

# Data Loss Prevention Starts at the Endpoint

---

Seeking Safety from the Data Loss Pandemic

## Contents

---

Introduction .....	3
Business and Financial Impacts Can Devastate .....	3
Endpoint Security Is the First Priority in Data Loss Prevention .....	3
LANDesk® Client Solutions Include Armor.....	4
Data Loss Vulnerabilities and LANDesk® Solutions.....	4
Advanced Systems and Security Management is a DLP Fundamental.....	5
In Data Loss Prevention, the Endpoint Is the Starting Point.....	6

This document contains confidential and proprietary information of LANDesk Software, Inc. and its affiliates (collectively "LANDesk") 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. Except as provided in LANDesk's terms and conditions for the license of such products, LANDesk assumes no liability whatsoever. 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 © 2008, LANDesk Software Ltd. All rights reserved.

LANDesk, Targeted Multicast and Management Gateway are trademarks or registered trademarks of LANDesk Software, Ltd. and its affiliated companies in the United States and other countries. Other brands and names may be claimed as the property of others. LSI-0732 04/08 JBB/NH/BT-FS

## Introduction

It's every CIO's nightmare: critical business data lost, stolen or maliciously exposed in a major breach of security systems or policy. It might be sensitive financial data, strategic plans, a new product design, customer account information or patient medical records. The vector of loss might be a stolen laptop, a misplaced disk or backup tape, a prohibited file-sharing application, a concealed thumb drive or a rogue wireless access point. The agent of loss might be an otherwise diligent manager with legitimate rights to the missing data, a disgruntled employee bent on revenge, or a professional thief executing a carefully orchestrated and targeted attack.

What is certain is that the frequency of major security failures, the scale of data loss, and the total cost of remediation and recovery are all skyrocketing. Consider the most commonly compromised class of data, personal identity information.

According to the Privacy Rights Clearinghouse (<http://www.privacyrights.org/>), the incidence of data loss and theft has increased by 1700 percent since 2004. More than 217 million records of U.S. residents were exposed due to security breaches between January 2005 and December 2007.

## Business and Financial Impacts Can Devastate

A recent study of the financial impacts of data loss conducted by the Ponemon Institute revealed that:

- The total costs of response and remediation associated with a major security breach and data loss—customer notification, compensatory services, opportunity loss, legal services, public relations, regulatory fines, brand damage and increased customer acquisition costs—rose 43 percent between 2005 and 2007 to an average of \$197 per record compromised.
- The average total cost per data loss incident was \$6.3 million.
- Lost or stolen laptops and mobile storage devices were the most common vectors of data loss, resulting in 49 percent of the breaches reported in 2007.

At the cataclysmic end of the impact range, 2007 saw the largest data theft ever reported; a wireless network break-in at a discount retail giant in which more than 94 million customer accounts were compromised, yielding credit, debit and drivers license numbers that were sold to identity thieves and credit

card forgers worldwide. At least 19 lawsuits were brought against the company, and investigations were launched by the Federal Trade Commission and 37 states attorneys general. The company recorded a \$107 million second-quarter charge to cover settlement costs, but a December article in InternetNews.com estimated total breach-related costs in the range of \$500 million to \$1 billion.<sup>1</sup>

Events like these are forcing organizations to devise comprehensive strategies to prevent data loss. Media and analyst attention has focused on network-based solutions to discover, classify and track sensitive information throughout the environment. While these approaches will undoubtedly figure in global strategies as they mature, they overlook a proven class of defensive tools that already exist in most enterprise environments, which can significantly improve data protection on the endpoint devices that are the most frequent point of security failure.

## Endpoint Security Is the First Priority in Data Loss Prevention

In fact, the most common vectors of business data loss all radiate from the desktop or laptop PC. They include the machines themselves—particularly laptops that routinely travel far beyond the enterprise perimeter, connect to many different networks, and are so frequently lost or stolen—and all of their peripheral storage devices, unsecured network interfaces, unauthorized software and ill-considered user behavior. Under-managed endpoints constitute a chronically porous perimeter where data can leak away undetected via USB devices, CD/DVD drives, and ad hoc bridges to Bluetooth personal area networks, 802.11 wireless LANs and P2P file sharing networks.

The most problematic of these are almost certainly the now ubiquitous USB devices—flash drives, portable disk drives, iPods and other portable media players. More than a billion of these extremely compact and portable devices have been sold, and they are now in common use in every environment, by conscientious employees, for entirely legitimate and productive applications. Their growing capacity and ease of concealment, however, have also made them a favorite tool of the data thief, adding thumb-sucking and pod slurping to the threat lexicon. A well-publicized demonstration of the latter stripped all the document files from a PC in just 65 seconds.

USB devices encapsulate the endpoint security challenge in miniature. Irresistibly useful and almost impossible to physically exclude from the environment, they must somehow be managed in a way that facilitates their productive uses and preempts malicious ones. IT's dilemma is how to secure its endpoint devices without impairing their users' productivity.

### LANDesk® Client Solutions Include Armor

Precisely because the PC and its peripherals are such a well-known knot of vulnerabilities, some of the most comprehensive armories of defensive tools and applications have been assembled within the leading enterprise suites of endpoint management and security software, of which LANDesk® Security Suite is a leading example. Protecting data on client systems has been a priority of LANDesk innovation from the company's inception, and significant new DLP functionality has been added in the current Security Suite release. Like all existing management, maintenance and security features, the new DLP capabilities are fully integrated into LANDesk Security Suite, and are implemented through a single client agent. The centralized management console controls endpoint discovery, patch management, access control, compliance enforcement, audit reporting and other security needs for the entire organization.

### Data Loss Vulnerabilities and LANDesk® Solutions

To better appreciate the breadth of DLP capabilities integrated within LANDesk® Security Suite, let's survey some of the most urgent client-side data vulnerabilities, and the features within the LANDesk® product suite that effectively secure them.

#### Problem #1: Data leakage via mass storage devices and removable media drives

As we noted previously, USB storage devices and media players are among the most common vectors of data loss, followed closely by CD/DVD burners and other removable media drives. Employees rely on them to store and transport data for entirely legitimate uses, but occasionally misplace the compact drives and disks. Not surprisingly, their ease of transport and concealment also attract a more predatory class of users, meaning that IT must find ways to control the use of such devices within the environment, and to secure the data those devices will inevitably carry beyond it.

- **The solution: Device read-write control and transfer encryption enforcement.** LANDesk® Security Suite provides IT managers with granular control of user access to portable

mass storage devices and media drives. Key features include read/write-level access control of all USB devices and removable disk drives. For the USB interface, it also provides an auditable record of file transfers to and from the client system, and supports encryption enforcement with the integrated LANDesk cryptography solution. The LANDesk client agent enforces access control policy with or without a connection to the corporate policy server—a critical consideration in preventing data loss from globetrotting mobile laptops.

#### Problem #2: Data loss through unauthorized applications

Another frequent culprit in data loss is unauthorized software running on the PC. IT must have the ability to control what applications can execute on its endpoints. The problem extends beyond common malware—viruses, Trojans, spyware and rootkits—and includes many different types of programs that can compromise host data, such as P2P file sharing applications that automatically set up network bridges, and may expose data even without the user's knowledge.

- **The solution: Integrated signature- and behavior-based execution control.** LANDesk® Security Suite offers IT complete control of what code can run on its endpoint systems. These include signature-based defenses such as real-time detection and removal of known viruses and other malware, and application blacklisting that works even when the client is off-network or the user renames the file.

To further defend against unknown applications, zero-day threats and targeted attacks, LANDesk Security Suite provides full integration with LANDesk® Host Intrusion Prevention System (HIPS), which adds a powerful combination of application whitelisting with heuristic and behavior-recognition techniques to detect typical patterns of malicious activity and effectively contain their sources, even in the absence of a known threat signature.

#### Problem #3: Data loss over unauthorized wireless connections

A third vulnerability that is frequently responsible for data loss or theft is a client connection with an unauthorized wireless network, including Bluetooth personal area networks, 802.11 wireless LANs and broadband wide area networks. An unmanaged wireless connection might be initiated by a Bluetooth device or wireless access point brought into the environment for an employee's personal convenience or for covert surveillance and traffic interception. A cellular WAN

link can be initiated from inside the perimeter by anyone with a service provider's PC card. Any of these connections can bridge the corporate network to an unknown environment, which can receive illicit data transfers or launch a targeted attack. IT must be able to control the communication channels of all clients in the environment.

- **The solution: Wireless channel access control and client-based access point discovery.** LANDesk® Security Suite places IT in charge of endpoint communications with access control over all client wireless interfaces, including Bluetooth, 802.11, and wide area broadband. In addition, an innovative new feature in the latest release uses client system wireless adapters to detect and report all APs within connection range. Network administrators can use the LANDesk management console to classify the reported devices and quickly identify rogue access points inside the environment or within eavesdropping range. Signal strength analysis at the reporting endpoints can even provide rough triangulation of the physical location.

Endpoint-based WAP detection significantly extends LANDesk's leadership in network device discovery, and offers IT an important new tool to protect the data on its client systems by knowing everything that exists within the enterprise environment.

#### Problem #4: Data leakage over ad hoc network bridges

Network bridging is an insider's data theft technique that involves simultaneously connecting to the corporate LAN and to an external wireless or dial-up network in order to inappropriately transfer data out of the secure environment.

- **The solution: Simultaneous connection blocking.** LANDesk® Security Suite provides a convenient setting that prevents a client system from initiating a wireless or dial-up connection while a LAN connection is active.

### Advanced Systems and Security Management Is a DLP Fundamental

Needless to say, the best solutions for endpoint data protection can't succeed if core capabilities aren't in place to manage configurations, maintain software, remediate problems and control client behavior on the network. LANDesk® Security Suite delivers a comprehensive solution set for every aspect of client management and security, all tightly integrated and centrally administered through a single management console.

- **Security configuration scanning** – Standard and high-frequency vulnerability scanning discovers antivirus, OS and application patching requirements proactively, at your own selected level of detail. Custom scans search for specific vulnerabilities, and threat analysis capabilities automatically evaluate configuration-related risks.
- **Antivirus management** – Choose and manage multiple antivirus solutions, and configure Windows firewalls directly from the LANDesk® Security Suite console. Enhance enterprise security with the ability to customize firewall settings for user job roles or unique system applications.
- **Spyware detection and removal** – Provides real-time protection against spyware, adware, Trojans, key-loggers and other malware with real-time threat alerts and direct access to LANDesk's comprehensive and constantly updated threat signature database.
- **Network access control** – LANDesk® Network Access Control (NAC) technology identifies and quarantines infected or unprotected machines so they can be repaired and updated as necessary before network access is granted. Compliance standards and policies are fully customizable, giving you granular control of endpoint-related risk.
- **Patch management** – Comprehensive patch management capabilities simplify patch research, acquisition and distribution. For example, LANDesk® Targeted Multicast™ technology expedites complex deployments to multiple targets and minimizes the bandwidth required for distribution. Parallel patching lets you cache updates on client machines for subsequent installation. Once you decide to install the patches, simply accept the patches for execution to quickly patch and protect your systems. You can 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 ongoing process.
- **Host intrusion prevention management** – LANDesk® Host Intrusion Prevention System (HIPS) technology enables lockdown of Windows startup modules and toolbars to prevent Trojan horses and spyware from quietly installing on endpoint computers and opening backdoors for attackers to steal data. Advanced rules allow IT to protect specific file types, such as documents, spreadsheets, etc. from unauthorized applications access.

## In Data Loss Prevention, the Endpoint Is the Starting Point

Data loss prevention is a war that must be fought day and night, without rest, on thousands of desktop and laptop battlefields, connecting inside the local network and traveling far beyond. Winning strategies will be as varied as the organizations designing them, but none will succeed without a comprehensive solution for securing the data on every client system and on all the devices that connect to it. Data security depends on a complete but flexible toolset capable of managing, maintaining and securing a diverse and mobile client population, in any location, at any time, without impairing the efficiency and productivity of its users.

That endpoint solution, LANDesk® Security Suite, is in daily use today, providing a multi-layered data shield for millions of desktops, laptops and other endpoint systems in the largest and most demanding business organizations worldwide. For more information on LANDesk® solutions for active endpoint security and data loss prevention, visit us at [www.landesk.com](http://www.landesk.com).

---

<sup>1</sup> 2007 Annual Study: U.S. Cost of a Data Breach. The Ponemon Institute.