Ivanti White Paper

CIS Controls: Implementing the Controls without Impacting End User or IT Productivity

ivanti

TABLE OF CONTENTS

This document contains the confidential information and/or proprietary property of Ivanti Software, Inc. and its affiliates (referred to collectively as " Ivanti"), and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein. For the most current product information, please visit www.Ivanti.com.

Copyright © 2016, Ivanti. All rights reserved. IVI-1695 07/16 WM/BB/DH

INTRODUCTION

Protecting corporate assets and mitigating security risk are formidable tasks. The threat landscape is ever evolving, and the IT environment grows increasingly complex. But that's not all IT must contend with. Business needs dictate that users have access to data from a variety of devices and locations. Productivity and the user experience need to be balanced with the need for effective security. Meanwhile, IT must strive for operational efficiencies and adhere to tight budgets.

To help protect corporate assets, many organizations adopt The Center for Internet Security (CIS) Critical Security Controls for Effective Cyber Defense. Now in its sixth version, the CIS Controls is a free set of internationally recognized measures for stopping known cyber attacks. Based on attack data pulled from a variety of public and private sources, the measures are specific, actionable, and effective. A study by the Australian government found that 85% of known security vulnerabilities can be stopped by deploying the top five CIS Controls. These include inventorying IT assets, implementing secure configurations, patching vulnerabilities, and restricting unauthorized users.

But while the CIS Controls can help IT organizations protect assets and mitigate the risk of attack via known vulnerabilities, the Controls can also impact efficiencies if not properly implemented and managed by IT. That's where AppSense and LANDESK come in.

Together, LANDESK, Shavlik, and AppSense provide a unified endpoint security solution that addresses many of the CIS Controls with an additional focus on manageability and the end user experience. Our products enable IT organizations to improve productivity for end users and the IT organization. Users get a personalized experience that follows them across devices, and IT can easily lock down devices—all while reducing operational overhead.

In this document we've outlined the CIS Critical Security Controls for Effective Cyber Defense Version 6.0. Each control is aligned with the applicable feature or capability in a LANDESK, Shavlik, and AppSense product so you can see for yourself the benefit of using a unified endpoint security solution.

CSC #1: Inventory of Authorized and Unauthorized Devices

Family	Control	Description	Capabilities	Product(s)
System	1.1	Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic, should be employed.	LANDESK uses active and passive discovery technologies to identify all devices and assets, and inventory them into a single place to simplify, secure, and manage IT processes.	LANDESK Security Suite LANDESK Management
System	1.3	Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.	LANDESK aggregates manufacturer, vendor, reseller, and service provider information from the moment of purchase. Passive discovery identifies devices that connect to the network and flag unauthorized devices.	LANDESK Asset Intelligence LANDESK Management Suite
System	1.4	Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.	LANDESK provides a comprehensive asset inventory populated from a variety of tools, including network scanners; passive network discovery; inventory scanners for Mac, Windows, Linux, mobile, and other device types; and SNMP scanning. You can see what assets you have, where they are, how they're being used, and how they're performing in order to make better decisions in any stage of the asset's lifecycle.	LANDESK Asset Intelligence LANDESK Asset Central
System	1.6	Use client certificates to validate and authenticate systems prior to connecting to the private network.	LANDESK uses a certificate-based authentication model that enables authentication through the software delivery of certificates. However, LANDESK cannot enforce the use of certificates.	LANDESK Management Suite

CSC #2: Inventory of Authorized and Unauthorized Software

Family	Control	Description	Capabilities	Product(s)
System	2.1	Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.	Automatic discovery in LANDESK leverages file execution, the MSI database and additional techniques to identify software assets. In addition to a comprehensive list of all software assets on every device, automatic discovery provides extensive usage information about those assets.	LANDESK Management Suite LANDESK Security Suite
System	2.2	Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow.	In addition to traditional whitelisting and support for digital signatures, AppSense's Trusted Ownership only allows the execution of applications introduced by trusted administrators to reduce the administrative overhead associated with traditional whitelisting. LANDESK's whitelisting can block or allow applications based on sources of trust including reputation, file attributes, locations, etc.	AppSense Application Manager LANDESK Security Suite
System	2.3	Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops. The software inventory system should track the version of the underlying operating system as well as the applications installed on it. The software inventory systems must be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.	LANDESK automatically identifies all software assets on each device. Usage information is also collected and software is mapped to the hardware assets. In a virtual environment, AppSense can also be used to audit connecting device attributes to ensure per device software license compliance.	LANDESK Management Suite LANDESK Security Suite

CSC #3: Secure Configurations for Hardware and Software

Family	Control	Description	Capabilities	Product(s)
System	3.1	Establish standard secure configurations of your operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.	LANDESK Management Suite facilitates the custom deployment of images while LANDESK Security Suite enables you to audit and implement specific security configurations.	LANDESK Management Suite LANDESK Security Suite
System	3.2	Follow strict configuration management, building a secure image that is used to build all new systems that are deployed in the enterprise. Any existing system that becomes compromised should be re-imaged with the secure build. Regular updates or exceptions to this image should be integrated into the organization's change management processes. Images should be created for workstations, servers, and other system types used by the organization.	LANDESK enables you to create provisioning templates to integrate all of your upgrade processes, including communications with users, moving user profiles, and standardizing Windows and Mac OS images. LANDESK uses hardware-independent imaging to configure machines quickly with the appropriate drivers. With AppSense also included as part of the build, workstation and server images are protected from unauthorized changes to prevent image sprawl.	AppSense Application Manager LANDESK Security Suite
System	3.3	Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible. Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network.	The LANDESK core server uses distribution package hashes to verify distribution packages in scheduled tasks.	LANDESK Management Suite
System	3.4	Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.	LANDESK enables you to remotely control devices from any HTML5 browser with secure, browser-based access.	LANDESK Management Suite

Family	Control	Description	Capabilities	Product(s)
System	3.5	Use file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. The reporting system should: have the ability to account for routine and expected changes; highlight and alert on unusual or unexpected alterations; show the history of configuration changes over time and identify who made the change (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command). These integrity checks should identify suspicious system alterations such as: owner and permissions changes to files or directories; the use of alternate data streams which could be used to hide malicious activities; and the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes).	LANDESK's directory monitoring capabilities enable you to specify folders to be monitored for file addition, deletion and modification. AppSense is able to enforce digital signature checks on executables as they launch if required. By using SHA1, SHA256 or ADLER32 AppSense can ensure that only executables that match can run. When using AppSense for whitelisting, AppSense also monitors any file rename or overwrite in addition to monitoring the ownership properties of a file.	LANDESK Security Suite AppSense Application Manager
System	3.6	Implement and test an automated configuration monitoring system that verifies all remotely testable secure configuration elements, and alerts when unauthorized changes occur. This includes detecting new listening ports, new administrative users, changes to group and local policy objects (where applicable), and new services running on a system. Whenever possible use tools compliant with the Security Content Automation Protocol (SCAP) in order to streamline reporting and integration.	LANDESK uses SCAP content to scan for security threats and policy settings. Includes alerting and inventory of services but doesn't alert for what's new or changes to administrative groups.	LANDESK Security Suite

Family	Control	Description	Capabilities	Product(s)
System	3.7	Deploy system configuration management tools, such as Active Directory Group Policy Objects for Microsoft Windows systems or Puppet for UNIX systems that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals. They should be capable of triggering redeployment of configuration settings on a scheduled, manual, or event-driven basis.	AppSense enables you to set up a corporate desktop environment and specify what users have access to, how they access it and what they can do with it. Policy settings are decoupled from the corporate desktop and managed independently, increasing your ability to deliver efficient service to the business, minimize desktop management costs and ensure users remain compliant with policies. LANDESK enables you to bundle multiple applications and deploy them anywhere by targeting users and distributing software to their devices. A built-in Gantt chart allows you to monitor progress and provide automated updates to stakeholders.	AppSense Environment Manager LANDESK Management Suite

CSC #4: Continuous Vulnerability Assessment and Remediation

Family	Control	Description	Capabilities	Product(s)
System	4.1	Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).	LANDESK scans for vulnerabilities that it can remediate with a patch. As this is not a comprehensive scan, LANDESK looks at a subset of the total pool of potential vulnerabilities.	LANDESK Security Suite Shavlik Protect & Patch
System	4.2	Correlate event logs with information from vulnerability scans to fulfill two goals. First, personnel should verify that the activity of the regular vulnerability scanning tools is itself logged. Second, personnel should be able to correlate attack detection events with prior vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable.	LANDESK scans for vulnerabilities that it can remediate with a patch and correlates its actions with vulnerability scanner output. Scan events are logged and can be audited. Vulnerability data is stored based on a first detection.	LANDESK Security Suite LANDESK AV Shavlik Protect & Patch
System	4.3	Perform vulnerability scanning in authenticated mode either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested. Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses. Ensure that only authorized employees have access to the vulnerability management user interface and that roles are applied to each user.	LANDESK scans for vulnerabilities that it can remediate with a patch in authenticated mode with agents running locally. You can use a dedicated account. Role-based access controls ensure that only authorized employees have access.	LANDESK Security Suite Shavlik Protect & Patch

Family	Control	Description	Capabilities	Product(s)
System	4.4	Subscribe to vulnerability intelligence services in order to stay aware of emerging exposures, and use the information gained from this subscription to update the organization's vulnerability scanning activities on at least a monthly basis. Alternatively, ensure that the vulnerability scanning tools you use are regularly updated with all relevant important security vulnerabilities.	LANDESK provides intelligence around the vulnerabilities it scans and the quality of patching packages, as well as application reputation.	LANDESK Security Suite Shavlik Protect & Patch
System	4.5	Deploy automated patch management tools and software update tools for operating system and software/ applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.	Shavlik delivers the latest software updates for third-party apps, including Windows, Mac and VMware. It also performs hypervisor, offline virtual machine and virtual template patching. Shavlik offers several options to deliver software updates and ensure patch compliance, whether a system is on the network or air gapped: agentless, agent-based or cloud-based. LANDESK easily and automatically assesses state and applies patches across the enterprise, allowing you to establish policies for when devices are patched leveraging distribution technologies to reduce the impact on the network and disruption to the user. Rollout automation allows for an automated process from definition download through pilot and production rollout phases.	LANDESK Security Suite Shavlik Protect & Patch
System	4.7	Compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk. Such acceptance of business risks for existing vulnerabilities should be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed, increasing the risk.	LANDESK and Shavlik can track and show the history of scans, including supersedence. However, this control is best addressed with a true vulnerability scanner.	LANDESK Security Suite Shavlik Protect & Patch

Family	Control	Description	Capabilities	Product(s)
System	4.8	Establish a process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets (example, DMZ servers, internal network servers, desktops, laptops). Apply patches for the riskiest vulnerabilities first. A phased rollout can be used to minimize the impact to the organization. Establish expected patching timelines based on the risk rating level.	LANDESK uses multiple technologies to distribute patches quickly across the network. Integrated project rollout features can deploy patches at scale and at speed while optimizing bandwidth utilization and hardware resources. Risk rating is based on the vendor patch. Devices can be patched in and out of network.	LANDESK Security Suite Shavlik Protect & Patch

CSC #5: Controlled Use of Administrative Privileges

Family	Control	Description	Capabilities	Product(s)
System	5.1	Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.	AppSense dynamically controls end-user privileges to provide users with only the administrative privileges they need. AppSense manages privileges at the application or individual task level instead of the session or account level. Privileges can be eliminated, elevated or lowered on a per user, application or task basis. Local admin accounts can be removed yet users can still access select applications or tasks that require admin rights. The system captures detailed logging information about ongoing changes to central application control and privilege management policies. Additionally, change logs are password protected to prevent tampering.	AppSense Application Manager
System	5.2	Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive.	AppSense reports on tasks and applications that require administrative rights.	AppSense Application Manager AppSense Insight
System	5.3	Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.	LANDESK can change passwords for default accounts on operating systems. AppSense can verify that default passwords have been changed.	LANDESK Management Suite AppSense Insight
System	5.4	Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system.	LANDESK can be configured to alert on event log information.	LANDESK Security Suite
System	5.5	Configure systems to issue a log entry and alert on any unsuccessful login to an administrative account.	LANDESK can be configured to issue a log entry but cannot alert.	LANDESK Management Suite

Family	Control	Description	Capabilities	Product(s)
System	5.6	Use multifactor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards, certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods.	Multifactor authentication is supported internally to LANDESK, but not to the rest of the environment. You can authenticate remote control and console login, which is tied to the OS login. Remote control supports smart cards.	LANDESK Management Suite
System	5.7	Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).	Strong passwords for local accounts are supported through the LANDESK systems. AppSense can push this policy to desktops.	LANDESK Security Suite AppSense Environment Manager
System	5.8	Administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems.	AppSense allows administrators to transition to administrator privileges using Sudo.	AppSense Insight AppSense Application Manager
System	5.9	Administrators shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.	This control is addressed largely through process. Registry settings, which can be pushed out via Group Policy Objects, can prevent the machine from being used to read email, compose documents or surf the Internet. AppSense can lock down the machine and ease configuration and replacement.	LANDESK Management Suite AppSense Environment Manager AppSense Application Manager

CSC #7: Email and Web Browser Protections

Family	Control	Description	Capabilities	Product(s)
System	7.1	Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers provided by the vendor in order to take advantage of the latest security functions and fixes.	LANDESK and AppSense can whitelist web browsers and email clients that are allowed to execute. LANDESK also handles version management of browsers and ensures that patches are up to date.	LANDESK Security Suite AppSense Application Manager
System	7.2	Uninstall or disable any unnecessary or unauthorized browser or email client plugins or add-on applications. Each plugin shall utilize application / URL whitelisting and only allow the use of the application for pre-approved domains.	AppSense can block a DLL file and therefore prevent a plugin from loading.	AppSense Application Manager
System	7.3	Limit the use of unnecessary scripting languages in all web browsers and email clients. This includes the use of languages such as ActiveX and JavaScript on systems where it is unnecessary to support such capabilities.	LANDESK allows you to configure settings to prevent scripts from running when unnecessary. AppSense allows you to push this setting to desktops. AppSense whitelisting can also be used to limit certain types of hosts.	LANDESK Management Suite LANDESK Security Suite AppSense Environment Manager
System	7.5	Deploy two separate browser configurations to each system. One configuration should disable the use of all plugins, unnecessary scripting languages, and generally be configured with limited functionality and be used for general web browsing. The other configuration shall allow for more browser functionality but should only be used to access specific websites that require the use of such functionality.	LANDESK enables you to deploy sandbox browsers through which virtual apps and sandbox browsers are available. Together, AppSense Application Manager and Environment Manager allow you to deploy two separate browser configurations to each system.	LANDESK Management Suite AppSense Application Manager AppSense Environment Manager
System	7.6	The organization shall maintain and enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. The organization shall subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.	AppSense uses whitelisting to enable access to approved websites. This level of control can be applied based on various contextual rules like location, IP address and connecting device properties allowing URL restrictions to be applied when required.	AppSense Application Manager

CSC #8: Malware Defenses

Family	Control	Description	Capabilities	Product(s)
System	8.1	Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers.	LANDESK can perform anti-virus, firewall, host-based IPS and alerting for desktops, and host-based IPS for servers.	LANDESK Security Suite LANDESK AV
System	8.2	Employ anti-malware software that offers a centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines. After applying an update, automated systems should verify that each system has received its signature update.	LANDESK can perform anti-virus for desktops. LANDESK can manage other vendors' anti-virus updates as well.	LANDESK Security Suite LANDESK AV
System	8.3	Limit use of external devices to those with an approved, documented business need. Monitor for use and attempted use of external devices. Configure laptops, workstations, and servers so that they will not auto-run content from removable media, like USB tokens (i.e., "thumb drives"), USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares. Configure systems so that they automatically conduct an anti-malware scan of removable media when inserted.	LANDESK provides device control. Device control enables blocking, authorized device usage and/or monitored usage.	LANDESK Security Suite LANDESK AV

CSC #9: Limitation and Control of Network Ports

Family	Control	Description	Capabilities	Product(s)
System	9.1	Ensure that only ports, protocols, and services with validated business needs are running on each system.	LANDESK can validate within the client-based firewall. AppSense Application Manager can also support per user, application-level firewalling based on port restrictions, IP address and host names. AppSense Environment Manager can update the local security policies on machines based on a contextual rule set.	LANDESK Security Suite AppSense Application Manager AppSense Environment Manager
System	9.2	Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	LANDESK's client-based firewall can be configured to drop traffic except those services and ports that are allowed. AppSense Environment Manager can ensure the firewall is enabled and configured. Application Manager can provide an extra level of firewall-like control.	LANDESK Security Suite AppSense Application Manager AppSense Environment Manager

CSC #11: Secure Configurations for Network Devices

Family	Control	Description	Capabilities	Product(s)
Network	11.6	Network engineers shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.	LANDESK or AppSense can lock down the machine to prevent engineers from accessing email, composing documents or surfing the Internet. However, the use of that machine is a process.	LANDESK Management Suite AppSense Application Manager AppSense Environment Manager

CSC #12: Boundary Defense

Family	Control	Description	Capabilities	Product(s)
Network	12.1	Deny communications with (or limit data flow to) known malicious IP addresses (black lists), or limit access only to trusted sites (whitelists). Tests can be periodically carried out by sending packets from bogon source IP addresses (non-routable or otherwise unused IP addresses) into the network to verify that they are not transmitted through network perimeters. Lists of bogon addresses are publicly available on the Internet from various sources, and indicate a series of IP addresses that should not be used for legitimate traffic traversing the Internet.	AppSense Application Manager can provide the application-level firewall, and Environment Manager can configure the Windows firewall. Neither product can do testing.	AppSense Application Manager AppSense Environment Manager

CSC #13: Data Protection

Family	Control	Description	Capabilities	Product(s)
Network	13.2	Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data.	LANDESK can encrypt hard drives and configure settings on devices where supported in MDM. Desktop encryption is achieved through integrated WinMagic solution.	LANDESK Management Suite WinMagic
Network	13.5	If there is no business need for supporting such devices, configure systems so that they will not write data to USB tokens or USB hard drives. If such devices are required, enterprise software should be used that can configure systems to allow only specific USB devices (based on serial number or other unique property) to be accessed, and that can automatically encrypt all data placed on such devices. An inventory of all authorized devices must be maintained.	LANDESK device control allows for full blocking or authorized device usage, including requiring the device to be encrypted. AppSense can push this policy to desktops.	WinMagic LANDESK Security Suite AppSense Environment Manager
Network	13.8	Block access to known file transfer and email exfiltration websites.	On a desktop level, AppSense can block access to known file transfer and email exfiltration websites, even when they leave the corporate network/firewall.	AppSense Application Manager

CSC #14: Controlled Access Based on the Need to Know

Family	Control	Description	Capabilities	Product(s)
Application	14.5	Sensitive information stored on systems shall be encrypted at rest and require a secondary authentication mechanism, not integrated into the operating system, in order to access the information.	WinMagic incorporates Trusted Platform Module, a feature of Wintel CPUs that allows encryption to be performed at the hardware level rather than only the OS.	WinMagic
Application	14.7	Archived data sets or systems not regularly accessed by the organization shall be removed from the organization's network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.	LANDESK collects access data by system, allowing you to determine whether a system is used or orphaned.	LANDESK Management Suite

CSC #15: Wireless Access Control

Family	Control	Description	Capabilities	Product(s)
Network	15.3	Use wireless intrusion detection systems (WIDS) to identify rogue wireless devices and detect attack attempts and successful compromises. In addition to WIDS, all wireless traffic should be monitored by WIDS as traffic passes into the wired network.	LANDESK performs wireless access point discovery.	LANDESK Management Suite LANDESK Security Suite
Network	15.4	Where a specific business need for wireless access has been identified, configure wireless access on client machines to allow access only to authorized wireless networks. For devices that do not have an essential wireless business purpose, disable wireless access in the hardware configuration (basic input/output system or extensible firmware interface).	LANDESK can support this process and ensure that configurations stay compliant.	LANDESK Management Suite
Network	15.7	Disable peer-to-peer wireless network capabilities on wireless clients.	LANDESK can define this policy as part of the provisioning process and ensure that configurations remain compliant. AppSense can push this policy.	LANDESK Management Suite AppSense Environment Manager
Network	15.8	Disable wireless peripheral access of devices (such as Bluetooth), unless such access is required for a documented business need.	LANDESK can define this policy as part of the provisioning process and ensure that configurations remain compliant. AppSense can push this policy.	LANDESK Security Suite

CSC #16: Account Monitoring and Control

Family	Control	Description	Capabilities	Product(s)
Application	16.3	Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor. Disabling instead of deleting accounts allows preservation of audit trails.	This is a process, but LANDESK can track the change to ensure it is done.	LANDESK Service Desk
Application	16.4	Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.	LANDESK can monitor accounts and log off users through client configuration and provisioning. AppSense also monitors accounts and logs off users after a period of inactivity.	LANDESK Management Suite AppSense Environment Manager
Application	16.5	Configure screen locks on systems to limit access to unattended workstations.	LANDESK can limit access to unattended workstations through client configuration and provisioning. AppSense allows you to configure screen locks to limit access to unattended workstations.	LANDESK Management Suite AppSense Environment Manager
Application	16.6	Monitor account usage to determine dormant accounts, notifying the user or user's manager. Disable such accounts if not needed, or document and monitor exceptions (e.g., vendor maintenance accounts needed for system recovery or continuity operations). Require that managers match active employees and contractors with each account belonging to their managed staff. Security or system administrators should then disable accounts that are not assigned to valid workforce members.	LANDESK facilitates the process of disabling accounts and the change activity associated with this control.	LANDESK Service Desk
Application	16.7	Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time.	Policy can be enforced by AppSense Environment Manager if contextual conditions are required and also enabled by LANDESK Security Suite.	LANDESK Security Suite AppSense Environment Manager
Application	16.10	Profile each user's typical account usage by determining normal time-of-day access and access duration. Reports should be generated that indicate users who have logged in during unusual hours or have exceeded their normal login duration. This includes flagging the use of the user's credentials from a computer other than computers on which the user generally works.	AppSense can provide a custom report.	AppSense Insight

CSC #18: Application Software Security

Family	Control	Description	Capabilities	Product(s)
Application	18.1	For all acquired application software, check that the version you are using is still supported by the vendor. If not, update to the most current version and install all relevant patches and vendor security recommendations.	Shavlik tracks end of life for a large library of software titles. AppSense can block applications based on version and other metadata.	Shavlik Protect & Patch AppSense Application Manager
Application	18.5	Do not display system error messages to end-users (output sanitization).	LANDESK sanitizes error output for its own software.	LANDESK Management Suite LANDESK Security Suite
Application	18.6	Maintain separate environments for production and nonproduction systems. Developers should not typically have unmonitored access to production environments.	You can support different environments within our products, and we are compliant within LANDESK and AppSense's own environments; however, we do not offer a product to enforce this control in your environment.	LANDESK Management Suite LANDESK Security Suite

CSC #19: Incident Response and Management

Family	Control	Description	Capabilities	Product(s)
Application	19.1	Ensure that there are written incident response procedures that include a definition of personnel roles for handling incidents. The procedures should define the phases of incident handling.	This control can be addressed via the Service Desk incident management process.	LANDESK Service Desk
Application	19.2	Assign job titles and duties for handling computer and network incidents to specific individuals.	This control can be addressed via Service Desk incident management and knowledge base articles.	LANDESK Service Desk
Application	19.3	Define management personnel who will support the incident handling process by acting in key decision-making roles.	You can make these definitions in the workflow process in Service Desk's incident management.	LANDESK Service Desk
Application	19.4	Devise organization-wide standards for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification. This reporting should also include notifying the appropriate Community Emergency Response Team in accordance with all legal or regulatory requirements for involving that organization in computer incidents.	This control can be addressed through SLA management as part of Service Desk's incident and problem management.	LANDESK Service Desk
Application	19.5	Assemble and maintain information on third-party contact information to be used to report a security incident (e.g., maintain an e-mail address of security@ organization.com or have a web page http://organization.com/security).	This control can be addressed with incident and asset management within Service Desk.	LANDESK Service Desk
Application	19.6	Publish information for all personnel, including employees and contractors, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities.	This information can be provided via the Service Desk Knowledge Base and notifications.	LANDESK Service Desk
Application	19.7	Conduct periodic incident scenario sessions for personnel associated with the incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the incident handling team.	The Service Desk incident management system supports periodic testing, but it's up to you to implement the process.	LANDESK Service Desk


ivanti