The Defence Signals Directorate Top 4 Mitigations Against Cyber Intrusion

An Implementation Guide for Project Managers

Microsoft

Contents

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

Introduction

Information security teams within Australian organisations are striving to achieve two key missions. On the one hand they're working to build a greater level of resilience to information security threats, whether they arise from accidental or deliberate actions by employees and partners, malware, or even targeted intrusions by determined attackers. On the other hand, they're trying to adapt to the changing technology landscape and demands of their business, especially within the context of cloud computing, the proliferation of devices and an increasingly mobile workforce.

This dual mission of building both resilience and adaptability is complex and difficult to deliver upon. It is challenging to identify the most important steps to take, to identify dependencies, quantify the business case and catalogue resource requirements for a program of work that effectively balances the inevitable complexities, risks and issues.

Fortunately, the work of the Defence Signals Directorate (DSD) in developing the Top 35 Strategies to Mitigate Targeted Cyber Intrusion provides an excellent starting point for prioritisation. Implementing the Top 4 mitigation strategies as a package is particularly important, as DSD has documented that 85% of the intrusions they responded to in 2011 involved adversaries using unsophisticated techniques that would have been mitigated by implementing application whitelisting, ensuring that modern applications are deployed and patched, deploying modern, patched operating systems and restricting administrative privileges. But these mitigations not only help organisations improve their resilience to attack: a modern computing platform that incorporates these measures will also be more manageable, have higher performance, be more configurable to support the flexible working practices demanded by business, and is typically operated at a lower total cost of ownership.

The goal of this paper is to provide a program framework for the implementation of the DSD Top 4 mitigations in a manner that delivers a real improvement in both resilience and adaptability. This paper is intended for a management audience who need to understand:

- A brief outline of how cyber intrusion occurs and the DSD Top 35 mitigations;
- How Microsoft technologies can be applied to implement these controls;
- The security and business benefits of each of the Top 4 mitigations;
- The stages and key activities, indicative timelines, inputs and outcomes of projects which can be used to implement each of the top 4 mitigations;
- Risks, issues, challenges and important contingencies to incorporate into implementation planning; and
- Links to further resources that can help with migration to a modern computing platform

The activities required to implement the mitigation controls will vary greatly between organisations, depending on their current operating state, scale, security sensitivity, dependence on legacy applications and the extent to which portions of the Top 4 have already been addressed. This document is primarily therefore aimed at organisations that currently use either a Windows XP, Vista or Windows 7 operating system, have a significant dependence on legacy applications, have sub-optimal patching processes, a moderate level of credential restrictions and no application whitelisting.

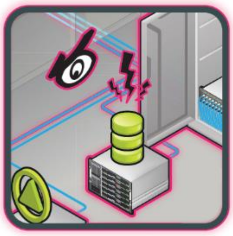
With most organisations facing an increasing risk of cyber intrusion and compelling events such as the end-of-support for Windows XP in April, 2014, this paper aims to help organisations move more rapidly on the path to full implementation of the DSD Top 35 Mitigations.

Understanding Cyber Intrusion

Targeted cyber intrusions can take advantage of a variety of technical and human weaknesses, such as Web servers susceptible to injection of code, unpatched browsers that inadvertently enable malware downloads or users who succumb to opening malware laden email attachments. There is no single pattern of attack, nor is there an entirely predictable sequence of events. An attack might be a single event that lasts for minutes, or a sustained progression of intrusions that last for months or even years. However, it is useful to conceptualise a targeted cyber intrusion in terms of three stages: code execution, network propagation and data exfiltration:

1 Code Execution

An adversary performs reconnaissance to select a target user, and sends this user a malicious email containing a malware-laden attachment or link to a Web site. This reconnaissance is easier if the user's email address and additional information is readily available on public web sites, social networking Web sites, or if the user uses their email address for purposes unrelated to work. By opening the attachment or visiting the Web site, malicious code is executed on the user's workstation and is typically configured to persist by automatically executing every time the user restarts their computer and/or logs on. The malicious code is remotely controlled by the adversary, enabling them to access any information that is accessible to the user.



2 Network Propagation

The adversary moves through the network to access information on other workstations and servers. Such information typically includes Microsoft® Office files, PDF files as well as information stored in application databases. Adversaries also typically access system information including computer and network configuration details, as well as details about users including organisation hierarchy, usernames and passphrases. Although passphrases might be stored as cryptographic hashes to frustrate adversaries, cracking such passphrase hashes to derive the passphrases may be fast, cheap and easy unless all users have selected very strong passphrases that are appropriately hashed. Other modern techniques, commonly referred to as 'pass-the-hash' approaches bypass the need to crack passwords, enabling attackers to traverse the network by impersonation using captured credentials. The appropriate use of multi-factor authentication may hinder adversaries.

3 Data Exfiltration

The adversary exfiltrates information from the network using network protocols and ports allowed by the organisation, such as HTTPS, HTTP, or in some cases DNS and email. The adversary typically leaves behind several compromised computers as a backdoor to facilitate further exfiltration of information in the future.

For further guidance, refer to http://www.dsd.gov.au/infosec/top-mitigations/top35mitigation-details.htm

The Risk of Windows XP End of Support

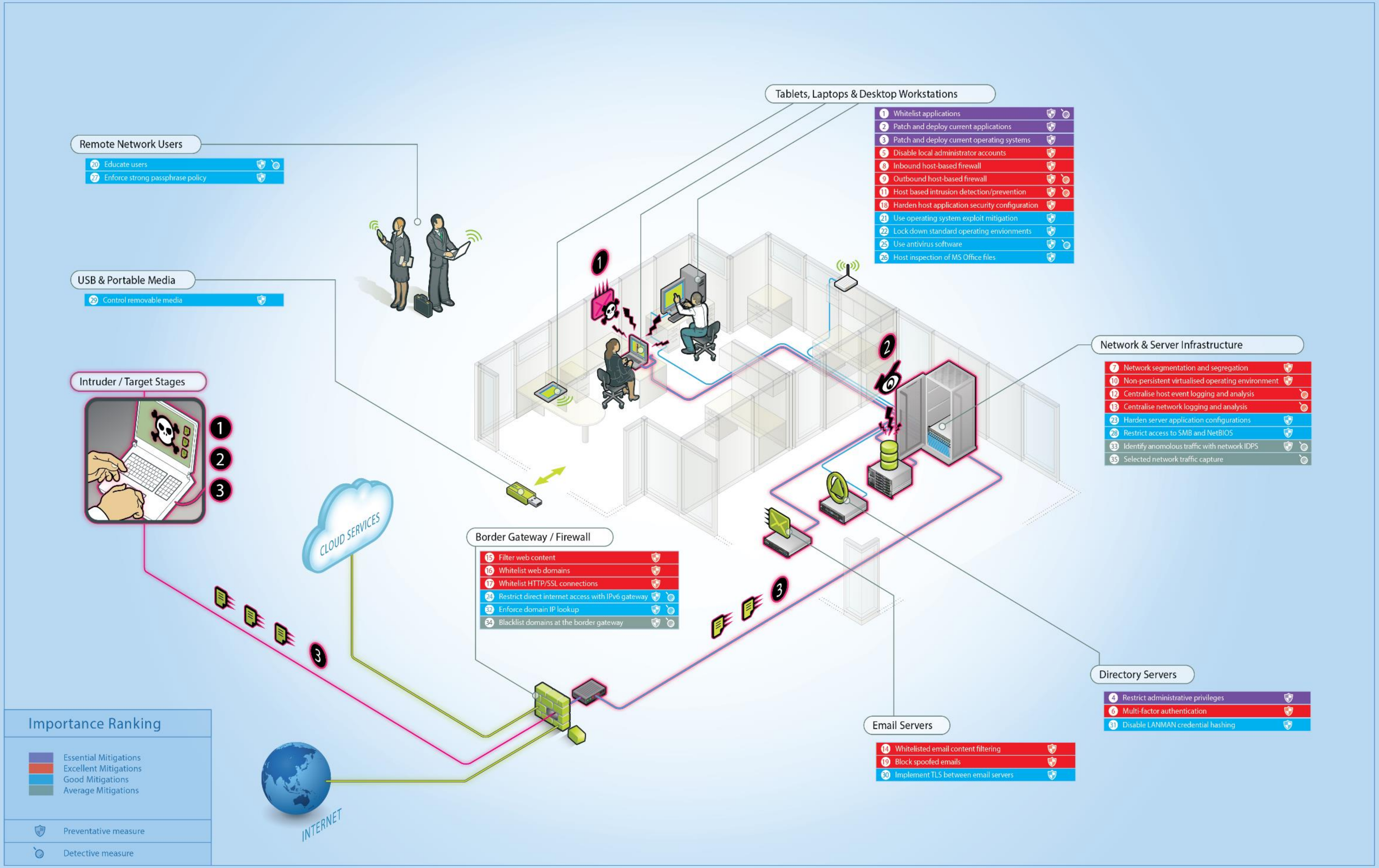
From April 8th, 2014 Microsoft will globally cease to provide extended support for Windows XP, meaning we will no longer provide freely available security updates. As a 12 year old technology, Windows XP was simply not designed for the cyber security threats that have emerged over the last decade. Despite enhancements and updates, all fundamental security improvements have been made in successor technologies such as Windows Vista, Windows 7 and more recently Windows 8.

The Australian Defence Signals Directorate recently published a broadcast strongly recommending government agencies migrate to a more modern computing platform, warning of the consequences of running an unsupported operating system past this date:

> *"DSD strongly recommends agencies using Windows XP SP3 and Office 2003 upgrade to newer supported operating systems and software*
>
> *Vulnerabilities in unsupported operating systems and applications won't be fixed, and cyber adversaries are aware of this and may identify these vulnerabilities as opportunities to target government systems. As a result, the likelihood of a successful cyber incident on an agency's system is increased, which consequently elevates the security risk profile of the agency.*
>
> *The latest versions of operating systems offer significant improvements in security features, functionality and stability. The latest versions of applications typically incorporate newer security technologies and mitigate known vulnerabilities. Using the latest versions of operating systems and applications, along with patch management, are some of the most effective security practices agencies can perform."*
>
> *DSD Broadcast October 2012 -*
> *Upcoming end of support for Microsoft Windows XP*
> *SP3 and Microsoft Office 2003*

Most federal and state government agencies and businesses in Australia have either already migrated off Windows XP or have plans underway to do so prior to April 2014. If you are not already well underway with the migration, the risks are real. They can be broadly classified as:

- **Security risks.** Windows XP is already challenged without the security protections needed to thwart determined attacks. With no security updates available post April 2014, the risk of intrusion and malware infection are significantly raised.
- **Unsupported business software.** Most Independent Software Vendors have already stopped testing new software versions on Windows XP, and new releases of critical business software will likely require Windows 7 at a minimum.
- **Unsupported hardware.** Hardware Vendors and OEM's have also stopped testing new devices on Windows XP. Many are currently shipping computers that will not support XP and device drivers are also not available.
- **Increased support costs.** Software Assurance will not provide support past April 8, 2014. Customers needing support on XP will be required to have Windows XP Custom Support Agreement (CSA) in place and additional costs incurred will include an Enrollment Fee, Per HotFix Fee, and a Per Device Fee.



Tablets, Laptops & Desktop Workstations

- 🟪 1 Whitelist applications 🛡 🔍
- 🟪 2 Patch and deploy current applications 🛡
- 🟪 3 Patch and deploy current operating systems 🛡
- 🟥 5 Disable local administrator accounts 🛡
- 🟥 8 Inbound host-based firewall 🛡
- 🟥 9 Outbound host-based firewall 🛡 🔍
- 🟥 11 Host based intrusion detection/prevention 🛡 🔍
- 🟥 18 Harden host application security configuration 🛡
- 🟦 21 Use operating system exploit mitigation 🛡
- 🟦 22 Lock down standard operating envionments 🛡
- 🟦 25 Use antivirus software 🛡 🔍
- 🟦 26 Host inspection of MS Office files 🛡

Remote Network Users

- 🟦 20 Educate users 🛡 🔍
- 🟦 27 Enforce strong passphrase policy 🛡

USB & Portable Media

- 🟦 29 Control removable media 🛡

Network & Server Infrastructure

- 🟥 7 Network segmentation and segregation 🛡
- 🟥 10 Non-persistent virtualised operating environment 🛡
- 🟥 12 Centralise host event logging and analysis 🔍
- 🟥 13 Centralise network logging and analysis 🔍
- 🟦 23 Harden server application configurations 🛡
- 🟦 28 Restrict access to SMB and NetBIOS 🛡
- ⬜ 33 Identify anomolous traffic with network IDPS 🛡 🔍
- ⬜ 35 Selected network traffic capture 🔍

Intruder / Target Stages

Border Gateway / Firewall

- 🟥 15 Filter web content 🛡
- 🟥 16 Whitelist web domains 🛡
- 🟥 17 Whitelist HTTP/SSL connections 🛡
- 🟦 24 Restrict direct internet access with IPv6 gateway 🛡 🔍
- 🟦 32 Enforce domain IP lookup 🛡 🔍
- ⬜ 34 Blacklist domains at the border gateway 🛡 🔍

Directory Servers

- 🟪 4 Restrict administrative privileges 🛡
- 🟥 6 Multi-factor authentication 🛡
- 🟦 31 Disable LANMAN credential hashing 🛡

Email Servers

- 🟥 14 Whitelisted email content filtering 🛡
- 🟥 19 Block spoofed emails 🛡
- 🟦 30 Implement TLS between email servers 🛡

Importance Ranking

- 🟪 Essential Mitigations
- 🟥 Excellent Mitigations
- 🟦 Good Mitigations
- ⬜ Average Mitigations

🛡 Preventative measure

🔍 Detective measure

Defence in Depth – The Top 35 Mitigations

#1 #2 #3 #5 #8 #9 #11 #18 #21 #22 #25 #26 #29

Strengthen workstation defences beyond the top 4 mitigations by deploying antivirus software, firewall restrictions, device encryption, and controls on removable media within a managed operating environment. Microsoft® System Center 2012 along with Windows® 8 provide a complete platform for end-to-end host protection along with guidance in the Microsoft Deployment Toolkit and Microsoft Security Compliance Management solution accelerators.

#4 #6 #31

Enforce strong user authentication by progressing towards enforcement of strong passphrases and the use of multi-factor authentication such as smart cards. Technologies like Microsoft® Forefront® Identity Manager and Active Directory provide a broad platform for identity management and strong authentication.

#14 #19 #30

Protect your email service from spoofed emails, spam, targeted phishing and email interception by whitelisting allowable attachment types so that vulnerable content types or executable files are prohibited, implementing Sender ID or Sender Policy Framework controls, and enabling additional authentication between email servers (TLS). These protections can be enabled in Microsoft® Exchange Server 2013 and complemented with new features for data loss prevention.

#15 #16 #17 #23 #24 #32 #34

Defend the web gateway and harden web applications by filtering the allowable content types and whitelisting allowable domain names for both normal and encrypted traffic. Firewall technology at the gateway should implement application layer protections, stateful inspection and content filtering. Harden web applications by addressing the most common and easily mitigated web application vulnerabilities, such as SQL injection and cross-site scripting.

#10 #12 #18

Monitor your system infrastructure by maintaining a central configuration and asset management database, automated management processes along with centralised monitoring of server, device and network equipment. Microsoft® System Center 2012 can provide these capabilities.

#7 #13 #33 #35

Monitor your network by centralising logging and using network based intrusion detection to identify and respond to anomalies. Network segmentation is also crucial along with network protections enforced by technologies like Network Access Protection in Windows Server® 2012.

#20 #27

Educate users about social engineering including how they can be targeted and how they should respond to suspicious requests, be careful of the information they release and report any incident. In turn, it's important to have a social engineering response process to identify if the threat is real and alert users to prevent an eventual successful breach from a sustained attack.

Implementing Mitigation #1 – Application Whitelisting

Application whitelisting is about identifying specific executables and software libraries that should be permitted to execute on a given system, then enforcing a policy so that only those identified components can operate. A system protected by explicit whitelisting of allowed applications will typically prevent malware such as a remote access tool from executing, providing an effective mitigation against the first stage of a targeted attack, even if the attack tool is not recognised by traditional signature based anti-malware.

Microsoft AppLocker is a set of policy settings and software components within Windows® 7, Windows 8, Windows Server 2008 and Windows Server 2012 that allow multiple levels of whitelisting enforcement as well as several methods of recognising whitelisted executables.

Self-Assessment:

Answer each of these questions with a score of 1 (lowest) to 5 (highest):

a Have you deployed application whitelisting to sensitive client systems (1 = no deployment, 3 = most sensitive clients, 5 = more than 80% of all clients) □

b How confident are you that the application whitelisting approach you've deployed has been tested and assured to function appropriately? (0 if not deployed) □

c If an unknown executable is blocked on one of your client systems, how confident are you that this event will be detected and reported upon? (0 if not deployed) □

d How comprehensive is your application whitelisting coverage? (1 = only allowing executables in known folders, 3 = allowing executables based on publisher and hash rules, 5 = only allowed scripts) □

□

Total score < 7: This project is highly recommended. You either have no application whitelisting controls deployed or they lack the coverage to be effective.

Total score =< 13: Although you have good whitelisting technical controls in place, you may need to strengthen processes and coverage to detect and respond to executable attempts. Undertaking the envisioning phase of this project would help identify the specific areas for improvement.

Total score > 13: You're confident you have strong controls in place. A (regularly scheduled) assessment and testing of whitelisting in use may confirm that confidence and identify some areas of improvement.

Project Goals:

1 Establish application whitelisting across sensitive client computers with an assurance that unknown, potentially malicious software is prevented from executing.
2 Ensure that attempts to execute non-whitelisted software executions are detectable and reported to aid in intrusion detection and response.
3 Minimise operational cost and productivity impact on both IT and end-users as a result of application whitelisting policies being enforced.

Expected Benefits:

1 Substantially increased difficulty for an attacker to execute code on a client system, thus improving the protective posture of the organisation.
2 Reduced possibility of user error or social engineering that might result in a user executing malicious code on a client system.
3 Increased ability to detect and contain the attempted execution of malicious software and/or software considered to be undesirable or unwanted.

Project Stages & Activities:

The specific sequence of activities to deploy application whitelisting will depend upon the current infrastructure, scope and scale of deployment and security sensitivity of the organisation, but could be indicatively summarised in the following stream of activity:

1 *Envision:* Determine the objectives for implementing application whitelisting and the scope and scale of deployment. This would include:

   a. Determine the high-level objectives and motivation for deploying application whitelisting including project goals and expected benefits.
   b. Determine the scope of the deployment which would include:
      i. Each of the computer roles that will have application whitelisting enabled, such as laptops, desktops, mobile devices, etc.
      ii. High-level mapping of the principal organisation roles and their unique requirements, e.g. Executive, IT administrator, Help desk operator, etc.
      iii. Building on the points above, develop global and role-specific application control objectives for the organisation.
   c. Define assumptions and identified risks for deploying application whitelisting.

2 *Plan:* Perform the detailed analysis of the computer roles, user roles and applications that need to be controlled, then develop a policy strategy for deploying application whitelisting and monitoring its effectiveness. This planning stage is likely to include:

   a. Building an inventory of all computer roles, all user roles on those computers and all applications that will be used.
   b. Design an application whitelisting policy along with a strategy for deploying this policy to target computers and roles.
   c. Design a process for support, maintenance and monitoring of application whitelisting events including the associated communications plans and change management processes.

3 *Develop:* In this phase, the detailed requirements from the Plan phase will be expressed as the technology-specific AppLocker rules, then tested for validation. Likely activities include:

   a. Deploy a base build onto at least one reference computer that will be used for authoring of AppLocker rules.
   b. Configure the Application Identity Service and place AppLocker in audit only mode so that rules can be configured and tested but don't yet block execution.
   c. Auto-generate AppLocker rules for each of the different categories of restriction and then manually edit them to meet exact requirements.
   d. Test all end-user and administrative use cases, and review audit entries in the Event Log. Tune rules as required, and continue testing until there are no audit entries indicating that a desired action would be blocked.
   e. Install applications and repeat the previous two steps for each application.
   f. Export AppLocker policies into individual XML files for later import into group policy.

4 *Stabilise:* In this phase, AppLocker policies are imported into Group Policy Objects (GPO's) and deployed to the target computers. The computers will operate in "Audit only" mode for validation and testing. In this phase no actual enforcement is occurring:

a. Configure the infrastructure for central collection of AppLocker events.

b. Deploy AppLocker policy via GPO's which entails:

   i. Creating the GPO's from the exported XML files in the planning stage.

   ii. Creating the enforcement GPO but placed in Audit only mode.

   iii. Filter GPO's with security groups and WMI filters to target their deployment to intended machines and users.

   iv. Link GPO's to the Organisational Units (OUs) in Active Directory.

c. Validate the deployment by:

   i. Verifying that correct GPOs and settings are being deployed to machines.

   ii. Monitor events being reported to the central event collection service.

   iii. Test the effective AppLocker policy, conduct acceptance testing and obtain authorisation to move AppLocker into Enforcement mode.

5 *Operate:* By the end of the Stabilise phase, AppLocker has been effectively deployed to all targeted computers, but it remains to be activated. Activities in the Operate phase include:

a. Communicate to users that application whitelisting is to be activated and outline the process for raising issues and exception requests.

b. Activating AppLocker by changing the enforcement GPO from Audit Only to Enforce Rules mode.

c. Implement the operation, maintenance, monitoring and reporting processes to deal with requests from users and possible indications of incidents.

Resources:

1 Internal resources required will include desktop and server administrators, IT management, information security team, human resources.

2 External resources may include a specialist on application whitelisting and infrastructure security.

Timeline Factors:

The timeline and effort required for the implementation of an application whitelisting project are greatly influenced by the number of different user and computer roles targeted. It is advised to implement whitelisting in a staged approach starting with users most likely to be targeted, and for a first project to be no more than 12 weeks duration. Additional scope can be pursued in further iterations.

Risks:

1. Productivity disruption – Restricting applications may have an impact on productivity if employees who are accustomed to running any applications (without implementation controls such as this) are now required to go through additional processes to run those applications. Thorough validation of the new restrictions, communications and training along with a streamlined provisioning process can help mitigate this risk.
2. Alignment of Policy and Procedures – Application whitelisting introduces a security control that needs to be integrated and maintained within the broader configuration management processes of the organisation. Failing to do this integration effectively may create delays or disruptions in the rollout of new applications or updates.
3. Inadequate Monitoring Processes – Some organisations implement application whitelisting only as a protective measure and fail to collect and monitor events triggered when unauthorised applications attempt to execute. This diminishes the value of application whitelisting as a detective control.
4. Complexity and Overreach – Scope management is critical, limiting at least a first phase of application whitelisting to just the user groups, applications and business systems with higher sensitivity, while future phases may extend the rollout coverage. It is likely that for some users (such as software developers) it may be inappropriate to implement comprehensive application whitelisting, although limited restrictions may still be appropriate.

Dependencies:

1. Microsoft AppLocker is only available in Windows 7 or later, and Windows Server 2008 and later. Although Windows XP has a type of application whitelisting called Software Restriction Policies, it is not viable to use this approach for a comprehensive, enterprise-wide deployment.

2. Although technically not a dependency, an effective implementation requires well designed Active Directory along with infrastructure for the management and monitoring of central events. These capabilities are provided by System Centre 2012.

Follow-on Projects (or mitigations that may be incorporated into this project):

1. Mitigation #18: *Workstation application security configuration hardening* can follow on from whitelisting with specific restrictions enabled within key applications. Consider that application whitelisting allows an executable to run, but the activity of that executable can be further restricted by configuration. As examples, this may include group policy based settings on browser behaviour (like Internet Explorer Protected Mode) or security settings within Microsoft Office products (such as macro restrictions).

2. Mitigation #22: *Computer configuration management* which can further harden the security of underlying host systems by disabling unneeded services, implementing additional exploit mitigation measures, or improving detection of events.

Implementing Mitigation #2 & #3 – Patch and Deploy Current Applications and Operating Systems

Deploying modern operating systems and applications, then keeping them up to date encompasses both the second and third mitigation strategy. These two are combined for the purposes of this guidance because a very similar project methodology can be applied to both.

DSD advises patching both the operating system and applications within a two-day timeframe for serious vulnerabilities, because once a vulnerability in an operating system or application is made public you can expect malware to be developed by adversaries within 48 hours. There is often a perception that by patching a system without rigorous testing, something is likely to break on the system. Balancing the risk between taking weeks to test patches and patching serious vulnerabilities within a two-day timeframe can be the difference between a compromised and a protected system.

For the purposes of this guidance, migration from Windows XP or another operating system to Windows 7 or 8 is treated separately. Very extensive guidance, project methodologies, tools and resources are available for precisely this purpose. Rather than reinvent those proven processes, a brief overview is provided at Appendix A with additional links to available resources. This guidance focuses specifically on establishing effective and comprehensive update management processes.

Self-Assessment:

Answer each of these questions with a score of 1 (lowest) to 5 (highest):

a	How confident are you that if a critical update is released for a Microsoft vulnerability, it can be deployed across your organisation to 100% of affected clients within 48 hours?	
b	How confident are you that if a critical update to a Java, Adobe or other commonly deployed non-Microsoft software product is released, it can be deployed to 100% of affected clients within 48 hours?	
c	Do you have a process in place to regularly scan clients and servers for vulnerabilities and missing updates? (1 = Rarely/never, 3 = Ad-hoc, usually only desktops, 5 = standardised for all systems)	
d	How do you treat client computers that don't have required updates installed? (1 = let them on the network anyway, 3 = restrict, but only if missing OS patches, 5 = rigorous quarantine & remediation)	
e	What proportion of your general employee base use an operating system less current than Windows 7 (1 = >80%, 5 = 0%)	
f	How confident are you that your third party applications (especially those that interact with online content) and network technologies are up-to-date with patches?	
	Total score < 10: This project is highly recommended. Your patching and update process is inadequate to protect your information.	

Total score =< 20: Although you have some controls adequate for Microsoft patching and broadly deployed 3rd party technologies, it is not sufficiently comprehensive. Undertaking the envisioning phase of this project would help identify the specific areas for improvement.

Total score > 20: You're confident you have strong patch management practices in place. An audit and review of these processes may confirm that confidence and identify some areas of improvement.

Project Goals:

1 Establish a mechanism to have visibility of operating system and application update status across all systems and applications of the organisation.
2 Establish a standard process for intelligence gathering of available updates, along with processes for assessing, testing, deploying and validating deployment of updates.
3 Move operating system upgrade, migration and management processes towards a lifecycle based approach.

Expected Benefits:

1 Substantially reduce the risk exposure of the organisation to attacks that exploit known vulnerabilities of operating systems and applications.
2 Reduced possibility of user error or social engineering that might result in a user executing malicious code on a client system.
3 Increase the consistency and efficiency of current update management processes.
4 Lifecycle based model helps to ensure that upgrade activities are more easily managed and less disruptive going forward. This will allow security driven updates to be more easily implemented, lowering risk and reducing total cost of ownership.

Project Stages & Activities:

The following assumes that update management processes and infrastructure needs to be put in place for operating systems, applications, network devices, mobile devices, equipment, etc. To simplify, this outline excludes a full description of activities that relate to the migration to a new operating system, such as from Windows XP to Windows 7, or 8. Appendix A does provide an overview of migration planning tools and approach.

1 *Envision:* Understand current patch management processes in the organisation, in particular around how comprehensive and consistent the existing processes are, then create a consensus vision on how best the organisation could improve. This includes:

   a. Understand existing processes for update management, including:
      i. How the organisation maintains an awareness of patches/updates that may be relevant.
      ii. How each class of device/application is currently patched, including desktop operating systems, mobile devices, network devices, client applications, server applications, equipment, 3rd party hosted applications, etc.
   b. Assess current exposure by examining actual update management outcomes versus procedure. For example, the procedure may say critical OS updates should be deployed within 48 hours, but do typical servers in the organisation have all critical updates actually deployed?
   c. Build a consensus vision for update management that covers the range of devices and applications required.

2 *Plan:* Identify the appropriate changes in the organisation's technology, policies and practices generally in a staged approach focusing on the highest risk areas. This plan is likely to include:

   a. Changes to the policy and procedures clearly cataloguing:

        i. Which devices need to have managed updates, and whether they are remote, located in the office, etc?
        ii. Which applications need to have managed updates, not only focusing on the priority applications like browsers, Adobe and Java but also other applications such as backup tools, communication software, etc?
        iii. The implications of not having updates applied for those application owners in the business.

    b. Technology changes which may include:
        i. Design and deployment of an update management solution. This may be an extension or configuration of existing infrastructure, such as System Center or deployment of additional functionality for capabilities like mobile device management.
        ii. Establishment of a monitoring and reporting capability to identify unpatched applications and devices, possibly with automated processes for quarantine and update or escalation.

3 *Develop*: Design and build the new policies, procedures and technical improvements for update management. This is likely to include:
    a. Workshops, documentation and validation of appropriate processes to identify candidate updates, assess their suitability for deployment, and package to deploy.
    b. Detailed audit of existing applications, computing devices, network equipment along with their versions and updates available.
    c. Detailed vulnerability scanning to identify missing updates.
    d. Build of infrastructure for the technology changes determined in the planning phase. There may be multiple stages of development depending on the scope of update management improvement.

4 *Stabilise*: Validate all of the changes, achieve an acceptance sign-off and deploy required infrastructure across the organisation. This is likely to be performed in stages that may involve:
    a. Progressive deployment of improved patch management practices, beginning with broadly deployed applications or client operating systems, then extending to server infrastructure, network devices and other equipment. Some changes may be staged ready for transition but not fully made operational.
    b. Training of staff, contractors, partners and other resources as appropriate.

5 *Operate*: Implementation of the improved processes with active monitoring and scanning to assess the effectiveness of the deployment. This is likely to be staggered as changes are progressively implemented across the organisation.

Resources:

1 Internal resources required will include desktop and server administrators, IT management, information security team, human resources.

2 External resources may include infrastructure security specialists, and auditors.

Timeline Factors:

Most organisations already have some level of update management process in place, usually most mature in the domain of operating system updates. The key determinant of timing is how well this existing process functions and can be leveraged to provide a comprehensive update management capability. One approach is to stage improvements in process and technical infrastructure over two to three month projects, each focusing on a different set of applications or infrastructure (such as client operating systems, applications, server infrastructure, network devices, etc).

Risks:

1. Service disruption – Updates can occasionally result in unintended consequences. Although Microsoft extensively tests updates for their effect on other Microsoft components, updates to applications and devices from other vendors may not undergo such rigorous testing. Therefore it is necessary to undergo a rapid, structured test of updates prior to deployment. Much of this testing can be automated to minimise delay in deploying patches to less than 2 days.
2. Bandwidth / Infrastructure Load – The deployment of updates, if not staged appropriately with infrastructure appropriately configured for distribution, can result in a high network load.
3. Alignment of Policy, Procedures, Culture and Technology – Update management requires the alignment of process and technologies across the organisation. Some users may no longer be permitted to use legacy applications, some legacy equipment or devices may need to be replaced. This can have an impact if the justification and policies are poorly communicated, sponsored and the changes orchestrated.
4. Complexity and Overreach – After performing a baseline audit or vulnerability assessment, many organisations find major deficiencies in their patch management practices. It is essential to control the scope of the improvement project and prioritise which systems and applications have the greatest risk of compromise due to an unpatched vulnerability.

Dependencies:

1. Comprehensive update management will require a technology infrastructure such as System Center. Although Windows Software Update Services provides solid capability for operating system updates, it is insufficient for patching of servers, applications and network devices.

Follow-on Projects (or mitigations that may be incorporated into this project):

None.

Implementing Mitigation #4 – Restrict Administrative Privileges

A primary goal of an attacker is to progressively raise their level of access to the organisation’s systems. At first, they may only have standard user access on a device, but they will endeavour to gain administrative access on that machine. From there, they may seek the ability to access multiple systems and eventually move towards obtaining the credentials of a highly privileged account such as an IT administrator or executive. There are many technical mechanisms to limit this escalation but they fundamentally rely on limiting users to only have the access and privileges they require to perform their role at a point in time.

Self-Assessment:

Answer each of these questions with a score of 1 (lowest) to 5 (highest):

a	How confident are you that administrative privileges to the core IT infrastructure of your organisation are only available to trusted, identified individuals?	
b	How confident are you that your IT administrators only log on with administrative privileges when they absolutely need them to perform a specific function?	
c	If a trusted administrator leaves your organisation, how confident are you that they can no longer access any systems within 24 hours?	
d	If an administrator account was compromised (e.g. Password lost), how confident are you that the compromise would be known, detected or reported within 4 hours?	
e	What proportion of your general employee base use Windows XP (1 = >80%, 5 = 0%)	
f	How confident are you that strong passphrases required for all accounts (i.e. >8 characters, complex, never reused)	
	Total score < 15: This project is highly recommended. Your controls are likely to be inadequate to protect your information and systems.	

Total score =< 25: Although you have some controls adequate for normal operation, they are unlikely to be sufficient to protect your organisation from a determined attacker. Undertaking the envisioning phase of this project would help identify the specific areas for improvement.

Total score > 25: You’re confident you have strong controls in place. An audit and review of access control privileges actually in use may confirm that confidence and identify some areas of improvement.

Project Goals:

1. Ensure that general employees are working with the minimum access and privileges to effectively perform their function at any point in time.
2. Ensure that administrative IT staff only have the access they require to critical systems and data and limit the potential for their access credentials to be compromised by an attacker.
3. Minimise the impact of additional access restrictions on the productivity of staff.

Expected Benefits:

1. Increased difficulty for an attacker to gain a foothold on the network, or expand this foothold to compromise more critical assets.
2. Reduced incidence of compromise by accidental or deliberate employee access.
3. Increased visibility and control over the levels of appropriate information access given to employees, partners and contractors.

Project Stages and Activities:

This project is broader than just implementing a single specific control or mitigation and will vary greatly based on current practices within the organisation, but could be indicatively summarised in the following stream of activity:

1 *Envision:* Understand the current practices around the provisioning, use and de-provisioning of administrative privileges and access rights, then create a consensus vision on how best the organisation can restrict administrative privileges. This would include:

   a. Determining if general users have administrative access on their devices, and how this can be controlled if some groups require such access (e.g. Developers, IT support, etc).
   b. Determining which users in the organisation have privileged access and how closely that matches real requirements. This also will involve assessing services and systems that execute with administrative privileges.
   c. Evaluating the current policy and practices for provisioning and de-provisioning users with administrative privileges and access rights.
   d. Understanding the technical mechanisms in place for authentication and control of administrative access. This would likely include a review of current authentication and directory technologies, current certificate or multi-factor authentication mechanisms, etc.

2 *Plan:* Identify the appropriate changes in the organisation's technology, policies and practices generally in a staged approach focusing on the highest risk areas. This plan is likely to include:

   a. Changes to the policy and procedures clearly identifying which roles within the organisation require administrative privileges and for what functions, how these privileges are granted, used and revoked.
   b. Technology changes which may include:
      i. Restricting administrative rights on the desktop
      ii. Modifying the membership of privileged groups such as domain admins.
      iii. Modifying the accounts used for services like backup, monitoring, etc to limit their access to the minimum necessary.
      iv. Implementing stronger authentication mechanisms (such as multi-factor authentication if appropriate) or restricting legacy forms of authentication (such as LanManager for example).
      v. Implementing improved role based governance and identity management solutions.

3 *Develop*: Design and build the new policies, procedures and technical improvements for administrative privilege restriction. This is likely to include:
   a. Workshops, documentation and validation of appropriate policies for privileged account governance and operations.
   b. Detailed audit of existing privileged account usage and mapping to a revised structure or roles.
   c. Build of infrastructure and solutions for the technology changes determined in the planning phase. There may be multiple stages of development depending on the scope of work as a big-bang approach in identity management is undesirable.

4 *Stabilise*: Validate all of the changes, achieve an acceptance sign-off and deploy required infrastructure across the organisation. This is likely to be performed in stages that may involve:
   a. Progressive deployments across general employee desktop fleet and similar deployment of the controls on IT administrators. Some of the changes may be staged ready for transition, but not fully made operational.
   b. Similarly, progressive deployment of new infrastructure or solutions to improve the authentication mechanisms, identity provisioning and governance systems.
   c. Training of staff, contractors, partners and other resources as appropriate.

5 *Operate*: Enforcement and monitoring of the administrative access restrictions. This is likely to be staggered as changes are progressively implemented across the organisation. Monitoring the effectiveness of the changes and dealing with unforeseen exceptions and consequences will be necessary.

Resources:

1 Internal resources required will include desktop & server administrators, IT management, information security team, human resources.

2 External resources may include identity management specialists, infrastructure security specialists, and auditors.

Timeline Factors:

This is the most variable mitigation in terms of scope and therefore timeframes, although any organisation implementing a solid project in this area is likely to achieve significant progress within a six month project timeframe. If the scope is extended to incorporate for example the implementation of a new identity management and provisioning solution or the broad roll out of multi-factor authentication, then this timeframe may be extended or this could be done as a separate improvement project.

Risks:

1 Productivity disruption – Restricting privileges may have an impact on productivity if employees who are accustomed to having administrative accounts will now have to go through additional processes to obtain those privileges. Thorough validation of the new restrictions, communications/training and a streamlined provisioning process can help mitigate this risk.

2 Service disruption – Not all administrator accounts are used by users. It is common for highly privileged accounts to be set up for services like backup, monitoring and replication. Restricting these accounts without thorough assessment can cause service disruption although this prospect can be reduced through detailed auditing and review.

3 Alignment of Policy, Procedures, Culture and Technology – This project requires as much attention to people issues of policy and process including training and support as it requires for technology. Human resources and senior management need to be fully integrated and supportive of the project.

4 Complexity and Overreach – When examining the current state of identity management, so many issues can surface that it becomes tempting to expand the scope towards an ideal solution. Scope management is critical limiting this project only to restriction of administrative privileges, while future projects may take a broader perspective.

Dependencies:

1 Technical limitations in Windows XP cause a decision to restrict administrative privileges to have a more significant impact on end user productivity than would be expected on Windows 7 and 8. Additionally, Windows XP does not provide the hardened authentication mechanisms of more modern operating systems. It is possible to implement this project while retaining Windows XP, but the outcomes would be limited and benefits reduced.

Follow-on Projects (or mitigations that may be incorporated into this project):

1 Mitigation #5: *Disabling local administrative accounts* to prevent network propagation using compromised credentials that are shared by multiple computers.

2 Mitigation #6: *Multi-factor authentication* especially implemented for remote access, which may involve smartcards or other tokens.

3 Mitigation #20: *User education*, especially around appropriate handling of information, setting of passphrases and precautions for use of privileged accounts.

4 Mitigation #27: *Enforce a strong passphrase policy* covering the complexity, length and restrictions on reuse of passphrases.

5 Mitigation #31: *Disable LanManager password support* and cached credentials on workstations and servers to make it harder for adversaries to crack passwords.

Appendix: Key Resources for Migration off Windows XP

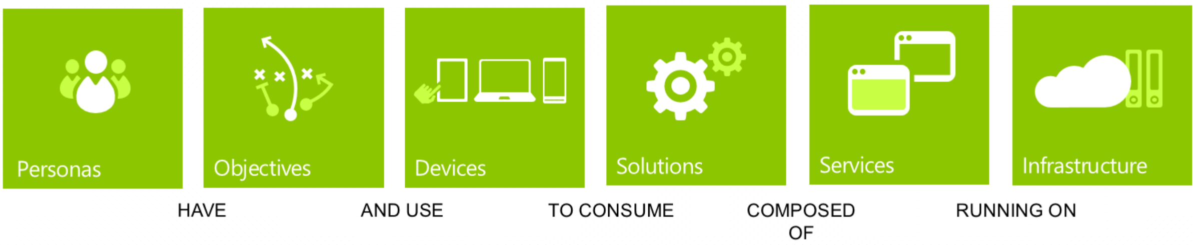
Microsoft provides extensive guidance, tools and resources to help with desktop deployment, upgrade and migration planning and implementation.

Planning and Implementation Approach

An effective migration from Windows XP to Windows 7/8 requires an end-to-end program that incorporates the lifecycle from strategy through planning, deployment and support. The key objectives of this program need to work towards objectives greater than simply achieving the same capabilities on a newer technology base, and include:

- Anywhere Connectivity: Provide employees with secure access to information and applications - whenever they need it, from wherever they need to work.
- Personalized Experience: Using client technologies and services that anticipate your users' needs, remember preferences, and adapt to an individual's unique way of working.
- Intelligent Infrastructure: Realize better security, streamlined management, and reduced costs, both on-premises and potentially in the cloud.

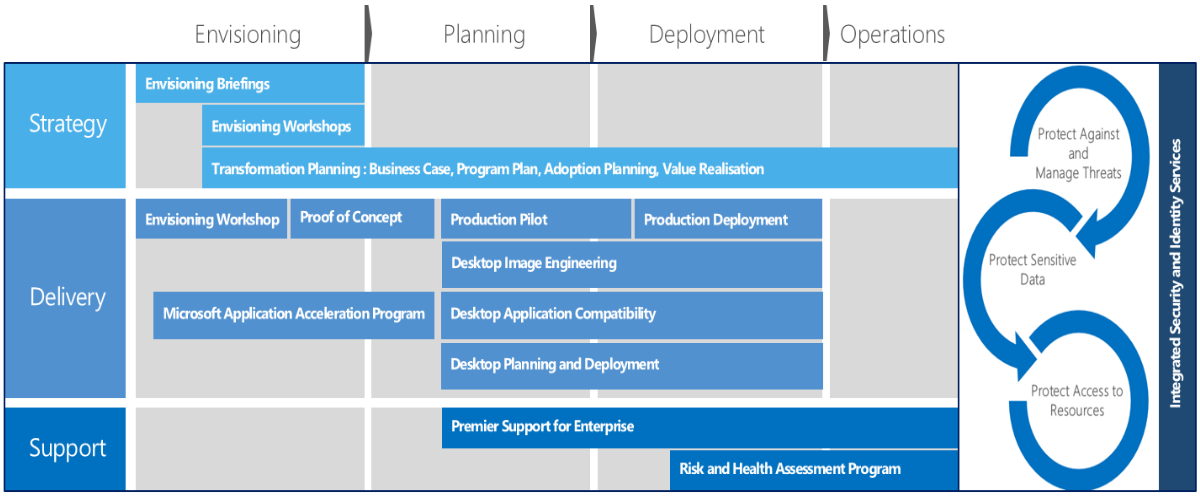
The methodology commences with a workforce analysis, this user-centric planning approach blends user and technical requirements, considering aspects such as applications, data, devices, location, and platform infrastructure requirements.



Personas HAVE Objectives AND USE Devices TO CONSUME Solutions COMPOSED OF Services RUNNING ON Infrastructure

Whilst the Migration Plan does vary for each organisation, the journey from Windows XP to a modern operating system (Windows 7/8) follows a common program delivery pattern. Further information is available at:

www.microsoft.com/en-us/microsoftservices/flexible_workstyle.aspx



Envisioning | Planning | Deployment | Operations

Strategy: Envisioning Briefings; Envisioning Workshops; Transformation Planning : Business Case, Program Plan, Adoption Planning, Value Realisation

Delivery: Envisioning Workshop; Proof of Concept; Production Pilot; Production Deployment; Desktop Image Engineering; Microsoft Application Acceleration Program; Desktop Application Compatibility; Desktop Planning and Deployment

Support: Premier Support for Enterprise; Risk and Health Assessment Program

Protect Against and Manage Threats
Protect Sensitive Data
Protect Access to Resources
Integrated Security and Identity Services

Assessment and Planning Tools

A collection of tested and proven guidance and automated tools to help you plan, securely deploy, and manage new Microsoft technologies - easier, faster, and at less cost - are freely available and fully-supported by Microsoft:

- Solution Accelerators: technet.microsoft.com/en-us/solutionaccelerators/
- Springboard series for Windows 8: technet.microsoft.com/en-us/windows/hh771457

Microsoft Assessment and Planning Toolkit

The Microsoft Assessment and Planning (MAP) Toolkit helps you perform a thorough assessment of the current environment, and a plan for how to execute the project. It includes several tools that fulfil three core functions: inventory, compatibility analysis and readiness reporting.

The MAP inventory tool takes a secure, agentless inventory of computing resources across your network. By leveraging technologies already within your network—including Windows Management Instrumentation (WMI), the Remote Registry Service, Active Directory Domain Services and the Computer Browser service—MAP doesn't require any installation.

Once your inventory is complete, MAP gives you a comprehensive analysis of the assets within your organization, including detailed information on the composition of the environment, as well as identifying issues that may pose a challenge to a smooth migration to Windows 7. MAP also has rich reporting features that give you more detailed insights into the current state of your IT infrastructure. MAP also includes tools to conduct a similar inventory and analysis for software within your environment. This helps you understand the existing state of deployed software within your organization. It also helps identify any issues that may pose a roadblock to successful deployment. The latest version can be downloaded at http://technet.microsoft.com/library/bb977556.aspx

Microsoft Deployment Toolkit

Once you've used MAP to get a comprehensive view of your infrastructure and mitigate any outstanding issues, it's time to start engineering your new deployment. Microsoft Deployment Toolkit (MDT) provides a complete framework and toolset for customizing, automating and deploying new Windows 7 and Windows 8 desktops.

With a centralized control panel called the Deployment Workbench, MDT streamlines the process of building and deploying a new operating system with three primary deployment scenarios:

- Lite-Touch Installation (LTI)
- Zero-Touch Installation (ZTI)
- User-Driven Installation (UDI)

Each scenario provides different levels of automation and user interaction based on your organization's needs and capabilities. You'll find expert guidance on choosing the best scenario in, "Using the Microsoft Deployment Toolkit," included in the MDT download. There are a number of approaches to creating images. You can opt to create a "thick image"—a complete capture of the entire desktop environment, including operating system, drivers, applications and so on.

Conversely, "thin images" represent a minimalist approach, including only what is absolutely necessary to create the desktop computing environment. You add applications and settings later in the process.

A “hybrid image” is just as it sounds: a “compromise” image that includes basic applications and customizations that apply to every user. You can apply further customization later. Once again, the “Using the Microsoft Deployment Toolkit” document will help steer you in the best direction.

Once you’ve selected a deployment approach and image style, MDT will walk you through the process of creating a deployment share (where your images will be stored, and from where they will be deployed) and creating customized Windows images. From there, you have a number of choices for actually deploying the image, based on your scenario. These may include automated deployment via System Center or a more manual version using customised boot media.

Application Compatibility and Virtualization

One of the more common issues IT professionals encounter during a desktop deployment is application compatibility. Legacy applications, including those developed internally, may still be business-critical and must be accounted for and identified. Application Compatibility Toolkit (ACT) can help you with that task. ACT helps to rationalise existing applications by identifying potential duplicates, conflicting versions and so on. By helping to standardise applications throughout the organization, you’re able to reduce the number of applications you need to test prior to deployment.

After completing the rationalisation process, ACT can help you test each application for Windows 7/8 compatibility. This may be as simple as presenting details provided by the application manufacturer indicating whether or not the application is compatible. In some cases, you may also be faced with in-house applications that require more detailed testing, or known incompatible applications that require mitigation in order to work properly with Windows 7/8.

Some applications have compatibility fixes—also known as shims—to work properly with Windows 7/8. You can make a large number of previously incompatible applications work quickly and easily using shims. For example, shims can make an application believe it’s running as an administrator when it’s not, or that it’s running on Windows XP when in fact it’s running on Windows 7.

For those incompatible applications you can’t mitigate with shims using ACT, you may need to employ virtualization technology like Virtual PC to run the application in Windows XP Mode, or Microsoft Enterprise Desktop Virtualization. These emulate a previous version of Windows and let you run applications within a virtual machine running an older operating system, and do so in a way that’s completely seamless and transparent to the user. Applications appear and operate as if they were installed on the desktop.