Ivanti Device Control

Data leakage caused by the accidental or sometimes malicious use of removable devices and/or removable media has reached alarming levels. Ivanti® Device Control enforces security policies on removable device usage and data encryption. The solution centralizes management of devices and data using a whitelist / "default deny" approach, plus it provides an additional layer of protection against malware introduced via physical means.

Protect Data from Loss or Theft

With more employees working remotely, access is required from outside the network. But the potential impact of data loss, be it accidental or malicious, is a very real concern. Today, removable media / devices are the most common data leakage routes—no file copy limits, no encryption, no audit trails, and no central management. Ivanti Device Control enables the secure use of such productivity-enhancing tools while limiting the potential for data leakage and its impact.

Key Features

Whitelist / "Default Deny"

Assigns permissions for authorized removable devices and media to individual users or user groups. By default, those devices / media and users not explicitly authorized are denied access.

Policy-Enforced Encryption for Removable Storage

Centrally encrypts removable devices (such as USB flash drives) and media (such as DVDs/CDs), plus enforces encryption policies when copying to devices / media.

Data Copy Restriction

Restricts the daily amount of data copied to removable devices and media on a per-user basis; also limits usage to specific time frames / days.

File Type Filtering

Controls file types that may be moved to and from removable devices / media on a per-user basis; helps limit malware propagation.

Centralized Management / Administrators' Roles

Centrally defines and manages user, user groups, computer and computer groups access to authorized removable devices / media on the network. By default, those devices / media and users not explicitly authorized are denied access.

Temporary / Scheduled Access

Grants users temporary / scheduled access to removable devices / media; employed to grant access "in the future" for a limited period.

Context-Sensitive Permissions

Access / usage policies remain enforced regardless of connection status, and can be tailored whether the endpoint is connected to the network or not.

Role-based Access Control

Assigns permissions to individual users or user groups based on their Windows Active Directory or Novell eDirectory identity, both of which are fully supported.

Tamper-proof Agent

Installs agents on every endpoint on the network. Agents are protected against unauthorized removal—even by users with administrative permissions. Only Device Control Administrators may deactivate this protection.

Flexible / Scalable Architecture

Provides organization-wide control and enforcement using scalable client-server architecture with a central database that is optimized for performance. Supports virtualized server configurations.

How Ivanti Device Control Works

1. Discover all removable devices that are currently connected or have ever been connected to your endpoints.

2. Assess all "plug and play" devices by class, group, model, and/or specific ID and define policy through a whitelist approach.

3. Implement file copy limitations, file type filtering, and forced encryption policies for data moved onto removable devices.

4. Monitor all policy changes, administrator activities, and file transfers to ensure continuous policy enforcement.

5. Report on device and data usage to document compliance with corporate and/or regulatory policies.

"One of the main benefits in deploying Ivanti Device Control is its whitelist feature, which ensures that no device, unless authorized, can ever be used, no matter how it gets plugged in. Flash memory USB devices represent a significant risk with the potential to steal company data or introduce 'malware', which could render the computer unusable and quickly infect other PCs on the same network. Device Control is a really strong, easy-to-use product, which is why Barclays chose this solution."

Paul Douglas
ADIR Desktop Build Team Manager
Barclays

Discover the Benefits of Ivanti Device Control

- Protects data from loss / theft
- Enables secure use of productivity tools
- Enhances security policy enforcement
- Delivers precise control with access limits
- Prevents malware infiltration via physical means / mapping of centralized and decentralized management structures
- Allows for monitoring of all file transfers to printers and physical media

www.ivanti.com

1.800.982.2130

sales@ivanti.com