

Layered Endpoint Security

Discovery

- Extended Device Discovery



Extended Device Discovery

Must Haves

- »» Discover any item on the network that does not appear the Core database but has IP address
- »» Scalable Discovery process
- »» Remove the ping sweep burden from the core
- »» Real-time subnet level discovery tracking
- »» Discover devices on network even if they have a firewall
- »» Manually group and create additional groups
- »» Create and schedule multiple discovery configurations
- »» Alert on found devices
 - Configure the Unmanaged device found alert

The image shows two overlapping windows from a network management software. The 'Scanner Configuration' window has a 'New configuration' entry in the 'Saved Configurations' list. Under 'Scan for devices on the net using the following discovery options', the 'SNMP' checkbox is checked and highlighted with a red box. The 'Additional devices to discover' section includes 'IPMI', 'Chassis', and 'Intel A'. The 'Scan devices using this IP range' section shows 'Starting IP: 10.16.240.1' and 'Ending IP: 10.16.240.240'. The 'SNMP Configuration' window shows 'Connection details' with 'Retries: 1' and 'Wait for response in seconds: 1'. The 'Port' is set to '161'. The 'Community name' is 'public'. A 'Configure SNMP V3...' button is visible at the bottom.

The 'Unmanaged Device Discovery' window displays a table of discovered devices. The table has columns for 'Device Name', 'IP Address', 'Subnet Mask', 'OS Description', and 'MAC'. A red box highlights the 'OS Description' column, with the text 'Additional Information from Printers Returned via SNMP' written below it.

Device Name	IP Address	Subnet Mask	OS Description	MAC
4100MKT	010.016.240.037	255.255.255.000	HP ETHERNET MULTI-ENVIRONMENT,ROM R.22.01,JETDIRECT,JD95,EEPROM R.25...	0001
NP16D0810	010.016.240.033	255.255.255.000	HP ETHERNET MULTI-ENVIRONMENT,ROM R.22.01,JETDIRECT,JD95,EEPROM R.25...	0001
4100ENG1	010.016.240.031	255.255.255.000	HP ETHERNET MULTI-ENVIRONMENT,ROM R.22.01,JETDIRECT,JD95,EEPROM R.25...	0001
COLOR4	010.016.240.035	255.255.255.000	HP ETHERNET MULTI-ENVIRONMENT,ROM V.29.11,JETDIRECT,JD115,EEPROM V.2...	0011
4100TLS	010.016.240.038	255.255.255.000	HP ETHERNET MULTI-ENVIRONMENT,ROM R.22.01,JETDIRECT,JD95,EEPROM R.25...	0001
4100CC	010.016.240.032	255.255.255.000	HP ETHERNET MULTI-ENVIRONMENT,ROM R.22.01,JETDIRECT,JD95,EEPROM R.25...	0001
COLOR5	010.016.240.036	255.255.255.000	HP ETHERNET MULTI-ENVIRONMENT,ROM R.22.01,JETDIRECT,JD95,EEPROM R.25...	0001
CANON5	010.016.240.039	255.255.255.000	Canon IR3300i #P	0000
CANON4	010.016.240.034	255.255.255.000	Canon IR3300i #P	0000
4100SALES	010.016.240.040	255.255.255.000	HP ETHERNET MULTI-ENVIRONMENT,ROM R.22.01,JETDIRECT,JD95,EEPROM R.25...	0001
NP13D47D1	010.016.240.235	255.255.255.000	HP ETHERNET MULTI-ENVIRONMENT,ROM C.25.80,JETDIRECT,JD115,EEPROM V.2...	000E
4100SEAST	010.016.240.238	255.255.255.000	HP ETHERNET MULTI-ENVIRONMENT,ROM C.25.80,JETDIRECT,JD115,EEPROM V.2...	000E
4100NCENTER	010.016.240.234	255.255.255.000	HP ETHERNET MULTI-ENVIRONMENT,ROM C.25.80,JETDIRECT,JD115,EEPROM V.2...	000E

Layered Endpoint Security

Lockdown & Configuration

- Agent Watcher
- Firewall Management
- Security Threat Assessment
- Connection Control Manager



Discovery

- Extended Device Discovery



Client Security Configuration Management

Must Haves

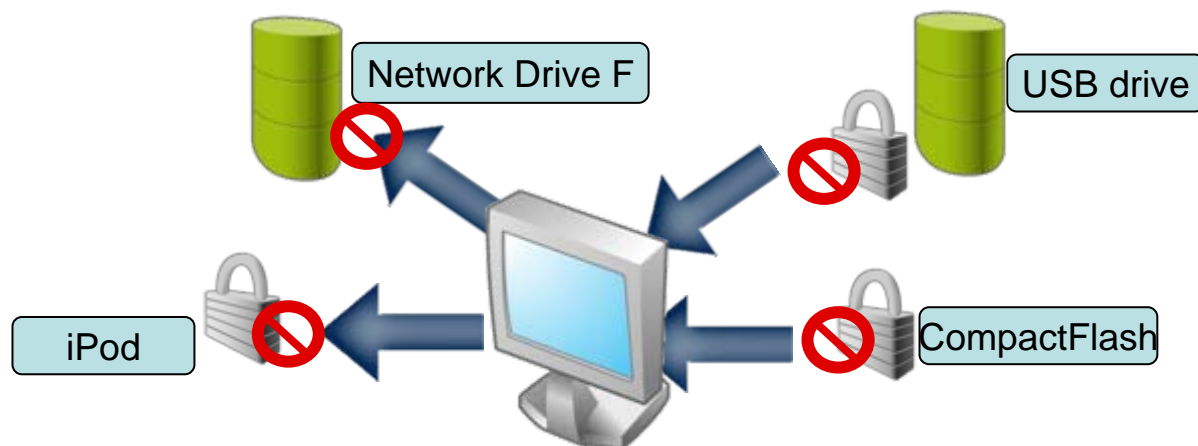
- »» Personal Firewall
- »» Password Enforcement
- »» Super-user Management
- »» IE Zone Configuration
- »» Custom Vulnerabilities
- »» Application Control



Device Connection Control / Lockdown

Must Haves

- »» Control over client network connections
- »» Ability to prevent data theft
 - Lockdown and limit access to peripheral devices
 - digital cameras
 - iPods
 - CompactFlash
 - USB devices



Layered Endpoint Security

*Patch Management
OS and Applications*

- LANDesk Patch Manager



*Lockdown &
Configuration*

- Agent Watcher
- Security Threat Assessment
- Firewall Management
- Connection Control Manager



Discovery

- Extended Device Discovery

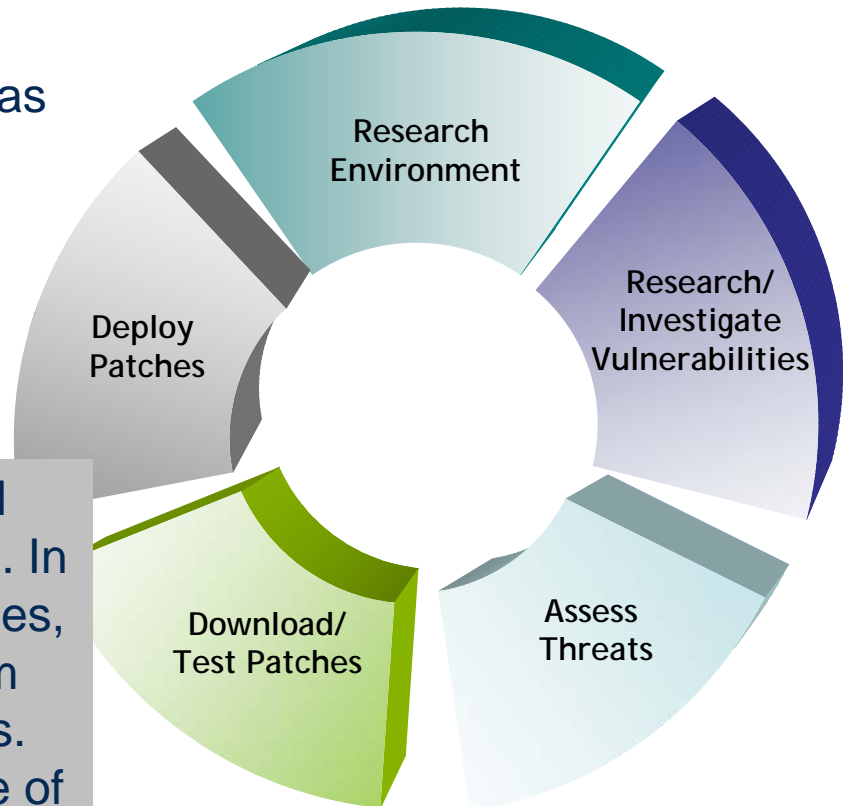


Automated Patch Management



Must Haves

- »» A solution that will Patch the OS and as well as applications
- »» Patch heterogeneous environments
- »» Automated process for:
 - Know when a patch is released
 - Assess threat to network



This SANS Top-20 2005 is a marked deviation from the previous Top-20 lists. In addition to Windows and UNIX categories, we have also included Cross-Platform Applications and Networking Products. The change reflects the dynamic nature of the evolving threat landscape.

www.sans.org

Layered Endpoint Security

*Prevent
Malicious SW*

- Anti-spyware
- Application Blocking
- AV enforcement
- **Antivirus, Rootkit Detection**



*Patch Management
OS and Applications*

- LANDesk Patch Manager



*Lockdown &
Configuration*

- Agent Watcher
- Firewall Management
- Security Threat Assessment
- Connection Control Manager



Discovery

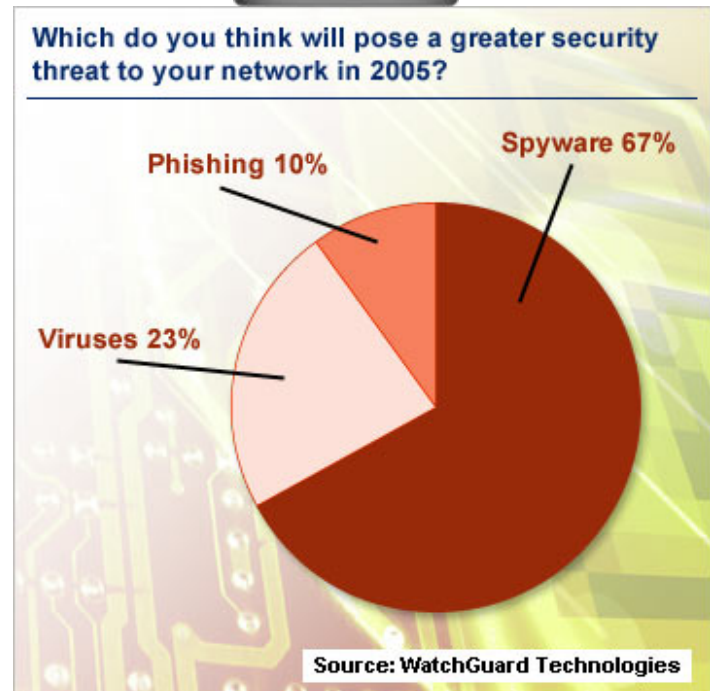
- Extended Device Discovery



Enterprise Anti-SpyWare, Anti-Malware Anti-Virus

Must Haves

- »» Policy enforcement
- »» Centralized management
- »» Detection and removal
- »» Continually monitor devices for suspicious activity
- »» Block spyware and adware from running
- »» Force Compliance



Layered Endpoint Security

Network Access Control

- LANDesk Trusted Access



Prevent Malicious SW

- Anti-spyware
- Application Blocking
- AV enforcement
- Antivirus, Rootkit Detection



Patch Management OS and Applications

- LANDesk Patch Manager



Lockdown & Configuration

- Agent Watcher
- Firewall Management
- Security Threat Assessment
- Connection Control Manager



Discovery

- Extended Device Discovery



Network Access Control

Must Haves

»» Protect your network against:

- Vulnerable Mobile devices
- Users who disable or change settings
- Visitors who may compromise security

»» Enforce security policies before devices enter network

- Allow only compliant devices
- Offer noncompliant devices the ability to become compliant
- Block noncompliant devices



Layered Endpoint Security

Knowledge & Verification

- Executive Dashboard
- Reporting



Network Access Control

- LANDesk Trusted Access



Prevent Malicious SW

- Anti-spyware
- Application Blocking
- AV enforcement
- Antivirus, Rootkit Detection



Patch Management OS and Applications

- LANDesk Patch Manager



Lockdown & Configuration

- Agent Watcher
- Firewall Management
- Security Threat Assessment
- Connection Control Manager



Discovery

- Extended Device Discovery



Reporting

Must Haves

»» Reports

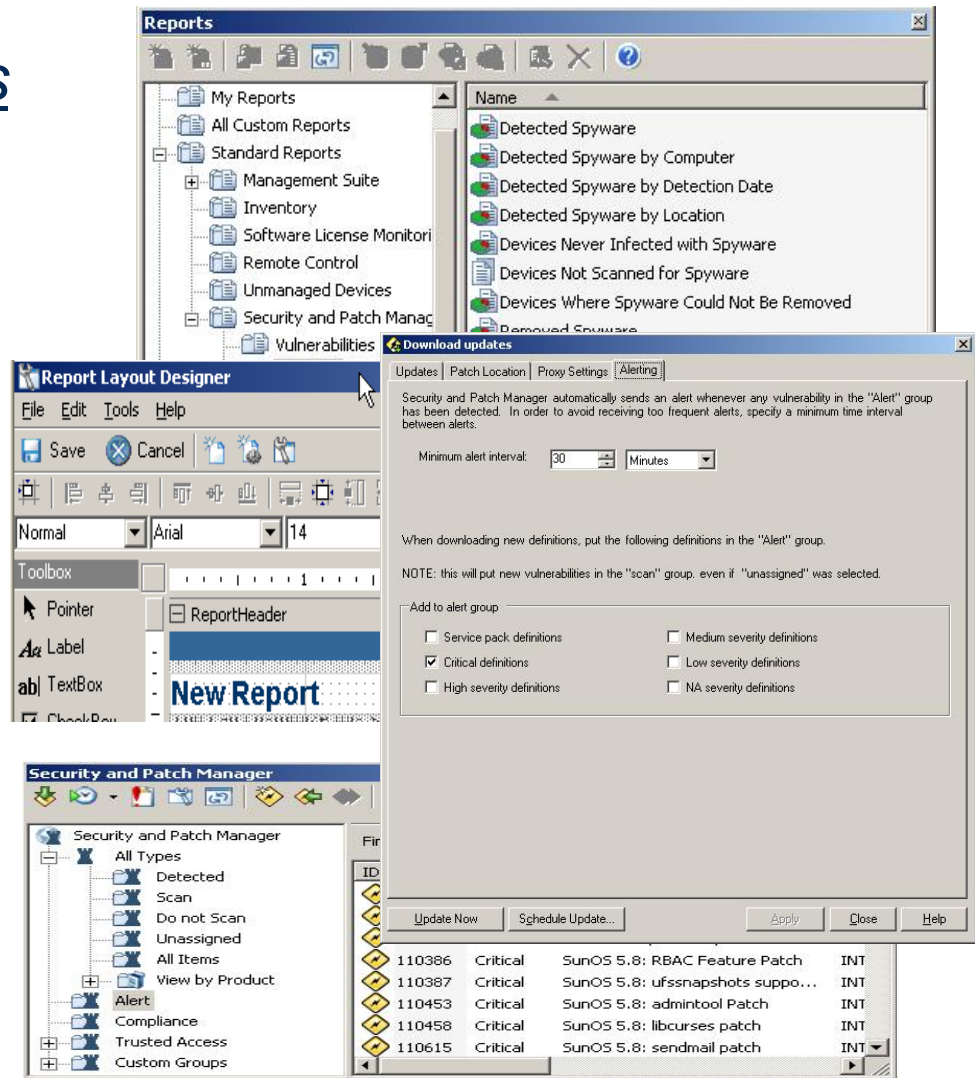
- Multiple “Canned” Security and Patch Manager reports
- Graphs and trending analysis
- Create your own reports using the LANDesk Report Designer

»» Report Delivery Options

- Email reports to the appropriate users with scope applied.
- Publish reports to a website
- Export reports to:
 - PDF,XLS, RTF,DOC,RPT

»» Alerts

- Ease of use and granularity
- Automatically add alerts around new definitions based on criticality when downloaded



Executive Dashboard

- »» High-level abstracted view of the managed environment
- »» Summarize current status in the following areas:
 - Vulnerabilities and security configuration
 - Installed OS base
 - Applied policies
 - Software licensing
- »» Installed as part of the web console on both the core server and rollup core server
- »» Configure the layout
 - Include only pieces of information you care about
 - Each user can configure their own layout

