

What's New for Security in Windows 10 and Server 2016 ?

Jason Fossen

Enclave Consulting LLC

Securing Windows with PowerShell (SEC505)

<http://www.sans.org/sec505>

About The Speaker

- Jason Fossen

- SANS Institute Fellow
- Consultant, Dallas, Texas, USA
- LinkedIn and Twitter:
 - @JasonFossen

- Author and Instructor of:

- The Windows day of Security Essentials (SEC401.5)
- Six-day Securing Windows with PowerShell (SEC505)
- Course SEC505 → <http://www.sans.org/sec505>



This talk was originally 3.5 hours long...

- Get the full slide deck:
 - <http://cyber-defense.sans.org/blog/downloads>
 - Get the SEC505 zip file, look in the Extras folder
 - Includes my Process Hacker talk and full notes
 - Include lots of PowerShell scripts
- Watch the full 3.5-hour webcast recording:
 - Goto www.sans.org > Resources > Webcasts > Archive

User Acceptance

Many platforms, one user interface



Desktop PC
Laptop
Tablet
Phone
Xbox
Surface Hub
Raspberry Pi
HoloLens
Car

Many platforms, one BSOD



Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

25% complete



For more information about this issue and possible fixes, visit
<http://windows.com/stopcode>

If you call a support person, give them this info:
Stop code: CRITICAL_PROCESS_DIED

Graphical User Interface

- Return of the Start Menu!
- Apps can run full screen or in normal windows
- Charms bar is gone
- Notification Area (like Android)
- Virtual desktops (like Linux)
- Settings app steadily replacing the Control Panel
- Switch between "Tablet Mode" and "PC Mode"

Cortana

- Cortana is not just "Microsoft Siri"
- Cortana is "Microsoft Watson" (as in, IBM's Watson)
- Cortana will be integrated into *everything*
 - Including Android, iPhone, Xbox, Office 365, Start Screen
- "Human language is the new user interface layer"
--Satya Nadella (speaking of "bots" generally).

Cortana Privacy Rampancy

- You might want to read the license agreement...
- <https://fix10.isleaked.com>
- Microsoft's official position:
 - <http://news.microsoft.com/stories/inthecloudwetrust/>
 - <https://player.vimeo.com/video/133627472>



Windows as a Service

Windows 10 Enterprise E3 and E5

- Windows 10 Enterprise E3 = \$7.00 / User / Month
- E3 = Windows 10 + Office 365 + Mobility Suite
- E5 = E3 + Windows Defender Threat Monitoring

Update Distribution Mechanisms

- Windows Update in Settings app
- Windows Server Update Services (WSUS)
- **Windows Update for Business (WUB)**
 - Uses same infrastructure as Windows Update
 - Permits the delay of installation of updates and upgrades
 - Manage through Group Policy, MDM, or registry edits

Servicing Branches

- **Current Branch** (All Editions)
 - All fixes and new features through Windows Update
- **Current Branch for Business** (Pro, Enterprise, Edu)
 - Update vs Upgrade
 - Max update delay: 12 months (WSUS), 1 month (WUB)
 - Max upgrade delay: 12 months (WSUS), 8 months (WUB)
- **Long-Term Servicing Branch** (Enterprise only)
 - Max delay: 10 years

Defer Upgrades and Updates

Defer Upgrades and Updates

Previous Setting Next Setting

☐ Not Configured Comment: GPO > Computer Configuration > Administrative Templates > Windows Components > Windows Update

☒ Enabled

☐ Disabled

Supported on: At least Windows 10 Server or Windows 10

Options:

Defer upgrades for the following

duration (months): 8

Defer updates for the following

duration (weeks): 4

☐ Pause Upgrades and Updates

Help:

You can also choose to delay updates for up to one month. If you do not delay updates, your PC will remain up to date with security updates as they become available.

If an issue arises with an update or upgrade, select "Pause Upgrades and Updates". This will delay updates and upgrades until the next monthly update or upgrade becomes available. Once a new update or upgrade is available, the value will go back to the previously selected option, re-enabling your validation groups.

Note: Definition updates will not be impacted by this policy.

Note: If the "Specify intranet Microsoft update service location" policy is enabled, then the "Defer upgrades by", "Defer updates by" and "Pause Updates and Upgrades" settings have no effect.

Note: If the "Allow Telemetry" policy is enabled and the Options value is set to 0, then the "Defer upgrades by", "Defer updates by" and "Pause Updates and Upgrades" settings have no effect.

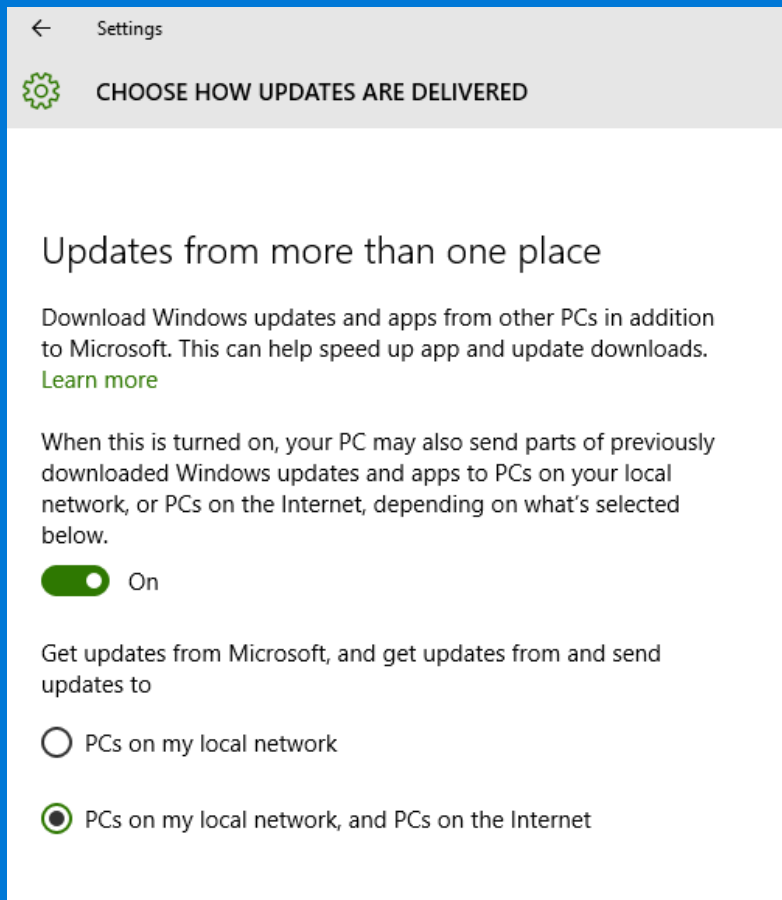
OK Cancel Apply

Maximum
Values ->

Pause: 35
Days Max

Peer-to-Peer Updates

- Similar to BitTorrent
 - SSL/TLS to transfer chunks
 - Digital signatures checked
 - Not just updates, apps too
 - Metered NICs excluded
- Pro & Home Editions
 - Both LAN and Internet updating
- Enterprise & Education
 - By default, local network only



To configure, go to Settings > Update & Security > Windows Update > Advanced Options.
To exploit, see Flame malware documentation for guidance and technical support...

Azure Active Directory

Azure Active Directory


- Planetary-scale authentication database
- Used today for Office 365, OneDrive, Outlook.com, Xbox, Windows Phone, and more
- One-way or two-way sync with your on-premises Active Directory...or just replace it entirely
- The Goal: enroll every human and every device


Windows 10

- Microsoft Account login or creation integrated into the Windows 10 installation process
- Log onto desktop with Microsoft Account or Organizational Account
- Single sign-on with Universal apps and MS Office
- All Settings > Accounts > Your Account

← Settings

— □ ×

 ACCOUNTS

Find a setting 

Your account

Sign-in options

Work access

Family & other users

Sync your settings

ThorMonty

hughhugh@yahoo.com


Administrator

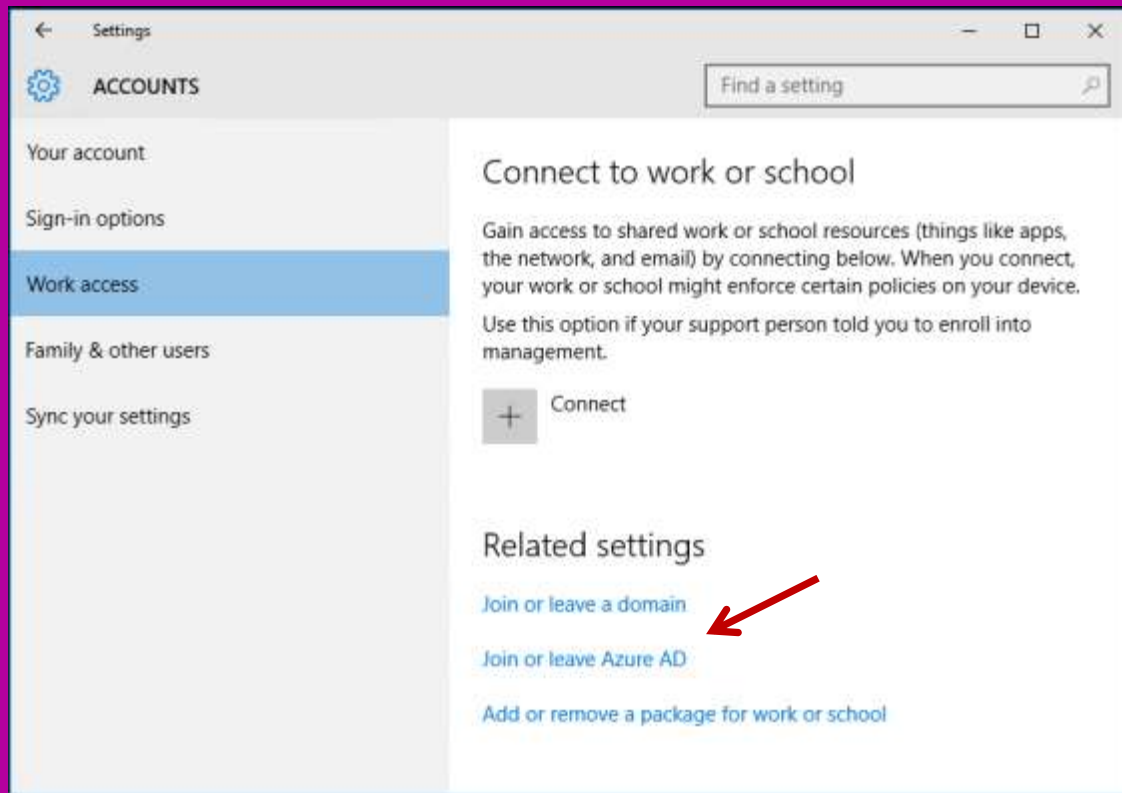
Billing info, family settings, subscriptions, security settings, and more

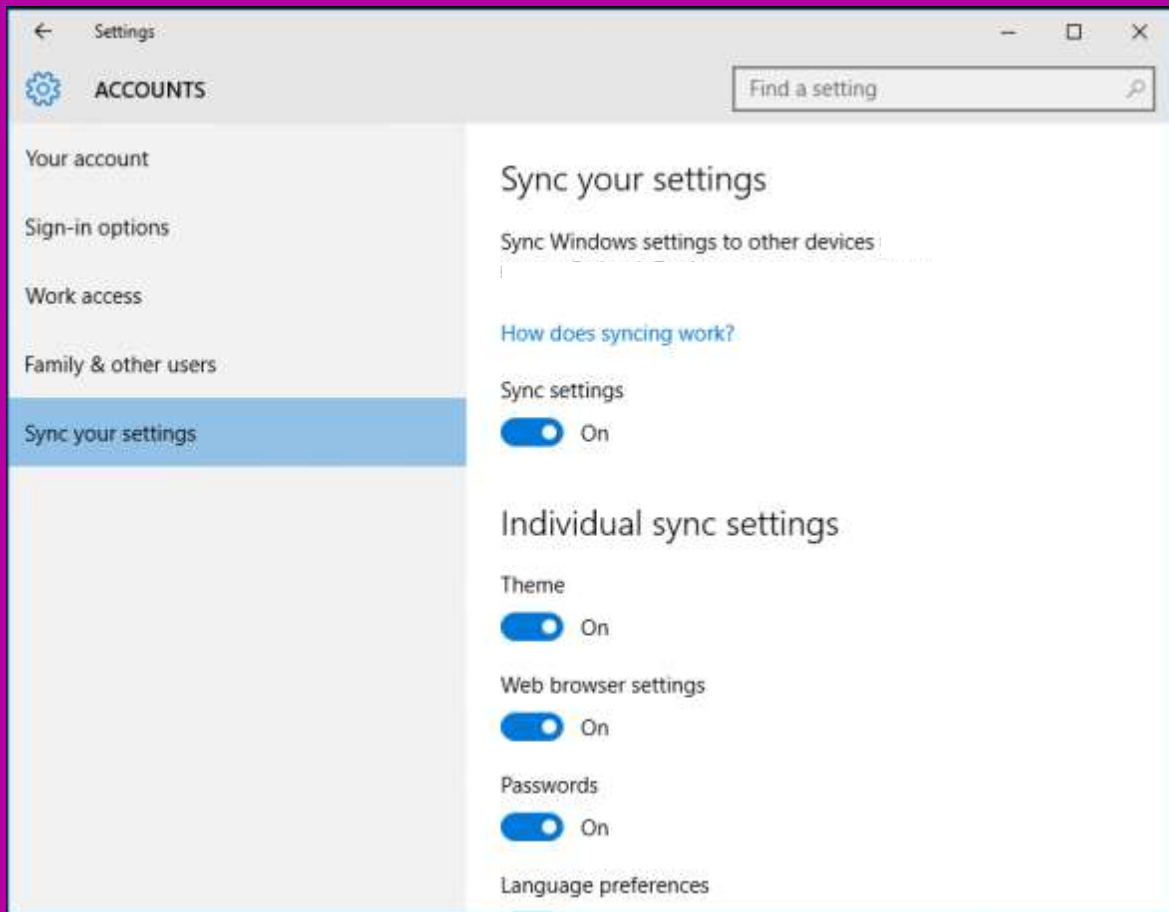
[Manage my Microsoft account](#)

[Sign in with a local account instead](#)

Your picture







Windows Hello

Hello = Biometrics Framework

- New biometric authentication support built into OS
 - Fingerprint and palm
 - Iris and retina
 - 3D facial geometry
- Plug-in support for new biometric data sources/devices

Fingerprint

- Supports surface, ultrasound, and thermal scanning
- Multiple individual fingers may be enrolled per user
- After five failures, user must enter PIN or passphrase
- Fingerprint data encrypted by TPM or passphrase



Image Credit: gizmag.com, Eikon Mini USB

Iris Scanner

- Lumia 950 XL Phone
- Infrared Iris Scanner
- Continuum docking station with HDMI and USB ports for keyboard and mouse



Infrared 3D Camera

- Built into phones, tablets, laptops, monitors
- Available as an external webcam (USB)
- Not just one camera, it includes:
 - Infrared laser emitter
 - Infrared camera
 - 1080p color image camera



Image Credit: japan.intel.com/realsense

The Australian Twins Test



- Six sets of twins:
 - "In the end, there were some cases of Windows Hello taking its time to identify a twin, but no case of it wrongly granting access."
 - But some false rejections when both enrolled on same computer
 - <http://www.theaustralian.com.au>

The Specs

- Authentication requires about 1 second
- 60 datapoints to construct vector map of face
- False Rejection Rate: 2-4%
- False Acceptance Rate: 1 in 100,000
- Liveness check can require the user to turn their head left and right a few centimeters



Your account

Sign-in options

Work or school

Family & other users

Sync your settings

PIN

You can use this PIN to sign in to Windows, apps, and services.

[Change](#)[I forgot my PIN](#)

Windows Hello

Sign in to Windows, apps and services using

Fingerprint

[Add another](#)[Remove](#)

Face

[Improve recognition](#)[Remove](#)

Automatically unlock the screen if we recognize your face



On

For extra security, require turning your head left and right to unlock the screen.



Off

Picture password

Sign in to Windows using a favorite photo

[Add](#)

Windows Hello setup



Your eyes couldn't be detected. Try moving your head slightly.

[Cancel](#)

Attacks

- 2D photograph will never work
- Maybe use multiple hi-res photographs from social media and a 3D printer to do an "evil twin" attack?
- After five scan failures, user must enter PIN
- TPM blocks further attempts after 32 PIN failures
- Facial geometry data encrypted with TPM or the user's logon passphrase, plus whole disk encryption

Microsoft Passport

Microsoft Passport

- Passport = public/private key web authentication
 - To be used by both Edge and Universal apps
- Designed to work with Windows Hello biometrics
 - Unlocks access to user's private keys
- Conforms to FIDO Alliance standards
 - FIDO = Fast Intity One

The FIDO Alliance

- FIDO Board Members:

- Microsoft
- Google
- PayPal
- Bank of America
- Visa
- MasterCard
- Samsung
- And others

- www.fidoalliance.org

- FIDO Goals:

- Replace passwords entirely (UAF)
- Augment password auth (U2F)
- Open scalable protocols
- Support many auth device types

- Important:

- One key pair per site, not shared
- Each device enrolled separately

Passport Requirements (1 of 2)

- PKI not required, key pair may be self-generated
 - But a PKI may be used instead of using "raw" keys
- Public key linked to the user's account *somewhere*
- May use Azure AD, on-premises AD, a hybrid of the two with sync, or a third-party identity provider
 - Azure AD is Microsoft's main target (all roads lead to Azure now)
 - On-premises AD requires Server 2016 and a schema update
 - On-premises AD also requires AD Federation Services

Passport Requirements (2 of 2)

- Windows 10
 - Any edition
 - Any type of device: phone, tablet, laptop, PC, maybe Xbox
- Client device joined to Azure AD, to an on-premises AD domain, or BYOD with a "work account" added
- TPM or smart card preferred, but not required

Credential Guard

Hardware & Firmware Requirements (1)

- UEFI 2.3.1 **Secure Boot** enabled and locked down
- **TPM** 1.2 or later in motherboard (for Credential Guard)
- Intel VT-x or AMD RVI **virtualization CPU extensions**
- Intel EPT or AMD RVI **Second Level Address Translation**
- Intel VT-d or AMD-Vi **IOMMU chipset** support

Hardware & Firmware Requirements (2)

- UEFI Secure Boot

- Firmware and OS loader must be signed and trusted
- UEFI variables for controlling boot and OS runtime settings

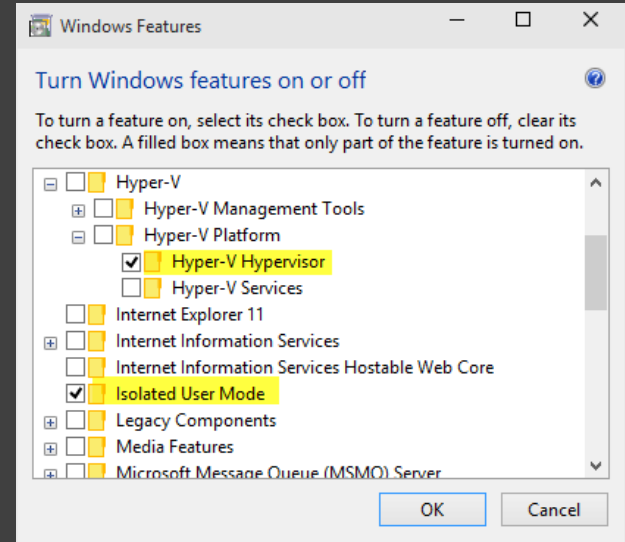
- Trusted Platform Module (TPM)

- Version 1.2 or later
- Crypto chip in the motherboard
- Virtual smart cards (and vTPM)
- Microsoft Passport key protection
- BitLocker key protection



Software Requirements

- Windows 10 Enterprise or Education Edition
- Only Microsoft corp trusted by UEFI for Secure Boot
- Physical host, not a VM
- All kernel-mode binaries signed by Microsoft



Where Are User Credentials In Memory?

- Run LSAISO.EXE in a tiny, hidden, hardened "VM"
 - Move LSASS.EXE credential secrets into LSAISO.EXE
 - Credential data never leaves the LSAISO.EXE process
 - LSASS requests non-replayable tokens from LSAISO.EXE
- Rely on type-1 hypervisor protections for LSAISO.EXE
 - Requires specific CPU and chipset features.
 - Normal kernel communicates with the "other kernel" through shared memory region (VMBus).

About that "Virtual Machine"...

- VM has no protocol stack
 - VM has no desktop or GUI
 - VM has a minimum set of Microsoft-only binaries
 - VM requires strict digital signature level protections
 - Communicates only through the hypervisor VMBus
-
- Even malware running in Ring 0 (kernel mode) in the hypervisor root partition cannot access VM

OK, It's Not A Real VM, But ...

CPU Protections	Normal User/OS Land	Virtual Secure Mode
Ring 3	Normal User Mode, LSASS.EXE	Isolated User Mode, LSAISO.EXE, vTPM, CI
Ring 0	Normal Kernel, Malware	Proxy Secure Kernel
Ring -1	Hyper-V Hypervisor & VMBus	
Hardware	CPU with VT-x, SLAT, IOMMU	

SLAT memory address translation tables map addresses, but these tables also include CPU-enforced *permissions*.

PowerShell

Open Source and Cross Platform

- PowerShell for Linux and Mac OS X
 - <https://github.com/PowerShell>
 - MIT License
 - .NET Core Framework open source too



SSH Client and Server (but not yet)

- "[T]his is the 3rd time the PowerShell team has attempted to support SSH. ... Given our changes in leadership and culture, we decided to give it another try ..."



Incident Response & New AV API

- **Greatly enhanced transcription logging**
 - Includes scriptblocks, Base64, in-memory only, console
 - Encrypt transcript data with your own public key
 - Manage through GPO or script to provide the key path/Base64
 - Decrypt at SIEM or with Unprotect-CmsMessage (uses CMS standard)
- **Anti-Malware Scan Interface (AMSI)**
 - Not just PowerShell: JScript, VBScript, Python, Ruby, etc.
 - AV after deobfuscation and just before it is executed

Security

- Enhancements for Just Enough Admin (JEA)
 - Control the commands/parameters available
 - Copy files within remoting sessions (no new open ports)
 - JEA Helper Tool 2.0+
- AppLocker can place PowerShell into "constrained language mode" to control interactive commands
 - `Get-Help about_Language_Modes -ShowWindow`
- Enhancements for Desired State Configuration (DSC)
 - The future of security templates and config automation; similar to Puppet

Subsystem for Linux



Run Linux binaries on Windows

- Not a Linux virtual machine
- Not Cygwin
- Not the old Services for Unix (SFU), which included user-mode binaries written by Microsoft
- The Goal: allow developers and sysadmins to run unmodified, user-mode, command-line Linux binaries directly on Windows, including bash, ruby, python, grep, ssh, apt-get, gcc, Docker tools, etc.

How does it work?

- Not enabled by default (go to Control Panel)
- Linux binary runs in a "pico process":
 - Pico processes do not include the Windows subsystem
 - Linux syscalls are intercepted (lxss.sys, lxcore.sys)
 - Windows kernel emulates Linux kernel APIs
 - Plan is to eventually implement all Linux syscall APIs
 - Maybe supported in Server Nano someday for daemons...

This will install Ubuntu on Windows, distributed by Canonical
and licensed under its terms available here:
<https://aka.ms/uowterms>

Type "y" to continue: y

Downloading from the Windows Store... 100%

Extracting filesystem, this will take a few minutes...

Installation successful!

Please enter a UNIX user name: root

Found UNIX user: root

The environment will start momentarily...

root@WIN10INSIDER:/mnt/c/WINDOWS/system32#

root@WIN10INSIDER:/mnt/c/WINDOWS/system32#

root@WIN10INSIDER:/mnt/c/WINDOWS/system32# cd ~

root@WIN10INSIDER:~#

root@WIN10INSIDER:~# pwd

/root

root@WIN10INSIDER:~#

root@WIN10INSIDER:~#

root@WIN10INSIDER:~# mount

rootfs on / type rootfs (ro,relatime)

tmpfs on /dev type tmpfs (rw,seclabel,nosuid,relatime,mode=755)

devpts on /dev/pts type devpts (rw,seclabel,relatime,mode=600)

proc on /proc type proc (rw,relatime)

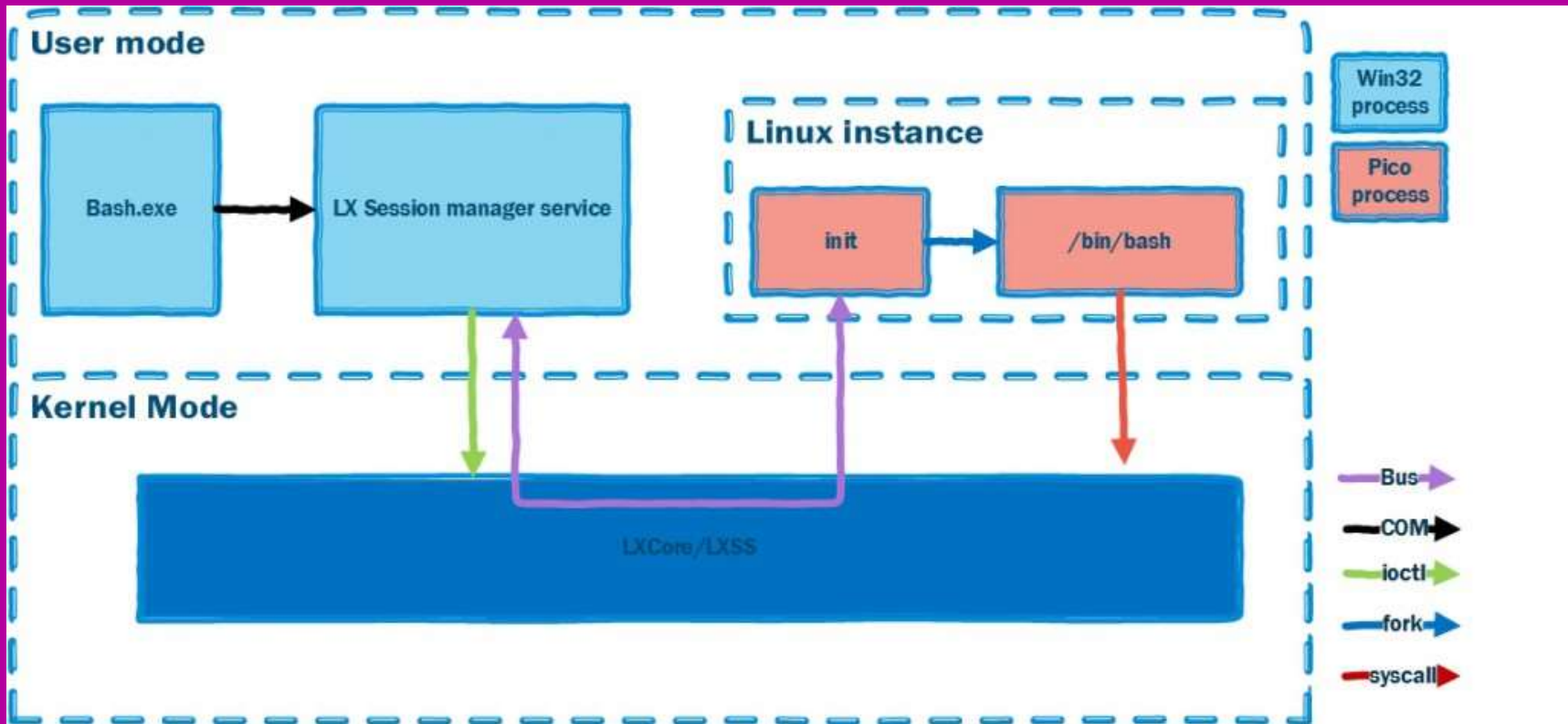
sysfs on /sys type sysfs (rw,seclabel,relatime)

root@WIN10INSIDER:~# █



Bash

```
root@WIN10INSIDER:/#  
root@WIN10INSIDER:/# ls -la  
total 125  
drwxrwxr-x 2 root root    0 Jan  1  1970 .  
drwxrwxr-x 2 root root    0 Jan  1  1970 ..  
drwxr-xr-x 2 root root    0 Apr 23 20:12 acct  
drwxr-xr-x 2 root root    0 Mar 23 20:45 bin  
drwxr-xr-x 2 root root    0 Mar 23 20:54 boot  
drwxrwx--- 2 1000 2001    0 Jan  1  1970 cache  
drwxrwx--x 2 1000 1000    0 Jan  1  1970 data  
drwxr-xr-x 2 root root    0 Apr 23 20:12 dev  
drwxr-xr-x 2 root root    0 Mar 23 20:54 etc  
drwxr-xr-x 2 root root    0 Jan  1  1970 home  
-rwxr-x--- 1 root root 22952 Jan  1  1970 init  
drwxr-xr-x 2 root root    0 Mar 23 20:54 lib  
drwxr-xr-x 2 root root    0 Mar 23 20:42 lib64  
drwx----- 2 root root    0 Mar 23 20:46 lost+found  
drwxr-xr-x 2 root root    0 Mar 23 20:41 media  
drwxrwxr-x 2 root 1000    0 Jan  1  1970 mnt  
drwxr-xr-x 2 root root    0 Mar 23 20:41 opt  
dr-xr-xr-x 1 root root    0 Apr 23 20:06 proc  
drwx----- 2 root root    0 Jan  1  1970 root  
drwxr-xr-x 2 root root    0 Apr 23 20:06 run  
drwxr-xr-x 2 root root    0 Mar 23 20:45 sbin  
drwxr-xr-x 2 root root    0 Mar 23 20:41 srv  
dr-xr-xr-x 1 root root    0 Apr 23 20:06 sys  
drwxrwxrwt 2 root root    0 Mar 23 20:54 tmp  
drwxr-xr-x 2 root root    0 Mar 23 20:41 usr  
drwxr-xr-x 2 root root    0 Mar 23 20:45 var  
root@WIN10INSIDER:/#  
root@WIN10INSIDER:/# ping localhost  
ping: icmp open socket: Socket type not supported  
root@WIN10INSIDER:/#
```



File Systems

- VOLFS
 - Full Linux support (symbolic links, case sensitivity, etc.)
 - /etc, /bin, /usr, and the other directories Linux needs
 - Hidden from Windows
- DRIVEFS
 - Partial Linux file system support, but still Linux-accessible
 - The C:\ drive in Windows will be mounted as /mnt/c
 - Hence, develop code in Linux, save files to Windows

Edge

Edge Is The New Default Browser

- Not included in Long Term Servicing Branch
- Desktop SKUs will still have IE installed
- Not many extensions available yet though
- Edge does not support:
 - ActiveX
 - Browser Helper Objects
 - VBScript
 - SilverLight



Edge Security

- Edge runs in an AppContainer sandbox
- Flash runs in a separate AppContainer process
- DEP + Forced ASLR + SEHOP
- Security Cookies (Stack Canaries)
- Low Fragmentation Heap
- Null Pointer Dereference Protection
- Control Flow Guard (Win8.1 Update 3)

Windows Server 2016

Server Nano

- **Nano runs completely headless**
 - No graphical desktop whatsoever
 - Runs the tiny OneCore kernel (similar to stripped-down Linux)
 - Can run from RAM drive (PXE boot, then SMB download of WIM image)
 - Managed through PowerShell remoting, DSC, WMI, serial cable EMS
- **Mainly intended for hosting VMs and web apps:**
 - Currently supports Hyper-V, Chef, PHP, Nginx, Python 3.5, Node.js, GO, Redis, MySQL, OpenSSL, Java (OpenJDK), Ruby 2.1.5, SQLite, and ASP.NET 5 (limited to Core CLR)

User name: _____
Domain: _____
Password: _____

ENTER Authenticate

Server Configuration

=====

Computer Name: Nano1

Workgroup: WORKGROUP

OS: Microsoft Windows Server 2016 Technical Preview 3 Tuva

Ethernet

192.168.1.119	fe80::e164:9f69:edd:4da2%3	00-15-5D-01-66-11
	2605:6001:e6c8:d000:e164:9f69:edd:4da2	

> Networking

Up|Dn Scroll|ESC Log out|Ctl+F6 Restart|Ctl+F12 Shut down

Default
Processes:

PowerShell
remoting into
Nano box
from admin
laptop ->

```
F:\Hyper-V-Images\Server2016-BETA3-Nano ($?: True : LastExitCode=0)
File Edit View Tools Debug Add-ons Help
[192.168.1.119]: PS C:\> Get-Process | Format-Table -AutoSize

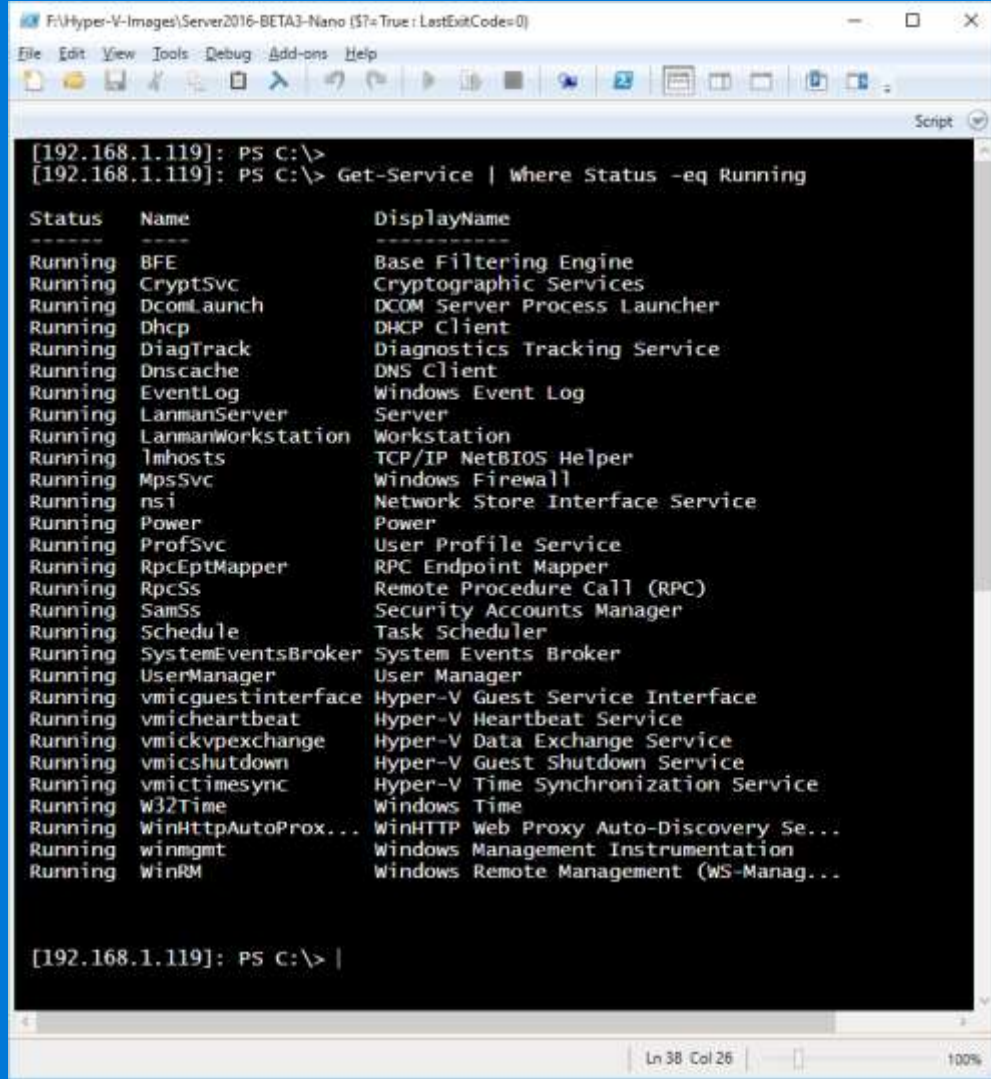
Handles  NPM(K)  PM(K)  WS(K)  VM(M)  CPU(s)  Id  ProcessName
-----
98        6     584   1592   2097161  0.00    320  csrss
66         5     800   3444   2097166  0.00   1044  EMT
0          0         0      4        0  0.00     0  Idle
598       17   3132   9248   2097187  0.13    396  lsass
166        8   1532   4772   2097166  0.00    376  services
44         3    296   1112   2097156  0.00    244  smss
351       15   5524  12804   2097228  0.13    280  svchost
175        8   1380   4856   2097177  0.06    488  svchost
235       13   1492   5304   2097178  0.05    524  svchost
132        8   1408   4984   2097175  0.06    620  svchost
119        7   1260   5692   2097175  0.00    632  svchost
273       15   7128  11580   2097192  0.09    688  svchost
385       17   5644  14112   2097230  0.16    760  svchost
210       13   2064   6792   2097179  0.00    796  svchost
326       25   3416  10296   2097197  0.06    820  svchost
286       28   3704   8752   2097189  0.06    888  svchost
302        0     80     76        2  0.84     4  System
72         7    660   3596   2097167  0.00    348  wininit
136        7   1668   6352   2097175  0.00   1360  WmiPrvSE
527       52  58896  77552   2097622  4.80   1584  wsmprovhost

[192.168.1.119]: PS C:\> |
```

Ln 28 Col 26 100%

Default
Services:

PowerShell
remoting into
Nano box
from admin
laptop ->



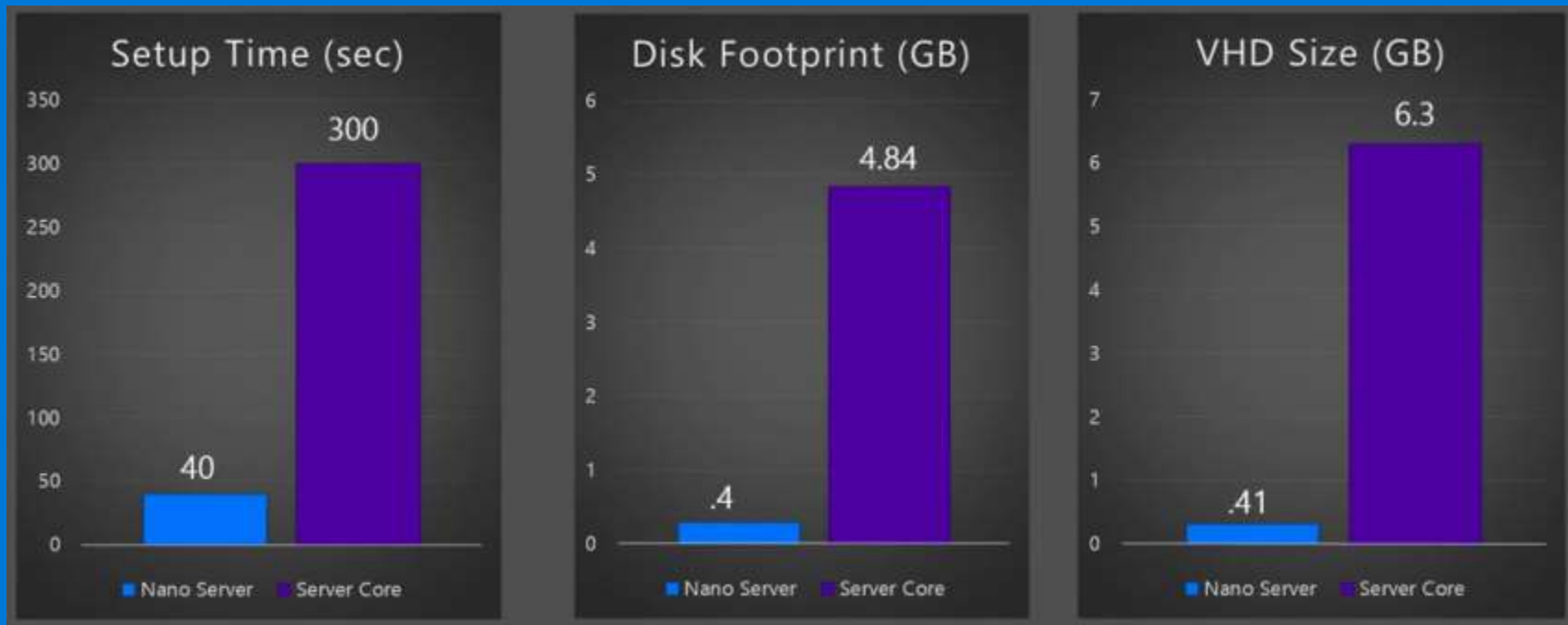
```
F:\Hyper-V-Images\Server2016-BETA3-Nano ($?)=True: LastExitCodes=0
File Edit View Tools Debug Add-ons Help
Script
[192.168.1.119]: PS C:\>
[192.168.1.119]: PS C:\> Get-Service | Where Status -eq Running

Status Name DisplayName
-----
Running BFE Base Filtering Engine
Running CryptSvc Cryptographic Services
Running DcomLaunch DCOM Server Process Launcher
Running Dhcp DHCP Client
Running DiagTrack Diagnostics Tracking Service
Running Dnscache DNS Client
Running EventLog Windows Event Log
Running LanmanServer Server
Running LanmanWorkstation Workstation
Running lmhosts TCP/IP NetBIOS Helper
Running Mpssvc Windows Firewall
Running nsi Network Store Interface Service
Running Power Power
Running ProfSvc User Profile Service
Running RpcEptMapper RPC Endpoint Mapper
Running RpcSs Remote Procedure Call (RPC)
Running SamSs Security Accounts Manager
Running Schedule Task Scheduler
Running SystemEventsBroker System Events Broker
Running UserManager User Manager
Running vmicguestinterface Hyper-V Guest Service Interface
Running vmicheartbeat Hyper-V Heartbeat Service
Running vmickvpexchange Hyper-V Data Exchange Service
Running vmicshutdown Hyper-V Guest Shutdown Service
Running vmictimesync Hyper-V Time Synchronization Service
Running W32Time Windows Time
Running WinHttpAutoProx... WinHTTP Web Proxy Auto-Discovery Se...
Running winmgmt Windows Management Instrumentation
Running WinRM Windows Remote Management (WS-Manag...

[192.168.1.119]: PS C:\> |
```

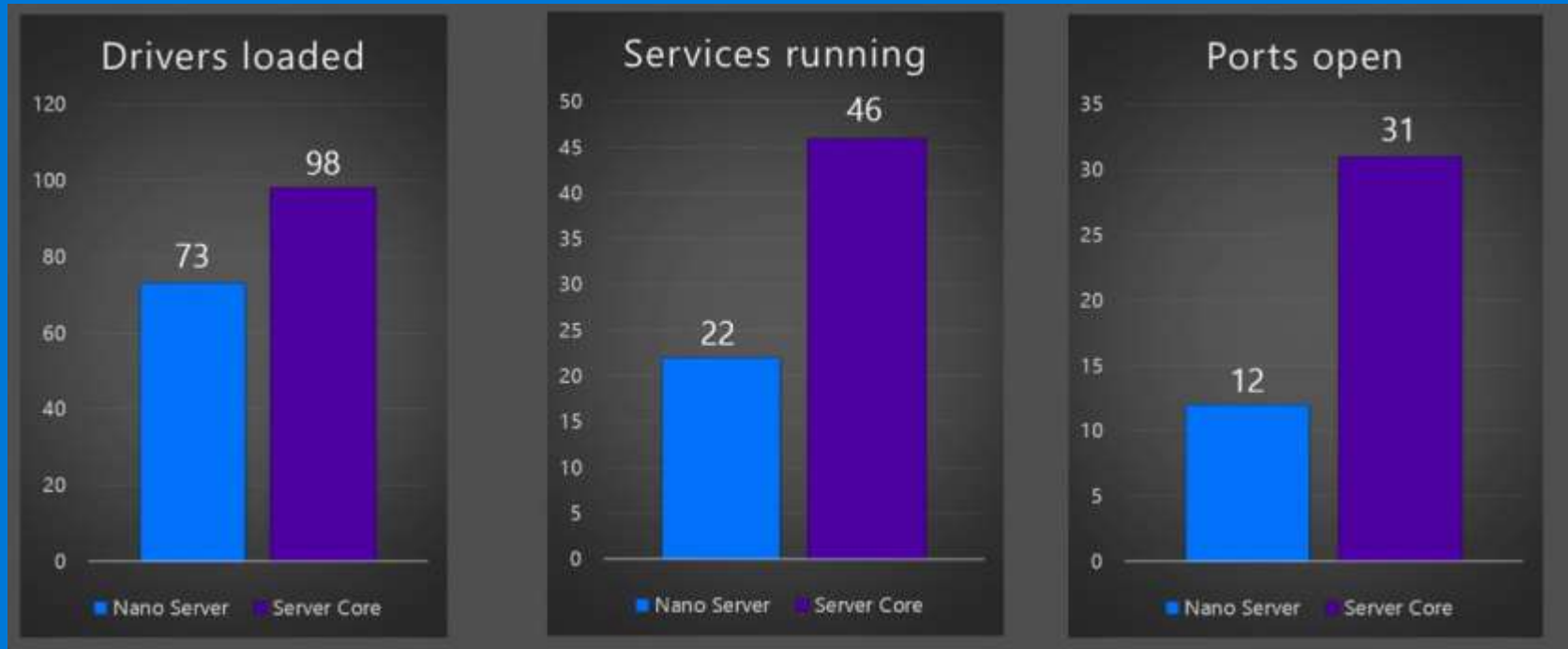
Ln 38 Col 26 100%

Nano vs. Core: Footprint



Credit: https://channel9.msdn.com/Events/Ignite/2015/BRK2461?WT.mc_id=IG15XCSOSC

Nano vs. Core: Attack Surface



Credit: https://channel9.msdn.com/Events/Ignite/2015/BRK2461?WT.mc_id=IG15XCSOSC

Server 2016 Supports Docker Containers

- Server Nano supports the container runtime
 - Best for pure web apps: ASP.NET, Node.js, Nginx, PHP, MySQL, etc.
- Server Core supports the container runtime
 - Best for anything that requires Windows API or full .NET support
- Nano/Core container hosts can themselves be VMs
 - Hyper-V supports nested VMs in Server 2016
- Manage with PowerShell or regular Docker tools

Even Better: Hyper-V Container Runtime

- Traditional containers run as *shared-kernel*
 - Not ideal for security, there can be "container escape"
- Hence, there are two container runtimes:
 1. Traditional shared-kernel runtime
 2. Hyper-V isolated runtime
 - This is not a VM that happens to have traditional containers inside it
 - Hyper-V uses hardware-assistance to wrap the containers
 - A container made for one can be used in the other runtime as-is
 - Windows containers FAQ: <http://aka.ms/WindowsContainers>

Hyper-V Container Runtime: Sessions

- Each container has its own MAC and IP address
 - Plugs directly into Hyper-V virtual switch, just like a VM
- You can RDP into a container to get a GUI desktop
- Each container has its own Session ID number:
 - Session 0: for kernel threads, device drivers, SMSS.EXE
 - Session X: for console, RDP sessions, and each container
 - Each container with its own LSASS.EXE, SVCHOST processes, files, etc!

What Else? (Not Enough Time...)

- Container support on Windows 10 too!
- Device Guard -- Unjailbreakable Windows?
- Provable PC Health -- Revenge of NAP!
- Enterprise Data Protection -- EFS rises again!
- MDM management support (not just with Intune)
- DNS Policies for split-brain DNS, sinkholes, etc.
- Many enhancements in Hyper-V (too many...)
 - See www.AidanFinn.com

Thank You for Attending!

- See you in my *Securing Windows* course (SEC505)?
 - <http://sans.org/sec505>
- Let's connect on LinkedIn and Twitter!
 - @JasonFossen
- Get my PowerShell scripts and this slide deck:
 - <http://cyber-defense.sans.org/blog/downloads>
 - Get the SEC505 zip file, then look in the Extras folder