WINDOWS 10 ENTERPRISE
New Security Features

Demystified!

J. Abernethy – mindSHIFT Technologies
Josh Quinn – mindSHIFT Technologies

#ILTALSS
#LSS26
TODAY’S AGENDA

• Windows 10 Security Fundamentals
• Managing Windows 10 Security
• New Windows 10 Security Features
WIN10 SECURITY FUNDAMENTALS

• Features Forward
  – Windows 7: NTFS, UAC, Windows Firewall, BitLocker, AppLocker, Least Privilege, SmartScreen
  – Windows 8: TPM Key Attestation, Kerberos Armoring, Modern App Isolation

• EMET now in Windows 10 core

• Other areas: LAPS, MBAM
Threat protection over time
Attackers take advantage of periods between releases.
Disrupt and out innovate our adversaries by design.

Great change with Windows and Software as a Services

Protection Gap

WINDOWS 10: SERVICING MODEL

PRODUCT RELEASE  THREAT SOPHISTICATION
WINDOWS 10: SERVICING MODEL
MANAGING WINDOWS 10 SECURITY

• Group Policy
• PowerShell
• Mobile Device Management
• System Center Configuration Manager
WINDOWS 10: HARDENING GUIDELINES

• OS Hardening guidelines still apply
  – Center for Internet Security: Win10 Enterprise Benchmark
  – DISA guidelines

• Update to the latest ADMX templates relevant to your branch

• Specific Windows 10 areas to focus:
  – Privacy settings
  – Modern Application Management
  – New Security Features
  – Windows 10 “enhancements” – e.g. WLAN HotSpots, Lock screen notifications
## WIN10 – NEW SECURITY FEATURES

### PROTECT, DETECT & RESPOND

<table>
<thead>
<tr>
<th>PRE-BREACH</th>
<th>POST-BREACH</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device protection</strong></td>
<td><strong>Breach detection investigation &amp; response</strong></td>
</tr>
<tr>
<td><img src="image1" alt="Device integrity" /></td>
<td><img src="image2" alt="Conditional Access" /></td>
</tr>
<tr>
<td><img src="image3" alt="Device control" /></td>
<td></td>
</tr>
<tr>
<td><strong>Threat resistance</strong></td>
<td></td>
</tr>
<tr>
<td><img src="image4" alt="SmartScreen" /></td>
<td></td>
</tr>
<tr>
<td><img src="image5" alt="Windows Firewall" /></td>
<td></td>
</tr>
<tr>
<td><img src="image6" alt="Microsoft Edge" /></td>
<td></td>
</tr>
<tr>
<td><img src="image7" alt="Device Guard" /></td>
<td></td>
</tr>
<tr>
<td><img src="image8" alt="Windows Defender" /></td>
<td></td>
</tr>
<tr>
<td><strong>Identity protection</strong></td>
<td></td>
</tr>
<tr>
<td><img src="image9" alt="Windows Hello :)" /></td>
<td></td>
</tr>
<tr>
<td><img src="image10" alt="Credential Guard" /></td>
<td></td>
</tr>
<tr>
<td><strong>Information protection</strong></td>
<td></td>
</tr>
<tr>
<td><img src="image11" alt="BitLocker and BitLocker to Go" /></td>
<td></td>
</tr>
<tr>
<td><img src="image12" alt="Windows Information Protection" /></td>
<td></td>
</tr>
<tr>
<td><strong>Device integrity</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Device control</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Device protection</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Threat resistance</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Identity protection</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Information protection</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Device integrity</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Device control</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Device protection</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Threat resistance</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Identity protection</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Information protection</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Device integrity</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Device control</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Device protection</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Threat resistance</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Identity protection</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Information protection</strong></td>
<td></td>
</tr>
</tbody>
</table>
DEVICE PROTECTION: DEVICE INTEGRITY & CONTROL

• Trusted Platform Module
  – What this allows, and why it is important
  – Foundation for many other technologies

• Secure Boot, Trusted Boot, ELAM
  – An advanced integrity check of your OS
  – Requires TPM 1.2, UEFI, Windows 8.1 or higher
  – Consider disabling pre-boot authentication!
WINDOWS 10: VIRTUALIZATION BASED SECURITY

- Separate virtual environment with small surface area
- May store Code Integrity Policies, Credential Information, future initiatives
- Requires UEFI / Secure Boot, virtualization Extensions, Trusted Platform Module
- Compatible with Hyper-V
THREAT RESISTANCE: DEVICE GUARD

• Previous Microsoft Whitelisting Options
  – Software Restriction Policies
  – AppLocker

• Challenges
  – Vulnerable to Kernel mode attacks
  – Management
THREAT RESISTANCE: DEVICE GUARD

- Provides a security model similar to mobile device operating systems.

- Only allows execution of signed applications and drivers but may be configured for “audit” mode.

- Firms can establish their own integrity policies for the “master image” and unsigned applications, but will need to manage catalogs and code signing.

- Leverages Virtualization Based Security Model.

- Challenges........................
THREAT RESISTANCE: MICROSOFT EDGE

• Current Security Features
  – SmartScreen
  – Universal App Model
  – Protected Extensions
  – Small Surface Layer

• Application Guard
  – Leverages Virtualization Based Security
  – Provides Browser Containerization and isolation
  – Available in Win10 Enterprise 16188 (Fast Ring)
IDENTITY PROTECTION: CREDENTIAL GUARD

• Defends Against Pass-The-Hash style attacks
• Requirements
  – Win10 Enterprise/Education (x64)
  – UEFI / TPM 2.0+
• Challenges
  – Domain Credentials only!
IDENTITY PROTECTION: WINDOWS HELLO FOR BUSINESS

• A world without passwords
• “Multifactor” – Something you have (an enrolled device), and something you know (a PIN)
• Biometrics provide convenience
• Challenges
INFORMATION PROTECTION:
WIP OVERVIEW

• Platform integrated, no mode switching

• Classifies data coming from managed network locations and repositories

• “Enlightened” Apps are able to distinguish between corporate and personal data

• Controls copy/paste behavior

• Supports selective wipe

• Leverages SCCM, MDM for policy management
INFORMATION PROTECTION: WIP CHALLENGES

• Number of Enlightened apps are limited
• Limited 3rd party repository support
• Auditing / monitoring is rudimentary
• Single user per device
• Redirected folders / Offline Cache are not supported
• May cause issues with application deployment
BREACH DETECTION: WINDOWS DEFENDER ATP

- Behavior-based, cloud-powered breach detection system
- Agent is built in to Windows 10
- Leverages Microsoft’s threat intelligence knowledge base
- Powerful tool for investigation and analysis across endpoints
WINDOWS 10 SECURITY RECOMMENDATIONS

Required
- BitLocker, MBAM, LAPS
- SecureBoot, UEFI, TPM
- OS Hardening, A/V, Firewall

Optional
- Credential Guard
- Windows Defender ATP
- Microsoft Edge Application Guard

Future
- Device Guard
- Windows Information Protection
- Windows Hello for Business
Thank You

J Abernethy
Manager – Legal Applications
J.Abernethy@mindSHIFT.com

Josh Quinn
Managing Director
Josh.Quinn@mindSHIFT.com

info@mindSHIFT.com
www.mindSHIFT.com