

LANDesk® Security Suite 8.7



Reviewer's Guide



This document contains confidential and proprietary information of LANDesk Software, Inc. ("LANDesk") and its affiliates and is provided in connection with the identified LANDesk® product(s). No part of this document may be disclosed or copied without the prior written consent of LANDesk. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. LANDesk products are not intended for use in medical, life saving, or life sustaining applications. LANDesk does not warrant that this material is error-free, and LANDesk reserves the right to update, correct, or modify this material, including any specifications and product descriptions, at any time, without notice.

Copyright © 2006, LANDesk Software, Inc. All rights reserved.

LANDesk, Targeted Multitask and Peer Download are trademarks or registered trademarks of LANDesk Software, Inc. and its affiliated companies in the United States and other countries. Other brands and names may be claimed as the property of others.

LSI-0523

0606/JBB/NH

About LANDesk Security Suite 8.7

LANDesk® Security Suite 8.7 combines system security with active vulnerability management and remediation, enabling secure configuration and access control at the endpoint at a lower cost. It simplifies and automates patch management, spyware and application blocking, antivirus and personal firewall policy enforcement, as well as the ability to limit network, volume, port and wireless communications access to each endpoint. It mitigates risk through compliance management and the rigorous enforcement of security policies for all endpoint devices.

Coinciding with the release of LANDesk Security Suite 8.7 is the release of the new LANDesk® Antivirus solution, which can be purchased as an add-on to LANDesk Security Suite or LANDesk® Management Suite. While the previous version of LANDesk Security Suite provided AV administration of third-party products, LANDesk Security Suite 8.7 with the LANDesk Antivirus add-on offers layered, enterprise-ready antivirus and rootkit detection from a single console for multiple points of protection on the desktop. This integrated antivirus console saves IT administrators time and money by reducing the need to manage separate products and consoles and by eliminating multiple agents on the client and the accompanying training involved. Fully integrated with the security and patch tools of LANDesk Security Suite, LANDesk Antivirus equips enterprises with the capability to quickly assess and mitigate virus risks on managed company resources.

LANDesk Security Suite leverages a centralized database to help organizations combat emerging threats and improve vulnerability management through comprehensive assessment scanning, detailed threat analysis and automated remediation. It simplifies and automates patch management, spyware and application blocking, antivirus and personal firewall policy enforcement, as well as the ability to limit network, volume, port and wireless communications access to each endpoint. It mitigates risk through compliance management and the rigorous enforcement of security policies for all endpoint devices.

Available both as a standalone endpoint security solution and as an extension to LANDesk® Management Suite, LANDesk® Security Suite delivers:

- **Cost savings** from the integration and unification of systems security and configuration management.
- **Increased efficiency** with vulnerability management for comprehensive and customizable assessment scanning, reduced vulnerability research time and automated remediation.
- **Mitigated risk** through compliance management and rigorous enforcement of security policies down to the endpoint.

Securing the Endpoints

With the ever-growing concerns surrounding the protection of enterprise computing assets, the typical IT operations manager or IT administrator is being tasked more and more with responsibilities to manage the security within their environment.

On top of having to worry about their traditional IT management stewardships, they now face an array of new challenges that include:

- **Keeping endpoints secure** – Enforcing security configuration settings and security policies consumes a lot of valuable resources.
- **Enforcing compliance** – While corporate mandates and best practices insist on end-node security policies, the inability to actually enforce those policies can expose the organization to security risks and regulatory non-compliance.
- **Dealing with infected machines** – Contamination from infected machines connecting to the corporate network causes significant network downtime and productivity loss.
- **Limited visibility** – A clearer perspective is needed concerning where the organization is vulnerable to attack.
- **Surviving ‘Super Tuesday’** – When the onslaught of new patches and updates arrive on the second Tuesday of every month, unless the organization has the ability to automatically discover, download, test and apply them all corporate-wide, the process becomes not only resource intensive and slow, but leaves the organization vulnerable to attack until each patch and update is successfully deployed.
- **Preventing the proliferation of malicious code** – The inability to keep spyware, adware, and viruses off endpoint devices causes downtime and increases help desk calls.
- **Stopping information leakage** – Poorly configured systems and slack access controls can cost an organization in terms of intellectual property loss, privacy breach, and unwanted publicity.
- **Relying on “Yet Another Console”** – As organizations invest in additional technologies to combat security issues, the complexity and difficulty of administering all of their different systems and security issues increases significantly if they are not unified under a single, centralized management console.

The time lag between patch releases and the exploitation of endpoint vulnerabilities continues to compress. In 2003, the Blaster virus struck 28 days after the vulnerability it exploited was first discovered. But in late 2005, both the Msddds.dll and WMF vulnerability attacked before patches were available. According to the Carnegie Mellon Software Engineering Institute's CERT Coordination Center, there were 3,780 vulnerabilities identified in 2004. At the end of 2005 the figure had climbed to 5,990. Through the first quarter of 2006, an additional 1,597 vulnerabilities had been identified.

Because of the zero-day exploit reality, patching, while integral, is no longer sufficient protection, and pattern files alone are too reactionary. An integrated, layered desktop security solution is vital.

LANDesk® Security Suite enables small to medium-size organizations as well as larger enterprises to take active control of configuration security, control device access and establish automated policies to maintain a secure computing environment. Organizations can:

- Scan for patch needs, malware threats and security configuration vulnerabilities
- Research, prioritize, download and distribute patches
- Remove spyware, adware, key-loggers and other malware
- Deny launch of unauthorized or prohibited applications
- Develop policies to automatically maintain security rules for each device
- Restrict network access and use of communications ports
- Protect systems and critical data with active control over communication, data port and media drive access and the ability to quarantine devices

From a single integrated console, LANDesk Security Suite provides organizations the benefits of centrally managed and automated:

- Inventory and Configuration
- Audit and Compliance Enforcement
- Malicious Software Protection
- Patch Management
- Network Access Control

Inventory and Configuration

A network is only as safe as its weakest device. Before any device can be secured, it must first be found and identified. Any device that cannot be seen or discovered cannot be secured, thereby creating a significant weak spot in the enterprise's protective armor. Before these weak spots can be eliminated, IT administrators need to know all they can about every device connected to their network.

The first step toward comprehensive endpoint security is to be able to gather from every endpoint device relevant security information that includes configuration settings, antivirus status, OS patch levels, firewall status, installed software, attached hardware, and any known vulnerabilities.

LANDesk® Security Suite utilizes IP FingerPrinting technology to perform Unmanaged Device Discovery. This technology enables the discovering of any device with an IP address on the target network, including computers, printers and network infrastructure devices. The automated asset discovery and inventory scanning capabilities provided by LANDesk Security Suite help organizations keep data current and ensure that all their computers are in line with established security standards.

Unmanaged Device Discovery

Unmanaged Device Discovery (UDD) technology in LANDesk® Security Suite finds clients on the network that have not yet submitted an inventory scan to the LANDesk® core database. UDD finds these unmanaged devices in a variety of different ways, including the following:

- **Standardized LANDesk® Agent** – Under this method, UDD discovers computers by looking for a standard LANDesk® agent from LANDesk® Management Suite, LANDesk® Inventory Manager, LANDesk Security Suite, or LANDesk® System Manager that already resides on the system.
- **Network Scan** – By doing an ICMP ping sweep, LANDesk Security Suite can perform a thorough search to discover any IP connected device within the network. Since this conducts an exhaustive search, this method can take a considerable amount of time. However, to reduce the scan time, administrators can limit the search to certain IP and subnet ranges. By default this option will use NetBIOS to gather information about the device. It also provides an IP FingerPrint option that instructs UDD to try to discover the OS type of each discovered device by analyzing its TCP packet responses.
- **Extended Device Discovery (XDD)** – LANDesk's new XDD capability provides a scalable discovery process for real-time subnet-level discovery tracking of unmanaged, networked devices, even if those devices have a firewall enabled. Briefly, here's how the XDD process works:
 - Agent is deployed to the client device
 - The client device becomes a listener and listens for ARP requests on the subnet
 - When it hears ARP requests, it verifies them against a table
 - If the Mac and IP address are not in the table, it performs a CBA ping
 - If successful, it adds the information to the table
 - If failure occurs, it reports back to the core that it discovered a node on its subnet that is not managed

- **NT domain** – IT administrators can configure LANDesk Security Suite to look for clients in a specified NT domain. This method discovers members whether the client computer is on or off.
- **LDAP** – LDAP scans discover clients located in specified LDAP directories. This method discovers members whether the client computer is on or off.
- **IPMI** – Discovers devices enabled with the Intelligent Platform Management Interface (IPMI). IPMI provides access to many device management capabilities; even if the device is turned off or it's OS is in a non-responsive state.
- **AMT** – Discovers devices enabled with Intel Active Management Technology ("AMT"). Intel AMT enabled machines have an embedded management engine that allows it to communicate independent of the state of the operating system or the machine's hardware.

LANDesk Security Suite allows IT managers to schedule automated UDD scans on a periodic basis at anytime of day or night. When UDD finds an unmanaged device for the first time, it tries to identify the device type to allow it to add the device to one of the following four categories in the unmanaged device list:

- Computers
- Printers
- Infrastructure (Contains routers and other network hardware)
- Other

IT administrators also have the ability to create their own groups to further categorize unmanaged devices. UDD tries to discover basic information about each device and displays the information in columns in the LANDesk Security Suite device list. By simply clicking a column heading, devices can be sorted by attribute. To find an individual unmanaged device, administrators have the option of scrolling through the list or using the Find bar in the UDD window.

The UDD technology in LANDesk Security Suite enables organizations to quickly identify unmanaged computers to facilitate the fast deployment of management software to the device. With the management software deployed, IT Managers can take immediate control of the device's configuration security, as well as the security configuration of all other discovered computers on the network, thereby significantly limiting the introduction of security threats onto the network.

Inventory Querying and Reporting

The foundation of IT security management begins with an organization's exact knowledge of what IT assets it has, being able to extract relevant data about specific assets, and use that data to plan IT tasks and report status. LANDesk® Security Suite features a powerful inventory scanner that catalogs detailed information about hardware, software, drivers, patches and more. The first time an inventory scan is run on a client it performs a full scan that catalogs all hardware and software assets on that machine. To safeguard gathered information during the scanning process, by default TCP/IP based scans will run in encrypted mode.

To reduce total bandwidth usage, the inventory scanner uses both scan file compression and delta scanning that only sends changes made since the last scan was completed. This results in intelligent use of bandwidth and resources, maximizing performance while minimizing costs and network impact. Inventory data can be viewed, printed, exported, used to define queries, group servers, and generate custom reports. The cataloged inventory data facilitates organizations' ability to manage, configure, safeguard, and maintain their devices, as well as assist them in quickly identifying potential security problems.

LANDesk Security Suite features powerful querying and reporting tools to help turn simple data into business intelligence that empowers organizations to manage systems more efficiently and effectively.

Key LANDesk Security Suite query and reporting features include:

- Detailed hardware and software inventory with SMBIOS 2.1 support for comprehensive information gathering, including expanded slot descriptions, memory configuration and network adaptor configuration.
- Extensive querying to enable administrators to focus information-gathering efforts on only those hardware or software elements that will provide the data they need.
- Report publishing features make it easy to save reports in a secure location and make report data available to any users, whether they can access LANDesk Security Suite or not. Reports can be published in HTML, PDF, XLS, DOC and RTF formats for easy portability and analysis.
- Reporting dashboard in the Web console provides thumbnail views for up to four different reports for instant access to inventory and status information to enable easy comparisons of generated data.

Queries

The queries in LANDesk® Security Suite provide the ability to search for and organize information stored in the core database about an organization's managed devices. Queries are essentially customized searches of the core database. For example, a query can be created that searches for a specific device configuration or condition. Queries are created by simply using one or more query statements that represent the desired conditions and then by relating those statements to each other by using standard logical operators.

In addition to being able to create queries for device information stored in the core database, it also has the ability to create LDAP queries for server information located in other directories. All query results can be used to create custom device groups, select targets for vulnerability remediation activities, and more.

Reporting

LANDesk® Security Suite includes a powerful reporting tool that enables organizations to select and run a wide variety of reports that provide critical information about the managed endpoints on their network. It uses an inventory scanning utility to add devices (and collected hardware and software data about those devices) to the LANDesk Security Suite core database. The reporting tool collects and organizes the gathered data, presenting it in valuable report formats.

IT managers have the option to use predefined management inventory and vulnerability detection reports, or they can create their own reports with the LANDesk® Security Suite Report Designer. The Report Designer gives organizations the flexibility they need to create and generate the reports that address their unique security concerns. It gives them full control over leveraging their management data as they see fit. With a simple right-click, any view on the console can quickly be turned into a report. Any query can also be turned into a report. Organizations even have the ability to have their company logo appear on the report.

The reporting tool also gives IT managers a variety of options in regards to how reports are presented, including scope filtered e-mail reports. For example, an organization-wide recurring spyware report can be generated and e-mailed to managers in different regions, but the managers will only receive information for the machines in their specific region. This scope based option enables IT managers to create one report, while allowing individual recipients to only see the report information specific to their roles and responsibilities.

Change Alerting

To manage and respond to vulnerability conditions and other events on the network, organizations can leverage the scan and alert capabilities in LANDesk® Security Suite to initiate the appropriate actions when certain events occur. Alerts can be generated to inform administrators when device configuration changes occur, security fixes become available, spyware downloads have been detected and blocked, outdated antivirus pattern files have been discovered and updated, unauthorized device or network connections have been attempted and stopped, or any number of security related events take place. Alerts can be configured so that specific individuals can be notified when certain security events occur on managed devices or if a device simply does not comply with corporate security policies.

LANDesk Security Suite can also send out alerts when the latest vulnerability definitions have been downloaded. It provides real-time alerting of the latest known security outbreaks. This allows IT administrators to immediately know about the latest security information published by LANDesk without having to open the LANDesk Security Suite Console.

LANDesk Security Suite gives organizations granular control over what events and vulnerabilities they should be alerted to. It gives them the flexibility to manage vulnerability alerting so they're not inundated with non-critical events, while empowering them to stay on top of and alerted to security policy infringements in a manner that is effective, efficient, and makes sense to their organizational needs.

Events that Generate Alerts

LANDesk® Security Suite can scan and alert on more than 4,000 defined vulnerability definitions in the following major security categories:

- Device inventory
- Device security configuration
- Application monitoring and blocking
- Spyware blocking and detection
- Antivirus status and enforcement
- Personal firewall management
- Patch management and remediation
- Network and device access control
- LANDesk® Trusted Access™ quarantines

IT managers can also create their own vulnerability definitions to alert on.

Alerts can be generated from any device event that can be scanned. These alerts can be configured to send e-mails or pager messages to specific individuals. They can generate an action such as loading an application, rebooting a device, shutting down a device, or sending an SNMP trap to an SNMP management console. Alerts can also display in the console, Dashboard list views, and log entries.

Since a wide variety of events or problems can generate an alert, some events might need immediate attention, while others might not necessarily be a problem, but just something that administrators need to be aware of to better manage the security of their enterprise.

Alert Actions and Severity

More than one action can be defined for an alert condition, such as sending an email message containing details on the alert, while at the same time initiating a remediation action on the device that generated the alert. Administrator defined thresholds can be used to determine the severity of alert notifications in the Console view and Dashboard of LANDesk® Security Suite.

LANDesk Security Suite uses alert severities to determine the current security status of the device, and to determine which alert actions (if any) to trigger. This gives administrators the power and flexibility to have a variety of alert actions execute based on the severity of the alert.

Possible severity and vulnerability levels include the following:

- Service Pack
- Critical
- High
- Medium
- Low
- Not Applicable
- Unknown

Alerts enable administrators to stay informed on the security status of devices and facilitate the overall response to and security management of specific events. They also allow key remediation tasks to automatically execute to detect or eliminate potential vulnerabilities.

Audit and Compliance Enforcement

Users in many organizations have the attitude that they should be able to configure their computers any way that they want and install whatever software they want, not realizing the impact that this behavior can have on the health of the enterprise network as a whole. Organizations need to be able to control machine configurations and keep them in a consistent state that complies with corporate security policies.

LANDesk® Security Suite gives organizations the ability to audit the computers in their network to verify compliance with flexible, pre-defined configuration policies. Not only does the solution alert IT personnel to non-compliant machines, but it also provides the option to have LANDesk Security Suite automatically enforce compliance by making the necessary configuration changes to the machines in question. For example, if a particular machine has antivirus pattern files that are not current with security policy, LANDesk Security Suite can force a pattern file update to bring the machine into compliance.

Security Configuration Audit

Attempts to share data or use certain applications are just a few ways that security holes open up when users stray from the computer configuration standards set by corporate security policies. The configuration threat analyzer in LANDesk® Security Suite can detect and remediate risky or unsafe configuration settings on an organization's networked computers. Examples of some the configuration security issues that it identifies include:

- Administrator group membership
- Available shares
- Unnecessary services
- File system type
- Guest account status
- Internet Connection Firewall status
- Local account password strength
- Local account password expiration
- Restrict anonymous users
- SQL Guest and Service Account Status
- Internet Explorer security settings

IT managers also have the ability to create their own threat definitions, as well as use VBScripts to identify and remediate those custom security configuration issues.

In addition to being able to audit and enforce compliance with system security configuration settings, LANDesk® Security Suite conducts comprehensive audits on endpoint devices for a wide variety of other potential vulnerabilities and security risks. When these vulnerabilities are discovered, the suite utilizes a variety of its different remediation and enforcement capabilities to eliminate the vulnerability and associated risk. These additional risk conditions that LANDesk Security Suite checks for and remediates include:

- Antivirus status
- OS security patch status
- Personal firewall status and configuration
- Unauthorized software
- Unauthorized hardware
- Industry known vulnerabilities
- Device overall health levels

Additionally, devices that attempt to connect to the network and that don't measure up to approved status levels for the above categories will be blocked from establishing a connection. This "connection control" and LANDesk® Trusted Access™ capability will be discussed in greater detail in the Network Access Control section.

LANDesk® Security Suite gives organizations the ability to scan endpoint devices for vulnerabilities and non-compliance at frequent intervals. With a simple right click in the console it also allows IT managers to initiate immediate scans on specific devices for compliance with specific policies. The active security policy monitoring in LANDesk Security Suite ensures ongoing compliance to security policy and provides precise knowledge for implementing improvement processes on a continuous basis.

Application Monitoring and Blocking

There are many applications that perform legitimate functions, but introduce unwanted network traffic or open up individual computers to exploit from outside the network. Products such as file sharing applications are not directly classified as malware, but can open these kinds of security holes. Similarly, many Instant Messaging packages allow file transfers that could enable risky or infected files to enter the environment, or could facilitate data theft or the transfer of sensitive files off-site. There are also applications that exist solely to create or exploit security holes and are often run unknowingly by users.

The central threats database in LANDesk® Security Suite maintains information on these known risky applications that can compromise security or flood networks with unwanted traffic. IT managers can stop the launch of these applications on their endpoint devices by simply adding those applications to their LANDesk Security Suite scan list. Following the next scan, any attempt to launch one of those applications by a managed endpoint device will automatically be denied. If desired, a notice can pop-up on users' endpoint devices informing them that they have attempted to launch an application that has been denied or blocked.

If users attempt to thwart application blocking by changing the name of a blocked application, LANDesk Security Suite will still recognize that application as a security threat and block it. In addition to the predefined list of thousands of risky or unwanted applications, organizations have the flexibility to extend security control even further. IT managers have the option to create their own definitions of applications that they want blocked.

While these defined applications represent potential security risks, inhibitors of productivity, or consumers of bandwidth, organizations may decide that they want to allow some of these applications to run in their environment. As with other vulnerability definitions in LANDesk Security Suite, IT managers have the ability to decide which applications they want to scan for and ultimately block. This level of flexibility makes it possible to temporarily block unknown applications and then unblock them at a later point if it's decided that they don't pose an actual threat.

Application blocking takes place on all managed devices, whether or not they are connected to the network. The locally installed LANDesk Security Suite agent maintains the list of banned applications and blocks any attempts to run the unauthorized software whether the device is in a connected or disconnected state.

Malicious Software Protection

Data security is one of the most pressing concerns of today's enterprises. Without question, malicious attacks from infected computers that connect to the network, outright data theft, and data loss from spyware and other malware place critical business data and the enterprise itself at risk. A key element of the preemptive protection capability in LANDesk® Security Suite is its ability to monitor, scan and enforce status levels for antivirus, anti-spyware, and personal firewalls. The solution utilizes frequent scans to detect non-compliance with established policies for these areas and then uses a variety of methods to remediate and enforce compliance.

Real-Time Anti-Spyware Blocking and Detection

Despite organizations' efforts to remove spyware from their endpoint devices, they often find that spyware keeps returning and they have to continually rediscover it and remove it. Not only does LANDesk® Security Suite scan, detect, and remove existing spyware, but it provides real-time protection against attempted spyware infections. Before a spyware or other malware program can even be installed on an endpoint device, LANDesk Security Suite will detect it and block the installation process.

Using threat definitions and remediation scripts from the LANDesk threats database, LANDesk Security Suite can automatically detect and remove threats in real-time from spyware, adware, keyloggers, Trojans and other malware, improving overall performance on the endpoints and protecting the network from unauthorized access or unwanted traffic. The central threats database is continuously updated to give access to the latest information. IT managers can also create their own definitions to effectively distinguish between acceptable applications and use of cookies or other tools, and unacceptable conditions that indicate infestation from spyware or other malware.

Alerts can be configured to notify end users when spyware programs try to install or have been blocked from installing on their endpoint devices. Additionally, LANDesk Security Suite provides detail reports on detected and blocked spyware signature counts to give organizations the ability to verify and visualize spyware trends and repair rates.

One of the most powerful features of spyware blocking and detection in LANDesk Security Suite is that it is not confined to endpoint devices connected to the network. The local LANDesk Security Suite agent will block Spyware and malicious software install attempts on any managed device, whether the device is in a connected or disconnected state.

LANDesk® Management Gateway

The LANDesk® Management Gateway in LANDesk® Security Suite takes the pain out of securely managing computers that reside outside of the corporate network. It enables full endpoint management without requiring direct network access or VPN solutions. It allows remote devices to access security, patch, and configuration management packages and policies from anywhere on the Internet. Virus and vulnerability definitions can be updated even when endpoint devices aren't connected to the corporate network. What's more, LANDesk Security Suite 8.7 increases the connection limit per management gateway to 4,000 simultaneous connections, an increase of 300%.

LANDesk® Antivirus: Enterprise-Ready Virus Protection Added to Single-Console Simplicity

LANDesk® Security Suite 8.7 extends active security management to the endpoint with capabilities that include quarantine, intrusion prevention, active threat analysis, spyware detection and removal, access control, and configuration security tools. By adding on LANDesk® Antivirus to LANDesk Security Suite, organizations broaden and extend security capabilities from a single console. The LANDesk Antivirus solution is fully integrated with the security and patch manager tools in LANDesk Security Suite and includes:

- Antivirus administration and configuration
- Scanning for and removal of malicious code such as viruses and spyware and the detection of rootkits
- Quarantine of malicious files
- Backup of files before cleaning for retrieval if the cleaning process damages the file
- Pattern file updates
- Phased roll-out of pattern file deployment
- Canned and custom reporting via dashboards, alerts and canned reports

Antivirus Administration and Configuration

This feature enables administrators to align antivirus management with other corporate policies by controlling antivirus settings, allowing the flexibility to determine who can deploy to what devices and how they are configured. Capabilities include:

- Enterprise-wide configuration of antivirus agents
- Administrator control over configuration
- Separate role-based administration to limit who can add, delete, or change the configuration of the LANDesk® Antivirus core and client settings
- End-user agent locked down
- Deployment and scheduling of approved antivirus configuration and install
- E-mail scanning
- Scan infectable files only
- Exclude files, directories, or extensions from scan
- Use heuristics to scan suspicious files or possible viruses
- Control access to quarantine/backup
- Schedule client side scans
- Assign to "Pilot Group" for early reception of pattern files
- Schedule or allow client-initiated updates

Scanning for and Removal of Malicious Code

This feature enables enterprises to quickly assess and mitigate virus risks on managed company resources. Capabilities include:

- Real-time protection and scanning
- Scheduled system scans to targeted machines
- Urgent "Red Button" or "Scan Now" capability

- Real-time scanning of Outlook e-mail
- Scanning for suspicious files
- End-user launch of antivirus scan

Quarantine of Malicious Files

Offers a controlled, methodical (or alternatively, rapid) and hands-off solution for detecting, trapping, removing and mitigating the effects of viruses and virus outbreaks on LANDesk protected computer systems:

- Quarantine and encrypt infected or suspicious files that cannot be cleaned
- Automatically scan the quarantined files when new pattern files are released and restore the file if cleaned successfully
- Define quarantine folder size and settings to restore quarantine and backup files
- Password protect and control if the end user can retrieve files from quarantine
- Cleaned files are also backed up in case of corruption by the cleaning process, for later retrieval

Pattern File Updates

Provides administrators control of virus definition files, empowering them to decide what versions are approved and when they are deployed. Capabilities encompass:

- Scheduled automatic updates of virus definition files
- Configure and control settings for updates
- Enabling of end users to download pattern files
- Enabling of end users to launch an antivirus update
- The ability to roll back to previous versions of virus definition files
- Automatic deployment of new virus definition files to pilot group with a configurable delayed deployment to the rest of the network

Phased Roll-out of Pattern File Deployment

The ability of administrators to control virus definition files empowers them to determine what versions are approved and to phase in when they are deployed, as well as to test definitions before deployment. Through this capability administrators can:

- Identify and target early adopters or assign computers to a “pilot group” for antivirus definition testing
- Quickly identify “Pilot” version
- Allow testing of virus definition files before full-scale deployment across the enterprise
- Delay deployments to the rest of the enterprise until a configurable amount of time has passed
- Stop the automatic process and leave systems on proven definitions or back up to a previous set

Alerts, Reports and Executive Dashboard

The LANDesk® Antivirus add-on provides real-time alerting for antivirus actions and status, enabling administrators to quickly address issues when alerted of virus threats, breaches and outbreaks. Antivirus alerts notifying of problems can be sent via e-mail, pager, etc. Administrators can control alert frequency and enjoy granular control over alerts on actions for quarantine, clean, and suspicious content.

The Report capability provides administrators with information about which resources are protected or vulnerable and what viruses are being discovered, cleaned and trapped, allowing decision makers to know where to focus resources.

- Antivirus information and configuration is reported up with inventory for easy creation of custom reports and queries
- Client side notification of virus detection and scanning process
- Allow testing of virus definition files before full-scale deployment across the enterprise
- Identification of computers that are infected, have not run an antivirus scan recently, or have outdated virus definition files
- Reports on antivirus activity and history

The Executive Dashboard quickly identifies virus outbreaks and illustrates virus control over time. Administrators can gauge the percent of computers with real-time antivirus enabled and with up-to-date antivirus definitions. Administrators can quickly and precisely identify and mitigate the risk of virus outbreaks in the enterprise. Example dashboard views include:

- Top five viruses found over the past 10 days or weeks
- Computers infected with viruses over the past 10 days or weeks

Built-In Antivirus Management and Enforcement

As mentioned previously, LANDesk® Antivirus as an add-on solution extends the power of LANDesk® Security Suite and LANDesk® Management Suite to deliver enterprise-ready antivirus and rootkit detection from the same console. Should organizations choose not to purchase the LANDesk Antivirus add-on, LANDesk Security Suite offers built-in antivirus enforcement that lets administrators manage their chosen antivirus solution, such as those listed below:

- McAfee
- Norton
- Sophos
- Symantec
- Trend-Micro

From the LANDesk Security Suite console, IT managers can configure their antivirus programs of choice for the effective monitoring, prevention and eradication of known viruses. It also scans the organization's endpoint devices to make sure that they have the appropriate anti-virus programs installed on their machine, along with all the latest engines, virus definitions and pattern files. If an endpoint device does not have the correct or most up-to-date programs and files installed, LANDesk Security Suite can be configured to automatically download them from the solution vendor's site and install them on the endpoint device.

Personal Firewall Management

In many organizations, little more than 10 percent of users turn on or properly use the personal firewalls on their machines, creating a significant hole in their device defenses. To stop intruders from gaining access to individual endpoints, LANDesk® Security Suite makes it easy to centrally manage the Windows Internet Connection Firewall settings of individual computers. Organizations can establish corporate policies for personal firewall settings and have LANDesk® Security Suite enforce those settings.

The personal firewall management capabilities in LANDesk Security Suite also provide the flexibility to allow organizations to establish different policies for certain individuals or groups. For example, it can allow a group of engineers or administrators to have an exception setting that allows a certain application to have Internet access whereas other users would normally not be allowed to have access for that application.

Patch Management

Staying up-to-date on the latest vulnerabilities, downloading relevant patches, testing patches, and deploying them to the endpoints is a fulltime job. Each month on Super Tuesday, organizations struggle to stay ahead of the onslaught of new patches and updates that arrive from Microsoft. Unfortunately, the patch management process is not only resource intensive and slow, but every second that a patch remains undeployed leaves the organization vulnerable to attack.

The vulnerability scanning and patch management capabilities in LANDesk® Security Suite help organizations establish ongoing patch-level security on the endpoint devices across their network. They can automate the repetitive processes of maintaining current vulnerability information, assessing vulnerabilities for the various operating systems running on managed devices, downloading the appropriate patch executable files, remediating vulnerabilities by deploying and installing the necessary patches on affected endpoints, and verifying successful patch installation.

LANDesk Security Suite includes the following key vulnerability scanning and patch management features:

- Constantly updated, centralized threats database that contains information on the latest vulnerabilities and patches, providing ongoing protection against new and emerging security and performance threats.
- Pre-tested patch installers and installation notes from the threat database have been tested to install as described by the originating vendor.
- Heterogeneous platform support with predefined, platform-specific vulnerability definitions from the security database, helping organizations quickly identify and resolve known patch threats.
- Pre-staging of patches during testing phase to accelerate overall patch deployment.
- Automated vulnerability scanning identifies known vulnerabilities and enables direct, policy-based or scheduled remediation of detected threats.
- Smart remediation that takes dependencies and supersedence into account to deploy only the patches that each individual endpoint device needs.
- User-defined vulnerability definitions enable IT staff members to create custom vulnerability definitions and patch responses to the unique conditions in their own environment. It allows for easy distribution of patches for custom software.

Centralized Threat Database

New worms and viruses pose a continuous threat to the health and security of endpoint devices, as do ordinary maintenance issues like software updates and bug fixes. New software is released every day, along with the patches to repair inevitable vulnerabilities. The vulnerability scanning and patch management capabilities in LANDesk® Security Suite make the process of gathering the latest known vulnerability, detection rules, and patch information quick and easy by letting administrators update vulnerabilities via a LANDesk hosted database.

This security service consolidates known vulnerabilities from trusted, industry/vendor sources. By establishing and maintaining up-to-date vulnerability and associated patch information, organizations can better understand the nature and extent of the security threats for all of their endpoint devices' operating systems, determine which vulnerabilities are relevant to their network environment, and customize vulnerability scanning and remediation tasks.

Every patch accessed through the LANDesk® security database has been validated to install as intended. In addition, the LANDesk patch engineering team performs basic conflict checking and patch dependency analysis, then provides installation notes to help organizations plan remediation.

LANDesk research and testing includes:

- LANDesk and its partners provide engineering notes from its extensive lab testing of patches
- Third-party notes and severity ratings from CIAC (Computer Incident Advisory Capability) created by the U.S. Department of Energy
- Links to Microsoft and other vendors' patch information

Heterogeneous Patch Management

Effective patch management in a mixed environment can be extremely difficult when administrators have to use different patch management solutions for the different client operating systems on their endpoint devices. But with LANDesk® Security Suite, mixed environment patch management is simple due to its heterogeneous support of the following platforms:

- Windows 98, XP, NT, 2000, 2003 (Vulnerability Assessment and Remediation)
- Macintosh (Vulnerability Assessment and Remediation)
- Linux Red Hat, SuSE (Vulnerability Assessment)
- Unix Sun Solaris, HP UX, IBM AIX (Vulnerability Assessment)

Patch Pre-Staging

While LANDesk and its partners perform thorough testing of patches in its compatibility lab, best practices indicate that organizations still need to test all patches in their own test environment before deployment into their production environment. While this testing phase is necessary, if not carried out in an effective manner it can leave endpoint devices unnecessarily vulnerable for an extended period of time.

The pre-staging capability in LANDesk® Security Suite helps organizations to eliminate wasted time and finalize patch deployment as soon as all patch testing has completed. While a specific patch is being tested in an organization's lab environment, the patch can be staged on each endpoint device by storing it in cache. Once testing has successfully completed and approval is given to actually deploy the patch, administrators can instruct LANDesk Security Suite to execute the deployment and almost instantly the patches install and take effect.

Automated Patch Management

LANDesk® Security Suite features technologies that use a detect-and-report methodology to enable both automated and manual responses to detected vulnerabilities. Organizations can scan for vulnerabilities as frequently as they like, such as on a weekly, daily, or hourly basis. They can also do focused vulnerability scanning on a subset of devices that need to meet higher standards in respect to security scans, such as devices used by individuals that fall into a special compliance group.

In addition to automated scanning, organizations can automatically repair or remove most security threats from managed endpoints through any of the following methods:

- **Scheduled tasks** – Patches or scripts can be pushed out to one or more vulnerable computers using the task scheduler. This is useful if administrators want to set up a task to run at a specific time in the future or as a recurring task.
- **Policy-based** – Based on the results of a database or directory service query, patches can be automatically deployed according to predefined policies. For example, administrators can configure a remediation policy so that it runs only on devices in a particular directory container or on devices running a specific OS.
- **Auto Fix repair** – Patches can be immediately distributed to any computer that needs it as soon as a vulnerability is detected. This is a convenient and quick method if there is a new known vulnerability that administrators want to scan for and repair in a single process.

In some cases, vulnerabilities may be detected that cannot be repaired automatically, such as some configuration settings. In these instances, administrators can conduct manual repairs using remote access and control tools or manually created software distribution packages to correct the problem.

Smart Remediation

Quite often patches or software updates require earlier versions of patches or software to be installed on the endpoint device before the new fix can be deployed. At other times, a new patch might supersede an earlier patch that has not yet been deployed. LANDesk® Security Suite employs smart remediation by installing only those patches that are needed on each individual endpoint and by making sure that any patch dependencies are deployed first and in the proper order. It also clearly identifies any patches that have become obsolete, allowing for a shorter path to a fully patched state.

LANDesk Security Suite provides patch rollback. If a newly deployed patch introduces problems on a particular device, it can be easily be rolled back to its previous working state.

Custom Patch Management

LANDesk® Security Suite provides administrators the flexibility to define multiple endpoint setting definitions. Those settings can apply to security scanning tasks, repair tasks, uninstall tasks and reboot tasks. This gives administrators the ability to apply different settings to different types of endpoint devices, or to separate different scanning and repair tasks. For example, when performing autofix patch repair, an administrator may want to apply different reboot settings than those used with spyware scanning and repair.

This level of control makes it possible for organizations to develop detailed security management plans, and to optimize security scanning schedules to more effectively protect their systems.

Patch Management History

Patch management events are logged in the LANDesk® core database to facilitate an organization's ability to gather the necessary historical data they need to better comprehend the patch management issues they face. This data can be intelligently organized and presented using the reporting tools inherent to LANDesk® Security Suite. In fact, the solution includes more than 60 ready-to-use security and patch management reports, in addition to the ability for administrators to create their own custom reports. These reports also generate a variety of graphs to further facilitate trend analysis.

Network Access Control

LANDesk® Security Suite gives organizations more power and flexibility in controlling access to resources on the network, as well as access to resources on individual endpoint devices. It also enables organizations to prevent unhealthy devices from connecting to the network at all.

Connection Control Manager

Information leakage is a vital concern for nearly all organizations. Their business data is one of their most valuable assets, if not the most valuable asset. Whether it's financial data, market research, competitive information, source code, digital media, product plans, or whatever, significant damage can occur to a business' well being if that data makes its way into the wrong hands.

Onsite visitors stick a thumb drive or PC card in a machine and a minute later data is stolen and out the door. Recent worries about Blue Tooth security create another area of concern, especially for computers that have access to sensitive information.

The Connection Control Manager in LANDesk® Security Suite enables organizations to flexibly control what types of devices can be connected to an endpoint computer as well as control the access levels that individual computers have to the network. It gives administrators a greater ability to control access to endpoint data, limiting the potential for mischief or data theft.

It provides network access controls over endpoints using either white lists (allowed networks) or black lists (disallowed networks). It also allows them to limit access to the communications ports on individual endpoint devices, such as Bluetooth and 802.11x wireless communications. It provides the ability to disable modem use and limit access to removable storage devices accessed through USB or Firewire ports. It can even control access to any local volume.

But not every user and every device need to have the same level of controls. While some users or devices might need to be able to use thumb drives or Blue Tooth personal area networks, others definitely do not. The Connection Control Manager in LANDesk Security Suite gives organizations the ability to segment users into groups or roles utilizing customizable access definitions and security policies. These variable security policies can be based on user login or on specific devices.

The Connection Control Manager provides the ability to control access to the following communications channels on managed computers:

- **Networks** – Inclusive rules can be created that limit network connections only to known, safe networks and exclusive rules can be defined that specifically disallow connections to unsafe network addresses.
- **Devices** – Access to local modems or USB drives can be disabled to keep users from transferring critical data to other media or networks. It provides granular USB controls that enable administrators to prohibit external disc devices while still allowing full USB mouse and keyboard function.
- **Volumes** – Access can be restricted to known disk volumes.
- **Ports** – USB or Firewire ports can be disabled.
- **Wireless access** – To protect against snoopers or malicious access, 802.11x networking or Bluetooth access can be disabled.

Also, since the Connection Control Manager definitions are stored locally in the device's LANDesk® Security Suite agent, connection control policies are enforced regardless of whether the device is connected or disconnected to the network. By providing strict control over endpoint access, Connection Control Manager helps organizations keep their critical data secure and where it belongs.

LANDesk® Trusted Access™

LANDesk® Trusted Access™ is a new scan and block technology from LANDesk available to organizations that utilize LANDesk® Security Suite. Not only does LANDesk Trusted Access block possibly infected computers from connecting to the network, but it also allows for quick remediation of the offending machine. This new scan and block capability of LANDesk Trusted Access, also known as network quarantine or network access control, protects the health of the network and reduces downtime by ensuring compliance to corporate security policies and reducing the risk of malware infections in the enterprise computing environment.

Keeping the Network Healthy

Organizations are becoming increasingly proficient at blocking infected e-mails and preventing malware downloads before they can reach their users connected computers. Unfortunately, one of the most common ways for viruses and other malicious code to penetrate network security is by hitching a ride on mobile computers that have journeyed beyond the protections of the corporate network.

Laptop users that check their e-mail at an Internet café or download software from their home Internet connections—or any other place that does not have the same controls as the organization's infrastructure— have the potential of becoming infected. When they return to work, if they are allowed to connect that infected laptop to the corporate network it opens the door for the infection to spread across the enterprise.

But traveling or remote users aren't the only sources for the spreading of harmful infections. Any endpoint device within the network that is inadequately protected can become infected and unknowingly act as a malicious carrier. Another threat comes in the form of trusted business partners that come onsite and want to be able to connect to the network. Accommodating such requests might be good for the relationship, but can be disastrous for network health if the health of the partner's laptops is uncertain.

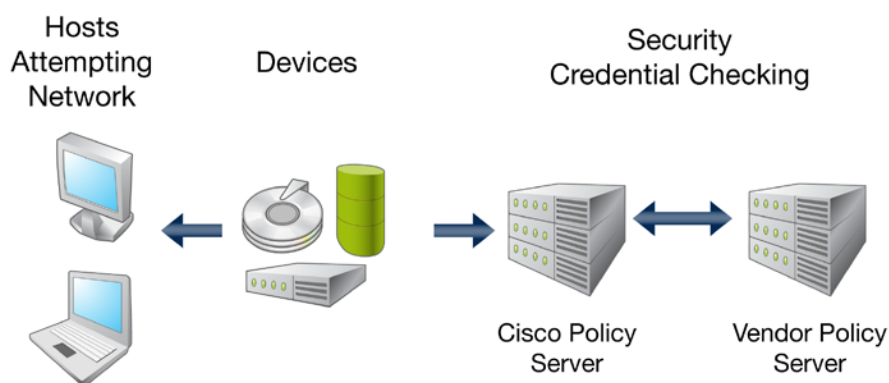
When these or any other computers try to connect to the organization's network, LANDesk® Trusted Access™ scans them to verify that they are healthy and conform to corporate policy for designated security attributes, such as up-to-date patches, proper antivirus patterns, security configuration threats, and more. If a computer is found to be out of compliance or unhealthy, it is not allowed to connect to the network. Furthermore, LANDesk® Security Suite can automatically attempt to remediate whatever problem is preventing that machine from connecting. Once the problem is fixed, the computer will be able to connect.

This scan and block capability gives organizations the confidence that any endpoint device attempting to connect to the network—whether it belongs to mobile users, desktop users, visitors, or even third-party contractors—will comply with corporate security policy before a connection is granted such that they won't be able to pose a threat of infecting the network.

Choice of Cisco Support or Hardware Independent

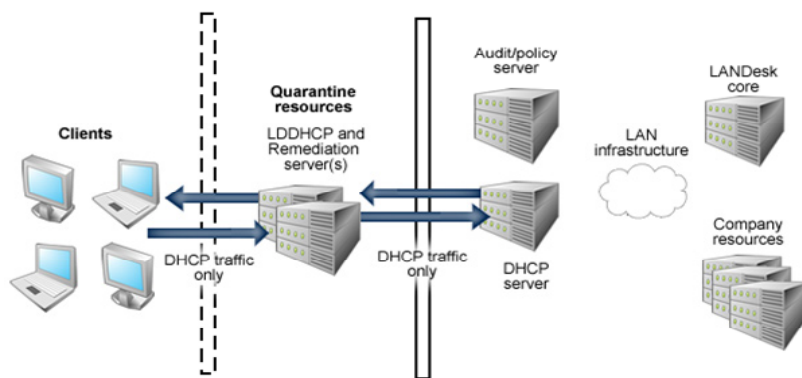
LANDesk gives its customers two compelling options for taking advantage of its scan and block technology. The first one is a Cisco Compatible option that supports and leverages. Network Admission Control from Cisco. This is ideal for organizations that have adopted a Cisco based strategy within their network infrastructure.

Cisco Network Admission Control



The second option is referred to as the DHCP version of LANDesk® Trusted Access™. It's a hardware independent option that provides the same level of functionality as the Cisco based solution, but instead leverages virtually any DHCP server device to deliver its scan and block capabilities.

LANDesk DHCP - Network HW Independent



Prevent, Protect, Set, and Enforce

Not only does LANDesk® Security Suite check the health of a device that tries to connect to the network, it also routinely auto-checks the security posture of all managed endpoint devices already connected. Any system—connected or trying to connect—that doesn't meet all security criteria is temporary blocked and put into quarantine. LANDesk Security Suite can then attempt to automatically remediate whatever problems are causing the device to be out of compliance. Once the device comes into compliance, it will leave quarantine and be connected to the network.

LANDesk® Trusted Access™ gives organizations comprehensive network access control, enabling them to:

- **Prevent** infected or unprotected systems from gaining network access
- **Protect** corporate resources from connected systems that become corrupted
- **Set** compliance standards
- **Enforce** security policies that endpoint devices must meet before being passed onto the corporate network

Comprehensive Network Access Control

One of the key aspects of LANDesk® Trusted Access™ that distinguishes it from other access control solutions is that it doesn't focus on just one security point. It spans multiple areas of concerns and allows organizations to leverage solutions from multiple vendors.

As part of its "prevent, protect, set, and enforce" capabilities, LANDesk Trusted Access blocks clients that don't meet the organization's policies for:

- Patch and vulnerability assessment
- Secure configuration settings
- Anti-virus patterns and engine files from Symantec, Norton, McAfee, and Trend-Micro
- Secure personal firewall settings (Windows ICF)
- Custom security policies

LANDesk Trusted Access also sets itself above other network access solutions by delivering the following key differentiators:

- Customizable scanning options to facilitate support of corporate security policies
- Ability to scan and block for multiples security types
- Single console with central management and granular control over access to network
- Comprehensive reporting on all connections, including pass/fail status and remediation status.
- Hardware independent network access control

The scan and block protection provided by LANDesk Trusted Access stops the proliferation of malicious code, reduces the risk of downtime, and ensures only security compliant devices can connect to the network, resulting in higher productivity gains, increased efficiency, enhanced user satisfaction, and lower IT costs all without adding manpower to improve security.

Single Unified Console

LANDesk® Security Suite gives organizations centralized management and protection of all their endpoint devices. It unifies all their security management efforts into a single console that includes:

- Device discovery
- Baseline configuration management
- Change alerting
- Configuration and settings enforcement
- Application monitoring and blocking
- Antivirus management

- Anti-spyware detection, removal and immunization
- Desktop firewall management
- OS, application, and custom vulnerability assessment
- Enterprise remediation
- Content management
- Scan and block network access control
- Connection control management

The LANDesk Security Suite console gives administrators extensive control over endpoint security management tasks with customization features that include dockable tool windows, pin windows, auto hide windows, and savable layouts. It enables administrators to easily and efficiently protect their IT assets, keeping their endpoints healthy, safe, and secure.

Leverages Core LANDesk® Services

In addition to LANDesk® Security Suite, LANDesk offers a comprehensive array of management solutions for servers, desktops and other devices, including LANDesk® Management Suite, LANDesk® Server Manager, LANDesk® System Manager, LANDesk® Asset Manager, LANDesk® Inventory Manager, LANDesk® Patch Manager, and LANDesk® Handheld & Embedded Device Manager. All LANDesk® management solutions are built on a common foundation of efficient, secure core technologies and services that include:

- Unified database schema that increases data integrity and core server scalability
- Improved scalability combines with role-based administration to reduce the number of core servers needed for effective management
- Integrated certificate-based authentication between the core and managed nodes increases management security

While this guide summarizes the major features of LANDesk® Security Suite, it does not describe product functionality in detail.

For in-depth product information, consult the latest versions of the *LANDesk® Security Suite User's Guide* and the *LANDesk® Security Suite Installation and Deployment Guide*. Both are included with the product.

For more information, visit LANDesk's support Web site at: <http://support.landesk.com>.

About LANDesk

LANDesk is an industry leading provider of integrated configuration and security management solutions for desktops, servers, and mobile devices.

LANDesk® management solutions enable IT to automate most IT processes, including:

- Endpoint security management, including vulnerability detection, patch management, spyware removal and device access control
- Asset and compliance management, including device discovery, hardware and software inventory, extended document and asset tracking with date-based alerting, and software license monitoring and reporting
- Configuration management, including software and patch distribution, OSD deployment and policy-based application install
- Problem resolution, including secure remote control, application healing and enterprise helpdesk integration
- Availability management, including real-time performance monitoring and alerting, predictive failure analysis and device update

LANDesk® solutions leverage existing investments in database, application and directory service technologies to create low cost of ownership and a fast return on investment.

