unauthorized executables on the network and detect users who have attempted to bypass existing security controls by renaming unauthorized applications.

What it does: Takes a copy automatically of any prohibited files that users have attempted to run and stores them in a secure repository for analysis.

Endpoint Analysis

Business benefits: Simplifies the management and control of application content across large enterprise desktop estates.

What it does: Endpoint Analysis is used to determine what applications are installed on endpoints within an enterprise environment. Remote machines must have the Application Control agent installed. It detects applications that have been installed using the Windows installer technology (MSI/MSP). A dependency walker ensures that all child components are also monitored and reported on. From this report, applications can then be added easily to rules or signature groups within the configuration.

Application Usage Scan

Business benefits: By highlighting which applications are being used and which are not, unlicensed software can be identified or restricted and licensed software can be removed, reducing both the amount of applications on a device and the cost of licensing those applications.

What it does: Scans a target device and identifies how many times individual applications have been executed on a per-user basis.

Ivanti Configuration Templates

Business benefits: Take full advantage of pre-built corporate policy best practice by importing Ivanti Configuration Templates.

What it does: Ivanti Application Control can import an unlimited number of configuration files and use these configurations in combination.

A selection of configuration templates such as 'common prohibited items' or 'Endpoint Analysis' are available from **https://community.ivanti.com/community/appsense**. This template library is maintained and updated frequently.

www.ivanti.com

1.800.982.2130

sales@ivanti.com