

# Layered IT Security for Today's Dynamic Threat Environment



## With LANDesk multi-layered security you can:

- **Discover and inventory** all the devices connected to your network and all the software running on those devices, regardless of whether a particular device is under management or a local firewall is operating.
- **Stay current with patching requirements** through integrated scanning, vulnerability assessment, patch download and staging, and distribution and maintenance for Windows operating systems, Office applications, and most common non-Microsoft PC software.
- **Maximize malware protection** with a combination of conventional, signature-based antivirus protection (including third-party solution enforcement capabilities) and a host intrusion prevention solution (HIPS) capable of blocking unauthorized code execution and irregular application behaviors.
- **Detect and remediate machines** that are out of compliance with security configuration standards, whether those machines are local or remote.
- **Enforce network access control (NAC)** with remote configuration assessment, quarantine and remediation capabilities for non-compliant machines.
- **Prevent data loss** through theft or negligence with policy-based access control over disk drives, communication channels, ports and modems. Enforce encryption on all allowed data and file transfers to USB devices.
- **Track and report security status** to document security policy implementation, demonstrate compliance, and quantify security ROI.

## Key Features

### Network Access Control Capabilities

- Identify and quarantine out-of-date or unpatched computers, whether managed or unmanaged.
- Enjoy compatibility with Cisco and LANDesk's DHCP network access control capabilities.

### Advanced Vulnerability Detection

- Run standard, custom and high-frequency scans to maintain the level of control, speed and frequency you need, plus monitor antivirus status in real-time and stay on top of pattern file updates for security compliance.
- Enjoy automated, "hands-off" deployment to pilot or test machines as patches become available.
- Define custom definitions and vulnerabilities to bring your systems into compliance with company or industry standards.
- Detect spyware, adware, Trojans, keyloggers and other malware.

### Remediation Tools

- Detect and remove spyware in real-time using the LANDesk® spyware/malware database.
- Control access to disk drives, modems, USB and communications ports, and wireless channels such as 802.11x and Bluetooth, including Bluetooth PAN.
- Stop unauthorized or prohibited applications, even on systems unconnected from the network even if end-users rename the file.

### World-Class Antivirus Protection and Scanning

- Access world-class, enterprise-ready antivirus capabilities and enforce real-time virus protection.
- Schedule automatic updates to virus definition files, controlling which versions are approved, when they are deployed and how they are configured. Enjoy low-bandwidth distribution of virus pattern files using LANDesk's patented Peer Download capability.
- Encrypt and quarantine suspicious files and known infections that can't be immediately cleaned.
- Access a simple graphical dashboard to identify virus outbreaks and chart control activities in real time.
- Give administrators a head start on new pattern files using LANDesk® Antivirus pilot deployment.

### Antivirus Enforcement and Firewall Capabilities

- Manage your chosen antivirus solution from McAfee, Norton, Sophos, Symantec or Trend Micro directly from your LANDesk® Security Suite console.
- Enable and configure the XP and Vista firewall from the LANDesk Security Suite console and identify unprotected wired and wireless machines.
- Configure one firewall for all systems, or customize the firewall configuration for individual systems or groups of systems.

### Patch Management Tools

- Identify OS and application patch needs automatically using LANDesk's comprehensive vulnerability assessment and patch database.
- Update all systems automatically using LANDesk's Automated Patch Deployment process.
- Control which vulnerabilities you receive alerts on and receive alerts on newly available definitions based on type and severity.
- Build custom patch packages to address any detected vulnerability; protect your custom patches against tampering with a secure MD5 hash algorithm.
- Download and prioritize patches, then distribute patches across the enterprise using efficient LANDesk® Targeted Multicast™ technology.
- Get to a fully patched state faster; only needed patches are downloaded from the LANDesk® database; obsolete patches remain available if needed.
- Patch dependency shows you which patches depend on other patches, so you know what new vulnerabilities a patch might introduce.
- Patch supercedence lets you download and distribute patches that are needed and filter out older and obsolete patches to give you a more rapid time to a fully patched state; obsolete patches remain available if needed.

### Security Assurance

- Maintain secure configurations using role-based administration and policy-based management tools.
- Control who can alter your corporate security policy with baseline configuration capabilities.
- Monitor and classify wireless access points.
- Prevent data leakage by monitoring and enforcing policies on users' USB drives, CDs, DVDs and other portable media.
- Control who can access which applications by group or user level to enforce security compliance.
- Identify systems using wireless network interface cards or running independent antivirus products; see the product's vendor and version of pattern files.
- Access reporting capabilities that include trend graphs and security policy and spyware reports.

Visit <http://secureit.landesk.com> for more information.

This information is provided in connection with LANDesk products. No license, express or implied, by estoppel or otherwise, or warranty is granted by this document. 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. For the most current product information, visit <http://www.landesk.com>.

Copyright © 2008 LANDesk Software Ltd. or its affiliated companies. All rights reserved. LANDesk, Peer Download, Targeted Multicast and Trusted Access are registered trademarks or trademarks of LANDesk Software Ltd. or its affiliated companies in the United States and/or other countries. Other names or brands may be claimed as the property of others. Each customer's results may vary based on its unique set of facts and circumstances. LSI-0738 0508/JBB/NH/CA

 **LANDesk** | make IT happen  
An Avocent® Company



A Cost-Effective, Incremental Path  
to Layered Endpoint Security

 **LANDesk** | make IT happen  
An Avocent® Company

Today's IT threat environment presents an extraordinary set of challenges for IT organizations struggling to secure large fleets of desktop and mobile laptop PCs. Not only are the financial impacts of major breaches staggering, the landscape of vulnerabilities and potential attack vectors is constantly shifting and evolving.

Today's attackers are increasingly well-organized criminal syndicates launching targeted attacks. Their strategies have shifted to an exploding number of application-level vulnerabilities and Web-based attacks launched from trusted sites. Data loss across ad hoc network bridges and removable mass storage devices is epidemic. And malware innovation shows no sign of slowing: by some accounts the total number of malicious software signatures associated with viruses, Trojans, keyloggers, spyware, adware and rootkits doubled in 2007, and zero-day attacks continue to be a particular problem.

### Conventional Defenses Can't Keep Up

The textbook solution for endpoint security is a combination of firewalls, intrusion detection systems (IDS) and antivirus software; but while all of these measures are essential they are no longer sufficient. Today's defenses must envelop every vulnerable asset in multiple defensive layers that present technically distinct barriers on every approach. They must somehow combine comprehensive endpoint management capabilities with an extensible armory of security solutions. Point products are readily available, but selecting, integrating and managing a do-it-yourself solution at enterprise scale can be prohibitively expensive and an administrative nightmare.

### Layered Security the LANDesk Way

LANDesk provides a simple, affordable and incremental path to layered endpoint security through a family of tightly integrated security products designed for flawless interoperability, convenient single-console management, and the efficiency and reliability of a single client software agent.

- **LANDesk® Security Suite** extends active security management to all endpoints, providing integrated patch management, active threat analysis and remediation, spyware detection and removal, network access control, configuration security tools, and innovative connection control management capabilities such as USB encryption and removable storage management.
- **LANDesk® Antivirus** adds best of breed enterprise-ready virus protection, rootkit detection, quarantine capabilities and centralized management at a lower investment than other industry-standard solutions.
- **LANDesk® Host Intrusion Prevention** adds zero-day threat protection with behavior-based execution blocking that prevents malicious application attacks right on the host.

The result is the industry's most comprehensive and flexible toolset for layered security implementation in complex enterprise environments.



### Discover and Inventory Hardware and Software

LANDesk® Management Suite users are accustomed to the convenience and transparency of real-time, subnet-level discovery technologies that easily identify, locate and inventory computer assets, assess their configuration and management status and determine whether a local firewall is enabled. They can even access systems at remote, distributed sites over the Internet, without a VPN. LANDesk® Security Suite extends these capabilities with a wireless access point discovery solution that uses notebook PC wireless NICs to locate and classify all access points within and adjacent to the enterprise environment, allowing administrators to block access to those that are unauthorized.

### Manage Patching Proactively

LANDesk® Patch Manager, available both as a standalone product and as part of the LANDesk Security Suite, provides integrated vulnerability assessment, patch research, download, staging and distribution capabilities for operating systems and applications in heterogeneous IT environments. LANDesk Targeted Multicast™ and Peer Download technologies accelerate deployment and reduce distribution bandwidth requirements with no additional hardware or router reconfiguration. Deployment can be automated and patches can be cached on target machines for subsequent activation and installation. And with the inclusion of LANDesk® Process Manager automated patch deployment, new patches can be configured with ongoing, fully automated update processes that leverage modifiable workflows, automated approvals and pilot groups.

### Enjoy World-Class Malware Protection

LANDesk multi-layer security offers three paths to known malicious code protection. LANDesk Security Suite provides real-time spyware detection and removal based on the LANDesk® spyware-malware database. It also lets you manage your choice of third-party antivirus solutions from McAfee, Norton, Sophos, Symantec or Trend Micro directly from the central management console. Better yet, you can choose LANDesk's own world-class add-in solution for single-agent simplicity. LANDesk® Antivirus leverages the Kapersky Labs engine and signature database to provide industry-leading protection against viruses, worms, Trojans, spyware, rootkits and other malicious code, with hourly updates from the industry's most complete threat signature database.

### Centralize Windows Firewall Management

With LANDesk Security Suite, administrators can centrally enable and configure Windows XP and Vista firewalls directly from the management console. You can easily identify unprotected machines whether wired or wireless, standardize on a single configuration, or customize for different user groups.

### Detect and Remediate Vulnerable Configurations

Standard and high-frequency vulnerability scanning capabilities pinpoint configuration, patching and software update requirements quickly and easily, based on your own needs and chosen level of detail. Custom scans let you define and search for specific condition sets. Defining and maintaining secure configurations is simplified with role-based administration and policy-based management tools.

### Control and Manage Remote Machines

Scanning and remediation capabilities can be extended beyond the corporate firewall with the LANDesk® Management Gateway, a plug-in appliance for remote locations that lets you manage any user, simply and securely, using any existing Internet connection, certificate-based authentication and SSL encryption. Patent-pending LANDesk technology eliminates the need for VPNs, leased lines or local management servers and lets you manage remote machines centrally and proactively, on your own schedule, not the user's.

### Control Network Access

LANDesk® Network Access Control lets you prevent compromised or non-compliant systems from connecting to your network until they have been fully remediated. The solution supports four of the most popular industry standards for network access control: Cisco NAC, IPSec, 802.1x, and DHCP. NAC is an essential tool for managing the inevitable security threats posed by mobile users and systems that operate outside the enterprise environment for long periods of time, often connecting with many unknown networks and environments in the interim.

### Prevent Data Loss

Connection Control Manager, a core technology in LANDesk Security Suite, lets you restrict network access to authorized networks or IP addresses and block communications with specified networks. Application blacklisting capabilities let you prevent users from launching unauthorized applications, even inadvertently. You control user access to disk drives, communication channels, ports and modems to help prevent data loss through theft or negligence. A unique new feature is the ability to encrypt all allowed data and file transfers to USB devices.

### Detect and Prevent Host Intrusion

The newest addition to the LANDesk endpoint armory is LANDesk® Host Intrusion Prevention System (HIPS), a new plug-in for LANDesk Security Suite. HIPS provides a variety of non signature-based malicious code defenses to supplement antivirus and anti-spyware systems and to defend against zero-day exploits. Available application whitelisting lets you specify exactly which applications will be allowed to execute on a system. Proven heuristic and behavior-recognition techniques identify attack vectors and actions of malicious code. LANDesk® HIPS gives administrators a powerful new tool for controlling which programs execute on a system and the behaviors that approved applications are allowed to execute.

### Document Compliance and ROI

LANDesk Security Suite makes it easy to track and document the progress and ROI of security initiatives with a variety of reporting options. Detailed historical reports on policy enforcement and patch deployment are displayed in an easily understood graphical format that clearly documents policies, performance, problem areas and trends over time.

### Leverage LANDesk Expertise in Your Environment

LANDesk Professional Services let you draw on the experience, talents and abilities of the people who develop award-winning LANDesk solutions to help you evaluate your endpoint security requirements, then design, implement and maintain a multi-layered security solution tailored to your environment and operational requirements. Defined security-related service offerings include:

- **Health Assessment** – An evaluation of your LANDesk infrastructure, designed to ensure that your systems, security and process management applications are up to date and performing as expected. Assessment areas include architecture, performance, maintenance and security.
- **Patch Level Assessment** – Provides expert assistance and consultation in LANDesk® patch management configuration, vulnerability scanning, and scan report interpretation.

"When we first did our vendor analysis, the big thing to hit us was the complete integration of the LANDesk® Security Suite product. Looking across the marketplace, it was the only solution that truly integrated its patch management with its security management in a cost-effective single management console and a single engine approach. ...Not only does LANDesk Security Suite give us a very clear understanding of our patch penetration, but now we can often achieve complete patch coverage overnight rather than taking multiple days."

— **Joe Riesberg**  
Manager of IT Security and  
Regulatory Compliance  
VCPI

# Layered IT Security for Today's Dynamic Threat Environment



## With LANDesk multi-layered security you can:

- **Discover and inventory** all the devices connected to your network and all the software running on those devices, regardless of whether a particular device is under management or a local firewall is operating.
- **Stay current with patching requirements** through integrated scanning, vulnerability assessment, patch download and staging, and distribution and maintenance for Windows operating systems, Office applications, and most common non-Microsoft PC software.
- **Maximize malware protection** with a combination of conventional, signature-based antivirus protection (including third-party solution enforcement capabilities) and a host intrusion prevention solution (HIPS) capable of blocking unauthorized code execution and irregular application behaviors.
- **Detect and remediate machines** that are out of compliance with security configuration standards, whether those machines are local or remote.
- **Enforce network access control (NAC)** with remote configuration assessment, quarantine and remediation capabilities for non-compliant machines.
- **Prevent data loss** through theft or negligence with policy-based access control over disk drives, communication channels, ports and modems. Enforce encryption on all allowed data and file transfers to USB devices.
- **Track and report security status** to document security policy implementation, demonstrate compliance, and quantify security ROI.

## Key Features

### Network Access Control Capabilities

- Identify and quarantine out-of-date or unpatched computers, whether managed or unmanaged.
- Enjoy compatibility with Cisco and LANDesk's DHCP network access control capabilities.

### Advanced Vulnerability Detection

- Run standard, custom and high-frequency scans to maintain the level of control, speed and frequency you need, plus monitor antivirus status in real-time and stay on top of pattern file updates for security compliance.
- Enjoy automated, "hands-off" deployment to pilot or test machines as patches become available.
- Define custom definitions and vulnerabilities to bring your systems into compliance with company or industry standards.
- Detect spyware, adware, Trojans, keyloggers and other malware.

### Remediation Tools

- Detect and remove spyware in real-time using the LANDesk® spyware/malware database.
- Control access to disk drives, modems, USB and communications ports, and wireless channels such as 802.11x and Bluetooth, including Bluetooth PAN.
- Stop unauthorized or prohibited applications, even on systems unconnected from the network even if end-users rename the file.

### World-Class Antivirus Protection and Scanning

- Access world-class, enterprise-ready antivirus capabilities and enforce real-time virus protection.
- Schedule automatic updates to virus definition files, controlling which versions are approved, when they are deployed and how they are configured. Enjoy low-bandwidth distribution of virus pattern files using LANDesk's patented Peer Download capability.
- Encrypt and quarantine suspicious files and known infections that can't be immediately cleaned.
- Access a simple graphical dashboard to identify virus outbreaks and chart control activities in real time.
- Give administrators a head start on new pattern files using LANDesk® Antivirus pilot deployment.

### Antivirus Enforcement and Firewall Capabilities

- Manage your chosen antivirus solution from McAfee, Norton, Sophos, Symantec or Trend Micro directly from your LANDesk® Security Suite console.
- Enable and configure the XP and Vista firewall from the LANDesk Security Suite console and identify unprotected wired and wireless machines.
- Configure one firewall for all systems, or customize the firewall configuration for individual systems or groups of systems.

### Patch Management Tools

- Identify OS and application patch needs automatically using LANDesk's comprehensive vulnerability assessment and patch database.
- Update all systems automatically using LANDesk's Automated Patch Deployment process.
- Control which vulnerabilities you receive alerts on and receive alerts on newly available definitions based on type and severity.
- Build custom patch packages to address any detected vulnerability; protect your custom patches against tampering with a secure MD5 hash algorithm.
- Download and prioritize patches, then distribute patches across the enterprise using efficient LANDesk® Targeted Multicast™ technology.
- Get to a fully patched state faster; only needed patches are downloaded from the LANDesk® database; obsolete patches remain available if needed.
- Patch dependency shows you which patches depend on other patches, so you know what new vulnerabilities a patch might introduce.
- Patch supercedence lets you download and distribute patches that are needed and filter out older and obsolete patches to give you a more rapid time to a fully patched state; obsolete patches remain available if needed.

### Security Assurance

- Maintain secure configurations using role-based administration and policy-based management tools.
- Control who can alter your corporate security policy with baseline configuration capabilities.
- Monitor and classify wireless access points.
- Prevent data leakage by monitoring and enforcing policies on users' USB drives, CDs, DVDs and other portable media.
- Control who can access which applications by group or user level to enforce security compliance.
- Identify systems using wireless network interface cards or running independent antivirus products; see the product's vendor and version of pattern files.
- Access reporting capabilities that include trend graphs and security policy and spyware reports.

Visit <http://secureit.landesk.com> for more information.

This information is provided in connection with LANDesk products. No license, express or implied, by estoppel or otherwise, or warranty is granted by this document. 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. For the most current product information, visit <http://www.landesk.com>.

Copyright © 2008 LANDesk Software Ltd. or its affiliated companies. All rights reserved. LANDesk, Peer Download, Targeted Multicast and Trusted Access are registered trademarks or trademarks of LANDesk Software Ltd. or its affiliated companies in the United States and/or other countries. Other names or brands may be claimed as the property of others. Each customer's results may vary based on its unique set of facts and circumstances. LSI-0738 0508/JBB/NH/CA

 **LANDesk®** | make IT happen  
An Avocent® Company



A Cost-Effective, Incremental Path  
to Layered Endpoint Security

 **LANDesk®** | make IT happen  
An Avocent® Company

Today's IT threat environment presents an extraordinary set of challenges for IT organizations struggling to secure large fleets of desktop and mobile laptop PCs. Not only are the financial impacts of major breaches staggering, the landscape of vulnerabilities and potential attack vectors is constantly shifting and evolving.

Today's attackers are increasingly well-organized criminal syndicates launching targeted attacks. Their strategies have shifted to an exploding number of application-level vulnerabilities and Web-based attacks launched from trusted sites. Data loss across ad hoc network bridges and removable mass storage devices is epidemic. And malware innovation shows no sign of slowing: by some accounts the total number of malicious software signatures associated with viruses, Trojans, keyloggers, spyware, adware and rootkits doubled in 2007, and zero-day attacks continue to be a particular problem.

### Conventional Defenses Can't Keep Up

The textbook solution for endpoint security is a combination of firewalls, intrusion detection systems (IDS) and antivirus software; but while all of these measures are essential they are no longer sufficient. Today's defenses must envelop every vulnerable asset in multiple defensive layers that present technically distinct barriers on every approach. They must somehow combine comprehensive endpoint management capabilities with an extensible armory of security solutions. Point products are readily available, but selecting, integrating and managing a do-it-yourself solution at enterprise scale can be prohibitively expensive and an administrative nightmare.

### Layered Security the LANDesk Way

LANDesk provides a simple, affordable and incremental path to layered endpoint security through a family of tightly integrated security products designed for flawless interoperability, convenient single-console management, and the efficiency and reliability of a single client software agent.

- **LANDesk® Security Suite** extends active security management to all endpoints, providing integrated patch management, active threat analysis and remediation, spyware detection and removal, network access control, configuration security tools, and innovative connection control management capabilities such as USB encryption and removable storage management.
- **LANDesk® Antivirus** adds best of breed enterprise-ready virus protection, rootkit detection, quarantine capabilities and centralized management at a lower investment than other industry-standard solutions.
- **LANDesk® Host Intrusion Prevention** adds zero-day threat protection with behavior-based execution blocking that prevents malicious application attacks right on the host.

The result is the industry's most comprehensive and flexible toolset for layered security implementation in complex enterprise environments.



### Discover and Inventory Hardware and Software

LANDesk® Management Suite users are accustomed to the convenience and transparency of real-time, subnet-level discovery technologies that easily identify, locate and inventory computer assets, assess their configuration and management status and determine whether a local firewall is enabled. They can even access systems at remote, distributed sites over the Internet, without a VPN. LANDesk® Security Suite extends these capabilities with a wireless access point discovery solution that uses notebook PC wireless NICs to locate and classify all access points within and adjacent to the enterprise environment, allowing administrators to block access to those that are unauthorized.

### Manage Patching Proactively

LANDesk® Patch Manager, available both as a standalone product and as part of the LANDesk Security Suite, provides integrated vulnerability assessment, patch research, download, staging and distribution capabilities for operating systems and applications in heterogeneous IT environments. LANDesk Targeted Multicast™ and Peer Download technologies accelerate deployment and reduce distribution bandwidth requirements with no additional hardware or router reconfiguration. Deployment can be automated and patches can be cached on target machines for subsequent activation and installation. And with the inclusion of LANDesk® Process Manager automated patch deployment, new patches can be configured with ongoing, fully automated update processes that leverage modifiable workflows, automated approvals and pilot groups.

### Enjoy World-Class Malware Protection

LANDesk multi-layer security offers three paths to known malicious code protection. LANDesk Security Suite provides real-time spyware detection and removal based on the LANDesk® spyware-malware database. It also lets you manage your choice of third-party antivirus solutions from McAfee, Norton, Sophos, Symantec or Trend Micro directly from the central management console. Better yet, you can choose LANDesk's own world-class add-in solution for single-agent simplicity. LANDesk® Antivirus leverages the Kaspersky Labs engine and signature database to provide industry-leading protection against viruses, worms, Trojans, spyware, rootkits and other malicious code, with hourly updates from the industry's most complete threat signature database.

### Centralize Windows Firewall Management

With LANDesk Security Suite, administrators can centrally enable and configure Windows XP and Vista firewalls directly from the management console. You can easily identify unprotected machines whether wired or wireless, standardize on a single configuration, or customize for different user groups.

### Detect and Remediate Vulnerable Configurations

Standard and high-frequency vulnerability scanning capabilities pinpoint configuration, patching and software update requirements quickly and easily, based on your own needs and chosen level of detail. Custom scans let you define and search for specific condition sets. Defining and maintaining secure configurations is simplified with role-based administration and policy-based management tools.

### Control and Manage Remote Machines

Scanning and remediation capabilities can be extended beyond the corporate firewall with the LANDesk® Management Gateway, a plug-in appliance for remote locations that lets you manage any user, simply and securely, using any existing Internet connection, certificate-based authentication and SSL encryption. Patent-pending LANDesk technology eliminates the need for VPNs, leased lines or local management servers and lets you manage remote machines centrally and proactively, on your own schedule, not the user's.

### Control Network Access

LANDesk® Network Access Control lets you prevent compromised or non-compliant systems from connecting to your network until they have been fully remediated. The solution supports four of the most popular industry standards for network access control: Cisco NAC, IPSec, 802.1x, and DHCP. NAC is an essential tool for managing the inevitable security threats posed by mobile users and systems that operate outside the enterprise environment for long periods of time, often connecting with many unknown networks and environments in the interim.

### Prevent Data Loss

Connection Control Manager, a core technology in LANDesk Security Suite, lets you restrict network access to authorized networks or IP addresses and block communications with specified networks. Application blacklisting capabilities let you prevent users from launching unauthorized applications, even inadvertently. You control user access to disk drives, communication channels, ports and modems to help prevent data loss through theft or negligence. A unique new feature is the ability to encrypt all allowed data and file transfers to USB devices.

### Detect and Prevent Host Intrusion

The newest addition to the LANDesk endpoint armory is LANDesk® Host Intrusion Prevention System (HIPS), a new plug-in for LANDesk Security Suite. HIPS provides a variety of non signature-based malicious code defenses to supplement antivirus and anti-spyware systems and to defend against zero-day exploits. Available application whitelisting lets you specify exactly which applications will be allowed to execute on a system. Proven heuristic and behavior-recognition techniques identify attack vectors and actions of malicious code. LANDesk® HIPS gives administrators a powerful new tool for controlling which programs execute on a system and the behaviors that approved applications are allowed to execute.

### Document Compliance and ROI

LANDesk Security Suite makes it easy to track and document the progress and ROI of security initiatives with a variety of reporting options. Detailed historical reports on policy enforcement and patch deployment are displayed in an easily understood graphical format that clearly documents policies, performance, problem areas and trends over time.

### Leverage LANDesk Expertise in Your Environment

LANDesk Professional Services let you draw on the experience, talents and abilities of the people who develop award-winning LANDesk solutions to help you evaluate your endpoint security requirements, then design, implement and maintain a multi-layered security solution tailored to your environment and operational requirements. Defined security-related service offerings include:

- **Health Assessment** – An evaluation of your LANDesk infrastructure, designed to ensure that your systems, security and process management applications are up to date and performing as expected. Assessment areas include architecture, performance, maintenance and security.
- **Patch Level Assessment** – Provides expert assistance and consultation in LANDesk® patch management configuration, vulnerability scanning, and scan report interpretation.

"When we first did our vendor analysis, the big thing to hit us was the complete integration of the LANDesk® Security Suite product. Looking across the marketplace, it was the only solution that truly integrated its patch management with its security management in a cost-effective single management console and a single engine approach. ...Not only does LANDesk Security Suite give us a very clear understanding of our patch penetration, but now we can often achieve complete patch coverage overnight rather than taking multiple days."

— **Joe Riesberg**  
Manager of IT Security and  
Regulatory Compliance  
VCPI

# Layered IT Security for Today's Dynamic Threat Environment



## With LANDesk multi-layered security you can:

- **Discover and inventory** all the devices connected to your network and all the software running on those devices, regardless of whether a particular device is under management or a local firewall is operating.
- **Stay current with patching requirements** through integrated scanning, vulnerability assessment, patch download and staging, and distribution and maintenance for Windows operating systems, Office applications, and most common non-Microsoft PC software.
- **Maximize malware protection** with a combination of conventional, signature-based antivirus protection (including third-party solution enforcement capabilities) and a host intrusion prevention solution (HIPS) capable of blocking unauthorized code execution and irregular application behaviors.
- **Detect and remediate machines** that are out of compliance with security configuration standards, whether those machines are local or remote.
- **Enforce network access control (NAC)** with remote configuration assessment, quarantine and remediation capabilities for non-compliant machines.
- **Prevent data loss** through theft or negligence with policy-based access control over disk drives, communication channels, ports and modems. Enforce encryption on all allowed data and file transfers to USB devices.
- **Track and report security status** to document security policy implementation, demonstrate compliance, and quantify security ROI.

## Key Features

### Network Access Control Capabilities

- Identify and quarantine out-of-date or unpatched computers, whether managed or unmanaged.
- Enjoy compatibility with Cisco and LANDesk's DHCP network access control capabilities.

### Advanced Vulnerability Detection

- Run standard, custom and high-frequency scans to maintain the level of control, speed and frequency you need, plus monitor antivirus status in real-time and stay on top of pattern file updates for security compliance.
- Enjoy automated, "hands-off" deployment to pilot or test machines as patches become available.
- Define custom definitions and vulnerabilities to bring your systems into compliance with company or industry standards.
- Detect spyware, adware, Trojans, keyloggers and other malware.

### Remediation Tools

- Detect and remove spyware in real-time using the LANDesk® spyware/malware database.
- Control access to disk drives, modems, USB and communications ports, and wireless channels such as 802.11x and Bluetooth, including Bluetooth PAN.
- Stop unauthorized or prohibited applications, even on systems unconnected from the network even if end-users rename the file.

### World-Class Antivirus Protection and Scanning

- Access world-class, enterprise-ready antivirus capabilities and enforce real-time virus protection.
- Schedule automatic updates to virus definition files, controlling which versions are approved, when they are deployed and how they are configured. Enjoy low-bandwidth distribution of virus pattern files using LANDesk's patented Peer Download capability.
- Encrypt and quarantine suspicious files and known infections that can't be immediately cleaned.
- Access a simple graphical dashboard to identify virus outbreaks and chart control activities in real time.
- Give administrators a head start on new pattern files using LANDesk® Antivirus pilot deployment.

### Antivirus Enforcement and Firewall Capabilities

- Manage your chosen antivirus solution from McAfee, Norton, Sophos, Symantec or Trend Micro directly from your LANDesk® Security Suite console.
- Enable and configure the XP and Vista firewall from the LANDesk Security Suite console and identify unprotected wired and wireless machines.
- Configure one firewall for all systems, or customize the firewall configuration for individual systems or groups of systems.

### Patch Management Tools

- Identify OS and application patch needs automatically using LANDesk's comprehensive vulnerability assessment and patch database.
- Update all systems automatically using LANDesk's Automated Patch Deployment process.
- Control which vulnerabilities you receive alerts on and receive alerts on newly available definitions based on type and severity.
- Build custom patch packages to address any detected vulnerability; protect your custom patches against tampering with a secure MD5 hash algorithm.
- Download and prioritize patches, then distribute patches across the enterprise using efficient LANDesk® Targeted Multicast™ technology.
- Get to a fully patched state faster; only needed patches are downloaded from the LANDesk® database; obsolete patches remain available if needed.
- Patch dependency shows you which patches depend on other patches, so you know what new vulnerabilities a patch might introduce.
- Patch supercedence lets you download and distribute patches that are needed and filter out older and obsolete patches to give you a more rapid time to a fully patched state; obsolete patches remain available if needed.

### Security Assurance

- Maintain secure configurations using role-based administration and policy-based management tools.
- Control who can alter your corporate security policy with baseline configuration capabilities.
- Monitor and classify wireless access points.
- Prevent data leakage by monitoring and enforcing policies on users' USB drives, CDs, DVDs and other portable media.
- Control who can access which applications by group or user level to enforce security compliance.
- Identify systems using wireless network interface cards or running independent antivirus products; see the product's vendor and version of pattern files.
- Access reporting capabilities that include trend graphs and security policy and spyware reports.

Visit <http://secureit.landesk.com> for more information.

This information is provided in connection with LANDesk products. No license, express or implied, by estoppel or otherwise, or warranty is granted by this document. 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. For the most current product information, visit <http://www.landesk.com>.

Copyright © 2008 LANDesk Software Ltd. or its affiliated companies. All rights reserved. LANDesk, Peer Download, Targeted Multicast and Trusted Access are registered trademarks or trademarks of LANDesk Software Ltd. or its affiliated companies in the United States and/or other countries. Other names or brands may be claimed as the property of others. Each customer's results may vary based on its unique set of facts and circumstances. LSI-0738 0508/JBB/NH/CA

 **LANDesk** | make IT happen  
An Avocent® Company



A Cost-Effective, Incremental Path  
to Layered Endpoint Security

 **LANDesk** | make IT happen  
An Avocent® Company

Today's IT threat environment presents an extraordinary set of challenges for IT organizations struggling to secure large fleets of desktop and mobile laptop PCs. Not only are the financial impacts of major breaches staggering, the landscape of vulnerabilities and potential attack vectors is constantly shifting and evolving.

Today's attackers are increasingly well-organized criminal syndicates launching targeted attacks. Their strategies have shifted to an exploding number of application-level vulnerabilities and Web-based attacks launched from trusted sites. Data loss across ad hoc network bridges and removable mass storage devices is epidemic. And malware innovation shows no sign of slowing: by some accounts the total number of malicious software signatures associated with viruses, Trojans, keyloggers, spyware, adware and rootkits doubled in 2007, and zero-day attacks continue to be a particular problem.

### Conventional Defenses Can't Keep Up

The textbook solution for endpoint security is a combination of firewalls, intrusion detection systems (IDS) and antivirus software; but while all of these measures are essential they are no longer sufficient. Today's defenses must envelop every vulnerable asset in multiple defensive layers that present technically distinct barriers on every approach. They must somehow combine comprehensive endpoint management capabilities with an extensible armory of security solutions. Point products are readily available, but selecting, integrating and managing a do-it-yourself solution at enterprise scale can be prohibitively expensive and an administrative nightmare.

### Layered Security the LANDesk Way

LANDesk provides a simple, affordable and incremental path to layered endpoint security through a family of tightly integrated security products designed for flawless interoperability, convenient single-console management, and the efficiency and reliability of a single client software agent.

- **LANDesk® Security Suite** extends active security management to all endpoints, providing integrated patch management, active threat analysis and remediation, spyware detection and removal, network access control, configuration security tools, and innovative connection control management capabilities such as USB encryption and removable storage management.
- **LANDesk® Antivirus** adds best of breed enterprise-ready virus protection, rootkit detection, quarantine capabilities and centralized management at a lower investment than other industry-standard solutions.
- **LANDesk® Host Intrusion Prevention** adds zero-day threat protection with behavior-based execution blocking that prevents malicious application attacks right on the host.

The result is the industry's most comprehensive and flexible toolset for layered security implementation in complex enterprise environments.



### Discover and Inventory Hardware and Software

LANDesk® Management Suite users are accustomed to the convenience and transparency of real-time, subnet-level discovery technologies that easily identify, locate and inventory computer assets, assess their configuration and management status and determine whether a local firewall is enabled. They can even access systems at remote, distributed sites over the Internet, without a VPN. LANDesk® Security Suite extends these capabilities with a wireless access point discovery solution that uses notebook PC wireless NICs to locate and classify all access points within and adjacent to the enterprise environment, allowing administrators to block access to those that are unauthorized.

### Manage Patching Proactively

LANDesk® Patch Manager, available both as a standalone product and as part of the LANDesk Security Suite, provides integrated vulnerability assessment, patch research, download, staging and distribution capabilities for operating systems and applications in heterogeneous IT environments. LANDesk Targeted Multicast™ and Peer Download technologies accelerate deployment and reduce distribution bandwidth requirements with no additional hardware or router reconfiguration. Deployment can be automated and patches can be cached on target machines for subsequent activation and installation. And with the inclusion of LANDesk® Process Manager automated patch deployment, new patches can be configured with ongoing, fully automated update processes that leverage modifiable workflows, automated approvals and pilot groups.

### Enjoy World-Class Malware Protection

LANDesk multi-layer security offers three paths to known malicious code protection. LANDesk Security Suite provides real-time spyware detection and removal based on the LANDesk® spyware-malware database. It also lets you manage your choice of third-party antivirus solutions from McAfee, Norton, Sophos, Symantec or Trend Micro directly from the central management console. Better yet, you can choose LANDesk's own world-class add-in solution for single-agent simplicity. LANDesk® Antivirus leverages the Kapersky Labs engine and signature database to provide industry-leading protection against viruses, worms, Trojans, spyware, rootkits and other malicious code, with hourly updates from the industry's most complete threat signature database.

### Centralize Windows Firewall Management

With LANDesk Security Suite, administrators can centrally enable and configure Windows XP and Vista firewalls directly from the management console. You can easily identify unprotected machines whether wired or wireless, standardize on a single configuration, or customize for different user groups.

### Detect and Remediate Vulnerable Configurations

Standard and high-frequency vulnerability scanning capabilities pinpoint configuration, patching and software update requirements quickly and easily, based on your own needs and chosen level of detail. Custom scans let you define and search for specific condition sets. Defining and maintaining secure configurations is simplified with role-based administration and policy-based management tools.

### Control and Manage Remote Machines

Scanning and remediation capabilities can be extended beyond the corporate firewall with the LANDesk® Management Gateway, a plug-in appliance for remote locations that lets you manage any user, simply and securely, using any existing Internet connection, certificate-based authentication and SSL encryption. Patent-pending LANDesk technology eliminates the need for VPNs, leased lines or local management servers and lets you manage remote machines centrally and proactively, on your own schedule, not the user's.

### Control Network Access

LANDesk® Network Access Control lets you prevent compromised or non-compliant systems from connecting to your network until they have been fully remediated. The solution supports four of the most popular industry standards for network access control: Cisco NAC, IPSec, 802.1x, and DHCP. NAC is an essential tool for managing the inevitable security threats posed by mobile users and systems that operate outside the enterprise environment for long periods of time, often connecting with many unknown networks and environments in the interim.

### Prevent Data Loss

Connection Control Manager, a core technology in LANDesk Security Suite, lets you restrict network access to authorized networks or IP addresses and block communications with specified networks. Application blacklisting capabilities let you prevent users from launching unauthorized applications, even inadvertently. You control user access to disk drives, communication channels, ports and modems to help prevent data loss through theft or negligence. A unique new feature is the ability to encrypt all allowed data and file transfers to USB devices.

### Detect and Prevent Host Intrusion

The newest addition to the LANDesk endpoint armory is LANDesk® Host Intrusion Prevention System (HIPS), a new plug-in for LANDesk Security Suite. HIPS provides a variety of non signature-based malicious code defenses to supplement antivirus and anti-spyware systems and to defend against zero-day exploits. Available application whitelisting lets you specify exactly which applications will be allowed to execute on a system. Proven heuristic and behavior-recognition techniques identify attack vectors and actions of malicious code. LANDesk® HIPS gives administrators a powerful new tool for controlling which programs execute on a system and the behaviors that approved applications are allowed to execute.

### Document Compliance and ROI

LANDesk Security Suite makes it easy to track and document the progress and ROI of security initiatives with a variety of reporting options. Detailed historical reports on policy enforcement and patch deployment are displayed in an easily understood graphical format that clearly documents policies, performance, problem areas and trends over time.

### Leverage LANDesk Expertise in Your Environment

LANDesk Professional Services let you draw on the experience, talents and abilities of the people who develop award-winning LANDesk solutions to help you evaluate your endpoint security requirements, then design, implement and maintain a multi-layered security solution tailored to your environment and operational requirements. Defined security-related service offerings include:

- **Health Assessment** – An evaluation of your LANDesk infrastructure, designed to ensure that your systems, security and process management applications are up to date and performing as expected. Assessment areas include architecture, performance, maintenance and security.
- **Patch Level Assessment** – Provides expert assistance and consultation in LANDesk® patch management configuration, vulnerability scanning, and scan report interpretation.

"When we first did our vendor analysis, the big thing to hit us was the complete integration of the LANDesk® Security Suite product. Looking across the marketplace, it was the only solution that truly integrated its patch management with its security management in a cost-effective single management console and a single engine approach. ...Not only does LANDesk Security Suite give us a very clear understanding of our patch penetration, but now we can often achieve complete patch coverage overnight rather than taking multiple days."

— **Joe Riesberg**  
Manager of IT Security and  
Regulatory Compliance  
VCPI