Endpoint Security Management

Protect against security threats, malicious attacks and configuration vulnerabilities through strong endpoint security control and maintenance.

LANDesk®

Protect your IT environment from the endpoint up

The Challenge:

Your network is exposed to a wide variety of risks, threats and attacks that put your data at risk. The latest security threats target individual computers to bypass perimeter security and attack from the inside. While strong perimeter security is critical, effective protection works from the endpoint up to secure assets and data at multiple points of attack.

Attacks on multiple fronts

Your data is being attacked on multiple fronts. Hardware or software flaws can corrupt files and put the actual bits and bytes at risk. Viruses and worms can attack files and server processes. Data can even be stolen by thieves with a USB drive and physical access.

Perimeter security measures provide the first layer of protection. But determined attackers have evolved spyware, trojans, keyloggers and other methods to deliver malicious code to your network interior. Authorized users can unwittingly vector malicious attacks through Internet downloads that bypass perimeter security.

A recent attack on the London offices of the Sumitomo Mitsui bank used keyloggers to steal access codes as part of an attempt to steal more than £220 M ($423 M). This kind of threat can also put corporate data at risk—including financial records—that can not only damage corporate credibility, but may also put your business at risk of prosecution.

Wolves in sheeps clothing

Many applications and utilities perform perfectly legitimate functions, but create serious security risks in the process. File sharing utilities are notorious for breaching perimeter security and creating both unwanted traffic on private networks, and opening access ports for malicious attackers to gain access to other network resources. In many cases, you simply can't afford to accept the security risks that come with otherwise legitimate applications.

Mass of information

The Carnegie Mellon Computer Emergency Response Team (CERT) reported more than 3700 distinct vulnerabilities in both 2003 and 2004 (see www.cert.org for more information). Trying to research, sort and prioritize the mass of information associated with those threats can bury your IT staff and reduce their ability to perform other critical tasks. Some organizations have chosen to wait for the announcement of a security exploit before repairing the underlying vulnerability, putting both data and business productivity at risk.

Beyond patch and anti-virus

Endpoint-based patch update and anti-virus tools can help protect the network interior, and many now include spyware removal. Unfortunately, such tools may not control access to network resources or stop legitimate (but risky) applications from running. While they help improve security, they only function across a narrow band of threats.

Time is critical

As the number of threats increases, the gap between a vulnerability's discovery and the release of a malicious exploit is shrinking. Keeping up with the sheer mass of patches, security bulletins, virus alerts and spyware announcements is increasingly difficult, and deploying protection against new threats is even more difficult.

You need direct, timely access to both threat information and problem remediation tools.

OVERVIEW

Business Need—Protect both network and data security from a single, central console.

- Quickly access, sort and prioritize descriptions, patches and remediation data
- Identify hardware and software assets accessible from the network
- Assess end-nodes for vulnerability to known configuration and security issues
- Rapidly deploy security patches and maintain secure configurations
- Detect and remove spyware, adware, key-loggers and other malware
- Stop unauthorized software from running
- Restrict endpoint access to unknown networks
- Control access to drives and ports
- Report security status at any time

Solution—Comprehensive endpoint security management from LANDesk

- Centralized security database aggregates the latest threat and vulnerability data
- Advanced discovery technology identifies all computing devices attached to the network
- Full hardware and software inventory shows you what's running in your environment
- Integrated scanner identifies known configuration and patch vulnerabilities
- Automated patch deployment and policy-based configuration maintenance tools
- Spyware removal protects against unauthorized access to network resources
- Configuration vulnerability checking helps identify non-secure endpoint settings
- Application launch blocking keeps risky or unauthorized applications from running on managed computers
- Connection Control Manager limits endpoint network access and controls access to drives and ports
- Asset and vulnerability reports keep you informed of security and remediation status

The LANDesk® Solution

LANDesk® Security Suite enables automated, centralized threat detection, research and prioritization, remediation and status reporting across the network. Use threat data from our centralized security database or create your own custom threat definitions to enable strong security management from the endpoint up.

Security Suite provides advanced endpoint security with:

- Centralized security database that aggregates the latest threat and vulnerability data in a single, comprehensive repository that you can automatically update on a recurring schedule
- Advanced discovery technology that identifies all computing devices attached to the network and enables you to target threat detection and remediation efforts on relevant systems
- Full hardware and software inventory that shows you what's running on your network so you can more effectively identify all computers in your environment and formulate your overall endpoint security plan
- Integrated vulnerability scanner that identifies known configuration and patch vulnerabilities and helps you quickly remediate potential security threats
- Automated patch deployment and policy-based configuration maintenance tools that help you establish and maintain secure configuration for each endpoint
- Spyware detection and removal that helps protect against unauthorized access to endpoint data or network resources
- Application Blocker technology keeps risky or unauthorized applications from running on managed computers to eliminate potential security holes
- Connection Control Manager that limits endpoint access to and from other networks, and controls access to the endpoint's drives and ports to help prevent data theft or snooping
- Asset and vulnerability reports that help keep you informed of security and remediation status

Security Suite helps you take active control of endpoint configuration security, control device access and automate security policy maintenance to establish strong security throughout your computing environment.

Unified endpoint security control

LANDesk® Security Suite integrates endpoint security configuration in a single, unified console for easy access and control. You can work with a wide variety of vulnerability types, create detection rules, define automated responses, configure endpoint access restrictions and more from a single, consistent interface.

Security Suite separates vulnerability detection rules from remediation measures to enable effective response to both current and future endpoint security threats without requiring a retooling of the interface to deal with new threat types.

Currently, Security Suite can detect and address patch vulnerabilities, spyware, risky applications, configuration vulnerabilities, and user-defined threats.

Security Suite uses a consistent methodology for addressing security threats.

- Download or create vulnerability detection rules
- Choose the vulnerabilities to scan for, and scan endpoints to identify vulnerabilities
- Remediate vulnerabilities through patches, scripts, removal tools and reporting for manual intervention
- Control access to networks and communications ports on the endpoint
- Deny the launch of risky applications
- Report endpoint security status and identify remaining trouble spots

This consistent model makes it easy to detect and eliminate vulnerabilities, then maintain endpoint security by controlling access to endpoint network and communications resources. Access control helps limit access to data resources, and prevent reintroduction of security threats into the environment.

More importantly, the ability to easily define and detect previously unknown types of vulnerabilities means your security team can stay ahead of security threats with immediate, proactive response.

Centralized security database

LANDesk® Security Suite detects security threats using vulnerability definitions that specify detection rules for each threat. These detection rules can then be tied to specific patches or scripts to automatically remedy threats, or to instructions for manually resolving potential problems.

Thousands of security threats are detected and reported every year, and researching and prioritizing the massive number of threats has become a serious problem for IT staff. The LANDesk® security database aggregates vulnerability data from multiple hardware, OS, application and security vendors it in a single, comprehensive database to help you quickly access current threat data and remediation resources. The security database also contains information on spyware, configuration vulnerabilities, risky applications and other types of threats. As new threats are detected, the database is automatically updated with the latest information.

Each threat definition in the database is evaluated and patches tested to install as designed. Threat definitions include severity information and URLs to vendor data to speed further research. Where necessary, additional information is attached to the threat definition to help you successfully eliminate vulnerabilities.

You can download threat definitions and patches separately so you can run vulnerability scans to identify actual vulnerabilities in your environment, then download only the applicable patches to minimize the time and disk space required for complete coverage. A scheduler can automatically download threat and patch data on a recurring basis, or you can manually access threat data at any time.

You can also create your own custom threat definitions and build your own patches and remediation scripts. This enables you to identify security issues or implement security policies specific to your environment. These tools make it possible to more quickly identify, prioritize and respond to security threats with a minimum of IT resource.

Advanced inventory management

It's critical to identify and secure all computers in your environment. A single non-secure computer can open

> "LANDesk® has established an early lead in the security management market segment. It is the only CSM vendor that has introduced integrated security management capability."
>
> DAVID FREELANDER
>
> THE FORRESTER WAVE™
>
> CLIENT SYSTEMS MANAGEMENT
>
> TOOLS, Q2 2005

holes in the network that put both data and other network resources at risk. You need access to current hardware, software and configuration data for all the computers in your environment.

LANDesk® Security Suite features powerful auto-discovery tools to help you identify and manage all the computers in your environment and close potential security holes. Unmanaged Device Discovery can perform detailed sweeps to identify computing devices and easily group them according to device type, such as computer, infrastructure, printer or other.

You can use this information to deploy management agents to computers so you can gather more detailed inventory data on hardware and software configuration that can be leveraged to help identify potential security threats. You can schedule Unmanaged Device Discovery scans to recur regularly so you can quickly identify new and unmanaged computers as they enter your environment.

Advanced inventory management enables you to take active control of the computers in your environment and more effectively implement security policies.

Efficient vulnerability scanning

LANDesk® Security Suite features a vulnerability scanner that runs on each managed computer to detect security threats. The scanner can use vulnerability definitions from the central security database as well as user-defined vulnerabilities, and can scan for specific files and file versions, registry entries, configuration settings and more.

To help reduce the impact on both managed endpoints and network resources, you can define which vulnerabilities the scanner looks for. You can limit scans to specific vulnerability types, such as spyware threats or patch vulnerabilities, and you can limit the specific vulnerability definitions used during a scan. For example, in a computing environment that is standardized on Windows XP, you can exclude Windows 2000, Windows 98, Linux, Solaris, and Mac OS vulnerabilities from your scan list.

You can schedule a recurring vulnerability scan, or manually scan endpoints at any time. The results of each vulnerability scan are sent to the core server where you can define automated remedies, manually respond to threats and generate vulnerability reports. Because the scanner looks for specific vulnerabilities, scan results clearly describe specific threats in your environment.

Automated patch deployment

When a patch vulnerability is detected, you can use LANDesk® Security Suite to deploy the appropriate patch to all vulnerable computers at once, taking advantage of exclusive LANDesk® technologies to speed patch delivery throughout your environment.

You can also configure Security Suite to automatically deploy patches to each endpoint as soon as a patch vulnerability is detected on a managed endpoint. The patch is distributed from your local patch repository using package deployment options you specify. You can perform silent installs and control how required reboots are handled to minimize impact on active users.

Patch reports help you track patch deployment status and identify failed installs so you can quickly follow up. You can also use reports to demonstrate security status and compliance to corporate security policies.

Spyware detection and removal

Perhaps the most pervasive current security threat comes from spyware, adware and other malware, including keyloggers, trojans, tricklers and snoopers. These threats are often downloaded by unwary users as parts of legitimate Web application suites or toolsets, and can not only open security holes on endpoints inside your network, but can seriously degrade both endpoint and network performance from unwanted traffic. Spyware applications are often

self-repairing, requiring a comprehensive removal strategy to completely eliminate all portions of the threat.

LANDesk® Security Suite features enterprise-level spyware detection and automated removal tools accessed through a single, centralized console for consistent security control throughout your organization.

Using data from the central security database, Security Suite can detect and remove more than 600 families of spyware, encompassing more than 37,000 individual spyware signatures for all the managed computers in your environment. Detected spyware is grouped into families to help you quickly identify the type of threat, rather than forcing you to wade through thousands of vague, repetitive or esoteric detection entries.

Spyware removal is automatic, and operates comprehensively across all components of a spyware infestation to keep the threat from downloading missing components and repairing itself. The security database is constantly updated to extend that spyware detection and removal capability as new threats are identified.

Application launch blocking

The most secure environment can be easily breached if an internal user opens up the network to intrusion through the use of risky or unauthorized applications such as file sharing utilities or other vectors for malware, worms or unsafe applications. These otherwise legitimate applications can open the door for easy intrusion and attack from malicious code that has infected outside files.

LANDesk® Security Suite can block the launch of risky or unsafe applications and keep them from running on managed endpoints. Many risky applications have already been identified in the LANDesk® security database, and you can extend that coverage by defining your own lists of prohibited applications. When the next vulnerability scan executes, the list of prohibited applications is downloaded to the endpoint and the LANDesk® agent will deny their launch.

Endpoint access control

Many otherwise secure computing environments are vulnerable to unauthorized access or data loss through wireless networks and communications ports such as Bluetooth. Similarly, the loss of critical data can often be traced back to someone using recordable CDs or removable USB drives to copy files directly off a computer within the firewall.

LANDesk® Security Suite features a Connection Control Manager that can limit communication with individual endpoints through networks, ports, drives and wireless channels. Define a set of rules that limit a computer's access to other networks and control access to each computer's communications interfaces, then use the familiar task scheduling interface to distribute those settings to selected targets.

Limiting endpoint access supplements existing configuration control, data encryption and network access control to help further protect critical data from both accidental loss and malicious theft.

Rapid Results

LANDesk® Security Suite is easy to set up and deploy, giving you the power to quickly take control of endpoint security management throughout your environment. Detect and eliminate threats, block risky application launch, restrict access to networks and communications ports, and automatically maintain security policies on each individual endpoint.

Security Suite is built on proven LANDesk® management technology, so you can easily upgrade to comprehensive endpoint configuration and security management with LANDesk® Management Suite. The upgrade takes only a few minutes and requires no additional hardware or software configuration.

LANDesk—Leading Solutions for Endpoint Security Management

LANDesk is an industry leading provider of easy to use, integrated solutions for desktop, server and mobile device management. LANDesk® management solutions are proven, with millions of managed nodes deployed worldwide.

Find out for yourself. Call or visit our Web site at http://www.landesk.com/ to learn more about LANDesk solutions, then download a fully functioning, time-limited product trial so you can see for yourself how LANDesk solutions can help ease your systems management pain from the first day of deployment.

Download a fully functioning, time-limited product trial so you can see for yourself how LANDesk® Security Suite can help ease your endpoint security management pain from the first day of deployment.

http://www.landesk.com

LANDesk®

Corporate Headquarters

698 West 10000 South

Suite 500

South Jordan, Utah 84095

www.landesk.com

FOR PRODUCT INFORMATION

Brazil ..... + (55 11) 3048-4080
Canada .....+ 1-800-982-2130
China .....+ 8610-8518-3138
Europe ..... + 44 (0) 118-902-6200
France 0810 000 212
Ireland ..... + 353 (0)1 809-4268
Italy .....+ 39 (02) 72 54 64 64
Japan ..... + 81 (3) 3435-8261
Mexico .....+ 52-55-5448-4933
U.S.....+ 1-800-982-2130

LSI-0355 0505/AH/SP/JA