LANDesk® Security Suite

Active Endpoint Security Management

LANDesk® | make IT happen
An Avocent® Company

Active Endpoint Security Management for Your Enterprise IT Systems

Data security is one of the most pressing concerns of today's enterprises. Increases in malicious attacks can end up costing your organization countless hours and budget to bring your systems into compliance and to ensure you are properly protected.

According to a recent Gartner study, by the end of 2007, 75% of enterprises will be infected with undetected malware that evaded their traditional perimeter and host defenses. The threat environment is changing. Financially motivated, targeted attacks are increasing, and automated malware-generation kits allow simple creation of thousands of variants quickly. However, security processes and technologies haven't kept up. To be truly protected, network-based security is where it has to start—at the individual device level with secure configuration and access policies. LANDesk provides the technologies you need to keep pace with today's threat environment.

LANDesk® Security Suite: Peace of Mind in a Single Console

LANDesk® Security Suite lets you automatically detect and deploy security patches with active endpoint security management from a single console. With this solution you can:

- Minimize network downtime, reduce help desk costs and protect critical data and user productivity by protecting against malicious attacks at the endpoint.
- Reinforce your efforts to comply with security policies by proactively identifying and automatically remediating potential configuration threats.
- Save time and reduce resource needs by automating remediation with security rules, policies and frequent compliance scanning.
- Protect systems and critical data with active control over communication, data port and media drive access and the ability to quarantine devices.
- Easily align IT operations with corporate security policies by setting a security policy once that ensures desktops across the network are protected and compliant.
- Realize greater data leakage control with included USB encryption and lockdown and CD/DVD read/write control capabilities, allowing you to truly manage your most important business data.
- Boost efficiency and cut infrastructure costs with a strong, efficient patch management process, which can be automated by integrating the parallel patch process found in LANDesk® Process Manager.
- Demonstrate return on your investment in security initiatives with detailed historical reports.

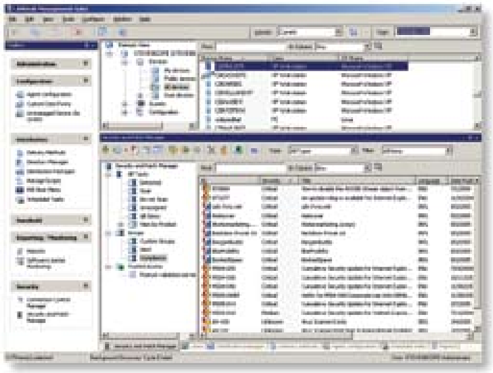
LANDesk Security Suite offers centralized management and protection of your IT assets from a single integrated console—giving you the power to boost system security and the value of IT throughout the enterprise.

Protect Your Enterprise

With LANDesk® Security Suite you minimize network downtime, reduce help desk costs, protect critical corporate data and ensure that users stay productive.

Again, using LANDesk® Trusted Access™ technology, LANDesk Security Suite lets you stop infected or unprotected systems from ever connecting to your corporate network. You control compliance standards and enforce security policies that endpoint devices must meet before connecting to, and in order to stay connected to, your corporate network—reducing the risk of downtime presented by infected machines and malicious intrusion.

> *"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



LANDesk® Security Suite moves beyond simple desktop lockdown to support advanced active endpoint security management. Built-in technology lets you block and quickly remediate outdated and unpatched computers and reduce the risks of downtime and malware infection. Once machines are connected to the network, another built-in technology—Connection Control Manager—checks for policy compliance before being allowed access. Then LANDesk Trusted Access acts as a catch for those unmanaged systems or guests on your network that may not have the same inherent policies on their systems. This two-pronged approach enables business continuity as both policy and compliance are enforced before allowing a connection to the corporate network.

Identify and Remediate

LANDesk® Security Suite's standard and high-frequency vulnerability scanning lets you detect antivirus, OS and application patch needs quickly and based on your own needs and chosen level of detail. Custom scans let you define the specific conditions scanned for. And threat analyzer lets you easily identify configuration risks.

Anti-spyware capabilities protect systems from attacks in real-time with access to LANDesk's regularly updated, comprehensive database of known spyware, adware, Trojans, key-loggers and other malware. Real-time alerting lets you easily stay on top of security needs and newly released definitions, their type and severity—so you and your IT team can put your energies elsewhere.

Connection Control Manager limits network access to authorized networks or IP addressees or blocks communication with specific networks. You control access to disk drives, communications channels and ports and modems to help prevent data loss and theft and protect against unauthorized access. Application blocking automatically stops prohibited applications from launching. And you can block applications from LANDesk Security Suite's extensive built-in list or create your own definitions.

Data leakage prevention permits greater control of portable media and protection of key corporate data. You can enforce policies that allow USB drives, CDs and DVDs to be "read-only." All file information that is transferred to a USB storage device is automatically encrypted, and you can keep tabs on your wireless network by discovering and classifying all unapproved wireless access points (WAPs).

Built-in antivirus enforcement lets you manage your chosen antivirus solution and enable and configure a Microsoft XP or Vista firewall directly from the LANDesk Security Suite console. And with LANDesk Security Suite's ability to customize the firewall configuration for individual systems or groups of systems, you can define your security policies for individual roles or intended use of a given device to further protect your enterprise. Firewall management policies also allow for different rules to be applied to each system based on the interface and the type of network your users connect to.

Patch management capabilities help you assess OS and application patch needs, quickly research and prioritize patches and automate patch distribution and maintenance. LANDesk® Targeted Multicast™ technology lets you speed patch deployments to multiple targets while minimizing the bandwidth used to reduce total network traffic without dedicated hardware or router reconfiguration. And LANDesk's automated patch deployment process lets you cache patches on computers. Once you decide to install the patches, simply accept the patches for execution to quickly patch and protect your systems. Easily automate this process with the inclusion of LANDesk® Process Manager Automated Patch Deployment. Set up new patches to automatically update and include this as part of your on-going process.

Comply with Security Policies and Prove It

With a solution to identify and stop security threats, you can easily comply with your security policies. Instead of leaving spyware and other issues up to individual end users, your security specialists stay in control of who has access to what and who can connect and who can't. You can set corporate security policies once and know that devices across the network are protected and compliant and that computers coming onto the network won't create havoc. And baseline configuration capabilities let you control who can alter your security policy.

LANDesk® Security Suite lets you easily track and demonstrate security initiative ROI with a variety of reporting options. Detailed historical reports on security policy enforcement and patch deployment are displayed in an easily understood graphical format that lets you clearly show progress on your security policies. You can identify what your security policy is composed of and quickly identify users whose Internet habits are perpetuating spyware on your network. And the LANDesk® executive dashboard presents a single, graphical view of the critical matters that concern your enterprise.

Access the Control You Need, When You Need It

Choose how and when to extend your systems and security management control with LANDesk's line of integrated solutions. Whether you start with one solution or several, they all work together smoothly, offering a single, intuitive management interface and the freedom to add solutions at any time.

Key Features

Network Access Control Capabilities

- Identify and quarantine out-of-date or unpatched managed and unmanaged computers using LANDesk® Trusted Access™.
- 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, key-loggers 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.

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.
- Know what new vulnerabilities a patch might introduce by seeing which patches depend on others.
- 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 www.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.

LANDesk® | make IT happen
An Avocent® Company