Written by Andy Kellett, June 2005

TA000852SYM

Operations

Butler Group Subscription Services

Security Management

TECHNOLOGY AUDIT

LANDesk Software

LANDesk Security Suite (version 8.5)

Abstract *LANDesk Security Suite is a key component of the LANDesk Management Suite, which provides tools that enable organisations to manage their desktops, servers, and mobile devices. Within the LANDesk product hierarchy, LANDesk Security Suite is tasked to provide organisations with enterprise-wide security management services. Specifically, it takes responsibility for systems-level security and availability, covering; threat analysis (the identification of vulnerabilities and security holes); spyware and adware detection and elimination; connection management; application blocking (prohibiting specified applications from being launched); and vulnerability scanning (identifying the need for patch updates and facilitating their deployment). The strength of the LANDesk Security Suite comes from its ability to provide real-time monitoring and protection services in distributed and mobile environments, which is particularly relevant to small to medium enterprise organisations as they strive to deliver IT services that are able to keep pace with the ever changing needs of their business operations.*

KEY FINDINGS

- ✓ Provides a comprehensive range of discovery, monitoring, access control, management, and protection services.
- ✓ Delivers strong, centralised, device security management.
- *i* Security is a key module of LANDesk Management Suite.
- ✓ Provides integrated links to Patch Management, vulnerability assessment, and remediation/update services.
- ✓ Scans, detects, and has the ability to remove spyware.
- *i* Security Suite can also operate as a standalone solution.

Key: ✓ Product Strength ✗ Product Weakness *i* Point of Information

LOOK AHEAD

LANDesk Software will continue to extend the functional range and depth of its systems management tools to meet the continually growing expectations of the marketplace. For LANDesk Security Suite this means ensuring that the solutions discovery, monitoring, access control, and protections services incorporate functionality that is relevant to the latest threat models.

Butler Group

▶ FUNCTIONALITY

In today's fast moving business environment, IT and its supporting services is tasked with delivering business continuity across operations that constantly change, and across technology infrastructures where the boundaries and perimeters are no longer fixed. LANDesk Software, as a leading supplier of automated systems management services, has recognised that at all levels of the operational infrastructure there is a growing need to provide facilities that match up to the control and service delivery needs of its customers. Hence the company's focus on building technology solutions that enable IT administrators to automate the delivery of systems management tasks and proactively control the mainstream IT resources – servers, desktops, laptops, and mobile devices – that are used to deliver everyday business services. The LANDesk Management Suite is the company's overarching flagship solution for delivering business management services. However, as the product model continues to mature the company also recognises that service management and business continuity needs to be supported from a secure environment. It is delivering this through LANDesk Security Suite, a product suite that is seen as a key differentiator for the company when positioning the company alongside its key systems management competitors.

Product Analysis

As shown in the following architecture diagram LANDesk Security Suite has been developed as an integrated component of the LANDesk Management Suite with the intention of providing organisations with the real-time security services that are needed to support the ongoing operation of their businesses. It sits alongside the LANDesk Patch Manager to provide real-time security management services.

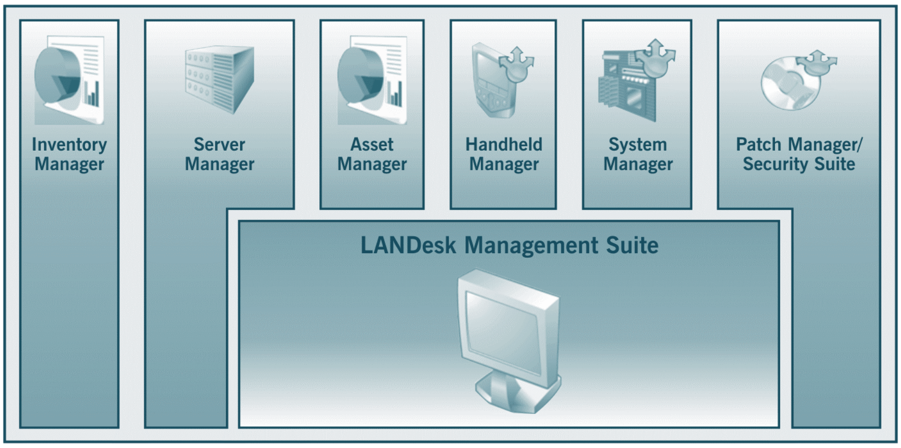

Figure 1: An Overview of the LANDesk Product Suite

Across the security industry there are a vast range of mixed and blended products that provide organisations with elements of monitoring and protection services. At this point in time, Butler Group takes the position that there are no vendors or solutions capable of addressing all the requirements of enterprise-level security. From a security perspective, we see each organisation as unique, their need for protection from malicious outside influences is consistent across all sectors of industry, but specific security requirements are driven by a combination of operational needs: for example, the requirement to open communications channels to third parties, such as business partners, and the associated systems complexity and management issues. Providing security solutions is no longer just about the delivery of protection services, there is now an inherent requirement for vendors to understand the individual needs of their customers, and to be able to react to those needs by providing solutions that deliver visibility and understanding alongside the protection model.

LANDesk Software achieves these objectives in a number of ways, but first of all its approach to IT security is in our view realistic. The company starts off by acknowledging that perfect device level security is almost impossible to achieve – a recognition that is somewhat refreshing in an industry sector that often stands accused of over inflating its own capabilities – but in doing so it also recognises that the successful delivery of security services through the use of technology can be empowered by good quality policy and process. LANDesk Software through the use of its proactive, policy-based, scanning, monitoring, and vulnerability management services is able to work with organisations to help them to understand their protection requirements and the actions that are needed to keep them operationally safe.

LANDesk Software does not pretend to have all the answers to the enterprise security management paradigm, but in saying that, in our opinion, neither does any of its competitors. Where LANDesk Software scores well is in its ability to blend together a range of security management products that are relevant to the needs of today's business community. There is a need to be able to support and protect complex and distributed network infrastructures, growing numbers and styles of mobile users, and the increasingly flexible and diverse range of third-party users that now demand access to corporate information and, without doubt, this is what the LANDesk Security Suite does best.

Furthermore, Butler Group believes that the LANDesk Security Suite is well positioned to deal with many of today's security challenges. As highlighted in the following diagram it deals with the key issues of security policy enforcement, and security management.

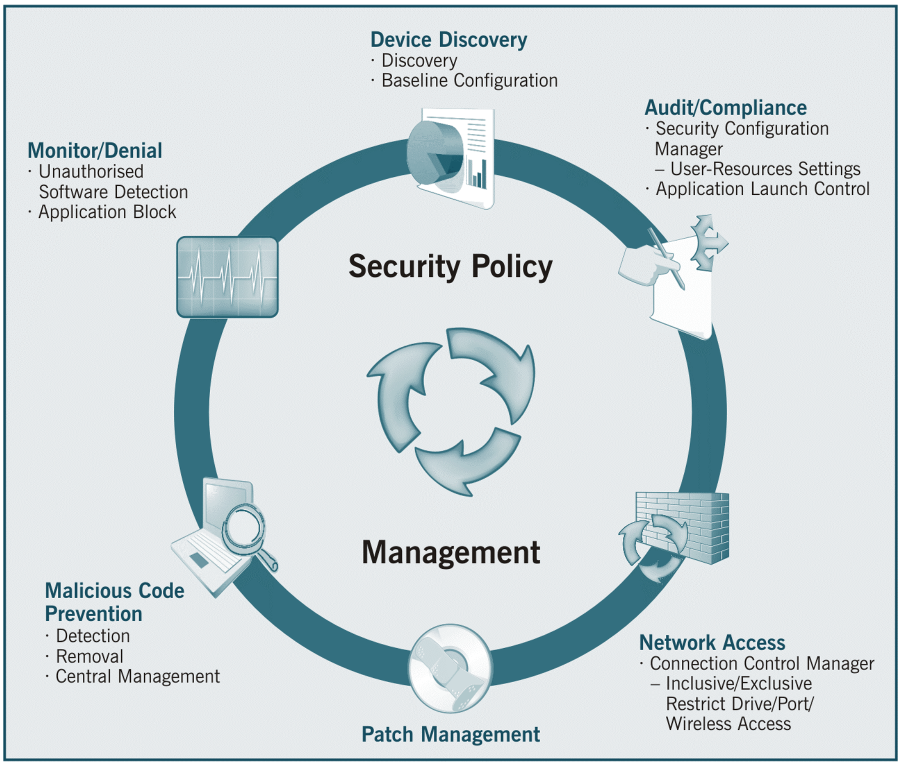
Device Discovery
· Discovery
· Baseline Configuration
Audit/Compliance
· Security Configuration Manager
– User-Resources Settings
· Application Launch Control
Monitor/Denial
· Unauthorised Software Detection
· Application Block
Security Policy
Management
Malicious Code Prevention
· Detection
· Removal
· Central Management
Network Access
· Connection Control Manager
– Inclusive/Exclusive Restrict Drive/Port/ Wireless Access
Patch Management

Figure 2: The LANDesk Security Suite

As shown in Figure 2 there are five core modules within the LANDesk Security Suite, and there is also an integrated link to the LANDesk Patch Manager Suite. The latest version of the new Security Suite is intended to deliver active, systems level, cross enterprise, security management. Functionally the solution is able to Analyse threats, scan for vulnerabilities, detect unwanted malware, block specified applications, and restrict/control the use of communications facilities.

Operationally it is able to:

- Identify security holes and existing configuration issues in order to support a safer real-time computing environment.
- Scan for vulnerabilities, and detect and report on patch update requirements.
- Detect and remove spyware, adware, Trojans, key-loggers, and other forms of malware, in order to protect against user and systems downtime.
- Inhibit selected applications from launching in order to protect against high-risk or corporate policy prohibited applications.
- Use management facilities to control and restrict communication to or from selected IP addresses, with the additional ability to lock down modem and USB ports.
- Provide automated Patch Management services through the security solutions integrated links to the LANDesk Patch Management component, so that devices can be kept secure and up to date with latest Operating System (OS) and application updates.

Other management components that sit within the LANDesk Management Suite product portfolio include the already highlighted LANDesk Patch Manager product that provides comprehensive and automated vulnerability assessment and patch management services.

LANDesk System Manager – that provides real-time component-level monitoring to ensure system health, availability, security, and configuration integrity.

LANDesk Handheld Manager – that provides the ability to manage handheld devices.

LANDesk Server Manager – that provides high levels of server availability and security through the use of its real-time monitoring and vulnerability management facilities, and through the use of its range of machine recovery tools that have been optimised to work in critical server environments.

LANDesk Inventory Manager – that provides automated asset discovery facilities at a network level, including hardware, software, network address structures, and includes attached devices, such as laptops, PDAs, and printers.

LANDesk Asset Manager – that provides organisations with the facilities to discover, track, and target systems assets.

Product Operation

Operationally the role of LANDesk Security Suite is to provide organisations with a centrally controllable security management facility. The justifications for deploying such a solution are many and various – increased risk of security breaches and the use of new threat models, spyware, key loggers etc.; the continued erosion of traditional network perimeters, and with it the reduced effectiveness of perimeter-based protection solutions; increased systems accessibility to third-party users and remote resources – the list goes on.

The supporting threat statistics can also make pretty uncomfortable reading: nine out of every ten PCs that regularly connect to the Internet are said to have been infected by the existence of spyware (with multiple instances in the 20s and 30s being fairly common). Also with a vastly increasing number of new threats being targeted at end-point devices – PCs, laptops, and other mobile connection devices – there is a growing requirement for solutions like the LANDesk Security Suite that can provide enterprise security management services.

In operational use the LANDesk Security Suite provides essential monitoring, identification, and where appropriate removal and reporting services. In the areas of spyware and its ilk the LANDesk Security Suite can be used to scan and detect the existence of spyware, adware, Trojans, key-loggers, highjackers, dialers, cookies, and other associated malware. In repudiation of the identified problems the solution can be used to remove identified spyware and to help immunise systems against problem re-occurrence. In support of the solutions removal and immunisation services, rollback and reporting facilities are provided to restore files and registry settings where necessary.

The solution's configuration verification and policy management facilities are used to eliminate potential security threats by verifying the legitimacy and applying rules to key systems activities, facilities, and services. These include amongst others:

- Administrator group memberships.
- Available shares.
- The presence of unnecessary services and facilities.
- Domain controllers.
- File system types.
- Guest account statuses.
- The status of Internet connection firewalls.
- Local account passwords.
- Operating system version controls.
- Password expiration requirements.
- Anonymous user restrictions.
- SQL guest and service accounts.
- Internet Explorer security settings.

The system's application blocker facilities are available for use in detecting applications from predefined and configurable lists, and content that is provided and periodically updated by LANDesk Software. Block and deny services can be used to deal with Trojans and worms, and in fact any other applications and transactions that do not conform to corporate policy standards.

LANDesk Security Suite also provides the ability to control client access to networks and systems by determining where each user is allowed to go. The solution uses an approved and disapproved list for authorised connections. In addition there is a facility to enable or disable network connections including: USB ports, modems, fixed and exchangeable disks and drives, systems ports (serial, parallel etc.), and wireless access.

Product Emphasis

Overall, the LANDesk Security Suite takes responsibility for the provision of device information management, systems vulnerability management, detection management, and protection management services, as well as supporting and underpinning audit and compliance issues. Associated patch management services; spyware detection; application monitoring; scanning and blocking facilities; and analysis and reporting services are also key elements of this extensive security service delivery tool set. All of which, Butler Group views as being relevant to the delivery of core enterprise security management services.

Although at the Client Systems Management (CSM)-level, LANDesk Software faces stiff competition from a number of established systems management vendors. It is the existence of the company's integrated Security Suite, and the extensive range of security and management services that the company has on offer, that Butler Group believes truly differentiates its overall product offerings from those of its competitors.

▶ DEPLOYMENT

As a key component of the LANDesk Management Suite, LANDesk Security Suite operates across the same range of platforms as its parent. The primary server requires Microsoft Windows 2000 or Windows 2003 server edition. Client support is provided for: Windows 9x, Windows NT, Windows 2000, Windows 2003, and Windows XP. In addition, the client also supports Macintosh (up to OS X), UNIX (HP-UX, AIX, and Solaris) Linux, Palm OS, and Pocket PC platforms. The data repository can be either Oracle or SQL Server, and LANDesk Software solutions are shipped with a runtime version of the Microsoft Database Engine (MSDE), with a schema provided on CD. There is also a Wizard provided to help users develop a schema if they prefer to use an existing database.

Although organisations could implement LANDesk Software solutions on their own, in the majority of cases the task is normally undertaken by the company's trained Expert Solution Providers (ESPs). An approach to deployment that is recommended by LANDesk Software, as certified ESPs have the required technical consulting, implementation, and support skills to architect and deploy the solution.

LANDesk Software systems deployments are not positioned as out-of-the-box solutions. Every organisation has its own individual requirements and, as is the case with any deployment that involves the use of CSM tools and Security Management services, Butler Group believes that it is extremely important to ensure that the services provided and their fit alongside the business operation is of paramount importance. In this case, following certification training, all relevant skills can be provided by the selected ESP. ESPs can also provide training to customers to enable them to manage their ongoing system requirements.

Project implementation times vary depending on the size, scope, and complexity of a customers requirements, and on the complexity of their operational infrastructures. Basic implementations can be measured in weeks – a recent 6K nodes/sets rollout for a customer was achieved in three weeks – but more complex and extensive deployments can be measured in months. LANDesk solutions can be deployed using a modular approach. Typically the first task that would be undertaken by an organisation would be auto discovery to check that the assets they actually have match those that they believe they should have. Once an inventory has been created the organisation is then in a position to decide what assets need to be managed and protected.

All of the LANDesk Software product components, including LANDesk Security Suite, require LANDesk Management Suite to be installed. The one exception to this is LANDesk Instant Support Suite, which can be used as a stand-alone helpdesk product.

LANDesk Management Suite licences are sold on a per node/seat basis, with a node/seat being a managed PC or a managed server. Consoles and required services running on servers are not charged for. Maintenance is charged at 25% of the licence fee, but is not mandatory. LANDesk Security Suite is sold on a perpetual license basis.

LANDesk Software believes that potential risks that might cause the project to fail, are centred around poor implementations carried out by non-technical staff, hence the company's recommended approach of using certified ESPs. Otherwise the only other issues may revolve around the incorrect scoping of requirements, which is common to many development projects, but should in this case be dealt with at the initial systems discovery stage.

▶ PRODUCT STRATEGY

LANDesk Software products are not seen as industry specific, although historically the company has been successful in the Finance, Government, Education, and Communications sectors. Its strongest market segments, in terms of business size, is typically 1,000 to 5,000 user organisations, although decent Return On Investment (ROI) has been achieved at the 250-user level, and the company's largest user has well over 100,000 users.

Going forward, LANDesk Software sees its key market opportunity coming from the convergence arena, with many customers needing to manage not only the resources of their own networks and clients, but also those that are connected to their clients – ensuring that the correct levels of security signatures and patching levels are in place, etc, which is an area of the CSM and security management market where LANDesk Software believes that it is ahead of its competitors. Butler Group agrees that the convergence and third-party management arena is going to be very important to many trading organisations in the near future, and we expect to see other mainstream CSM and security vendors also taking this potential market opportunity extremely seriously.

LANDesk Software's route to market is twofold, through channel partners – the company's ESP sellers – and through strategic alliances via OEM, ISV, and SI partner channels. Key business partnerships include ISVs such as BMC, BKSystems, Eden, FrontRange, Intuit, Microsoft, PeopleSoft, Peregrine, Remedy, Symantec, Touchpaper, and XcelleNet; Systems Integrators such as, ACS, Convergsys, IBM, IC3, Northrop Grumman, Siemens, and Unisys; and OEM partners such as Acer, Asus, Clearcube, Dell, Founder, Fujitsu, Gateway, Gigabyte, Hitachi, HP, Intel, Lenovo, Micron, Microsoft, MPC, NEC, TongFang, Toshiba, Touchpaper, and Wincor Nixdorf.

LANDesk Software typically makes one major release and one interim (refresh) release each year. The company also has a formal process in place to ensure that it keeps abreast of which enhancements are important to its customers and prevailing market conditions.

▶ COMPANY PROFILE

LANDesk Software was originally an offering from LAN Systems, and was created in 1985. The company, LAN Systems, was acquired by Intel in 1991, and the LANDesk product continued to perform well for the company over the next 11 years. Despite this, LANDesk was not a good fit for Intel's business model and after much discussion Intel formally decided to spin LANDesk off. LANDesk Software became a company in its own right on 18 September 2002 and the 90-day transition period ended on 18 December 2002. The new company, LANDesk Software Inc., has its headquarters in Salt Lake City, Utah in the US. It also has another office in the US as well as offices in the UK, Europe, Ireland, Japan, Brazil, China, and Mexico.

LANDesk Software is backed by three strong venture capital companies: The investor with the largest stake is Vector Capital of San Francisco. The other investors are vSpring Capital from Salt Lake City and Intel Capital.

In the two years or more since the new company was founded, LANDesk's employee base has grown from 125 to over 400 with revenues growing in parallel alongside. Since 2002 the business, which has just completed its 19th consecutive quarter of operating profitability, has achieved year-on-year growth averaging 57%. Operating across 18 countries through more than 4,000 specialised LANDesk software specialists, the company is localised in eight languages, which are: English, French, German, Italian, Brazilian Portuguese, Spanish, Simplified Chinese, and Japanese.

The stated goal for LANDesk Software is to become publicly traded within four years of its spin-off from Intel. The company is currently tracking slightly ahead of that goal and, subject to market forces, expects to achieve its target. Currently it is growing significantly faster than its market sector competitors, and although as a privately run company financial figures are not available, as already stated LANDesk is able to claim 19 continuously profitable quarters as testimony to its competitiveness and financial wellbeing. The company has shipped more than 250 million nodes of its management software to over 15,000 installations worldwide. Customers include: Honeywell, Reckitt Beckinser, Merck, and Henkel.

▶ SUMMARY

LANDesk Software, with the LANDesk Management Suite, is strongly positioned as an established and leading provider of CSM-based technology solutions. In Butler Group's opinion the addition of the LANDesk Security Suite as an integrated component of this enterprise management platform represents a significant step forward by adding security management into the mainstream CSM mix; something that many of its established competitors are only just beginning to consider. However, in this highly competitive market sector, size may be a limiting factor, although LANDesk mitigates against this issue through the use of its established range of business and channel partners to support its trading position.

Butler Group positions the company as being strong in the areas of market, technology, and thought leadership, and we would expect to see it continuing to develop its technology roadmap at the leading edge of the CSM arena. The key components of the LANDesk product set are all home owned, allowing it to develop integrated security and configuration management capabilities within the confines of a single enterprise platform.

▶ CONTACT DETAILS

LANDesk Software Inc. Headquarters
698 West 10000 South
South Jordan
UTAH 84095
USA

Tel: +1 800 982 2130

E-mail: info@landesk.com

www.landesk.com

LANDesk Software UK
Theale House, Brunel Road
Theale, Reading
Berkshire, RG7 4AQ
UK

Tel: +44 (0)118 9026200
Fax: +44 (0)118 9026566

E-mail: infoeurope@landesk.com

www.landesksoftware.co.uk

Important Notice: This report contains data and information up-to-date and correct to the best of our knowledge at the time of preparation. The data and information comes from a variety of sources outside our direct control, therefore Butler Direct Limited cannot give any guarantees relating to the content of this report. Ultimate responsibility for all interpretations of, and use of, data, information and commentary in this report remains with you. Butler Direct Limited will not be liable for any interpretations or decisions made by you.

About Butler Group: Butler Group is the premier European provider of Information Technology research, analysis, and advice. Founded in 1990 by Martin Butler, the Company is respected throughout the business world for the impartiality and incisiveness of its research and opinion. Butler Group provides a comprehensive portfolio of Research, Events, and Subscription Services, catering for the specialised needs of all levels of executive, from IT professionals to senior managers and board directors.