

# Press Release

---

## **LANDesk Helps Organizations Protect Against Data Leakage**

### *LANDesk Security Suite 8.8 offers increased wireless access point discovery, automated patch management processes and new USB encryption controls*

Salt Lake City – January 30, 2008 – LANDesk Software, a leading provider of integrated systems, security and process management solutions, today announced the immediate availability of version 8.8 of the company's LANDesk® Security Suite. This latest release has been designed to increase enterprise systems security by introducing new data leakage protection, wireless access point discovery, enhancements to patch management, host intrusion prevention (HIPS) and other enterprise level upgrades.

"Data leakage is a critical security issue that keeps security administrators up at night because of the widespread impact it has on an organization," said Steve Workman, vice president of product management, LANDesk Software. "USB thumb drives, iPods and smartphones all have the ability to carry large amounts of proprietary corporate information out of an organization without knowledge or oversight. By offering data leakage protection inside LANDesk Security Suite, customers now get a critical layer of data security on top of all of the other existing features and benefits of the suite."

The data leakage protection in Security Suite reduces the risk that corporate data will leave the corporation, whether intentionally or inadvertently. New USB encryption and read / write controls allow administrators greater discipline and control over the transfer of confidential information. Policies can be set to only allow the reading of content contained in various types of media such as USB, CD or DVD. Administrators can also enforce group, departmental or company-wide policies to encrypt all information transferred from a computer onto USB media for another layer of data leakage protection.

New wireless access point discovery capabilities secure the network by discovering unapproved wireless access points to prevent unauthorized data transfer. End nodes report to the LANDesk core management server the access points within sight of their wireless NIC while on the corporate network. Application blacklisting, using new unique configurations, allows administrators to control applications used by different individuals or departments to increase productivity and improve security. Various blacklists of applications can be created and policies can be applied to users or devices.

Additionally, new whitelisting and buffer overflow protection within LANDesk HIPS guard desktops from malicious software and exploits that take advantage of programs waiting on a user's input. Features such as learn-mode, protection against 'stack and heap-based attacks,' and support of all major third party antivirus vendors adds to the existing comprehensive features of host intrusion prevention.

"Desktop management solution vendors continue to integrate additional critical security layers into their solutions to ease the burden of managing multiple consoles to enforce corporate policies in order to comply with industry standards and regulations," said Jimmy Misenheimer, Information Systems Project Leader at Baptist Health. "And Enterprises are turning to security suites from systems management vendors for desktop security because of their expertise in desktop management."

Other enhancements to LANDesk Security Suite include improved performance and reduced footprint of integrated antivirus solutions, and centralized management of Microsoft XP and Vista firewalls. Upgrades to patch management include the integration of LANDesk® Process Manager's parallel patch process to automate the deployment of patches and improvements to the local scheduler, while alerting system and management reporting allows for greater administrative flexibility and enterprise management.

LANDesk's Network Access Control (NAC) is one of the most robust solutions available—supporting four different access methods including Cisco, DHCP, IPSec and 802.1X. Version 8.8 includes automated remediation of noncompliant desktops through the 802.1x network access control standard.

The new LANDesk Security Suite enhancements are all based on the company's automated management platform and integrate with the award-winning LANDesk® Management Suite, LANDesk® Server Manager, and LANDesk® Handheld and Embedded Device Manager. Additionally, LANDesk Management Suite 8.8 fully integrates with the recently introduced LANDesk® Management Gateway Appliance, the first LANDesk appliance for managing enterprise systems disconnected from the local network. The Management Gateway Appliance provides an easy configuration interface, automatic self update feature, as well as system configuration for backup and recovery.