
Creating a Secure Desktop

Derek Melber

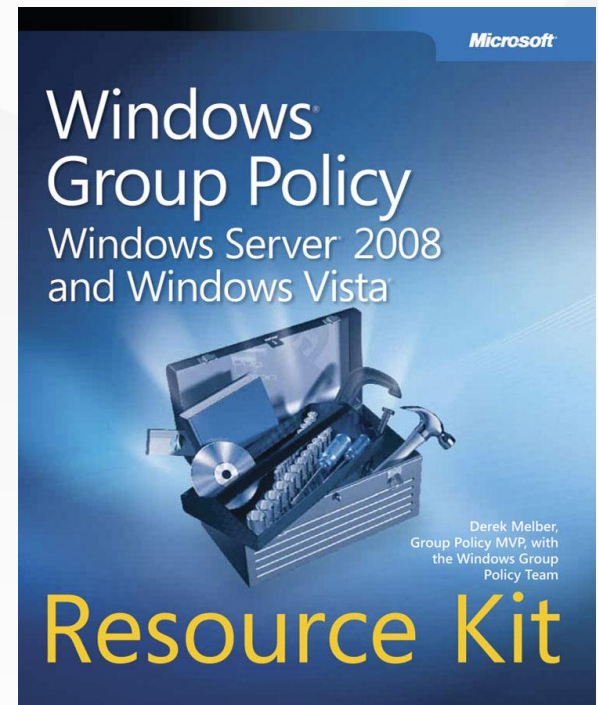
MVP, MCSE

derekm@braincore.net

About your Speaker

Derek Melber MCSE, MVP

- **President – BrainCore.Net**
 - www.braincore.net
 - derekm@braincore.net
- **MSPress Author**
 - “Group Policy Resource Kit”
- **Services**
 - Group Policy Training and Consulting
 - Auditing Windows Security Consulting



Endpoint Security Issues

- **User has full control over computer**
 - Configurations are modified
 - Productivity time for user is reduced
 - Help desk calls increase
 - Computer support cost increases

Endpoint Security Issues

- **Malware, viruses, spyware run as logged in user and with their privileges**
 - All Internet facing applications run as logged on user
 - Viruses “attempt” to access as administrator
 - Once administrator, malicious code is spread to next computer

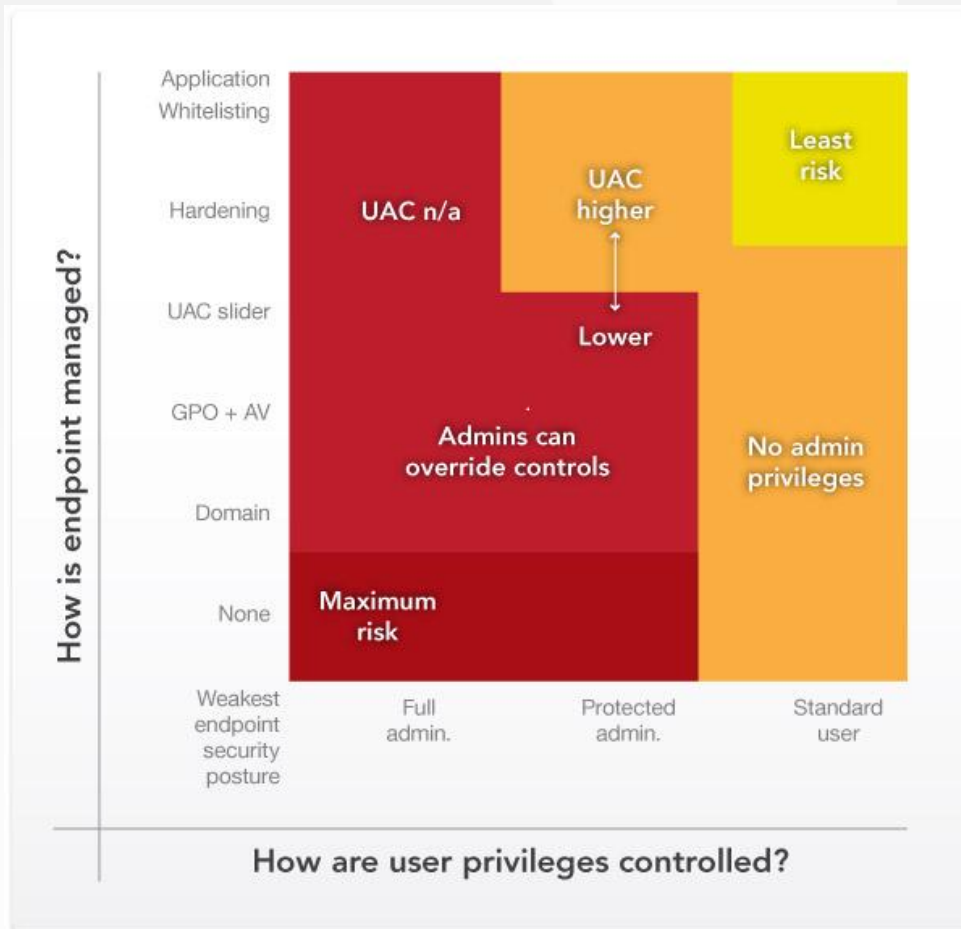
Endpoint Security Issues

- **Malicious applications can be installed**
 - Hacker tools
 - Applications that contain viruses
 - Web server
 - Internet shared files and applications

Endpoint Security Issues

- **License management negated**
 - User can install any application
 - Application might not be licensed
 - Company is liable for all apps installed on computers
 - Fines are high when not meeting vendor licensing

Endpoint Security Matrix



Security options

- **Basic Group Policy Security Settings**
 - Last user name display
 - CTRL+ALT+DEL control
 - Legal Notice
 - Administrator and Guest account controls
 - LAN Manager controls
 - Anonymous controls



Windows 7 IE Security

- **IE Protected Mode**
 - UAC
 - Mandatory Integrity Control (MIC)
 - User Interface Privilege Isolation (UIPI)



Desktop Security

- **Security Controls via Group Policy Preferences**
 - Services and Service Accounts
 - Local User Passwords
 - Local Group Membership



Windows 7 UAC

- **UAC – User Account Control**

- Allows admins to run as “standard user”, even though logged in with admin credentials.
- Can prompt standard user for “admin credentials” when running apps and features that require admin privileges
 - Glorified Run As
 - Requires std user to know “admin credentials” (same issues as Run As)

Windows 7 UAC

- UAC

- Microsoft introduced Slider Control is result of “industry complaints”
- Reduces prompting...
- Windows 8 is same

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
[Tell me more about User Account Control settings](#)


Always notify



Never notify

Never notify me when:

- Programs try to install software or make changes to my computer
- I make changes to Windows settings

 Not recommended but can be selected if you use programs that are not certified for Windows 7 because they do not support User Account Control

Anti-Virus

- **Staple for nearly every computer**
- **Benefits**
 - Efficient in catching known malicious applications
 - Vendors are always sending updates
- **Disadvantages**
 - Only as good as signature file for known malicious applications
 - We still get infected!

Firewall

- **Common for most desktops/laptops today**
- **Free and default with Windows 7 (and it works!)**
- **Benefits**
 - Efficient in restricting avenues of communication
 - Works with built-in Windows technologies (IPSec, isolation, etc)
- **Disadvantages**
 - Does not deny the running of applications locally
 - Does not protect the transmission of data

Whitelisting

- **Considered excellent security for application control**
- **Benefits**
 - Efficient in controlling which applications are allowed/denied
- **Disadvantages**
 - Does not solve privilege management
 - Creating approved list of applications is difficult
 - Creating a denied list of applications is difficult
 - Must constantly maintain updated lists

Windows 7 AppLocker

- **AppLocker (Whitelisting)**
 - Only runs on Windows 7
 - Replacement Software Restriction Policy
 - Allows for Rules to be created, which control which applications will function or not
 - White listing
 - Black listing
 - Windows 8 is same

Whitelisting

- **Whitelist does not allow standard user to run application!**
- **Whitelist without privilege management is only slightly secure**
- **Whitelist with user running as local admin is very dangerous!**

Comprehensive Secure Desktop

- **Configure user to not have admin capabilities**
 - Group Policy Preferences
- **Need applications to run for standard users**
 - No built-in capabilities to provide this level
 - Modifying file/Registry ACLs will not solve all issues
 - Group Policy can't provide this solution



Why Users Typically are Local Administrators

- **Run essential business applications**
- **Install software or ActiveX controls**
- **Running Windows features**
 - Defragging hard drive
 - Altering control panel settings
 - Change system clock
 - Altering IP address settings
- **Add local printers (Windows XP)**

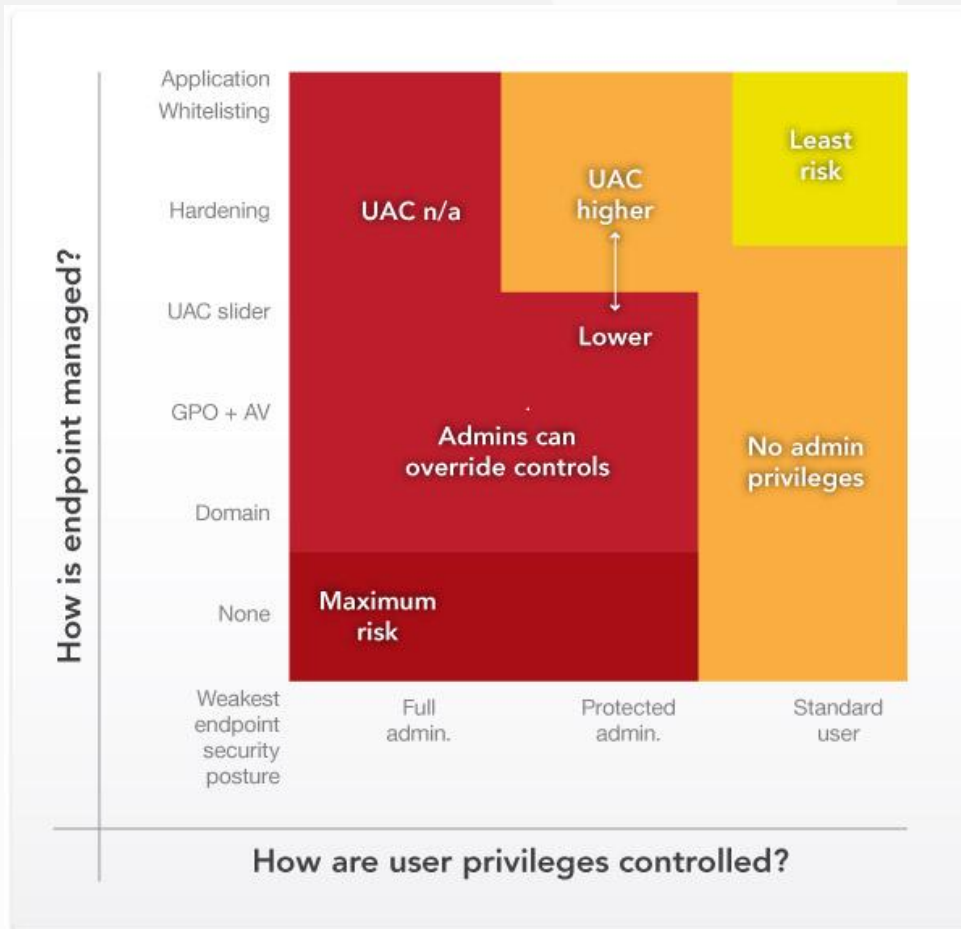
PowerBroker Desktops Provides Privilege Management and Whitelisting

- **Essential Business Applications**
 - User can still run application, but does not have local admin rights
 - Control local executable
 - Control applications using DFS share
- **Allow install of software and ActiveX controls**
- **Windows Features**
 - Change System Time
 - Disk Defrag
 - Installing local printers
- **Operating System Applications**
 - Command Prompt
 - Services for Windows (DNS, DHCP, etc)
- **Add local printer (XP)**

PowerBroker Solves Privilege Management and Whitelisting Issues

- **Determination of applications requiring elevation**
 - BeyondTrust PowerBroker PBReports
 - Takes months of effort down to less than week
- **Creation of rules for applications requiring elevation**
 - BeyondTrust PowerBroker PBReports
 - Takes weeks of testing down to right-click
- **Deployment of privilege management solution into existing Active Directory/GP design**
 - BeyondTrust PowerBroker Collections and Item-Level Targeting
 - Takes redesign of Ous and ignores entire step

Endpoint Security Matrix



References

- **Derek Melber**
 - derekm@braincore.net
- **Documents**
 - http://www.windowsecurity.com/Derek_Melber/
 - <http://www.windowsnetworking.com>
 - <http://www.beyondtrust.com/White-Papers/>
 - <http://www.microsoft.com/download/en/details.aspx?id=26137>



References

- **Books**

- Group Policy Resource Kit

- <http://www.microsoft.com/learning/en/us/book.aspx?ID=9556&locale=en-us>

- Auditing and securing Windows Series

- http://www.amazon.com/Auditing-Security-Controls-Windows%C2%AE-Directory%C2%AE/dp/0894135635/ref=sr_1_2?ie=UTF8&qid=1332543195&sr=8-2
 - http://www.amazon.com/Auditing-Security-Controls-Windows%C2%AE-Directory%C2%AE/dp/0894135651/ref=sr_1_4?ie=UTF8&qid=1332543195&sr=8-4

Thank You!

Derek Melber
derekm@braincore.net

To learn more about PowerBroker Desktops:

<http://www.beyondtrust.com/PBWD-Eval/>