Network Access Control with LANDesk® Trusted Access™ Technology

White Paper
Introduction: The Convergence of Security and Systems Management................... 3
An Even More Complete, Layered Security Solution and Single Console Simplicity...... 3
Securing Mobile Users.......................................................................................... 4
Which LANDesk® Trusted Access™ Solution is the Best Fit?............................... 5
Solution Matrix.................................................................................................... 9
Conclusion .......................................................................................................... 9
References .......................................................................................................... 9
Introduction: The Convergence of Security and Systems Management

Today’s IT management roles are converging, with IT operations staff performing more of the traditional security responsibilities in addition to their desktop and server management functions. With the avalanche of blended threats and worms and the proliferation of malware, including spyware, IT managers are increasingly challenged with managing multiple security and patch point products.

LANDesk® Security Suite with LANDesk® Trusted Access™ technology provides a single interface for real solutions to common security challenges, such as:

- How do I keep infected or unprotected systems from connecting to my corporate network?
- How can I quickly determine where I’m vulnerable?
- How do I protect my corporate resources from connected systems that become corrupt?
- Now that I know that I have a problem, how do I fix it?
- How do I manage systems no matter where they’re located?

The logical answer to keeping your network and systems secure is to prevent unhealthy or unauthorized users on the network in the first place. This requires a layered security solution, including network access control with LANDesk Trusted Access technology.

An Even More Complete, Layered Security Solution and Single Console Simplicity

There is no silver bullet when it comes to network security. The difficulty of managing and securing the corporate infrastructure requires multiple layers of security from the endpoint to the server.

LANDesk® Trusted Access™ technology allows network and security administrators to extend the power and benefit of security policies that are defined in the LANDesk® Security Suite and enforce network access control. LANDesk Trusted Access technology can use these polices to govern whether a device is permitted to access the corporate network. If a device seeking access to the network can demonstrate that its patch level, security settings, virus signature and other custom parameters are in compliance with the predefined policy structure, then it is permitted to access the network.

By using the integrated LANDesk® console, an IT team can easily create the policies that define the level of protection that a system must have. When a device attempts to access a trusted network:

1. The device is temporarily blocked from gaining access and is placed in a quarantined network, sometimes called a sandbox.
2. The quarantined device is then scanned.
3. The results of the scan are sent to the server to determine if the device meets the minimum requirements.
4. If the managed device passes the minimum requirements, it is allowed on the network.
5. Devices not meeting this level are blocked and redirected to a virtual network where remediation services can be performed.
LANDesk Trusted Access technology is an integrated component of LANDesk Security Suite, which can be used with LANDesk® Host Intrusion Prevention System (HIPS) and LANDesk® Antivirus technologies for an even more complete, layered security solution and even broader centralized control over the entire network environment. LANDesk Trusted Access technology:

- Extends active security management to endpoints. Use it for policy enforcement, quarantine and remediation capabilities, and more.
- Has configurable provisions for previously allowed devices. Trusted devices can be granted access without the mandatory “every time” scan and can be scanned on a periodic basis to ensure conformity.
- Delivers enterprise-ready network access control using the single console simplicity found only with LANDesk® solutions. It extends world-class policy enforcement and remediation to the enterprise for a lower investment than other industry-standard solutions.

**Securing Mobile Users**

Mobile users or road warriors present a unique challenge to policy enforcement. For example, consider the CEO who has just returned from a week-long trip overseas. While he was out of the office, he never logged into the corporate network and as a result doesn’t have the latest patches and virus definitions uploaded to his laptop. When he comes back into the office, he will be quarantined until his machine is made compliant with the new policies.

One of the key differentiators of the LANDesk® solution that makes it so compelling is its ability to manage remote users whether they are at home, in the hotel, or located at a satellite office. The LANDesk® Management Gateway is industry-leading technology that breaks the network barrier and gives LANDesk the power to reach beyond previous limitations by leveraging the Internet. This means your network administrators can now go beyond the local or wide-area network to administer with the same functionality that LANDesk® Management Suite and LANDesk® Security Suite provide—and do it with nothing more than an Internet connection.

It should make no difference where your employees are located. Today, doing business means being mobile. LANDesk helps you retain control and productivity with an internet-based solution—no VPN is required.
Which LANDesk® Trusted Access™ Solution is the Best Fit?
The LANDesk® Trusted Access™ solution supports four of the most popular standards for network access control: Cisco NAC, IPSec, 802.1x, and DHCP.

Integrated Cisco NAC Solution
LANDesk offers a Cisco-certified solution and is a member of the Cisco NAC partner program that provides access to the latest Cisco product information and support. In order to provide network access control, Cisco utilizes VLANs and interface connections to quarantine devices. The LANDesk Cisco NAC solution requires Cisco hardware and is an excellent option where Cisco hardware is already in place or being included as part of a network upgrade.

Figure 1: LANDesk – Cisco NAC Solution
**IPSec Solution**
LANDesk leverages IPSec security certificates that are built into most operating systems to provide network access control at a base level. This solution works by providing certificates signed by the LANDesk® core certificate authority to clients that have passed an initial posture check by the LANDesk® core server. If the initial posture check fails, the client is assigned a unique certificate that isolates it from communicating with any other host on the network. If a client is quarantined, it is given a prompt that instructs it on how to comply with the policies outlined by the core server. Once the client is in compliance with the policy, it is assigned a healthy certificate from the core server and can then communicate with other systems on the network provided those systems have healthy certificates.

![Figure 2: LANDesk – IPSec Solution](image-url)
802.1x Solution
The LANDesk® RADIUS (Remote Authentication Dial-In User Service) proxy is an 802.1x RADIUS proxy solution that works with all major switching vendors supporting the 802.1x standard. The LANDesk RADIUS proxy can participate with an existing AAA identity-management architecture authenticating users and endpoints, or act as an independent RADIUS proxy for environments requiring only endpoint compliance validation. The LANDesk RADIUS proxy provisions switch port access dependent upon authentication results for connected endpoints.

Figure 3: LANDesk 802.1x Solution
LANDesk® DHCP (LDDHCP) Solution
This process uses different IP address assignments to create quarantined networks. It is hardware independent, easy to implement and affordable. It relies on the organization’s routing and Dynamic Host Configuration Protocol (DHCP) services to be configured to support LDDHCP, and may require minor changes in the infrastructure configuration.

Figure 4: LANDesk – DHCP Solution
Solution Matrix

According to Forrester Research, 63% of enterprise business will invest in some form of network access control in 2007. The following matrix can help you determine the right LANDesk® Trusted Access™ solution.

<table>
<thead>
<tr>
<th>LANDesk® Trusted Access™ Solution</th>
<th>Supported Operating Systems</th>
<th>Description</th>
<th>Use Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NAC</td>
<td>Windows XP, 2003, Vista, Mac, Linux</td>
<td>The LANDesk® posture validation server provides the network health policies to the Cisco ACS server. The Cisco ACS server in turn enforces network admission based on the client’s adherence to these policies. The LANDesk® remediation and core servers provide remediation for clients that do not meet the predefined policies.</td>
<td>Existing (or future) Cisco architecture.</td>
</tr>
<tr>
<td>IPSec</td>
<td>Windows XP, 2003, Vista</td>
<td>IPSec enforces policies utilizing a certificate-based enforcement methodology. Only clients with healthy certificates can communicate on the network. Those clients that fail to meet policy are given a unique, pre-shared key that isolates them from the network. Doesn’t currently support VPN.</td>
<td>Ideal for networks that utilize static IP addresses or have limited choice regarding network infrastructure.</td>
</tr>
<tr>
<td>802.1x</td>
<td>Windows XP, 2003, Vista</td>
<td>802.1x provides NAC by requiring that the LANDesk® agent be active on the client machine. Requires switches that support the MD5 802.1x standard.</td>
<td>Ideal for IT administrators that utilize RADIUS servers to provide access to the network. Support for Microsoft and other major RADIUS servers.</td>
</tr>
<tr>
<td>LANDesk DHCP</td>
<td>Windows XP, 2003, Vista, Mac</td>
<td>The LANDesk DHCP (LDDHCP) server enforces the security policies defined by the administrator. Requires a LANDesk remediation server and router with IP forwarding for each DHCP server.</td>
<td>Provides a network hardware-independent solution through LANDesk DHCP services. Controls both managed and un-managed Windows and Mac devices.</td>
</tr>
</tbody>
</table>

Conclusion

LANDesk® Trusted Access™ technology can play a critical role in keeping a network safe while allowing key business partners, consultants and outside providers to perform the business tasks needed to optimize business processes.

At LANDesk, our mission is to provide you and your company with the most comprehensive IT security and management tools available anywhere on the planet. It is easy for any company to claim that it has what it takes. We encourage you to check into our background, our customers, and what the industry analysts say about our vision and execution. Even more importantly, let us prove it to you. As the saying goes, “The proof of the pudding is in the eating.” Let us pilot our solution in your environment, and then compare it against our competitors. We are confident you won’t be disappointed.

References