LANDesk® Solution Brief

Five Reasons to Reevaluate Your Security Strategy

Avocent | LANDesk®

The growing complexity of endpoint security creates extraordinary challenges for organizations. With the increased value of information and intellectual property, data theft has become the domain of well-organized crime syndicates seeking to reap financial gain. As a result, potential attack vectors continue to multiply and the threat landscape constantly shifts and evolves to stay ahead of security improvements in operating systems and applications. In an attempt to combat this growing array of threats to their information infrastructure, organizations often employ an arsenal of diverse security solutions, which not only lead to increased costs, conflicts, and complexity, but fail to provide the level of protection they really need.

To successfully secure their information infrastructure, organizations need to reevaluate their overall security strategy with the following five factors in mind:

1. Malware innovation continues to accelerate
2. Unmanaged mobile and remote users escalate risk
3. Data loss vectors continue to multiply
4. Today's multiple threat vectors require multiple layers of protection
5. Integrated management AND security creates a better managed and protected infrastructure

Malware Innovation Continues to Accelerate

The desire to tarnish a competing brand's image, gain a competitive edge by destroying or stealing intellectual property, or profit from the theft of sensitive customer data are all drivers to motivate full-time professional attackers to continually invent new and innovative ways to overcome organizations' standard security measures and defenses. As this type of malware innovation continues to accelerate, the time between known vulnerability to patch to exploit continues to shrink.

For example, on October 23, 2008, Microsoft released a patch that addressed a known vulnerability that affected millions of corporate computers. The day after the patch became available, exploits already began to surface. One of these exploits included the Conficker.C or "Kido" virus, a third-generation variation of the original Conficker virus.

The innovative variations to the Kido virus include measures to avoid detection and removal, along with new infection methods. It scans and kills processes for security products, including the disabling of firewalls, patch deployment, and antivirus software. Still, according to F-Secure, as of mid-January 2009, at least 33% of systems had still not been patched to protect against the Kido virus. [1]

This delay in patch deployment can be attributed to a number of factors, including the lack of automated patch management processes. However, since most organizations delay patch deployment by first staging and testing their patches in non-production environments before deploying them enterprise-wide, having automated patch management processes alone is not sufficient to combat the new breed of adaptive and innovative malware. This becomes even more evident with the rise of zero-day attacks.

To address these concerns, Avocent's LANDesk® solutions combat malware on multiple fronts. In addition to robust, automated patch management, LANDesk provides malware protection by combining host intrusion prevention systems (HIPS) with conventional, signature-based antivirus and anti-spyware protection that is aggressively updated and centrally managed.

LANDesk® Security Suite provides advanced vulnerability detection to automatically detect and remediate spyware, adware, Trojans, key-loggers and other malware. To further supplement the suite's antivirus and anti-spyware capabilities, it includes LANDesk® Host Intrusion Prevention System (HIPS) that employs a variety of non signature-based malicious code defenses to supplement protection against zero-day exploits.

LANDesk HIPS employs proven heuristic and behavior-recognition techniques to identify typical patterns and actions of malicious code, including kernel-level, rule-based file system protection; kernel-level, rule-based registry protection; system startup controls; multiple methods for detecting stealth rootkits; and kernel-level network filtering. LANDesk HIPS gives administrators a powerful tool to combat the rise of innovative malware by enabling them to control what code can execute on a system and the behaviors that approved applications are allowed to execute.

2 Unmanaged Mobile and Remote Users Escalate Risk

As an organization's mobile and remote workforce grows, its risk levels and security vulnerabilities increase as well. A key contributing factor to this risk escalation is the fact that few of these users regularly connect to the network. Launching their VPN client is often a bother. Many of these mobile or remote users only visit corporate or branch offices on rare occasions. The infrequency of connecting to the network prohibits organizations from regularly and consistently managing the system security of these endpoints, including keeping these systems updated in a timely manner with the latest patches and anti-malware signatures.

With the LANDesk® Management Gateway Appliance, organizations can manage these mobile and remote endpoints without requiring a dedicated leased line or VPN. The gateway appliance utilizes certificate-based authentication and SSL encryption to provide a secure transport from the corporate network to mobile and remote endpoints, enabling systems and security management of these previously unreachable endpoints whenever they connect to the Internet.

3 Data Loss Vectors Continue to Multiply

The threat of data loss grows as professional hackers look for and discover more avenues to steal valuable information. While the vectors for data loss continue to multiply, USB storage devices and media players are among the most common vectors, followed closely by CD/DVD burners and other removable media drives. Extremely compact and portable USB devices have become ubiquitous. Billions of flash drives, portable disk drives, iPods and other portable media players have been sold and have been put to use for legitimate and productive purposes. However, their ever-increasing storage capacity and ease of concealment make them a favorite tool for data thieves. Whether it's thumb-sucking or pod slurping, they can be used to strip a PC of all its document files in minutes or less.

USB devices create a significant endpoint security challenge. Due to their undeniable usefulness, they are almost impossible to physically exclude from an organization's environment. Still, they must be managed in a way that enables productive usage while preventing malicious manipulation. To address this need, LANDesk Security Suite provides IT managers with granular control of user access to portable mass storage devices and media drives.

LANDesk Security Suite provides read/write-level access control of all USB devices and removable disk drives. It gives organizations the flexibility to completely lockdown USB devices on certain groups of endpoints or all endpoints, keeping them from being able to write data through the USB interface. It provides the option to allow data to be written to USB devices only after proper user password authorization. Through its USB encryption capabilities, the solution can also enforce password protection of all data written to USB devices. Regardless of whether or not an endpoint is connected to the network, the LANDesk client agent enforces an organization's centrally managed policies for access control, which is a critical requirement for organizations with a mobile workforce.

To address other venues of data leakage, LANDesk Security Suite also provides wireless channel access control and client-based access point discovery. It gives organizations access control of endpoint communications over all client wireless interfaces, including Bluetooth, 802.11, and wide area broadband. In addition, it has the ability to leverage client system wireless adapters to detect and report all access points within connection range. This enables network administrators to classify 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.

Today's Multiple Threat Vectors Require Multiple Layers of Protection

To defend against the shifting and multiplying threats against their infrastructure and endpoints, organizations can no longer just rely on a combination of firewall, intrusion detection and antivirus point solutions. While these measures are necessary, they're inadequate against today's dynamic threats and attack vectors. To protect against the innovative and relentless nature of today's threats, organizations need to protect their assets with a multi-layered protection infrastructure comprised of automated core and incremental defensive technologies that work together to stop attacks at every level and entry point, while enabling their operation to be uniformly managed from a single, centralized administration console.

LANDesk offers organizations a simple, affordable and incremental path to layered endpoint security through a family of tightly integrated and automated solutions. These solutions work together seamlessly to provide coordinated security and management capabilities that are centrally administered through a single management console and that leverage the efficiency and reliability of a single client software agent.

Combination of Core and Incremental Capabilities

To successfully protect against the ever-changing and diverse multiple threat vectors, an effective multi-layered security solution must comprise an array of core and incremental technologies, including:

Asset Discovery and Inventory

It's impossible for an organization to adequately secure its network and endpoints if it doesn't know what endpoints it has connected to its network and what software those endpoints have running on them. Multi-layered security needs to include the basic capabilities of asset discovery and inventory for all connected hardware and software, regardless of whether a particular device is under management or a local firewall is operating.

LANDesk® Management Suite provides automated and transparent real-time, subnet-level discovery to locate and identify connected endpoints, inventory their assets, assess their configuration and management status, and determine whether they have a local firewall 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 network adapters to locate and classify all access points within and adjacent to the enterprise environment, allowing administrators to block access to those that are unauthorized.

Automated Patch Management

Staying current with OS and application security patches is one of IT's most complex and labor-intensive workloads. Consequently, too many organizations leave themselves vulnerable to unnecessary cost and risks by not implementing an effective patch management strategy. Some organizations lack procedural controls and processes that expose them to increased risk. Others employ manual processes that lead to errors and single points of failure.

An automated, robust patch management solution that includes scanning, vulnerability assessment, download and staging, distribution and maintenance capabilities is an essential component of any multi-layered security solution. Patch maintenance must also extend beyond Microsoft Windows and Office applications to other vendor software solutions used by the organization.

LANDesk® Patch Manager, included as part of the LANDesk Security Suite, automates vulnerability assessment and patch management across heterogeneous IT environments. It integrates vulnerability assessment, patch research, download, staging and distribution capabilities, plus it helps organizations establish and maintain baseline security, stability and performance of their different applications and operating systems.

LANDesk Patch Manager actively scans managed computers against industry-standard information sources to identify application and operating system vulnerabilities. It allows organizations to establish policies that automatically install specific patches for specific operating systems. Organizations can choose to apply different remediation methods for detected vulnerabilities, including autofix remediation that downloads and installs new patches automatically as they become available. It also monitors, tracks, and reports patch deployment to ensure correct configuration and successful remediation on each targeted endpoint.

Malware Protection

To defend against multi-point attacks inherent in much of today's malicious code, malware protection must comprise several components. These include 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. As mentioned previously, LANDesk delivers in all of these areas through its multi-layered security offerings.

Vulnerability Detection and Remediation

Organizations must be able to balance the requirements of endpoint security with the needs of user productivity. They must ensure that user endpoints are configured in a way that enables users to be productive, while not placing the enterprise at risk. This requires the ability to standardize security configurations based on business rules and user roles.

To address this need, LANDesk enables organizations to centrally administer configuration management policies for all endpoints based on the needs of individuals, groups, and job responsibilities. Moreover, it automatically scans for and remotely remediates non-compliant machines. Based on an organization's custom level of detail, the LANDesk solution offers standard and high frequency vulnerability scanning capabilities that quickly pinpoint configuration, patching and software update requirements, and other specific vulnerability conditions.

Data Loss Prevention

To prevent data loss, organizations must be able to enforce policy-based control over data movement, especially in terms of USB devices and other removable media. LANDesk provides flexible, policy-driven read/write-level access control of all USB devices and removable disk drives. LANDesk delivers wireless channel access control for all endpoints as well.

Proactive Mobile Management

To minimize the risks typically created by an organization's mobile and remote workforce, organizations must be able to extend their scanning and remediation capabilities beyond the corporate firewall. The LANDesk Management Gateway Appliance addresses this need securely without requiring VPNs or dedicated leased lines.

Security Status Tracking and Reporting

Regardless of how well protected an organization assumes it is, it places itself at significant risk if it can't measure the actual effectiveness of its security efforts on every endpoint. Organizations need the ability to report on and document the implementation of, and compliance with, security policies enterprise-wide.

LANDesk Security Suite lets organizations track and demonstrate security initiative ROI with a variety of reporting options. It provides detailed historical reports on security policy enforcement in an easy-to-understand graphical format that clearly shows security policy progress. It enables IT and security managers to see what elements and attributes make up their security policies. It also lets them quickly identify users that have Internet habits that tend to perpetuate spyware throughout the enterprise. Plus it provides security trend analysis and performance analytics. The LANDesk executive dashboard presents a single, graphical view of the critical matters that concern the enterprise.

Additionally, LANDesk Security Suite reports on endpoint update requirements, patch levels, patch deployment failures and success, and repaired patch histories. It reports on custom vulnerability parameters. It also provides real-time alerting of security outbreaks and breaches with control over which vulnerabilities will initiate an alert based on type, severity and other conditions.

Most Comprehensive and Flexible Layered Security Toolset

As the industry's most comprehensive and flexible toolset for layered security, the following LANDesk offerings provide the essential combination of integrated core and incremental capabilities needed in a successful multi-layered endpoint security implementation:

- **LANDesk Security Suite** extends active security management to all endpoints, providing integrated patch management, active threat analysis and remediation, spyware detection and removal, network access control, configuration security tools, and innovative connection control management capabilities such as USB encryption and removable storage management. The suite includes LANDesk Host Intrusion Prevention, which adds zero-day threat protection with behavior-based execution blocking that prevents malicious application attacks right on the host.
- **LANDesk Antivirus** adds best of breed, enterprise-ready virus protection, rootkit detection, quarantine capabilities and centralized management at a lower investment than other industry-standard solutions.

- **LANDesk Management Gateway** Appliance uses certificate-based authentication and SSL encryption to provide anytime, anywhere management over the Internet of mobile and remote endpoints, including the ability to perform patch management, update endpoint security policies, execute antivirus/anti-spyware enforcement and management, block applications, perform security threat management, and more.
- **LANDesk Management Suite** provides active control of an organization's computing platforms, including extensive platform support for Windows, Mac OS, Unix, Linux and handheld and embedded device operating systems. It enables organizations to demonstrate compliance to security and configuration standards. It includes inventory management capabilities that enable the discovery, inventory and configuration management of networked computing devices.

Integrated Management AND Security Creates a Better Managed and Protected Infrastructure

Too often organizations view endpoint management and endpoint security as separate endeavors. This perspective not only leads to significant security gaps, it creates excessive administration overhead and swells infrastructure costs and complexity.

As discussed, it's impossible to secure an endpoint if it can't be managed, and it's impossible to successfully manage an endpoint if it can't be secured. These facts alone drive the need for integrated endpoint management and security. However, other important factors exist that further drive the need for endpoint management and security integration.

Using management and security software applications comprised of diverse suites and point products can lead to conflicts on the endpoints and can even result in one agent disabling the other agent. For example, a security patch may not be applied because the antivirus agent disabled the patch agent. Such conflicts can cause downtime and expose endpoints to unnecessary risks. The lack of integration that exists between separate security and management products also hinders an organization's efforts to successfully secure all of their endpoint at every level and to protect them against every threat vector.

Additionally, deploying separate management and security solutions results in multiple agents running as their own individual processes on the endpoints. This can unnecessarily consume more memory and processing power than occurs with a single agent that provides both endpoint security and management.

And when it comes to training and IT skills, using separate security and management solutions requires additional training and increases the learning curve for IT personnel. In contrast, an integrated endpoint management and security solution that relies on a unified user interface and administration console reduces the learning curve, cuts down training costs, and facilitates cross-training of IT personnel.

What's more, an integrated endpoint security and management approach can significantly reduce cost and complexity in other areas. For example, not only are licensing costs generally higher when you add up the expense of deploying multiple point solutions or non-integrated management and security suites, these isolated solutions create significant infrastructure clutter that is more difficult to manage and maintain., plus there is often costly overlap that exists between these different solutions.

LANDesk offers systems lifecycle management AND endpoint security management capabilities that rely on a single agent, and that work in concert under the control of a single, easy-to-use console for the discovery, management, updating and protection all of an enterprise's deployed systems. This unified platform for both endpoint security and management enables organizations to implement specific solutions or a suite of solutions incrementally as their growing needs require.

When all is said and done, LANDesk enables organizations to implement the security and management capabilities needed to combat today's complex and ever-changing threat landscape. Organizations can secure and manage their endpoints in a way that not only strengthens their overall security, but also streamlines operations, reduces costs, enables higher service levels, and fosters greater business success.

References

1. "Kido Worm Keeps On Truckin' via USB Thumb Drives", Chris Maxcer, *TechNews World*, January 16, 2009

Visit www.landesk.com for more information.

Avocent | LANDesk®