Application Control for Windows

Increase Endpoint Security and Reduce IT Workload and Cost

Ivanti® Application Control for Windows offers IT unprecedented control over endpoints, reducing security risk while providing a great user experience for Windows environments. In addition to contextual application control, the solution delivers secure Windows privilege management that lets you remove users' full admin rights and prevents unauthorized executables such as malware, ransomware, unlicensed software, and other unknown applications from being installed or executed. Application Control also Ivanti enables your IT team to manage application access and user privileges efficiently across your desktop and server estate.

Full Windows Support

Application Control delivers full support for Windows Server 2022 and extended support for Windows 10 and 11, expanding its ability to stop ransomware and malware. It provides IT admins with enhanced, granular end-user controls to improve end-user personalization and endpoint security.

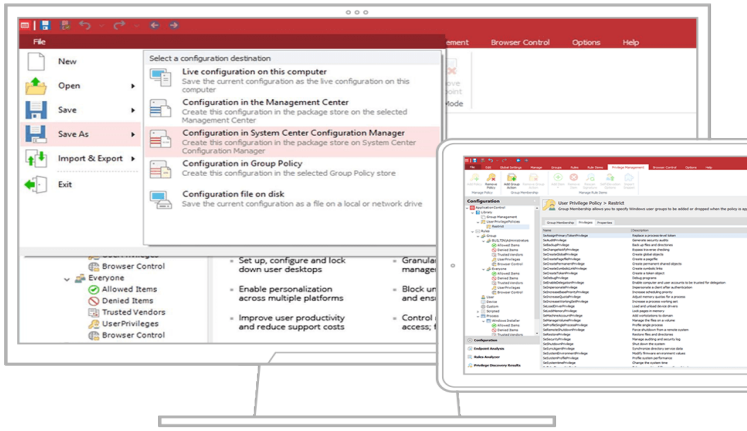
Zero Day Malware Mitigation: Trusted Ownership™

Application Control uses Trusted Ownership checking for out-of-the-box endpoint security. It relies on examining the NTFS owner of an application. If an application is introduced, and hence owned by, a non-trusted owner (e.g., a standard user), the application is prevented instantly from running.

However, if an application is introduced and owned by a trusted owner (e.g., an administrator or a software deployment system such as Microsoft UEM), then every user can run the application, unless otherwise stated. This alleviates the ongoing burden of maintaining allowed lists associated with other application control solutions when application or operating system content requires patching.

Digital Signatures

You can assign SHA-1, SHA-256, or ADLER32 digital signatures to applications and files to ensure application integrity and to prevent modified or spoofed applications from executing.



Allowed and Denied Lists

Application Control allows authorized access to server applications, services, and components, based on application allowed lists. Additionally, IT can check file metadata – including vendor, certificate, publisher, version, and more – to ensure applications, components, and scripts are original and are preventing modified or spoofed applications from executing.

Windows Privilege Management

Providing users with full admin rights can leave endpoints vulnerable, significantly increasing security and manageability costs, decreasing productivity, creating legal and liability issues, and making compliance difficult. By removing users' full admin rights and providing them with elevated privileges for just the apps or tasks they need, you can simplify endpoint security, reduce support calls, and lower TCO.

On-Demand Policy Change Requests

Ivanti Application Control simplifies management of temporary access requests for IT helpdesk staff. Users can respond directly to denial of access notifications with a request for temporary access. These requests can be routed directly to an integrated Ivanti Neurons for ITSM or ServiceNow helpdesk for immediate response, fully automated where appropriate.

URL Redirection

Ivanti Application Control for Windows provides autonomous, seamless redirection of prohibited URL's to a known, trusted web page.

Application Archiving

Application Control automatically copies prohibited files that users have attempted to run and stores them in a secure repository for secured analysis.

License Management

Application Control is recognized by Microsoft for enforcing device-based software license control. By controlling which users or devices have permission to run named applications, you can define limits on the number of application instances, which devices or users can run the application, when users can run a program, and for how long.

User Workspace Manager

Application Control for Windows is part of the Ivanti User Workspace Manager (UWM) suite, which also includes Application Control for Linux, Environment Manager, Performance Manager, Browser Manager and File Director. Using a centralized management console for all of the Windows-based applications in the suite, UWM helps organizations to deliver responsive, secure desktops that provide an outstanding employee experience, save money on servers, manage users more effectively and reduce endpoint security risk.

Reporting and Insights

Application Control outputs a series of configurable events that track environment-wide instances of execution denials, elevation of privileges and other access-associated tasks. Application Control stores the audited events in the database, enabling you to report on the activities of your defined policies in order to ensure that they are not preventing legitimate activities from being carried out. You can access pre-built dashboards and reports generated from this aggregated event data via the Ivanti UWM Management Center or the Ivanti Xtraction self-service reporting software.

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com