Application Control for Windows Servers

Secure Windows Servers with Role-Based User Access

Ivanti® Application Control for Windows Servers lets you control server access and reduce risk by limiting the administrative rights of users who must log onto a server to perform specific, job-related tasks. This is especially advantageous if the server is multi-purpose (for example, SQL and IIS) with multiple admin users, or if the organization must comply with regulations that dictate computing infrastructure security practice.

With Application Control for Windows Servers, IT can limit administrative privilege to specific consoles, applications, services, and commands.

Limit users to performing specific tasks only when logging onto servers

Using Ivanti Application Control for Windows Servers, IT can limit administrative privilege to specific consoles, applications, services, and commands, reducing the risk of admins introducing malware, halting essential services, or affecting performance of mission-critical services.

Privilege Elevation

Providing full admin rights on a server to users untrained as IT system administrators creates multiple risks, like starting or stopping services and installing or removing software in error. This can increase security risk and manageability costs, decrease productivity, create legal and liability issues, and make it difficult to achieve compliance. By removing full admin rights from users and providing them with elevated privileges for just the tasks they need for their job, you can simplify endpoint security, reduce support calls, and lower TCO.

Application Control

Ivanti Application Control for Windows Servers allows authorized access to server applications, services, and components, based on application whitelisting. Using Application Control, IT can assign an SHA-1, SHA-256, or ADLER32 digital signature to ensure file integrity. 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.

System Controls Protection

Apply System Controls to elevate or restrict access to specific services, prevent removal or modification of server applications and processes, and prevent clearing of named event logs.

Application Blacklisting

Quickly implement blacklists to control admin access to critical applications and server operating system components. Blacklisting prevents key server resources from being modified and increases server protection within the data center.

Command Line Matching

With Application Control for Windows Servers, you can apply security policies to launching applications and their associated command line arguments. For applications like Windows PowerShell in server environments, you can limit admin access to launching specific files and scripts or running the application only under certain conditions.

Application Network Access Control

This capability prevents network access without employing complex controls like routers, switches, and firewalls. It can eliminate security vulnerabilities caused by IT admins who gain access to secured data center or network resources from specific servers.

Contextual Control

Application Control employs extensive condition checking to manage server resource access based on the context of the logged-on user. You can assess context based on conditions that include, but are not limited to: user, group or OU membership, device name, device IP or MAC address, connecting client info, operating system, site membership, date and time, or even custom rules created using PowerShell, VBscript, or Jscript. In addition, fully integrated support for Microsoft RDSH, Citrix XenApp, Citrix XenServer, and VMware ensures security policies can also be applied to remote sessions.

www.ivanti.com

1.800.982.2130

sales@ivanti.com