

The Hydra and the Onion

A Multi-layered Security Model for Today's
Dynamic IT Threat Environment

Contents

The Growing Complexity of Endpoint Security	3
Constructing the Iron Onion: Core Elements of Multi-Layer Security.....	3
Desperately Seeking Integrated Endpoint Security	4
Layered Security the LANDesk Way.....	4
LANDesk Endpoint Security: Layer by Layer	5
Wrap Your Assets in Layers of LANDesk Iron.....	6

The information in this document is provided in connection with Avocent/LANDesk products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Avocent's terms and conditions for the license of such products, Avocent Corporation and its affiliates, including LANDesk, ("Avocent") assume no liability whatsoever, and Avocent disclaims any express or implied warranty, relating to the sale and/or use of Avocent products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Avocent products are not intended for use in medical, life saving, or life sustaining applications.

Information regarding third-party products is provided solely for educational purposes. Avocent is not responsible for the performance or support of third-party products and does not make any representations or warranties whatsoever regarding the quality, reliability, functionality or compatibility of these products. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technologies discussed herein, and is advised to seek the advice of competent legal counsel, without obligation of Avocent.

Avocent retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Avocent makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein.

Copyright © 2008, Avocent Corporation. All rights reserved. LANDesk and Avocent are registered trademarks Avocent Corporation or its affiliates. *Other brands and names are the property of their respective owners
LSI-0xxx 0508 JBB/JJ/BT-FS

The Growing Complexity of Endpoint Security

It's possible, theoretically speaking, that somewhere there exists a job that grows simpler over time. It's certain, however, that securing all the endpoints in an enterprise IT environment is not that job. Criminal innovation is too creatively and maliciously engaged just outside every firewall and open port. That's the consensus view of industry analysts and security experts as captured in the spring crop of security trend articles and papers. Without exception these observers note that the threat environment continues to evolve rapidly. None of the trends they discern are the least bit likely to ease the CIO's insomnia.

- With improvements in operating system security, attack strategies have shifted to application-level vulnerabilities in browser, office, media player, backup and security software, often with botnet recruitment as the goal.
- Web-based attacks have increased dramatically, including not only phishing scams but attacks launched from trusted sites that have been compromised. Often these serve uniquely coded attacks to each visitor to evade signature-based security.
- Information theft is now the province of multi-national crime syndicates. Many corporate network intrusions are targeted attacks aimed at personal information and intellectual property theft, and launched from inside and outside the organization.
- The vectors of data loss are multiplying: notebook PCs are still the most common, but removable mass storage devices—particularly the ubiquitous and easily concealed USB drives—and ad hoc wireless network bridges are gaining fast.
- Malware innovation continues to accelerate. 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.

To defend their internal resources against this growing bestiary of threats, most organizations rely on a combination of firewalls, intrusion detection systems (IDS) and antivirus software. But while all these measures are unquestionably necessary, they are not an adequate defense against today's dynamic combination of evolving threats and diverse attack vectors.

Today's CIO might as well be battling the mythical Hydra—a nine-headed serpent that instantly grew two ferocious heads for each one cut off. The only way to effectively defend critical IT assets against such relentlessly inventive assault is to emulate the onion—to envelop every asset in multiple defensive layers that present many independent and qualitatively distinct barriers on every approach.

Constructing the Iron Onion: Core Elements of Multi-Layer Security

Implementing a multi-layer security strategy requires a diverse range of management and defensive capabilities, all of which should be network-based and capable of fully automated operation. A basic list of core functionality would certainly include:

Asset discovery and inventory

You can't secure a network without knowing what devices are connected and what software is running on those devices. Basic capabilities should include discovery and inventory of all connected hardware and software, regardless of whether a particular device is under management or a local firewall is operating.

Patch management

Staying current with operating system and application security patches is one of IT's most complex and labor-intensive workloads. A robust patch solution that includes scanning, vulnerability assessment, download and staging, distribution and maintenance capabilities is essential. Maintenance must extend beyond Windows and Office applications: non-Microsoft browsers, media players, backup and security software are increasingly frequent targets.

Malware protection

Malicious code defense should include several components: conventional signature-based antivirus and anti-spyware protection that is aggressively updated and centrally managed, combined with a host intrusion prevention solution (HIPS) capable of blocking unauthorized code execution and detecting irregular application behavior, even in the absence of a recognized malware signature.

Vulnerability detection and remediation

The ability to standardize security configurations based on business rules and user roles is essential, as is the ability to automatically scan for and remotely remediate non-compliant machines.

Network access control

Managing the configuration of machines already on the network is futile unless the same discipline is applied to those requesting new connections. Access control functionality is required that provides remote configuration assessment, with quarantine and remediation capabilities for non-compliant machines.

Data loss prevention

Removable mass storage devices and compact media have made it easy to copy, carry and conceal sensitive information, for legitimate and or malicious purposes. Data security requires the ability to enforce policy-based control over data movement, even by those with legitimate access rights.

Security status tracking and reporting

Organizations need the ability to document the implementation of security policies, compliance with those policies, and the ROI on security investment. Capabilities should include historical reporting, trending and performance analytics.

Desperately Seeking Integrated Endpoint Security

Two things are immediately obvious with even a quick reading of the diverse requirements listed above. One is that addressing all of these needs with separate point solutions would be prohibitively expensive and an administrative nightmare. The second is that significant overlap exists between the requirements of endpoint security administration and core PC lifecycle management. Not surprisingly, providers of both systems management and security products are moving to expand and consolidate their offerings into integrated solutions. A recent Gartner Magic Quadrant report¹ on Endpoint Protection Platforms aptly describes the current market environment.

“The traditional point product antivirus, anti-spyware and personal firewall products have been eclipsed by broader suites of related security technologies, which Gartner has labeled the endpoint protection platform (EPP). Basic component technologies in EPP suites include antivirus, anti-spyware, HIPS and a personal firewall. Advanced EPP suites will include network access control (NAC) and data protection technologies such as DLP and full disk encryption. The requirements for holistic NAC solutions and the demanding management needs of large enterprises are also forcing EPP suites to replicate some PC configuration life cycle management tasks, such as security configuration management, asset discovery, patching and software management. By combining multiple related technologies into a single management framework, EPPs have the promise of increasing security while lowering complexity, cost and administrative overhead.”

The authors go on to locate LANDesk in the visionary quadrant of EPP providers, returning, on the way, to the theme of advanced management functionality as a critical component of endpoint security.

“The management capability of EPP suites is a substantial differentiator. Simply maintaining the security status of large PC fleets that are increasingly mobile for long periods of time is difficult. As NAC becomes an integrated feature of EPP suites, management capability has been forced to expand from simply maintaining the security posture of the EPP components to checking the security configuration, software inventory and patch levels. The new EPP management consoles are beginning to add PC configuration lifecycle management capabilities to ensure the security and integrity of clients. Meanwhile, some PC lifecycle operations vendors are starting to add defensive security tools to their offerings. These two markets will continue to slowly converge, although it will not be until after 2010 that a significant percentage of the market will buy completely integrated tools from a single vendor.”

While Gartner’s timeline for integrated security adoption may be accurate for the industry as a whole, the fact is that existing LANDesk customers have a world-class solution for layered endpoint security that is already proven in the marketplace and ready for immediate deployment.

Layered Security the LANDesk Way

LANDesk’s approach to layered security begins with comprehensive hardware and software management capabilities and provides a logical, incremental path for organizations to add tightly integrated security features that leverage the same client-side software agent, server infrastructure and administrative console. LANDesk® Security Suite is designed to extend, complement and leverage LANDesk® Management Suite, and can itself be extended through two equally well-integrated add-on products: LANDesk® Antivirus and the LANDesk® Host Intrusion Prevention System. Where third-party products are already deeply embedded in customer security strategies, LANDesk provides full integration and centralized administration of these tools through the LANDesk management console.

The result is the industry’s most comprehensive and flexible toolset for layered security implementation in complex enterprise environments. With LANDesk, customers can deploy exactly the management and defensive technologies necessary to secure the critical assets in their own unique environments. They can manage all their security resources

through a single console, and automate routine processes to reduce costs and lighten administrative workloads. And perhaps most importantly, they can deploy a security infrastructure that will scale and adapt readily as business and technology requirements dictate

LANDesk Endpoint Security: Layer by Layer

To fully appreciate the range and power of LANDesk® software to implement flexible, highly customized, low-maintenance layered security solutions, it will be helpful to examine the unique functionality available to each layer.

Hardware and software discovery

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.

Intelligent patch management

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.

Versatile anti-malware protection

LANDesk Security Suite offers users two paths to known malicious code protection. You can manage your choice of third-party 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.

Flexible 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.

Vulnerability detection and remediation

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. Scanning and remediation capabilities can be extended beyond the corporate firewall with the LANDesk® Management Gateway, a plug-in appliance that lets you manage any mobile user simply and securely, using any existing Internet connection, certificate-based authentication and SSL encryption. Patent-pending LANDesk technology may eliminate 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 users'.

Network access control

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.

Data loss prevention

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 enforce encryption on all allowed data and file transfers to USB devices.

Host intrusion prevention

The newest addition to the LANDesk endpoint armory is HIPS, a new plug-in for the 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 typical patterns and actions of malicious code. LANDesk HIPS gives administrators a powerful new tool for controlling the code that executes on a system, and the behaviors that approved applications are allowed to execute.

Built-in compliance and ROI reporting

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.

Wrap Your Assets in Layers of LANDesk Iron

The bottom line on endpoint security is that today's threat environment is simply too dynamic for any point solution to afford effective protection. The only practical and survivable defensive strategy is to deploy multiple layers of protective technology, carefully chosen for tight integration, central management, and convenient automation.

LANDesk provides the industry's most comprehensive and fully-integrated solution set for layered security development. Beginning with the unparalleled system and software management capabilities of LANDesk Management Suite,

we add essential security technologies—data loss prevention, application control, malicious code protection, network access control, host intrusion prevention, compliance and comprehensive patch management—painstakingly integrating each new defensive increment into the common management framework.

In a world where the Hydra lurks just outside the firewall, nothing beats another layer of iron. For more information on LANDesk solutions for layered endpoint security, visit us online at www.landesk.com.

^[1] *Magic Quadrant for Endpoint Protection Platforms, 2007*. Peter Firstbrook, Arabella Hallawell, John Girard, Neil MacDonald. Copyright: Gartner, Inc. Published: December 21, 2007.