

企业信息安全管理 之

细节决定成败

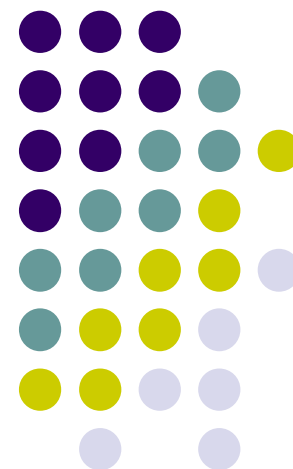
赵粮

hi2005@gmail.com

zhaolianga@lenovo.com

<http://blog.zhaol.cn>

4/18/2007



Strategies of Security Operations



Protect Perimeter

- **Secured Wireless**
- **Secured Remote User**
- Secured Web and Internet Access
- Messaging/Email Firewall

Comply to Security Policy and Laws

- **Forced audit and record protection**
- **Forced Patching**
- Helpdesk Process
- Automate Vulnerability Scans
- Automatic Port Shutdown

Lenovo Information Security Policy

Lenovo Information Security Standard

Secure Desktop Computing

- **Forced AV and Update**
- **Forced LANDesk and Asset Mgmt**
- **Domain Group Security Policy**
- Active Directory based access control
- Desktop computing standard

Safeguard Critical Assets

- **Identity and access management processes**
- Classified information assets
- Separation of Duties
- Integrated Physical Security

桌面安全管理之不可承受之重



桌面安全管理不可承受之重

主题：网络安全 | 标签：安全, ITIL, 电信, SOX, 咨询, SOC, 道可道非常道 | 浏览(3090) | 评论(6) | 2006-07-18

现在在内控的大旗下，桌面安全管理项目车轮隆隆，各路人马狼烟四起、厮杀在一处。前不久陆续接到各路十多个战报，端的是令人目不暇接。曾记否，今年年初写2006安全技术发展趋势时，没有将“桌面安全管理”列入引起争论不少，现在桌面安全管理果然杀气阵阵，难道不是2006的大热点吗？当初我的解释是桌面安全管理不是某个技术和产品，而是很多个/很多类产品的集成。现在观察一下各路的需求说明，心中还是被再次触动了一下。“桌面安全管理，你到底要承受多重”……

各路厂商大点名：

国外：Microsoft(AD+SUS+SMS), CA (DSM), HP, IBM, Symantec(Sygate), BigFix, Landesk, ...

国内：华为、中兴、联创、北信源、安氏...

有哪些朋友的产品没有列出，多多包涵，随时和我联系

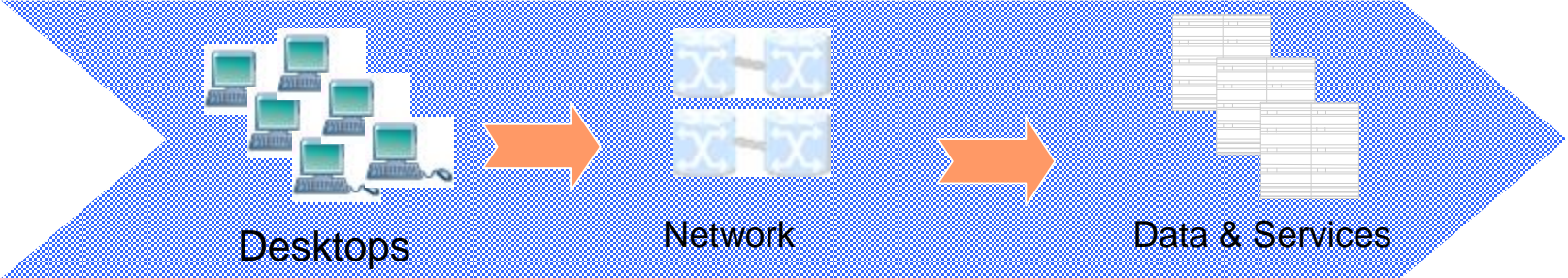
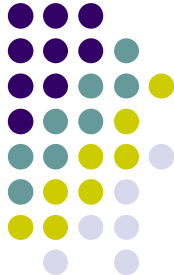
http://blog.zhaol.cn/Article_31879

主要需求点：

*we don't want to be in a situation where we **comply** the IT policy but **loose the serviceability** to our customer and increase lenovo operation cost.*

— An business executive

Desktop Management and IT Structure

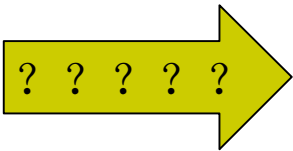


Challenges

- Large volume, so that large amount of IT investment, including h/w and s/w license
- Heavy helpdesk requests
- Most of security threats come from desktops
- Various potential legal issues

Countermeasure and Strategy

- Standardized configuration
 - To simply configuration management and helpdesk support
 - To minimize the license cost and potential legal risks
- Streamlined the new-hire / replacement / restore processes
- Hardened desktop security policy, corresponding audit and monitoring
- Solid identity and organization directory via Active Directory



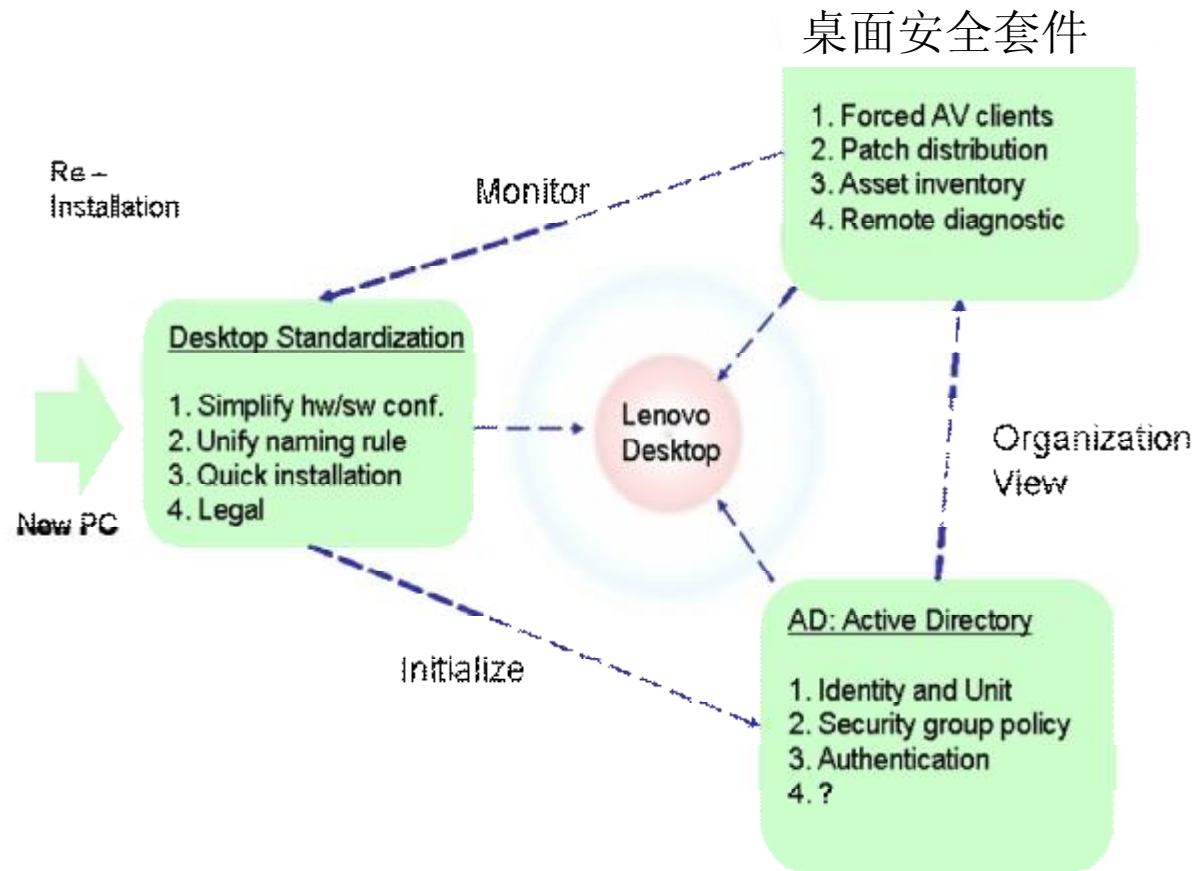
- ▣ 资产管理
- ▣ 补丁分发
- ▣ 远程控制
- ▣ 安全策略管理
- ▣ 集成的桌面防火墙
- ▣ 桌面反病毒集成
- ▣ 端口和外设管理
- ▣ 外联管理
- ▣ 网络访问管理
- ▣ 财务管理

Closed-loop in Desktop Security



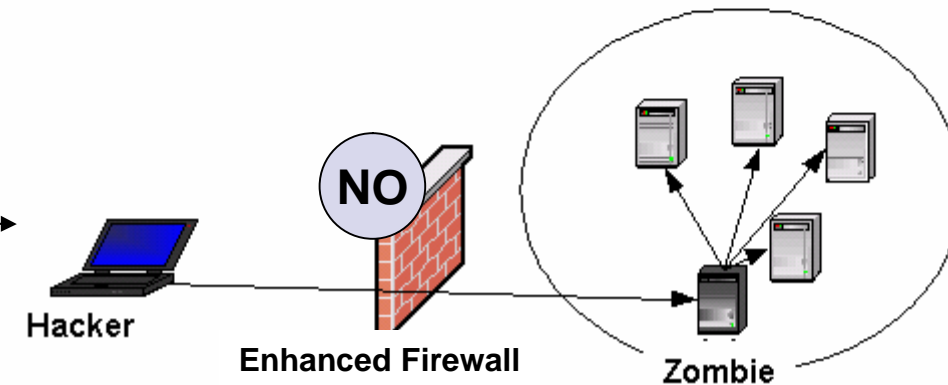
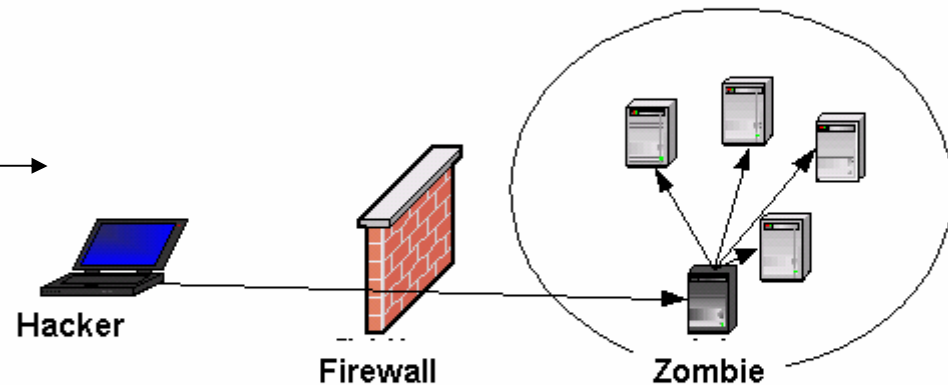
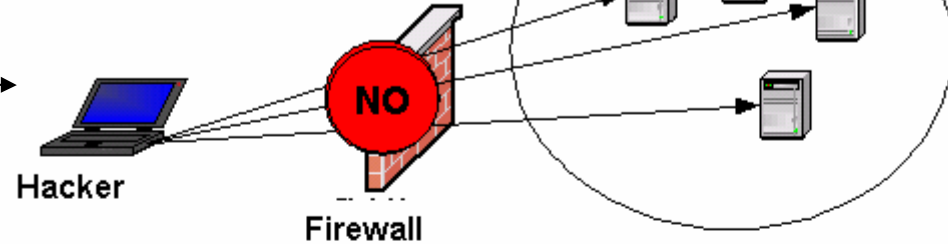
Virus Free

- ☒ Virus
- ☒ Worm
- ☒ Bot
- ☒ Spyware
- ☒ Adware
- ☒ "greyware"
- ☒ ...

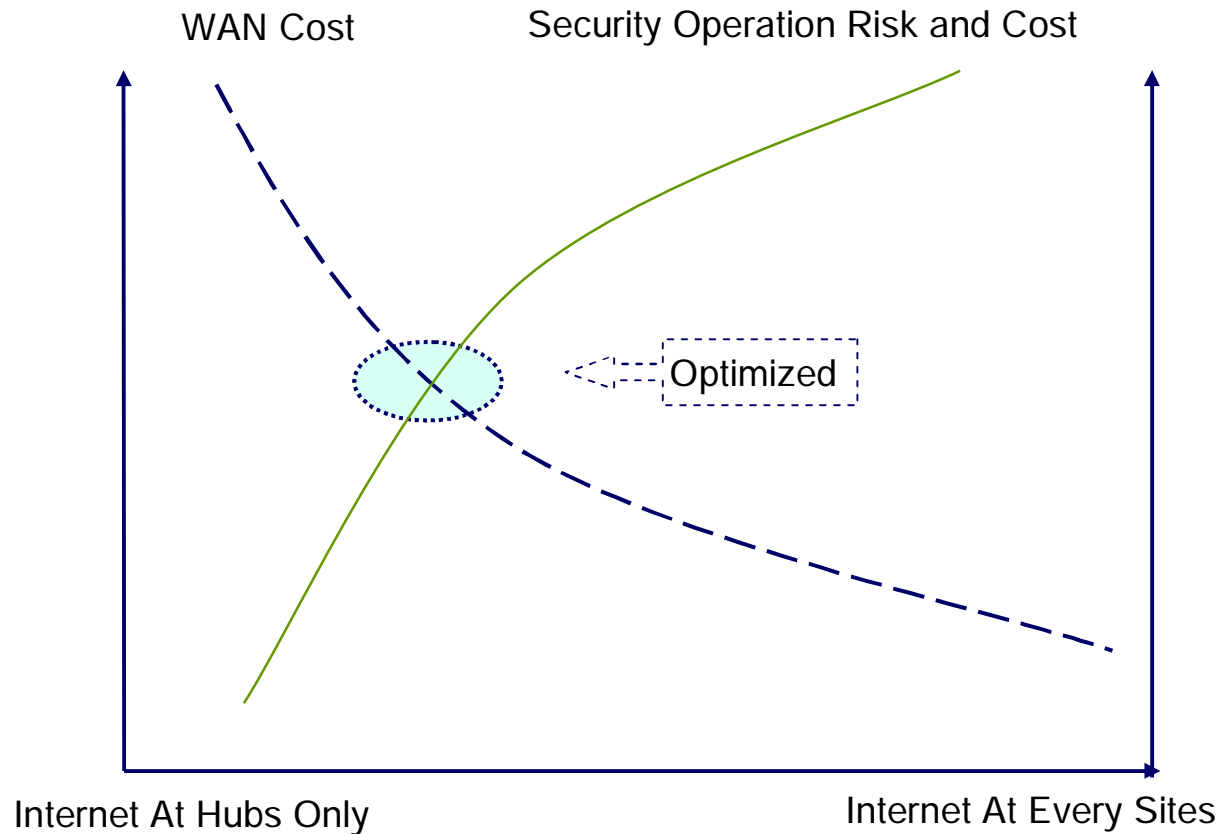


Springboard for attacks

- Generally speaking a proper configured firewall can well protect intranet desktops
- P2P/IM software has been eroding the network perimeter protected by traditional firewalls
- A desktop which has been controlled by some malware/spyware acts as Zombie and springboard for Internet attacks.
- A single remote accessed desktop that uses proxy-enhanced firewall won't be controlled by outside hackers so that intranet mission critical devices are protected from internal attacks



WAN Cost versus Security Operation Risk and Cost



----- **What's your recommendation ?** -----

关于细节



Before / During Meetings

- Announce when a meeting involves Lenovo Confidential Information
- Verify conference call attendees
- Keep conference room doors closed

| 宣传 Awareness

| VIP Support

| 安装管理率 Installation/Managed Rate

| 处罚

| 分工

| 关于的技术的技术

| ...

Conference Room Security

After Meetings

- Clear all papers and documents
- Dispose of Lenovo Confidential documents in confidential waste bins
- Erase white boards



Questions and Answers



"And now at this point in the meeting I'd like to shift the blame away from me and onto someone else."