



Reducing Cost with AppSense:

## Ensuring Microsoft application licence compliance in virtual environments

Many Microsoft applications, including Microsoft Office™, Project™ and Visio™, are licensed on a per-device basis. This means a desktop application license is required for each device that is able to access the application. This can be a complex and costly model to adhere for organizations using Microsoft Windows® Terminal Services, Citrix® XenApp or Hosted Virtual Desktops.

In most cases, these applications are only used by a percentage of the user base, or to be more precise, from only a percentage of the total number of devices in the organization. This poses two areas of concern for nearly every organization using server based computing or virtual desktops:

1. Every licensed where the user does not actually use the application is an unnecessary and costly expense to an organization
2. Devices which are not licensed yet are able to access the application are in breach of Microsoft licensing. Non-compliance can result in a costly fine or legal proceedings

A common misunderstanding is by 'publishing' applications to a limited user group, that group is compliant with the Microsoft license agreement. However, Microsoft applications are licensed per device; a license is required for each client that can execute the application. Group Policies and Software Restriction Policies cannot be used as a means of enforcing licensing control, as these apply to users or groups of users and not the device.

AppSense Application Manager is the only technology that can enforce application access by connecting device, enabling compliance with Microsoft licensing. AppSense customers have saved over \$2,000 per user over 3 years and seen a return on investment in just a few months.

### Lifeline Community Care Achieves Immediate Return on Investment

“ When we came to rolling out Microsoft Project™ we would have needed to purchase 600 device licenses as opposed to only 30, which is the number of people who would actually be using the product. With AppSense Application Manager we were able to place Project on a Citrix server yet fully support Microsoft's licensing requirements for only 30 users. While it can be looked at providing license cost savings of several thousand dollars, in reality is was the difference between being able to introduce the software and not able to because of costs. ”

Peter Spence, State IT Manager,  
Lifeline Community Care.

### Chandler Macleod Avoids Purchasing Superfluous Licenses

“ One of the main software licensing problems facing every Terminal Server/Citrix site is the requirement for each application to have the same number of licenses as there are devices which have access to the servers. This is the case even if only 10 users have authority to use the application. In a server farm where up to 750 devices have access and there are 25 applications, the cost of maintaining software license compliancy is literally staggering. AppSense Application Manager gives the ability to control the users and devices that have access to specific applications, thereby avoiding the purchase of an enormous number of superfluous licenses. ”

Dave Thomas, CIO, Chandler Macleod.

### KEY FEATURES

- > Monitor application execution by device
- > Restrict application execution by device, user and group
- > Restrict application installation by device, user and group
- > Can be used on Terminal Server / Citrix XenApp, VMware View, Citrix XenDesktop as well as physical PCs

### KEY BENEFITS

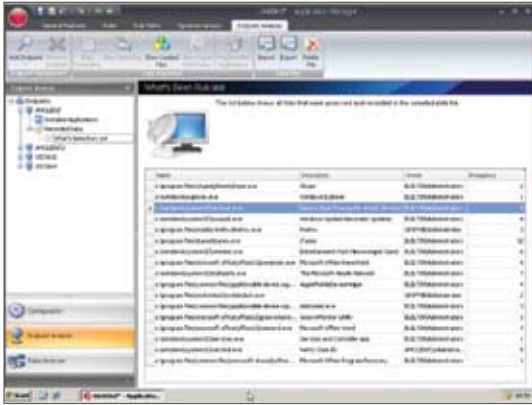
- > Visibility into application use in virtual environments
- > Understand your entire license compliance position
- > Save unnecessary costs in unused licenses
- > No need for multiple point solutions, one technology for all platforms

**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.

**End Point 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 which applications are being used and which are not, unlicensed software can be identified and restricted and licensed software can be removed, reducing both the amount of applications on a device and the cost of licensing those applications.

**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.

**White & Black List Configurations**

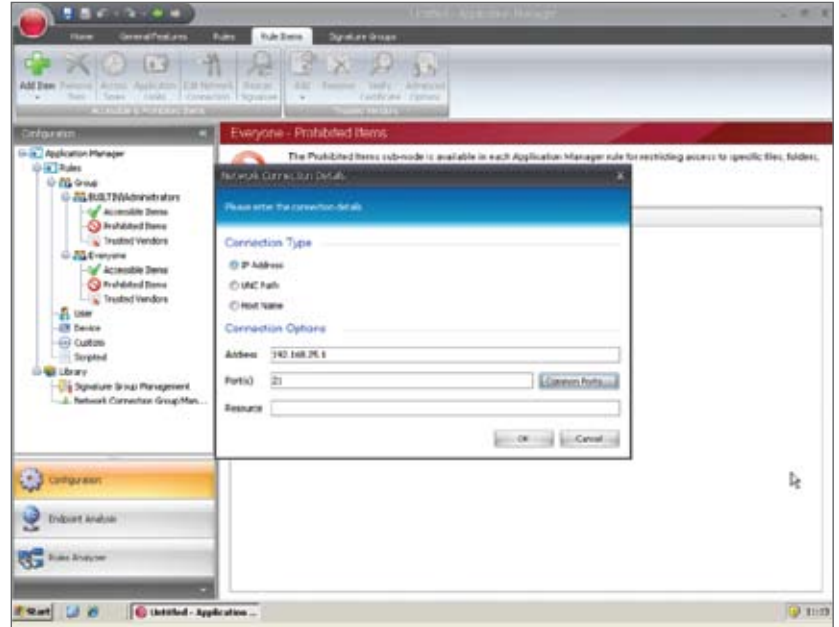
White & black List configurations can be used in conjunction with Trusted Ownership to control known applications which pass the NTFS owner check. Applications that users should not have access to such as administrator owned tools like cmd.exe or ftp.exe are automatically denied. Or, create white lists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

**Digital Signatures**

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

**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 & FTP locations. Policy can be tailored to dynamically change based on user or device properties.



**Self Authorizing Users**

Allow nominated power users to execute applications they have introduced into the system. Applications can be added to a secure machine whilst 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.

**Application Limits & Time Restrictions**

Apply policy to control the number of application instances a user can run, along with at what times it can be run. Policy can be created to control or enforce licensing models by controlling application limits on a per device basis.

**Extensive File Support**

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

**AppSense Configuration Templates**

Take full advantage of pre-built corporate policy best practice by importing AppSense Configuration Templates. AppSense Application Manager is able to 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 [www.myappsense.com](http://www.myappsense.com). This template library is maintained and updated frequently.



AppSense Management Suite is used in server based computing environments such as Microsoft Terminal Services and Citrix XenApp, and is also used in hosted virtual desktop environments and local PCs to ensure users receive a consistent, predictable and responsive working environment.



personalization and policy management



resource entitlement



scalable, resilient framework

To learn more about AppSense Management Suite, please visit [www.appsense.com](http://www.appsense.com)

