Product Datasheet
Ivanti Application Manager

Achieve practical, cost effective balance between IT compliance and user demand

Key features:

- Granular, elegant Windows rights elevation
- On-demand change request management
- Enterprise-grade change tracking and control
- Custom Conditions Engine
- Contextual application entitlement
- Application network access control
- Software licensing control
- Passive-mode monitoring
- Integrated auditing events

Key benefits:

- Maintain environment in desired state
- Increase visibility into application landscape
- Enforce licensing, ensure compliance
- Reduce support calls
- Increase user acceptance
- Virtually unlimited contextual entitlements
- Elevation controls for Windows 10

About Ivanti

Ivanti is the leading provider of User Environment Management solutions for the secure endpoint. Ivanti technology allows IT to secure and simplify workspace control at scale across physical, virtual and cloud-delivered desktops. Ivanti solutions have been deployed by 3,600 enterprises worldwide to 9 million endpoints. Ivanti is now part of the Ivanti family with offices around the world. For more information please visit

www.appsense.com

User application entitlement

Whether a user environment is delivered through server-based computing, virtual or physical desktops or a combination of the above, it is essential that users receive only the applications they require and are unable to introduce unknown executables into the environment.

The use of unauthorized software destabilizes user environments and makes it more difficult for IT teams to troubleshoot corrupt desktops. In a shared user environment such as server-based computing, those costs are exacerbated when the action of one user impacts many. Current methods for enforcing application usage are limited to complex scripts or high maintenance black and white lists.

Trusted OwnershipTM

Using secure, kernel-level filter drivers and Microsoft NTFS security policies, Ivanti Application Manager intercepts all execution requests and blocks any unwanted applications. Application entitlement is based on the ownership of the application or file. If a file is owned by a 'Trusted Owner' (such as an administrator) it is entitled to launch. Application entitlement is based on the ownership of the application, with default ownership being administrator. By using this method, current application access policy is immediately enforced 'out of the box' without the need for scripting or list management. This is called Trusted OwnershipTM. In addition to executable files, Ivanti Application Manager also manages entitlement to application content such as ActiveX controls, VBscripts, batch files, MSI packages and registry configuration files.

Privilege management

This dynamically controls end-user privileges with surgical precision, providing users with only the administrator privileges they need while keeping IT support costs from skyrocketing. By removing the need for a local administrator user account, Ivanti manages privileges at the application or individual task level instead of at the session or account level. Privileges can be raised, lowered or even eliminated on a per user, application or task basis.

Not just applications

In addition to applications, Ivanti Application Manager ensures outbound connection requests to UNC paths and URLs are also managed by entitlement, providing one solution for all application and network entitlement rules. Connections, URL's and applications can be done through the UI (user interface), not scripts.

Contextual entitlement

The extent to which an employee has access to corporate applications can depend on the context of the accessing device. For example, a user in an Internet café will typically have a different level of application access than an employee within the secure confines of the corporate LAN. Ivanti Application Manager utilizes information about user context, such as location, device or connection type, and even time of day, to determine entitlement.

Off-line entitlement

With employees becoming increasingly mobile, it is imperative that entitlement rules are enforced when the user is not connected to the corporate network. Ivanti Application Manager ensures employees only access the applications and resources for which they have permission off-line.

License management

Ivanti Application Manager is recognized by Microsoft® for enforcing device-based software license control. Running the software in passive mode enables monitoring, auditing and reporting to detail the frequency of application access across the user and device base. By controlling which users or devices have permission to run named applications, limits can be placed on the number of application instances, which devices or users can run the application, the timing of when users run a program and for how long. License audits and access restrictions based on number of licenses can be enforced regardless of the method of application delivery. License auditing can be used in virtual and physical desktop environments.

Product Datasheet
Ivanti Application Manager

Ivanti Application Manager features:

Quick start configuration templates

Take full advantage of corporate policy best practices by importing Ivanti configuration templates. Ivanti Application Manager 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 'end-point analysis' is available from the template library, which is updated frequently.

Privilege management

The privilege level of a user, group or role can be elevated or reduced for applications and control panel applets. Local admin accounts can be removed yet users can still access select applications or tasks that require admin rights.

Privilege discovery mode

Rapidly scan and report on existing desktops and identify applications and tasks that require admin rights. Flexible reporting options make it very easy to add the results to a configuration.

On-demand change request management

Enable end-users to request emergency privilege elevation or application access in situations where productivity is blocked. Users can initiate the request right from the application dialogue box. Fulfillment of urgent change requests can be delegated to level 1 help desk analysts using a simple fulfillment portal. Privilege elevation can be fulfilled on either a permanent or time-limited basis.

Passive monitoring

Monitor application usage without preventing users from running the applications. Passive monitoring can be enabled or disabled on a per-user, device or group basis and provides an extremely useful tool to accurately track user behavior prior to full implementation or to understand application usage for software license management.

Endpoint analysis

Identify all executable files on a target device and group the files into authorized and unauthorized to quickly create policy. Configurations can be deployed to a user, group of users, machine or group of machines. Within minutes, application entitlement will automatically control application usage.

Application usage scan

Scan a target device and identify how many times individual applications have been executed on a per-user basis. By highlighting the applications that are or are not being used, unlicensed software can be identified and restricted and licensed software can be removed, reducing the amount of applications on a device and the cost of licensing those applications.

Trusted Ownership™

Protect the system without complex lists and constant management. Only code installed and owned by 'trusted owners' is allowed to execute. The trusted owners list can be extended to suit any environment or content directory infrastructure.

White & black list configurations

White and black list configurations can be used in conjunction with Trusted Ownership to control known applications that pass the NTFS owner check. Applications that users should not have access to, such as administrator owned tools like cmd.exe or ftp.exe, are automatically denied. Or, create white lists to guarantee that only known and trusted applications can execute on a system.

Digital signatures

Assign SHA-1, SHA-256 or ADLER32 digital signatures to applications and files to ensure application integrity. Modified or spoofed applications are prevented from executing.

Extensive file support

In addition to controlling .exe files, script, batch and registry files are also controlled. Digital signatures can be applied to scripts to ensure content remains unaltered.

Application limits and time restrictions

Apply policy to control the number of application instances a user can run and what times they can be run. Policy can be created to control or enforce licensing models by controlling application limits on a per-device basis.

Application network access control

Control network access without complex controls such as routers, switches and firewalls. Outbound connections from a target device are subject to entitlement rules. Connections include access to UNC paths (including all files & folders on that drive), servers, IP addresses, URL's, devices and FTP locations. Policy can be tailored to dynamically change based on user or device properties.

Custom Condition Engine

Leverage the power of Ivanti Environment Manager conditions engine, allowing unlimited control when creating 'Custom Rules'. IT can now create multiple 'Custom Rules' that use Conditions such as Operating System, File/Registry, and Device type to target rules against any combination of desktop environment parameters.

URL redirection

If a web browser is left open on a web page or web app and the user reconnects from a new device or location, the browser can be redirected to a predefined safe address. Variables can define when redirection occurs, and rules can be set for which URLs should be prohibited and redirected, and all on a per rule or global basis.

Self-authorizing users

Allow nominated power users to execute applications they have introduced into the system. Applications can be added to a secure machine while outside the office without relying on IT support. A comprehensive audit details information such as application name, time and date of execution and device. Furthermore, a copy of the application can be taken and stored centrally for examination.

Web-level application installation rights

Control a white list of approved websites from which users are authorized to install software. For example, from known sites such as www.adobe.com and www.gotomeeting.com. This provides end users with access to business applications such as Adobe Reader, Adobe Air, Adobe Flash Player and the GoToMeeting web conferencing client without IT application delivery bottlenecks and inefficiencies.

Application-level application installation rights

Some organizations may require more granular control over the applications that users can install from approved websites. An IT administrator may wish to allow installation of Adobe Reader but block any other applications from www.adobe.com. Approve specific applications by version and ActiveX control class ID within the named website as needed. This ensures only trusted versions of specific applications may be installed from the web by end-users.

Enterprise-grade change tracking and control

Capture detailed logging information about ongoing changes to central application control and privilege management policies. Change logs are password protected to prevent tampering.