Achieving Security Maturity

A Layered Approach to Endpoint Security

LANDesk® SOFTWARE

LSI-0909 1010 HB/BB/DL

Contents

Executive Summary

Criminal innovations in malware are increasingly creative and costly, and the threat environment continues to evolve rapidly. The volume of unique malware is expanding, with more and more of it being Web based. IT departments are responding with an increasing number of barriers to cyber attacks and data loss, not only because of the growing complexity of protecting data, but also to reduce the need to disclose an embarrassing loss of confidential customer data.

Companies' efforts to boost security may prompt them to react and purchase even more point products that may make them ***feel*** more secure rather than ***be*** more secure. These organizations tend to be more reactive in nature, which is the status quo among most organizations. The problem is this proliferation of advanced attacks doesn't allow you to simply be reactive any more. Companies with more mature security systems and practices take a more proactive stance to security. Being more proactive involves deploying multiple layers of integrated protective technology that make breaching networks more difficult. The following table indicates some of the tendencies of reactive organizations versus those that are more proactive or have more mature IT security:

Reactive Organizations	Proactive Organizations
▪ Low-level security ▪ Multiple point solutions ▪ Inefficient use of IT resources ▪ Manual methods to quarantine threats ▪ IT Security manages all security processes	▪ Multi-layered security ▪ Integrated security solution ▪ Processes that are reduced to minimal steps ▪ Automatic ways to quarantine threats ▪ IT Operations manages known security processes while IT Security continues to monitor and investigate threats

The LANDesk approach to layered security is to simplify each security layer. LANDesk begins with the comprehensive hardware and software management capabilities of LANDesk® Management Suite, which 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. These capabilities include anti-malware, device and application control, data protection, application whitelisting, firewall, host intrusion prevention (HIPS), network access control (802.1x), and comprehensive patch management. Each new defensive increment integrates into the common management platform and works as one cohesive application.

This paper reviews why organizations need a mature, layered approach to create security management and how LANDesk can help customers meet their need for a layered approach.

Growing Complexity in IT Security Requires Mature Security Management

The need for more resilient endpoint security is growing. Today's IT threat environment presents extraordinary challenges for IT organizations struggling to secure large numbers of desktop and mobile laptop PCs. With an even more mobile workforce using multiple devices that access corporate resources, it's even more important that IT security take in to account the user's location and the context around whether they are inside or outside the firewall. The financial impacts of major breaches are staggering; the landscape of vulnerabilities and potential attack vectors are constantly shifting and evolving. Today's threat environment is simply too dynamic for any point solution to afford effective protection.

Consider the growing threats that IT departments face every day:

- With improvements in OS security, attack strategies now focus on exploiting the vulnerabilities of applications, including browsers, office productivity tools, media players, backup software, smart phones, iPads, and even security software. Often the goal in these attacks is botnet recruiting.
- Web-based attacks have increased dramatically, including not only phishing scams but also 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 multinational 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. These attacks are usually detected after the intruders are long gone.
- 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.

In addition, greater cooperation and collaboration between the IT Security team and the IT Operations team within an organization is needed. In many cases, these two IT groups within an organization are at odds. IT Security is worried about risks and threats, defining policies, and assessing the environment, while the IT Operations areas—server admin, network admin, and desktop admin—fret over availability and performance, keeping an environment stable, managing change, and not allowing anything in that will disrupt availability and performance.

IT Security often drives policy and recommends and deploys new technologies rapidly in reaction to attacks and threats, sometimes forcing technology into the environment that may have management or performance issues. IT Operations is looking for technologies that have consolidated interfaces, administration, reporting, and workflows that won't cause foreign disruption to availability and performance.

Speaking at the 2010 Gartner Security & Risk Management Summit outside Washington, D.C., vice president and distinguished analyst Mark Nicolett said in the Best Practices in IT Security and IT Operations Integration session:

> "As information security threats and the technologies for dealing with the threats mature, these activities should be turned over to the operations side of the IT organization. Your information security organization should be focused on emerging new threats and technologies. This requires that the information security team 'let go' of the more routine, mundane threat protection technologies. A good example of this are viruses (the threat) and antivirus (the protection) technologies. They're well-understood with mature technologies. The desktop operations group should handle the antivirus software and signature updates. Information security may set the policy, but operations runs the show. Another example is patch management, which should be merged with software distribution—why have two groups and two processes doing this separately? This does not mean that information security and operations converge. Rather, each focuses on what it does best. Operations people don't want things to change, and this isn't always the right approach when security threats are involved.
>
> "Let your information security professionals focus on what they do best, and address new threats effectively. Let your IT operations professionals focus on what they do best, and operate the mature systems efficiently." [1]

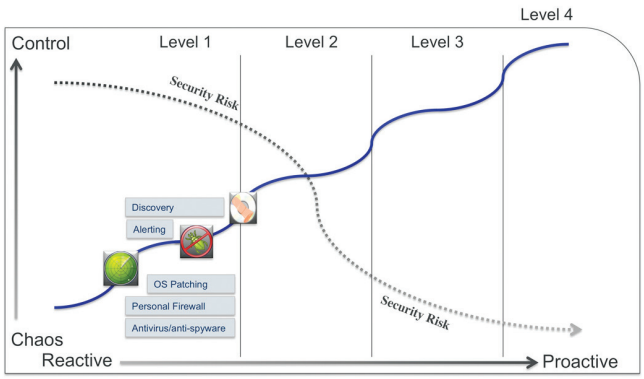
IT Security professionals have a few choices available in order to drive their organizations toward more mature security solutions. They can continue to deploy point solutions and then try to manage them separately or have IT Operations manage them. They can deploy point solutions and "rip and replace" them as they find more consolidated security solutions. Or, they can find a solution that ties into IT Operations workflow for managing endpoint devices and leverage integrated security at multiple layers.

A Mature, Systematic Approach to Security Management

The path to security maturity requires a diverse range of layered endpoint protection, management, and defensive capabilities, all of which should be integrated and capable of fully automated operation.

Level 1: Start with a Strong Perimeter and Asset Intelligence

As illustrated below, the first step toward developing security is to understand what software and hardware are in the environment, implementing the first barriers to malware attacks, keeping all the operating systems patched, and generating reports to show the security status at any given time.



Endpoint Security Maturity Curve

Asset Discovery and Inventory

It's also important to see not only the devices you manage, but all devices connected to your network, because you cannot secure a network without seeing what's connected and what software is running on those devices. You need the capability

1 Mark Nicolett, "2010 Gartner Security & Risk Management Summit, National Harbor, MD, "Best Practices in IT Security and IT Operations Integration" session speaker notes, slide 4.

to discover assets across the enterprise network, whether they are at the corporate site or in remote locations, and maintain that inventory in real-time.

Malware Protection

As a baseline of security, you need malware software such as antivirus and anti-spyware in place to block or protect against specific threats. These security applications are continually updated with new malware patterns to be able to block known attacks. However, blacklisting is becoming less effective against the surging volume of new threats and is almost useless against targeted threats.

As a result, many companies are bolstering their security with non-signature based solutions such as application control and whitelisting in order to block all but specific applications, or to block the use of any non-approved applications. In addition, malicious code defense should include other components, such as conventional signature-based antivirus and anti-spyware protection that is aggressively updated and centrally managed. This should be combined with a host intrusion prevention solution (HIPS) capable of blocking unauthorized code execution, protecting from buffer-overflow exploits, and detecting irregular application behavior, even in the absence of a recognized malware signature.

Personal Firewall

For more protection, IT administrators should employ a personal firewall that blocks specific in-bound or out-bound connections. The best firewalls can dynamically change blocking actions depending on whether the machine is connected to a trusted or a non-trusted network, and can even alert and log any firewall violations. Some firewalls go even further, restricting which applications may access the network, and how.

A firewall for end users is normally placed between a protected network and an unprotected one. It acts like a gate to protect assets to ensure that nothing private goes out and nothing malicious comes in. The personal firewall can be configured to allow or deny incoming and outgoing connections and can alert IT about any violations and then log them. Some firewalls can change policies based upon whether the user is on a trusted or a non-trusted site. The firewall can also control or block applications to help minimize the corporate risk

Operating System Patch Management

Maintaining patches to Microsoft Windows and other operating systems is vital to reducing the security risks associated with OS vulnerabilities. Here, discovery and inventory are key to awareness of what is on the network. You can then establish policies that install patches automatically for specified operating systems. In addition, automatically downloading and installing new patches as they become available reduces effort and risk.

The LANDesk Approach:

When it comes to **asset discovery and inventory**, LANDesk Management Suite users are accustomed to the convenience and transparency of real-time, subnet-level discovery technologies that 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.

LANDesk offers organizations two paths to **malware protection to make life easier**. You can either use LANDesk malware solutions or you can manage third-party antivirus and spyware point products from a single LANDesk console. If you choose to use the world-class LANDesk® Antivirus solution, the malware protection integrates with LANDesk Management Suite and LANDesk Security Suite and provides single-agent simplicity while letting you see all the security activities in one console.

LANDesk Antivirus is powered by the Kaspersky Lab engine and signature databases to deliver outstanding protection against viruses, worms, trojans, spyware, rootkits, and other malicious code, with hourly updates from the industry's most complete threat signature data base. Combining the speed and incremental pattern file updates of Kaspersky Lab with patented LANDesk distribution technologies eases the headache of updating the clients without impacting the network.

LANDesk also delivers antivirus protection for mail servers. The LANDesk® Antivirus – Mail Server solution adds another protective layer to endpoint security to safeguard your corporate mail servers against external threats, prevent virus outbreaks within corporate networks, and filter out unsolicited

email. Its main mission is to defend mailboxes, public folders, and relayed email located on Microsoft Exchange Server against malicious programs. It does this by scanning email traffic and messages in mailboxes and public folders, and by disinfecting infected objects using information in the current version of its signature databases.

You can choose LANDesk Antivirus software by simply selecting one button in the management console and LANDesk does the rest—from removing your previous antivirus application to pushing LANDesk Antivirus out to all machines.

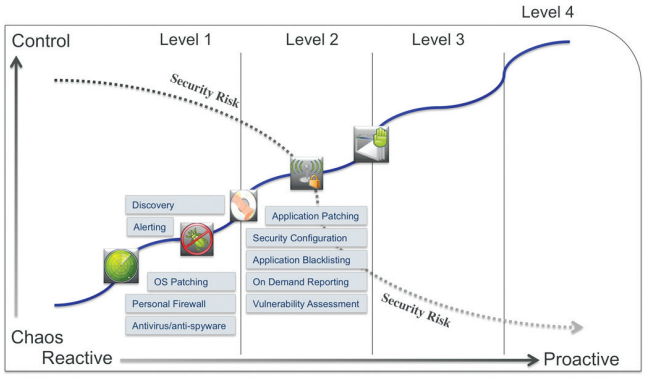
If you choose to keep or implement an antivirus point product from another vendor, LANDesk Security Suite manages other antivirus products from CA, ESET, Kaspersky Lab, McAfee, Sophos, Symantec, or Trend Micro directly from the LANDesk central management console. You're free to determine how best to protect your organization and LANDesk solutions can support your plan.

The LANDesk endpoint **personal firewall** limits access to authorized networks or IP addresses to ensure increased system protection and to dramatically reduce the potential for effective system attacks. From a simplification standpoint, you don't need to implement multiple consoles and multiple agents, reducing the cost of supporting different point solutions. The firewall technology in LANDesk Security Suite requires only a single point of management for application control and firewall configuration. IT administrators can allow or deny incoming or outgoing connections, and can deliver alerts and log firewall violations. LANDesk location-aware policies support your efforts to reduce the chance of data loss and infection with dynamic policies that adjust security settings—including application control, anti-malware configuration, and removable storage restrictions—based on the environment a given machine is in.

With LANDesk Security Suite, administrators can also centrally enable and configure the Windows firewall 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.

Level 2: Become More Proactive with Greater Intelligence and Systematic Remediation

With the security foundation established, IT departments look to become more proactive via vulnerability assessment, application patching, whitelisting, and application control.



Endpoint Security Maturity Curve

Vulnerability Assessment

Vulnerabilities are weaknesses in the overall security of a device. Threats exploit those weaknesses resulting in potential damage to the computer or personal data.

A company's IT department needs to assess the vulnerability of the environment and determine what can be done to protect company assets. Once IT staff sets the user roles in the organization and the security policies for the IT environment, they can then assess any potential security flaws and fix them before a breach occurs.

Application Patching

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

Whitelisting and Application Control

Organizations with greater security experience and maturity have witnessed that blacklisting alone is ineffective, so they have come to rely on a combination of blacklisting, firewalls, intrusion detection systems (IDS), and antivirus software. While all these measures are necessary, they are inadequate against evolving threats and diverse attack vectors, which

prompts organizations to employ whitelisting to declare what applications and connections are allowed and block the rest. When whitelisting is done right, it may reduce the need for blacklisting and antivirus applications.

According to Gartner, Inc.,

> "Standard anti-malware signature engines are rapidly losing effectiveness against the surging volume of new threats, and have very little value against targeted threats. Non-signature-based solutions (such as a host-based intrusion prevention system—HIPS) and proficient operations procedures (such as asset discovery, configuration management, vulnerability assessment, software management and whitelisting) are needed to help inoculate PCs against unknown threats." [2]

LANDesk Security Suite makes it easy to implement a whitelisting strategy. First, you can set up the whitelisting to learn from existing behaviors of your applications and then set policy establishing what is acceptable with existing applications, blocking other applications that may contain malware, which would infect your environment. You can define trusted and non-trusted networks using LANDesk location-aware functionality and then set the policies for the entire enterprise. All of these policies can be seen in a single view on the IT administrator's console. The ability to define location-aware policies enables you to "loosen the reins" or tighten security policies within your enterprise.

Many IT departments are discovering the benefits of using host-based intrusion prevention (HIPS) technology as part of their endpoint security. HIPS technology integrates a firewall, sandboxing, and application controls of various system-level actions. It is useful in protecting laptops that are used in non-trusted environments (such as hotel Wi-Fi networks) and also helps prevent rogue applications from performing malicious actions. Once the HIPS function finds suspicious behavior, it not only prevents the behavior, it can alert the IT administrator of a problem.

Buffer overflow protection has become an important component of HIPS. This capability protects the environment against exploits that take advantage of programs awaiting user input. Buffer overflow protection enhances the security of executable programs by detecting buffer overflows on stack-allocated or heap-allocated variables as they occur, and preventing them from becoming serious security vulnerabilities.

In a September 2009 SANS Institute report, we see that operating systems appear to be the target of many attacks:

> Operating systems continue to have fewer remotely-exploitable vulnerabilities that lead to massive Internet worms.
>
> Other than Conficker/Downadup, no new major worms for OSs were seen in the wild during the reporting period. Even so, the number of attacks against buffer overflow vulnerabilities in Windows tripled from May-June to July-August and constituted over 90% of attacks seen against the Windows operating system. [3]

The LANDesk Approach:

LANDesk Security Suite simplifies IT's effort to become more proactive in establishing security maturity. The solution provides standard and high-frequency **vulnerability assessment** scanning capabilities to pinpoint configuration, patching, and software update requirements quickly and easily. You can set up custom scans to define the levels of detail to search for specific condition sets. Defining and maintaining secure configurations is simplified with role-based administration and policy-based management tools.

LANDesk also provides the broadest vulnerability assessment for thousands of applications, enabling you to view potential risks and determine whether you meet company standards. This is particularly important if your organization needs to comply with standards such as:

- PCI – Payment Card Industry
- FDCC – Federal Desktop Computer Configuration
- SCAP – Security Content Automation Protocol
- FISMA – Federal Information Security Management Act
- HIPAA – Health Insurance Portability and Accountability Act

LANDesk **intelligent patch management** is part of LANDesk Security Suite, which provides integrated vulnerability assessments, patch research, downloading, staging, and distribution capabilities for operating systems and applications in mixed IT environments. The patch solution supports various Windows operating systems as well as Macintosh and Linux operating systems.

2 Peter Firstbrook, Arabella Hallawell, John Girard, Neil MacDonald. "Magic Quadrant for Endpoint Protection Platforms"; Gartner, Inc., May 4, 2009, p. 2

3 "The Top Cyber Security Risks", SANS Institute, September 2009 ; http://www.sans.org/top-cyber-security-risks/

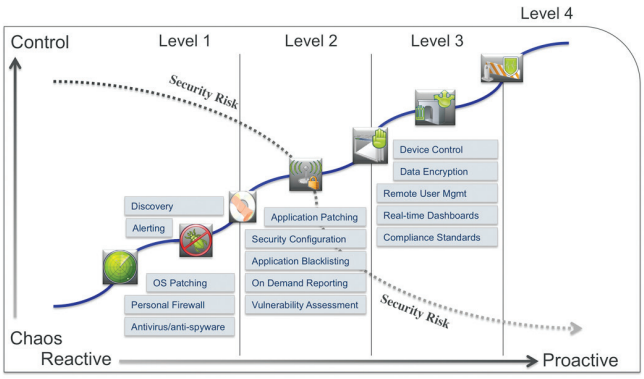
LANDesk® Targeted Multicast™ and LANDesk® Peer Download™ technologies accelerate deployment and reduce distribution bandwidth requirements with no additional hardware or router reconfiguration. For example, one large multinational company deploys patches to more than 77,000 nodes throughout the world using just five servers, and achieves over 95% remediation within five days. Another organization sent out more than 846,000 patches to 118,000 nodes in February 2010 alone, with a 95% success factor.

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.

LANDesk® Host Intrusion Prevention (HIPS), a feature in LANDesk Security Suite, provides **application control** for a variety of non signature-based malicious code defenses and application control to supplement antivirus and anti-spyware systems and to defend against zero-day exploits where malware patterns are not available. Proven behavior-recognition techniques block malicious activity. LANDesk HIPS is a powerful tool for controlling the applications that execute on your systems, and specifies which behaviors the approved applications are allowed to perform.

Level 3: Protect What's Important On the Inside—Your Data

In order to comply with corporate security policies and regulatory requirements, companies must do what they can to maintain the security of corporate confidential information and personal information (both employees and clients/customers). In this third level of security maturity, it is vital to encrypt data and to set and enforce policies at the end user.



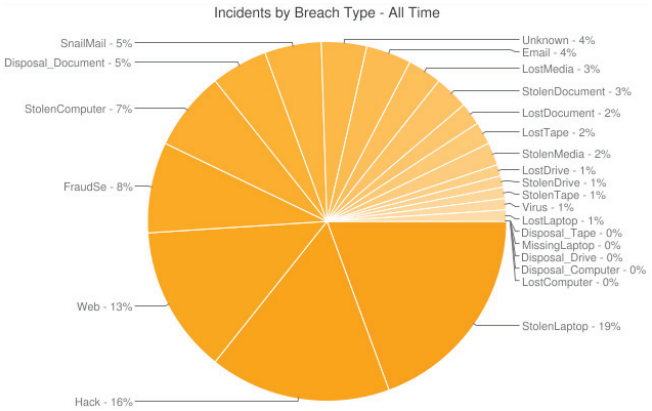
Endpoint Security Maturity Curve

Device Control and Data Loss Prevention

IT departments need to set company confidentiality policies and then identify policy violations and potential data leaks easily. It's even better if IT can block high-risk actions (such as copying company confidential files) and control user access to disk drives and communication channels to help prevent data theft.

Data Encryption

Removable mass storage devices and compact media have made it easy to copy, carry, and conceal sensitive information, and have also become a handy vector for spreading malware. According to the Open Security Foundation's DataLossDB, which gathers information about events involving the loss, theft, or exposure of personally identifiable information, approximately one third of data loss incidents are attributed to lost or stolen computers, laptops, drives, and media.



Source: DataLossDB.org

Data security requires the ability to enforce policy-based control over data movement, even by those with legitimate access rights. You should also prevent users on a wired network from bridging to unsecured networks and transferring data outside your IT environment.

Encryption comes in many forms, including user data encryption that protects information that only an individual user should see (e.g. Social Security data), external media encryption for USB, iPod, and other external storage devices, and system data encryption.

Mobile and Remote Users

IT departments want to gather hardware and software inventory, assess vulnerabilities, and remediate any risk concerns, whether the user is at corporate headquarters, in a remote office, or perhaps out of the office temporarily. The goal is securing the network without getting in the way of

user productivity; e.g. not locking out a user who reconnects to the corporate network after being on the road and instead updating their applications and operating system as they reconnect. Being able to carry out antivirus enforcement, management, and blocking applications for users outside the corporate firewall is vital to maintaining a secure environment.

Maintaining Compliance for Data Security

Many think complying with regulation like PCI, SCAP, FDCC, etc., is an onerous task that adds little value to security. In fact, complying with such standards enhances the company's security posture because these standards require organizations to follow best-known practices that fill in gaps that may have otherwise been missed.

For example, many regulatory standards require strong passwords that are at least eight characters long, with a combination of upper and lower case, numbers, and symbols, and that do not include the user's name. Thus a password like 'steve' would be rejected because it would be easy to guess, whereas "$teVe136" would be acceptable and less likely to be a vulnerability that could allow a security breach. Such strong passwords would help prevent the Conficker/Kido worm from co-opting a machine.

Compliance with such standards is an indicator of your organization's security maturity, provides a guide for the best security practices and a way to check an IT environment, and helps protect user and customer data.

Real-time Dashboards (Layered Views)

event occurs. Having a dashboard that lets you control the information that steams in makes recognizing problems easier, and being able to customize the dashboard to the company environment makes managing security still easier and boosts the confidence of administrators.

The LANDesk Approach:

Device Control Manager, another core technology in LANDesk Security Suite, allows you to set your **device control and data loss prevention** policies and identify policy violations and potential data leaks easily. Device Control Manager logs the files that are copied to removable media and even maintains a shadow copy. You can see what was copied and the device blocking actions in a single activity window. You control user access to disk drives, communication channels, ports, and modems to help prevent data loss through theft or negligence. A new feature is the ability to enforce encryption on all allowed data and file transfers to portable devices like USB sticks.

CREDANT **data encryption**, available from LANDesk, fills the security gaps left by file-folder based encryption products, while avoiding the management, data recovery, security, and productivity issues associated with full disk encryption or hard disk encryption solutions. You can quickly distribute powerful data encryption technology to all endpoints via LANDesk management tools to encrypt user data; application data; and external media such as USB sticks, external drives, iPods, SD cards, etc. You can also protect data from access by unauthorized users as well as safeguard data that's not protected by other encryption layers.

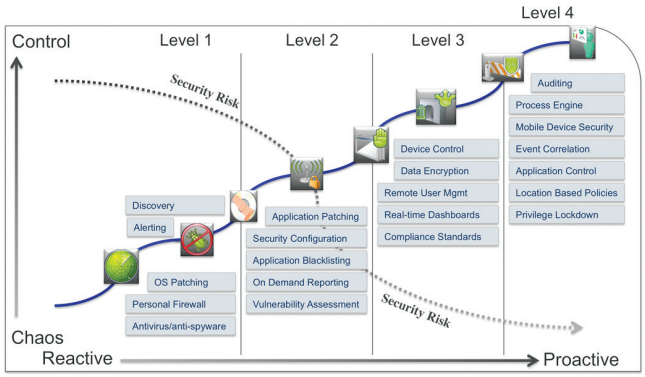
The capabilities of LANDesk Security Suite can be extended **beyond the corporate firewall** with the LANDesk® Management Gateway Appliance, a plug-in device that lets you manage any mobile user simply and securely, using any existing Internet connection, certificate-based authentication, and SSL encryption. The appliance helps you ensure that mobile users receive patches, AV signatures, and other configuration updates seamlessly while they are on the road, ensuring that when they return to the home network, they are already compliant with your security policies. This gateway technology can eliminate the need for VPNs, leased lines, or local management servers and enables you to manage remote machines centrally and proactively, on your own schedule, not the users' schedules. The LANDesk Management Gateway Appliance lets you manage systems anytime, anywhere—without punching a hole in your firewall. It includes automatic redundant backups to ensure configuration and log information is always available.

LANDesk Security Suite enables you to conduct comprehensive assessments to **enforce alignment with compliance standards** such as PCI, FDCC, SCAP, and SOX.

In addition, a variety of **robust reporting capabilities**—including trend graphs as well as security policy and spyware reports—ease the tracking and documenting of security initiatives. Detailed historical reports on policy enforcement and patch deployment are displayed graphically that clearly documents policies, performance, problem areas, and trends over time. This type of compliance reporting is mandated when compliance is being audited to specific PCI, FDCC, SCAP, HIPAA, and SOX regulations.

Level 4: Optimize Your Security Processes

With the first three levels of security implemented, IT departments can become even more proactive by ensuring compliance with corporate and regulatory standards and investigating any new vulnerabilities and new modes of malware attack. These final steps include refining your policies based on attacks you have seen, automating processes to maintain security with minimal steps, using whitelisting and HIPS, and using more advanced methods of maintaining secure configurations, including location-based policies and privilege lockdown.



Endpoint Security Maturity Curve

Refining Your Policies and Settings

One of the best ways to ensure compliance with corporate policies or regulations is to audit or gather and maintain security events, whether those are outside attacks or actions taken by employees. Not only will reports from the event log provide an overall view of what has happened, they can provide real-time alerts to any threats occurring in the environment.

Driving Security through a Process Engine

Automating security processes not only saves time and effort, it also reduces risk because you lessen the chance of human error. What's more, once the process is modeled and documented, you have an easy way to improve it. For example, let's say you have set up your environment with whitelisting. What if a user needs access to a new application? The first steps might be to load the application in a lab, test it, then apply the learning mode with LANDesk Security Suite to identify the application's patterns. From there you would set the new whitelisting to include the new application, package up the application, and push out the application and license to the user.

Now if you tie these steps together in a workflow, most of them can be completed automatically with the insertion of automatically generated emails to the right people for approvals. You could simplify this even further by having the system access a site and pull the file patterns down, match them with the application, and push the application out to users. The possibilities for automating the processes are virtually limitless.

Event Correlation

On a daily, if not hourly basis, organizations recognize their antivirus software has discovered a new virus trying to get into the environment. When that happens, IT departments would ideally like to know their HIPS system has seen the problem and then either automatically prevent an action, or notify the end user for permission.

In addition, when the HIPS function senses the problem and alerts the IT department, the system logs the event and then IT can submit the problem to the antivirus solution vendor for follow up. The vendor then resolves the problem and submits signatures back to the source of the alert with minimal intervention by IT. Automating the processes with the process engine to include the event correlation not only reduces effort, it reduces overall risk to the enterprise by solving the problem automatically.

The LANDesk Approach:

Refining policies and settings with the use of dynamic LANDesk location-aware policies, reduces the chance of data loss and infection. Dynamic policies can adjust security settings based on the environment a selected machine is in—including application control, anti-malware configuration, HIPS, whitelisting, device control, LANDesk personal firewall, and removable storage restrictions.

You can **drive security through the LANDesk Process Management engine**, which enables you to design and document a process using a simple drag-and-drop user interface, showing your workflow in action. You can employ the solution to automate business processes that include security management and patch management. LANDesk Process Management ensures that the policies you establish are enforced throughout the organization and automatically documents the process, making compliance to standards easier and faster.

LANDesk Security Suite features an activity view that brings together all security activity from antivirus, firewall, HIPS, whitelisting, and device control in a "single pane of glass", offering you quick access to late-breaking security events. You can also build **event correlation** processes that key off alerting events in order to locate and address events precisely and automatically.

Simplifying Your Move up the Mature Security Model

The bottom line on endpoint security is that today's threat environment is simply too dynamic for any single point solution to afford effective protection. The only practical and survivable defensive strategy is to move to a more mature security model that incorporates multiple layers of protective technology.

LANDesk customers enjoy a world-class solution for layered endpoint security that is proven in the marketplace and ready for immediate deployment. Customers 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.

As stated in a recent independent Forrester Research report:

> "Over the past few years, as the security organization has had to grapple with an increasingly complex threat landscape and a much more visible role in the organization, the expectations of the business have also significantly increased. The business expects that security will do all this and take on additional responsibilities while keeping its headcount virtually static. As a result, there is often a disconnect between what a security organization can realistically deliver and what the business perceives it can deliver. Security organizations today must be agile and high-performing—capable of addressing a multitude of responsibilities and needs simultaneously." [4]

Becoming an agile, high-performing IT organization requires, among other things, moving beyond point solutions to a more mature security model that incorporates multiple layers of protective technology. LANDesk customers enjoy a world-class solution for layered endpoint security that is proven in the marketplace and ready for immediate deployment. Customers 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.

For more information on LANDesk solutions for layered endpoint security, visit us online at www.landesk.com.

4 Khalid Kark and Rachel A. Dines, "Security Organization 2.0: Building A Robust Security Organization", Forrester Research, Inc., May 10, 2010, p. 1