

HIGH
 PUSHBACK BY END USERS
 LOW

Ask first

No Brainers*

<ul style="list-style-type: none"> Disallow Microsoft Accounts (may impact Azure AD) Password policies Restrict Local Admin Tools (some) Enforce UAC? Disallow Software Installs Enable SmartScreen Disable Terminal Server Services (RDP) Disable (or enable) firewall(s) Disable Protocols (TEST FIRST) 	<ul style="list-style-type: none"> Data protection policies Email lockdown Social Media lockdown Alert / Action on Excessive Logon Failures Monitor for Ransomware Disable AppData EXE
<ul style="list-style-type: none"> Local Admin Account protection policies Disable Guest Account Restrict Local Admin Tools (some) Disable Windows Keylogger Enable Logon Message Disable UPnP Disable Autorun Uninstall Blacklisted Applications Disable Office Macros Disable OLE Log All Logon and Logoff Events 	<ul style="list-style-type: none"> User Logon Report Disable "stores" Enhance Security Event Logging (HIPAA) Monitor Event Log Clearing (Ransomware) Alert on Excessive Logon Failures (Ticket only option) Monitor for Ransomware (Ticket only option) Alert on Unencrypted (Bitlocker) Disk (HIPAA)

Prevent Issues

Generate Revenue

BENEFIT TO SERVICE PROVIDER

*NOTE: use your judgment and situational factors to determine if our suggested No Brainers would actually be No Brainers in your environment.