How does Microsoft 365 address the requirements of the ASD Essential Eight?

Microsoft 365 and the Essential Eight

- Published on January 21, 2018
  https://www.linkedin.com/pulse/microsoft-365-essential-eight-aaron-dinnage/

In February 2017 the Australian Signals Directorate published their latest Strategies to Mitigate Cyber Security Incidents. As part of this revised guidance the ASD have include a new priority list of mitigations called the “Essential Eight”. Building on the more established “Top 4” controls, which are **mandatory** for all Australian government organizations, the Eight are specifically designed to create a baseline cyber security posture that prevents malware, limits the extent of incidents, and facilitates data recovery.

It's almost a year later and much has been written about the Essential Eight, and there are lots of great resources on the ASD web site. However, this article will take the perspective of an organization adopting Microsoft 365. We'll look at the elements within the customer's control to effect adherence to the Eight as well as the things Microsoft does in delivering the products and services. You'll see me refer to these below as *Customer Controls* and *Microsoft Controls*, respectively. Put another way, there will be a list of Microsoft products and features that customers may deploy to address the Eight, and a second list of things Microsoft does *behind-the-scenes*.

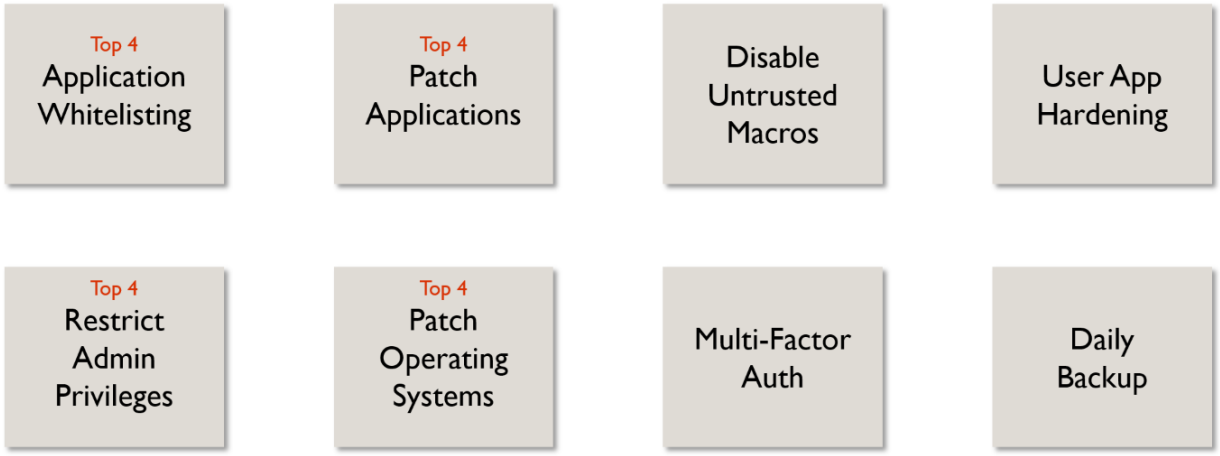
As we walk through each of the items in the Essential Eight you'll find a quote from ASD briefly describing the item, clicking on this will link to further reading sourced directly from the ASD web site. You may notice that a number of the items in the Eight are affected by the recent update to the ASD Information Security Manual Controls, where applicable I've highlighted the relevant control updates.

I'll follow this article with a longer discussion of the ISM Control Updates published in November 2017, also from the perspective of adopting Microsoft 365. But that is for another day.

I'm using Microsoft 365 as shorthand here to describe the three individual technology components, which are Office 365, Enterprise Mobility + Security (EM+S), and Windows 10. I'll call them out separately as we get into each item of the Eight but refer to them collectively as Microsoft 365 for brevity. To learn more about the Microsoft 365 suite please refer to my earlier article Unpacking Microsoft 365.

The intent of this article is twofold. Firstly, it is to give you practical advice about Microsoft 365 implementation within the context of the Essential Eight. And secondly, to give you an appreciation for what Microsoft does to secure the technology itself. Hopefully, this will not only highlight some ways you might further enhance your Microsoft 365 deployment, but also assist in any threat and risk assessments you might be completing in the process.

The ASD Essential Eight



Application Whitelisting

"A whitelist only allows selected software applications to run on computers."

Application whitelists are perhaps the strongest measure to prevent malware from infecting an environment as they explicitly prohibit any unknown process from running. However, application whitelisting is by its very nature a restrictive approach that can be difficult to manage, particularly in end-user computing scenarios. Microsoft 365 introduces a number of capabilities that can aid in this.

Note that the 2017 ISM Controls Update includes a new control requiring whitelisting that is based on publisher certificates to now be scoped to both the publisher name and product name, ISM Control 1471.

Application Whitelisting is a Top 4 control.

Customer Controls

- Windows Client and Server operating systems can be configured with built-in application whitelisting through AppLocker. This is the key whitelisting technology built in to Windows, but can prove challenging to deploy to user endpoints on account of the way people use these devices.
- Windows 10 includes Windows Defender Application Control, a collection of application whitelisting technologies that build on something called configurable Code Integrity (CI). Application Control provides a more manageable hardening approach that may be used to augment existing application whitelisting strategies.
- For application whitelisting in a mobile device environment Microsoft has Intune, part of EM+S. Whilst Intune can be used as an MDM, what's more relevant here is the Application Management (MAM) features which allow customers to sandbox organization data into sanctioned apps and managed identities to better accommodate BYOD scenarios.
- Extending on this data segregation approach, it is recommended to look into Windows Information Protection back on the desktop and server environment.

Microsoft Controls

- Microsoft employs application whitelists to monitor activity within the Microsoft Cloud Infrastructure and Operations environment. Process logs are automatically analysed by machine learning and overseen by Microsoft engineers.
- As an ASD Top 4 item, Microsoft's approach to application whitelisting was audited in the most recent IRAP assessment. Please refer to the IRAP report for more information.

Patch Applications

Top 4
Patch Applications

"A patch fixes security vulnerabilities in software applications."

One critically important mechanism to protect a system from malware or intrusion is to patch application security vulnerabilities in a timely fashion.

The applications of Office 365 support new ways to achieve this, along with new mobile and desktop management features of EM+S.

Note that the 2017 ISM Controls Update includes new and updated guidance calling out specific timelines for this to occur, see ISM Controls 1144, 0940, and the new ISM Control 1472.

Patch Applications is a Top 4 control.

Customer Controls

- The System Center suite includes capabilities to manage updates & patching in on-premises and IaaS environments. System Center Config Manager is included in EM+S.
- Microsoft Intune provides application management features that enforce application patch levels for mobile and Windows 10 devices.
- Office 365 ProPlus includes Update Channels to help customers stay patched whilst balancing their organizations change management requirements.

Microsoft Controls

- Microsoft 365 employs rolling updates across the application stacks within the various services. These deliver continuous application version and patch currency.
- As a true 'evergreen' SaaS service, Microsoft 365 is automatically maintained at the latest versions and patches on the service side whilst customers have access to the latest client operating system and productivity applications at all times.
- As an ASD Top 4 item, application patching was audited in the most recent IRAP assessment. Please refer to the IRAP report for more information.

Disable Untrusted Macros

"Microsoft Office applications can use software known as 'macros' to automate routine tasks."

Whilst Macros provide a powerful tool to automate tasks within Office and improve productivity across the suite, that flexibility can occasionally be exploited by malware. When used in conjunction with user education and other anti-malware mechanisms, disabling access to untrusted macros is an important step in securing an enterprise environment.

Microsoft has comprehensive Macro security guidance in this TechNet Article.

Customer Controls

- Office 2016 includes a new mechanism to automatically disable macros from external sources.
- Windows continues to include the traditional group policy levers to more forcefully disable macros with configuration granularity across a variety of scenarios.
- Windows 10 now includes Windows Defender Exploit Guard, featuring Attack Surface Reduction (ASR) which can block Office applications from creating executables, launching child processes, process injection, importing executable code into macros, or executing obfuscated macro code. This is a potent weapon against macro-based attacks, amongst others.
- Windows Defender Advanced Threat Protection rolls up the data feeds and management of Windows Defender features and integrates preventative protection, post-breach detection, investigation and response into a single security portal which can view and manage the security feeds and events across an organisation.
- Office 365 Advanced Threat Protection includes scanning for macro malware across email, file sharing, and Microsoft Teams.

Microsoft Controls

- Microsoft does not execute macros within the service platform, except within the detonation chamber employed by Office 365 ATP.

User Application Hardening

"Block web browser access to Adobe Flash Player (uninstall if possible), web ads and untrusted Java code on the Internet."

User Application Hardening is a particularly interesting area of the Essential Eight, because the configurations and mechanisms used all vary according to the application. Whilst some general advice is useful, it is important to apply this thinking across all user applications.

With the 2017 ISM Controls Update there is new guidance relating to user application hardening. Specifically, ISM Control 1411 has been updated to read:

"Any security functionality in applications should be enabled and configured for maximum security. **"**

This suggests that organisations should be turning on the **full** set of security features in Microsoft 365, not the minimum or 'entry-level', as is so often the case. I'm thinking here specifically of features like Advanced Threat Protection in Windows and Office 365, Identity Protection in Azure AD, and Microsoft Cloud App Security in EM+S.

Further, guidance around disabling unused features has been separated out on its own under the new ISM Control 1470, which states:

"Any unrequired functionality in applications should be disabled. **"**

Customer Controls

- Microsoft Intune Device Management and Application Management can both play a role in hardening mobile devices and applications.
- Windows 10 includes the Microsoft Edge web browser, which has settings to block Flash and does not run Java or Silverlight.
- Windows Defender Application Guard protects Microsoft Edge users from non-approved web addresses using virtualisation, thereby mitigating the threat of malicious websites whilst giving trusted web applications the access and functionality they require.
- Microsoft 365 technologies no longer utilise any Flash, Java, or Silverlight in the user experience.

Microsoft Controls

- Flash, Java, and Silverlight are not used in the delivery of Azure or Office 365 services.
- Microsoft system administration terminals do not have internet access.

Restrict Administrative Privileges

Top 4
Restrict Admin Privileges

"Only use administrator privileges for managing systems, installing legitimate software and applying software patches."

It remains all too common for high levels of standing admin access to exist within an organization, leaving a serious security risk of both attacker lateral movement and insider attack.

Given the ongoing risks posed the 2017 ISM Controls Update has a number of updates and new controls relating to admin access. Control 1469 has been added and states:

"Unique domain accounts with local administrative privileges, but without domain administrative privileges, should be used for workstation and server management. **"**

This advice is in line with the principles of *least privilege*. See the ASD publication Secure Administration for further information.

Restrict Administrative Privileges is a Top 4 control.

Customer Controls

- Microsoft recommends running separate accounts for Admin access.
- Office 365 does not require licenses for Admin accounts, and includes Multi-Factor Authentication for them. This creates a great baseline for securing admins, but more advanced features may require a license be allocated.
- Microsoft recommends Privileged Identity Management to provide time-bound admin access and deliver a zero-standing admin permissions configuration for both Office 365 and Azure.
- Using Office 365 Customer Lockbox Microsoft customers can have final approval over a Microsoft admin performing a task that brings them into contact with the customer's data (see Lockbox below).

Microsoft Controls

- Microsoft developed an internal process known as 'Lockbox' to provide time-bound admin access and deliver a *no standing admin permissions* configuration for Office 365 and Azure.
- No Microsoft engineer has an account with standing access to administer the services.
- Admin access is granted at a fixed time, scope, and duration to complete a given work item.
- For more information on the Lockbox process please refer to the white paper "Office 365 - Administrative Access Controls" from the Microsoft Service Trust Portal (under Trust Documents, FAQs and White Papers).
- As an ASD Top 4 item, restricting administrative privileges was audited in the most recent IRAP assessment. Please refer to the IRAP report for more information.

Patch Operating Systems

Top 4
Patch Operating Systems

"A patch fixes security vulnerabilities in operating systems."

Like the requirement to Patch Applications, patching operating systems is another critical mechanism to protect a system from malware, intrusion, corruption, or disruption. Components of Microsoft 365 introduce enhancements to the management of this process.

Note that the 2017 ISM Controls Update includes new and updated guidance calling out specific timelines for this to occur, see ISM Controls 1144, 0940, and the new ISM Control 1472.

Patch Operating Systems is a Top 4 control.

Customer Controls

- EM+S includes Microsoft Intune for mobile device and application management and System Center for managing updates & patching in on-premises and IaaS environments.
- Windows Update for Business further enhances update management and automation with the ability to ascribe 'update rings' which then automatically ensure devices are kept to a particular update cadence. Windows Update for Business integrates with both Intune and System Center.

Microsoft Controls

- Microsoft 365 utilises rolling updates across the service infrastructure. These ensure continuous operating system version currency to latest patch levels.
- As an ASD Top 4 item, patching of operating systems was audited in the most recent IRAP assessment. Please refer to the IRAP report for more information.

Multi-Factor Authentication

"Having multiple levels of authentication makes it a lot harder for adversaries to access your information."

Multi-Factor Authentication (sometimes referred to as Two-Factor Authentication or 2FA) is now a critical element in the protection of an organisations data, systems, and user identities. When services are externally accessible, MFA is essential for the security of those services. Passwords alone are simply not enough.

However, MFA has a reputation for creating friction with users. The challenge is to adopt smart MFA technology which adapts to the various user, device, and network conditions to only interrupt the user when necessary to enforce the right security posture. For example, an organization may permit access when the user is connecting from a trusted device in a secure location, but challenge the user to provide an additional pin or one time passcode when outside of the secure location. This is just one example of some of the logic that can be applied, though far more sophisticated scenarios and outcomes are available.

Customer Controls

- Office 365 includes simple Multi-Factor Authentication for Admin accounts.
- EM+S includes Conditional Access, this allows organisations to provide contextualised, intelligent Multi-Factor Authentication to Office 365 and other SaaS, and even on-premises, applications.
- Windows 10 includes biometric factors (Windows Hello), TPM, and Virtual Smartcard technologies.

Microsoft Controls

- Multi-Factor Authentication is an integral component of both the physical access controls and the 'Lockbox' process for engineer access.
- All physical and logical access requires MFA.

Daily Backup

"Regularly back up all data and store it securely offline."

Backup is perhaps one of the most important mechanisms to protect against both malicious and inadvertent data corruption or loss. In every customer journey to Office 365 it is a concern that naturally comes up, and it is something that occasionally challenges organizations to think differently about backup.

Traditional and SaaS backup methods differ substantially and force customers to confront long held beliefs and re-focus on their requirements, not simply "*the way we've always done it*".

You'll find many references to "offline" and "disconnected" storage of backups within the Essential Eight guidance on the ASD web site (even in headline quotes such as the one at the top of this section). However, there are now provisions included in the guidance to call out cloud services and put special considerations around them.

Additionally, the 2017 ISM Controls Update now accommodates cloud services, such as Microsoft 365, by removing the specific need for offline storage. Under **Backup Strategy**, new text was introduced to address online backups:

"Mechanisms must be implemented to mitigate the risk of agency data being unavailable due to compromise or deletion. Such mechanisms include storing backups offline where practical. If backups are stored online, such mechanisms include …"

The text goes on to explain ways to ensure online backups are appropriately safeguarded. All of which are commonplace for the more mature Software-as-a-Service offerings such as Microsoft 365.

The relevant ISM Control within this section (0119) has been updated to include the following text:

"ensure that backups cannot be maliciously modified/corrupted or deleted without appropriate authorisation."

Up until now the prescribed way to prevent modification, corruption, or deletion of backups was through offline storage, but this updated guidance creates room for online storage with appropriate controls in place.

This update highlights a growing understanding that cloud services can achieve the same or greater levels of security and resiliency as traditional IT, but that they often achieve it in new or different ways. This further highlights the importance of *prescriptive* security guidance being updated regularly and responsively to reflect the state of the industry.

It's a credit to the ASD that the Essential Eight, and the ISM more broadly, now reflect the state of modern and mature cloud services such as Office 365. They no longer prescribe methods incompatible with SaaS cloud offerings, and are therefore no longer able to be called out as a blocker to cloud adoption.

Customer Controls

- Office 365 includes features to secure content, such as Putting Content on Hold, Records Management, File Versioning, and User Self-Service File Recovery. These create customer accessible data backups in service, ranging from end-user driven through to managed by policy.
- Additional Microsoft 365 services like Cloud App Security can be added to detect unusual behaviour (i.e. mass content modification/deletion) to aid in the identification of, and recovery from, incidents.
- Windows 10 includes built-in backup capabilities such as System Restore, Shadow Copies of Shared Folders, Server Backup, and System Center Data Protection Manager.
- Additional protection against malware based data corruption can be achieved with Windows Defender Controlled Folder Access, which blocks unauthorized applications access to important files and folders.

Microsoft Controls

- Office 365 includes multiple synchronous and asynchronous backups across data centres within the region at greater than daily frequency.
- Within each data centre content is replicated multiple times across highly redundant storage physically spread across the facility and actively monitored for corruption.
- You can read more about the resiliency and backup features of Office 365 in the white paper "Office 365 - Data Resiliency" which is available in the Microsoft Service Trust Portal (under Trust Documents, FAQs and White Papers).

Conclusion

I hope this has been a useful exploration of the Essential Eight, from a slightly different angle to the usual. If you'd like to understand more about the technologies mentioned in this article please reach out to your Microsoft Account team, Microsoft Support team, or preferred Microsoft Gold Partner, as they will be very happy to expand on the information provided here. You can also send me a note or a comment below.

You may have noticed multiple references the most recent IRAP documentation throughout this article. Microsoft online services customers can access the latest IRAP assessment documents through the Microsoft Service Trust Portal (under Compliance Reports, GRC Assessment Reports). There is additional implementation detail contained in the IRAP documents not shared publicly. I recommend using these reports to further your understanding of the mitigations Microsoft has in place and also in completing risk assessment work. It's worth taking a look at the assessors recommendations too!