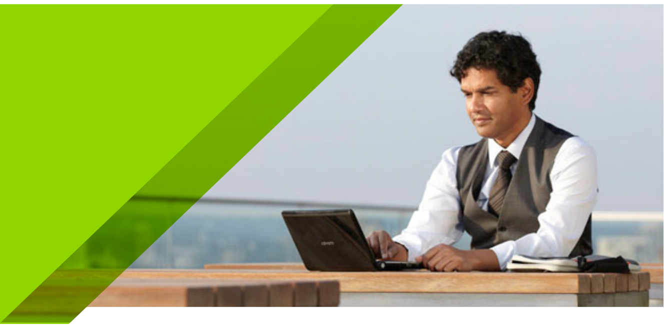
AppSense Application Manager
Product datasheet

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
- 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

About AppSense

AppSense helps corporate IT teams deliver the ultimate in user experience and productivity on both physical PCs and virtual workspaces while optimizing security and lowering both operations and infrastructure costs. AppSense achieves this by separating policy, performance, profile, privilege and data away from the underlying operating system, applications and devices. AppSense DesktopNow and DataNow then deliver it back to the workspace in real time, via any delivery technology, physical, virtual, or cloud. AppSense solutions have been deployed by 3,200 enterprises worldwide to over 7 million desktops. The company is headquartered in Sunnyvale, CA with offices around the world.

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 Ownership™

Using secure, kernel-level filter drivers and Microsoft NTFS security policies, AppSense Application Manager intercepts all execution requests and blocks any unwanted applications. 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 Ownership™. In addition to executable files, AppSense 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, AppSense manages privileges at the application or individual task level instead of at the session or account level. Privileges can be eliminated or lowered on a per user, application or task basis.

Not just applications

In addition to applications, AppSense 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 also be terminated based on rules.

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. AppSense Application Manager utilizes information about user context, such as location, firewall settings and even time of day, to determine entitlement.

Offline entitlement

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

License management

AppSense 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.

AppSense Application Manager
Product datasheet

AppSense Application Manager features:

Quick start configuration templates

Take full advantage corporate policy best practices by importing AppSense configuration templates. AppSense 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 tens of thousands of 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 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 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 applications such as .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.

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.

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. White list 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.

LANDESK® Management Suite

LANDESK® Management Suite increases user and IT productivity. It helps IT administrators automate software and OS deployments, fix user issues quickly, and track software assets. This solution positions LANDESK as a leader in the Gartner Magic Quadrant for Client Management Tools. It integrates the management of all end-user devices in a unified endpoint management experience and provides core IT management services that can be leveraged by other LANDESK or LANDESK partner solutions.

Manage All User Devices

No matter what leading device or OS your users have in their hands, you can manage it with LANDESK Management Suite. It also integrates with leading service management, asset management, and security management solutions to ensure your users are secure, their devices are known, and they have the right experience to work productively.

Improve Productivity with User-Centered IT

LANDESK Management Suite is core to enabling User-Centered IT, which automates IT tasks to drive productivity for IT while providing a more modern experience for all users. Minimize the impact on user productivity caused by system outages, virus attacks, security intrusions, change and configuration activities, and other IT issues. Save IT administrators from jumping between five to seven different consoles and free up time to work on more business-related initiatives.

Sustain IT Reliability

The solution provides a more integrated management of all software and hardware components across your network infrastructure. Administrators and managers can maintain endpoints as a single entity through the most intuitive, integrated IT interface of any client management solution.

Control Assets, Compliance, and Costs

Boost your level of control over business risks and costs due to fines, overbuying licenses, adhering to corporate service level agreements, and consuming excessive energy that affect your budget and the bottom line.

LANDESK Management Suite offers a broad spectrum of technical capabilities, including the following that customers rely on consistently:

Unified Endpoint Management

LANDESK Management Suite discovers and inventories all management data about users and their devices. You gain one-click access to see, configure, and manage the IT policies and processes related to users and groups and all their associated devices. Actions are intelligent and only take effect on the devices to which they apply. Manage mobile and desktop operating systems such as iOS, Android, Windows, Mac OS X, Linux, Unix, and Chromebooks across highly distributed environments.

Roll Out Projects Faster

Deploy to thousands of machines in mere minutes, anytime, without consuming expensive corporate bandwidth. Organize, automate, and roll out to different groups of users the operating systems, software distribution, and patching projects throughout multiple deployment stages. This capability is especially helpful for maintaining the release cadence for modern operating systems and patches.

Streamline Provisioning and OS Migrations

Create provisioning templates in minutes to integrate all your upgrade processes, including communications with users, moving all user profiles, laying down all supported and licensed applications, and standardizing your Windows and Mac OS X images. Use hardware-independent imaging to configure machines quickly with the appropriate drivers.

Integrate IT Actions Everywhere

LANDESK Management Suite provides enhanced core IT functions that other solutions leverage. Take action when it comes to a service desk incident by controlling the user's device remotely and resolving the issue. Reclaim unused software automatically to maintain a pool of licenses to cut software license costs. Automate and optimize complex IT processes faster, which are available to integrate with third-party partner solutions.

Provide Visibility into Activities and Success

Experience on all devices the role-based workspaces for IT analysts, administrators, asset managers, and security administrators that provide the right information, at the right time, in the right context to take action. See dashboards, reports, data visualizations, and other alerts about your IT environment. Also see your success rates and communicate the benefits of IT to your management through increased visibility.

Visit www.landesk.com for information on secure remote control, power management, and additional features.

Visit our website: http://www.LANDESK.com
Speak with a representative: 1.800.982.2130

Or email us at: sales@LANDESK.com
For specific country offices visit www.LANDESK.com

LSI-1543 10/15 AS/BB/DL

LANDESK

Shavlik Patch for Microsoft System Center

Sales Fast Start Card

Elevator Statement

Shavlik® Patch for Microsoft System Center maximizes your organization's investment in Microsoft System Center Configuration Manager (SCCM) by reducing risks from unpatched third-party applications in an easy-to-use and integrated solution.

Solution Value Proposition

Organizations that are using Microsoft System Center Configuration Manager (SCCM) have made a significant investment in the management platform but have an enormous gap for patching or updating non-Microsoft applications. Third-party patching has generally either been ignored or proven too cumbersome to address the needs of large enterprises. With 86% of vulnerabilities identified in third-party applications, keeping them up-to-date becomes even more critical to the security and integrity of the enterprise. Shavlik Patch integrates into SCCM to leverage the scalability of the product and keeps IT workers in a common interface, reducing training time. It automates the process of downloading patch information and distributing patches through SCCM for hundreds of applications based on Shavlik's years of experience patching workstations and servers.

TARGET MARKET & AUDIENCE

What is Shavlik Patch?

A true, fully integrated SCCM add-in that includes access to current patching data licensed via a single or multi-year subscription.

Who am I talking to?

- Director of IT or Windows IT Network Admin and/or budget owner
- SCCM administrator or budget owner
- Windows security manager

Why is this market attractive?

- Growing number of corporate security breaches in the news
- 75% of attacks use publicly known vulnerabilities in commercial software that could be prevented by regular patching (CSIS)*
- 90 million endpoints managed by SCCM
- Fills a gap in a major global business problem that Microsoft won't invest in
- Expands relationships with existing and prospective customers who own and are actively using Microsoft SCCM

* http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf

GAIN ACCESS & EXPLORE: DISCOVER/QUALIFY

Pain Points	Qualifying Questions	Follow-Up Questions	Solution
Security hacks, vulnerabilities, and missing patches cause downtime, data loss, and unemployment	- What is the risk of not patching your infrastructure? - What are you using to patch systems currently?	- What is the cost/risk of doing this manually? - Are you happy with your patch-compliance audit results? - Is your patching process cost effective and comprehensive? - What if we could provide a solution to update and patch third-party, non-Microsoft applications, helping you cut labor hours and regain valuable IT resources to focus on other critical IT tasks?	- With Shavlik Patch you can patch hundreds of third-party applications and versions along with all Microsoft applications, leveraging the infrastructure of SCCM. - Use the Shavlik Patch plugin for the SCCM console to import and manage, sync, and deploy critical patch information using the familiar workflows and features of SCCM.
Adding additional infrastructure or clients	- Are you using SCCM to currently patch workstations?		
Growing number of application updates is over-burdening staff	- How much time does your organization spend on patching third-party applications?		
Patching is ignored because of complexity	- How do you patch your third-party applications? - How many applications do you currently support?		

Common Objections	Objection Responses
I already have a process to deploy patches using SCCM	Does your process support third-party applications? Is it fully integrated? Does it require additional platforms? Do you spend large amounts of time researching and defining individual patches? Shavlik Patch integrates into SCCM to deploy third-party patches saving IT resources and time.
I don't have the budget for a new deployment tool	If your CIO or CFO discovered that your environment was in a position of unnecessary risk, would they view it as acceptable? If not, would they be willing to allocate budget dollars as an exception? How does the budget exception process work, and who is involved? Do you have authority for smaller purchases, such as an add-in for SCCM?
Microsoft already supports third-party applications	Although Microsoft has been talking about this for years and implemented some basic tools, very little has been done to solve the overall problem. They have included minimum tools to pacify customers, but these tools require more effort than necessary. As a result, Microsoft looks to partners like Shavlik to solve these problems for them.
I'm thinking about using X software in addition to SCCM to patch applications	Though there are many solutions on the market that can deliver third-party patch capabilities, many do not integrate into SCCM and/or require an additional infrastructure for patching. Shavlik Patch seamlessly integrates into SCCM and uses all the existing mechanisms and workflows to update and deploy third-party patches, enabling even the largest of enterprises to gain control of the patching process without additional consulting.
I have a patch expert on premise who is already defining and deploying patches	Shavlik has years of experience in creating and deploying patches. What is the risk of a single employee or group of employees researching and distributing patches? How much time does it take out of their day to accomplish this? Shavlik Patch defines and deploys patches for thousands of organizations that have already been tested. This patch information comes from Shavlik's years of experience patching customers systems.

Shavlik Patch Pricing and Packaging

Solution	Description	Pricing/Packaging
Shavlik Patch for Microsoft System Center	▪ Maximizes the investment in SCCM by adding third-party patching with Shavlik Patch ▪ Start deploying third-party updates in minutes within SCCM ▪ Manage and download patch information within SCCM with an easy-to-use Shavlik Patch plugin for the SCCM console	▪ **Shavlik Patch for Microsoft System Center: Term License + Basic Support for 1 year:** $5/endpoint; minimum order quantity of 100 (S-SCUP-G-TLSS-C) ▪ **Shavlik Patch for Microsoft System Center: Term License + Basic Support for 2 years:** $8/endpoint; minimum order quantity of 100 (S-SCUP-2G-TLSS-C) ▪ **Shavlik Patch for Microsoft System Center: Term License + Basic Support for 3 years:** $9/endpoint; minimum order quantity of 100 (S-SCUP-3G-TLSS-C)

More information

SellingShavlik.com

Shavlik Patch product page
shavlik.com/products/patch

Contact Shavlik
shavlik.com/contact

Shavlik Support
shavlik.com/support

sales@shavlik.com

LANDESK® Service Desk

Imagine a comprehensive yet easy-to-use IT service management solution that enables you to deliver quality IT and business services consistently across the enterprise. Available on-premise, in the cloud, or as a hybrid model, LANDESK Service Desk is a highly configurable solution that offers all the capabilities expected from an enterprise-class service management system, including ITIL®-verified process as well as market-leading self service.

Manage and Automate Workflows and Processes

LANDESK Service Desk is a process-driven solution that enables you to manage and automate the lifecycle of your processes—from initiation to updating to closing. The powerful process core ensures that no process can be circumvented. The solution is PinkVERIFY 2011 in 15 ITIL processes.

- Build, modify, and automate ITSM and business processes or get started quickly with pre-defined configurable processes such as incident, request, change, HR, and more.
- Automate repetitive tasks such as password resets or service request fulfilment, freeing staff for other projects.
- Orchestrate cross-system IT automation to create efficiencies and reduce human error.
- Gain the ability to take action, resolve issues, and manage your service portfolio.

Benefit from Technology that's Easy to Use and Own

The solution is very scalable and flexible. You can set up and design the service desk system easily to meet business needs. You can also configure the solution without coding to meet changing requirements and realize faster time-to-value without disrupting users.

Leverage Role-Driven Workspaces for IT and End Users

LANDESK Service Desk incorporates the intuitive, role-driven experience and the secure, anytime self-service of LANDESK Workspaces. Users can access everything they need to interact with IT from one place. They can log or solve their own IT issues, view information, or request apps and services from the service catalog.

- Build and give end users access to innovative capabilities like SnapIT so they can capture error messages on mobile devices and gain access to knowledge automatically.
- Deliver and maintain services automatically—all tied to back-end process and IT policy.

Workspaces offers management, staff, and end users a secure, mobile, location-aware interface accessible from any major platform or device, including iOS, Android, PC, and Mac, or from any HTML 5 browser. LANDESK Service Desk empowers service management teams with the right tools, data, and actions they need to do their jobs—enabled through the same, familiar user interface for each role.

Gain Visibility into Operations with Reports and Dashboards

Quickly report performance against business goals and foster continuous service improvement. Create reports easily, based on the metrics you use to demonstrate value to the business. LANDESK Service Desk is SDI Performance Results Report compliant. From drillable dashboards to trend graphs* based on KPIs, you'll gain context for decisions and planning.

Employ Impact Analysis to Reduce Risk from IT Changes

Apply context to change management decisions with the LANDESK® Configuration Manager* capability. Reduce the number of change-related incidents by building relationships between configuration items and map services to the infrastructure in order to understand who or what is impacted by change requests for services.

Connect IT Silos through Simplified Integration

The solution integrates with multiple LANDESK® products and connects to other industry-leading IT systems, applications, and data to improve service-level response time.

- Simplify integration with pre-built connectors for data sources and directory services.
- Use in-context right click access to drive tools such as remote control and software deployment in LANDESK® Management Suite without leaving the service desk environment.
- Alternatively take advantage of your investment with integration to Microsoft System Center Configuration Manager (SCCM)* and Novell ZENworks.*

Detect and Resolve Issues Before Users Are Aware

LANDESK® Event Manager* receives and interprets important events from any tool that can post to the Event Manager interface and initiates an appropriate process response in LANDESK Service Desk. Monitor the event and update open processes automatically. Resolve issues before users are aware.

** Capabilities require LANDESK Service Desk Enterprise edition. All other capabilities are available with LANDESK Service Desk Standard edition.*

Visit our website: http://www.landesk.com/itsm
Speak with a representative: 1.800.982.2130

Email us at: sales@LANDESK.com
For specific country offices visit: http://www.LANDESK.com