Microsoft Security

Meeting Essential Eight requirements with Microsoft Security

Guidance for Western Australian Government agencies.

For more information on any of these capabilities please contact your Microsoft Account Team:

Glenn Winton
Account Executive
glennwi@microsoft.com

Mark Randell
Account Technology Strategist
mark.randell@microsoft.com

Antoinette Jago
Security Solution Specialist
ajago@microsoft.com

Michael Gadsden
Account Executive
mgadsden@microsoft.com

Charles Poulsen
Account Technology Strategist
charles.poulsen@microsoft.com

Brian Carter
Azure Apps and Infrastructure Specialist
brian.carter@microsoft.com

Beau Faull
Compliance Technology Specialist
beau.faull@microsoft.com

Michael Richards
Security Technology Specialist
michael.richards@microsoft.com

Jeff Beckitt
Cloud Endpoint Technology Specialist
jeff.beckitt@microsoft.com

Microsoft has previously provided guidance on technologies within the Whole of Government Framework that could help address each requirement in the Western Australian Government SECC Top 5, including additional controls that could be acquired through optional licensing.

With the new Whole of Government Agreement under CUAMS2019 (Supply of Microsoft product licences and licensing solutions[1]) and the change of alignment to the ACSC Essential Eight, we have created a series of documents providing information on the new capabilities available within Microsoft 365 and Azure, as well as guidance on how to implement these solutions to help meet the Essential Eight requirements.

Document Title	Version and Date
Essential Eight on a Page http://aka.ms/ausec/e8wagov	1.0, November 2021
Meeting Essential Eight requirements with Microsoft Security http://aka.ms/ausec/e8wpwagov	1.0, November 2021
Microsoft 365 Compliance on a Page http://aka.ms/ausec/compwagov	1.0, November 2021
Meeting compliance requirements with Microsoft 365 http://aka.ms/ausec/compwpwagov	1.1, November 2021
Microsoft 365 Security on a Page http://aka.ms/ausec/secwagov	1.0, November 2021
Meeting security requirements with Microsoft 365 http://aka.ms/ausec/secwpwagov	1.0, November 2021

Please note that the intent of this document is to educate on technical capabilities and how they may be utilized to support Essential Eight requirements, not to provide explicit configuration guidance. This document represents a view from Microsoft at the time of writing and is subject to change as new capabilities or requirements are released.

For an example of the configuration of Microsoft solutions to meet the Essential Eight Maturity Level Three, Microsoft suggests reviewing the Protected Utility Blueprint[2] from the Digital Transformation Agency as this was developed in consultation with Microsoft and tested by independent security assessors.

Microsoft strongly recommends working with a Certified Partner to ensure People, Processes, and Technology are all adequately addressed in designing a risk-based solution to meet your Agency's unique requirements.

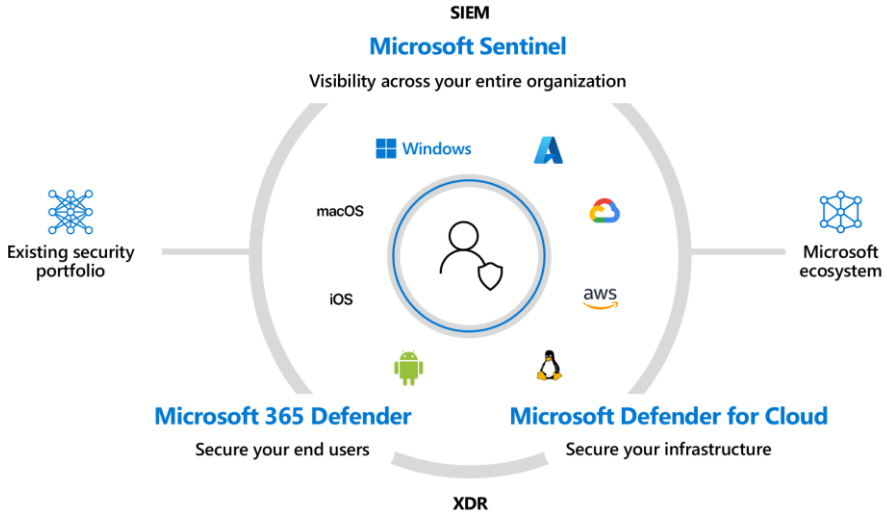
1. https://www.wa.gov.au/government/cuas/supply-of-microsoft-product-licences-and-licensing-solutions-cuams2019
2. https://desktop.gov.au/blueprint/index.html

Microsoft Licensing Considerations

Microsoft Defender provides an end-to-end eXtended Detection and Response (XDR) solution for your entire estate across the Microsoft cloud, on-premises data centres, and third-party public or private cloud platforms. **Microsoft 365 Defender** offers a set of connected best-of-breed solutions for your data, device endpoints, identities, and apps through **Microsoft Defender for Endpoint Plan 2**, **Microsoft Defender for Identity**, **Microsoft Defender for Office**, and **Microsoft Defender for Cloud Apps** (formerly known as Microsoft Cloud App Security).

Microsoft Defender for Cloud offers similar integrated threat protection across server endpoints, containers, networks, IoT devices on the edge, and managed apps, however in the context of the Whole of Government Agreement we focus primarily on the use of **Microsoft Defender for Servers**.

The XDR capabilities of Microsoft Defender delivered through Microsoft 365 Defender and Microsoft Defender for Cloud provide rich insights and prioritized alerts, but to gain visibility across the entire environment and include data from other security solutions such as firewalls the solutions can all be connected to **Microsoft Sentinel**, Microsoft's cloud-native Security Incident and Event Management (SIEM) solution.



Microsoft 365 Defender provides protection capabilities for end users and client devices and is licensed per-user as part of **Microsoft 365 E5** or the **Microsoft 365 E5 Security add-on to Microsoft 365 E3**. The E5 offerings also include **Azure Active Directory Premium Plan 2**, which itself is a grouping of Identity Protection, Privileged Identity Management, Entitlement Management, and Access Reviews.

For server and infrastructure protection the Whole of Government Agreement includes **Microsoft Defender for Servers,** which is available natively for servers in Azure Infrastructure as a Service (IaaS), and through **Azure Arc** for servers hosted in other platforms such as on-premises data centers, GovNext, Amazon Web Services or Google Cloud Platform. Microsoft Defender for Servers provides the bridge between the two areas of user security and infrastructure security through its inclusion of Microsoft Defender for Endpoint on the server.

To provide a single location for monitoring and response **Microsoft Sentinel** is included in the government agreement as the cloud-based Security Incident and Event Management (SIEM) solution. Sentinel also provides true Security Orchestration, Automation and Response (SOAR) capabilities above and beyond the automated investigation and response features of the Microsoft Defender platform.

The **Microsoft 365 E3** suite includes standard versions of the advanced solutions available in the E5 packages including Exchange Online Protection, a subset of Microsoft Defender for Office; Cloud App Discovery, a subset of Microsoft Defender for Cloud Apps; and Microsoft Defender for Endpoint Plan 1, which includes the next-

generation antivirus, attack surface reduction, and cross-platform capabilities of the full Microsoft Defender for Endpoint suite.

Product Name	Billing Type
End User Security – included in the Whole of Government baseline	
Microsoft 365 E3 *(includes Azure AD Premium Plan 1, Cloud App Discovery, Exchange Online Protection, Microsoft 365 apps for enterprise, Microsoft Defender for Endpoint Plan 1, and Microsoft Endpoint Manager)*	User/month, billed annually
Microsoft 365 E5 Security add-on to Microsoft 365 E3 *(includes Azure AD Premium Plan 2, Microsoft Defender for Cloud Apps, Microsoft Defender for Endpoint, Microsoft Defender for Identity, and Microsoft Defender for Office 365)*	User/month, billed annually
End User Security – optional extras	
Microsoft 365 E5 Compliance add-on to Microsoft 365 E3 *(includes Information Protection & Governance, Insider Risk Management, and eDiscovery & Audit)*	User/month, billed annually
Microsoft 365 E5 *(includes Microsoft 365 E5 Compliance, Microsoft 365 E5 Security, Meetings & Voice, and Advanced Analytics)*	User/month, billed annually
App governance add-on to Microsoft Defender for Cloud Apps	User/month, billed annually
Premium assessment templates for Compliance Manager	Template/month, billed annually
Microsoft Experts on Demand	Flat rate, billed annually
Infrastructure Security	
Microsoft Defender for Servers	Server/hour, billed monthly
Microsoft Sentinel *(data ingestion)*	GB/day, billed monthly
Log Analytics *(data ingestion)*	GB/day, billed monthly
Log Analytics *(log retention)*	GB/month, billed monthly
Logic Apps	Per hour or execution, billed monthly
Azure Automation Update Management	No additional cost
Azure Arc	Per server per month, billed monthly. Included with Microsoft Defender for Servers.
Azure Backup	Per instance and GB/month, billed monthly
Azure Bastion	Per hour and GB/month, billed monthly

More information on licensing of the Microsoft 365 services is available from https://docs.microsoft.com/en-us/office365/servicedescriptions/microsoft-365-service-descriptions/microsoft-365-tenantlevel-services-licensing-guidance/microsoft-365-security-compliance-licensing-guidance.

Another resource, maintained by a Modern Work Specialist with Microsoft Australia but not an official Microsoft publication, is the Microsoft 365 Maps site at https://m365maps.com.

Microsoft licensing offers many different options to meet our customers varying needs, but with this flexibility comes a degree of complexity so we recommend you work with your reseller or Microsoft Account Team to ensure you select the best solutions for your business requirements.

Introduction to the Essential Eight

The Essential Eight are a selection of the 37 controls in the ACSC's Strategies to Mitigate Cyber Security Incidents deemed to have the greatest relative security effectiveness. The Essential Eight are designed primarily to protect Windows-based, Internet-connected systems but many of the recommendations can be applied more broadly.

The mitigation strategies that constitute the Essential Eight are: **application control, patch applications, configure Microsoft Office macro settings, user application hardening, restrict administrative privileges, patch operating systems, multi-factor authentication** and **regular backups**.

While not specifically mentioned in the Essential Eight, the Office of Digital Government SECC Top 5 included a requirement to implement a password filtering solution to prevent the use of weak or known bad passwords. Microsoft encourages the use of Azure AD Password Protection (https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises) to provide this capability in both Azure AD and Active Directory environments until such time as passwordless authentication methods (https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless) can eliminate the need for passwords entirely.

In the following sections of this document we will describe the individual Microsoft solutions that can be employed for mitigation and reporting of each strategy, and in Appendix A we have provided a summary table mapping the Essential Eight to Microsoft solutions.

More information on the Essential Eight is available from https://www.cyber.gov.au/acsc/view-all-content/essential-eight, and the full list of mitigation strategies is available from https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents.

Essential Eight Maturity Model

With the July 2021 update to the Maturity Levels, the ACSC has defined four maturity levels (Maturity Level Zero through to Maturity Level Three) to help organizations implement the Essential Eight. With the exception of Maturity Level Zero, the maturity levels are based on mitigating increasing levels of adversary tradecraft and targeting.

Instead of treating each strategy independently, the ACSC now requires organizations employ a risk-based approach and implement them as a package, planning to achieve the same maturity level across all eight mitigation strategies before moving onto higher maturity levels.

The ACSC also advises the Essential Eight outlines a minimum set of preventative measures to be considered as a baseline, and additional mitigation strategies and security controls may need to be considered, including those from the Strategies to Mitigate Cyber Security Incidents and the Australian Government Information Security Manual.

Because the content may change over time we have opted not to include detail on the Maturity Levels in this whitepaper and recommend review of the information available from https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model.

For those organizations looking for an example on how to implement Microsoft solutions for the Essential Eight, we recommend review of the Digital Transformation Agency's Protected Utility Blueprint, available from https://desktop.gov.au/blueprint/index.html. The blueprint is a design to secure Microsoft 365 desktops, developed with Microsoft and tested with independent security assessors. While the blueprint does provide detailed guidance for implementing the Microsoft solutions, we recommend customers work with a Microsoft Certified Partner to ensure the overall design adequately reflects the needs of their organization.

Mapping the Essential Eight

The following section lists Microsoft products and services mapped to the Essential Eight strategies at a high level. Although we make references to the Maturity Model this information is not specific to achieving any particular level and instead is intended simply to educate on Microsoft's capabilities.

Application Control

The purpose of application control is to ensure only trusted code is allowed to run on a system. At Maturity Level One the aim is to prevent code execution from user profiles and temporary folders, with further restrictions around organization-approved executables and drivers on all workstations and servers at the higher levels.

The ACSC provides a guide for **Implementing Application Control** at https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-application-control.

Primary controls:

- Microsoft Defender for Endpoint provides the core capabilities to centrally log and query events across all endpoints through event collection in the EDR sensor.
- Windows Defender Application Control, part of Windows 10/11 and Windows Server 2016 and above, controls which drivers and applications are allowed to run on Windows devices. WDAC policies apply to the computer as a whole and affect all users of the device. Rules can be defined based on the reputation of the app as determined by the Microsoft Intelligent Security Graph, a managed installer function determined by the identity of the process that initiated the installation, or more traditional methods such as codesigning certificates or file names/paths/hashes.
- AppLocker was introduced with Windows 7 and like WDAC can be used to control which applications are permitted to run on Windows devices. AppLocker rules can be defined based on codesigning certificates, attributes of a file such as the name, version or hash, or the path from which the file is launched. Although Microsoft recommends the use of WDAC over AppLocker, AppLocker may be necessary to provide application control on legacy Windows operating systems such as Windows 8 or Windows Server 2012 R2, and AppLocker's ability to target rules to specific users or groups means it is often deployed as a complement to WDAC on shared computers.

Supporting controls:

- Adaptive Application Controls in Microsoft Defender for Servers uses machine learning to analyze the applications running on Windows and Linux servers and create a list of known-safe software for your workloads. Security alerts will be generated if any applications run other than those defined as safe.
- Microsoft Endpoint Manager or Active Directory Group Policy can be used to configure policies such as WDAC rules and set restrictions on Control Panel applets. With the managed installer function of WDAC, applications and updates deployed by Microsoft Endpoint Manager can be automatically trusted for execution.

Patch Applications

Identifying vulnerabilities and applying patches or updates to remediate them is critical to ensuring the security of your environment. Care must be taken to ensure deployment in a timely fashion while at the same time protecting the stability and availability of the environment; with Internet-connected devices and zero-day vulnerabilities we no longer have the luxury of extended testing periods to ensure compatibility, and as a result Microsoft recommends the use of update rings to incrementally deploy and validate updates, catching and

remediating any potential issues before they impact the entire user base. The Maturity Model for this strategy defines shorter windows for applying updates and more frequent use of vulnerability scanners as the levels progress. The Maturity Model also requires the removal of any applications or extensions no longer supported by the vendor.

The ACSC provides a guide for **Assessing Security Vulnerabilities and Applying Patches** at https://www.cyber.gov.au/acsc/view-all-content/publications/assessing-security-vulnerabilities-and-applying-patches.

Primary controls:

- Microsoft Endpoint Manager includes capabilities to manage updates and patching in the cloud and on-premises. Endpoint Manager combines services you may know and already be using, including Microsoft Intune, Configuration Manager, co-management, and Windows Autopilot. In addition, the Microsoft Desktop Analytics and Office 365 Client Dashboard can provide further insight into application inventory and compatibility. Co-management enables you to concurrently manage Windows 10 or later devices by using both Configuration Manager and Microsoft Intune.
- Microsoft Defender for Endpoint includes Threat and Vulnerability Management which provides continuous discovery of vulnerabilities and misconfigurations, prioritization based on business context, and built-in remediation processes through unique integration with Microsoft Endpoint Manager. Email alerts can be configured to notify security personnel of newly detected vulnerabilities.

Supporting controls:

- Attack surface reduction in Microsoft Defender for Endpoint provides controls to target software behaviors that can be exploited by an attacker to compromise your devices. These behaviors are sometimes seen in legitimate applications, such as launching executable files and scripts that attempt to download or run files, however by restricting these capabilities wherever they are not required to meet a business function you can increase the security posture of your devices. Rules can be implemented in audit mode to assess the impact to your users, and Microsoft Defender for Endpoint can recommend rules to enable based on observed patterns of behavior.
- Exploit protection in Microsoft Defender for Endpoint helps protect devices from malware that uses exploits to spread and infect other devices. Mitigation policies can be applied to either the operating system or individual applications. Exploit protection is enabled by default in Windows 10, and each mitigation can be controlled individually or set to audit mode to test policies without impacting normal system function. Examples of exploit protection include Control Flow Guard (CFG) and Data Execution Prevention (DEP).

Configure Microsoft Office macro settings

Macros are pieces of code embedded within Microsoft Office files that were originally intended to enhance user productivity by automating repetitive tasks or extending functionality in documents. Unfortunately this ease of use has resulted in macros frequently being abused by threat actors to compromise unsuspecting users. Given this risk of exploitation, the Maturity Model directs that macros be disabled for users without a demonstrated business requirement at a minimum, and increasingly restricted for all other users.

The ACSC provides a guide for **Microsoft Office Macro Security** at https://www.cyber.gov.au/acsc/view-all-content/publications/microsoft-office-macro-security.

Primary controls:

- Microsoft Defender for Endpoint includes Attack Surface Reduction rules that can limit the behaviors available to Microsoft Office and other applications such as Adobe Reader. Rules need to be enabled individually and should be configured in Audit mode to determine impact to users before being enforced. Currently there are 16 rules that can be configured including "Block Adobe Reader from

creating child processes", "Block Office applications from injecting code into other processes", "Block executable content from email client and webmail" and "Block Win32 API calls from Office macros".

- The Antimalware Scan Interface (AMSI) is an open interface through which antivirus solutions including Microsoft Defender for Endpoint can inspect script behavior by exposing contents in a form that is both unencrypted and unobfuscated. Windows leverages AMSI extensively in JavaScript, VBScript and PowerShell, and Microsoft 365 Apps for Enterprise integrates with AMSI to scan macros and other scripts at runtime.
- Application Guard for Microsoft Office helps prevent untrusted files from accessing trusted resources by opening them in a secure container that is isolated from the rest of your data through hardware-based virtualization. Files executing within the sandbox do not have access to the Internet or any local or network-based file storage, and depending on your configuration choices may not allow printing, access to the camera and microphone, or even copying/pasting.

Supporting controls:

- Safe Attachments in Microsoft Defender for Office 365 provides an additional layer of protection for e-mail attachments that have already been scanned in Exchange Online Protection. Files are executed in a virtual environment to evaluate their behavior and block anything deemed potentially malicious. Safe Attachments can also be configured to protect SharePoint Online, OneDrive for Business and Microsoft Teams, providing the same detonation capabilities for files shared through these channels as by e-mail.
- Safe Documents uses the cloud backend of Microsoft Defender for Endpoint to scan opened Office documents in Protected View or Application Guard for Office. Macros and other active content within the document cannot be executed in Protected View, and if the file is determined to be malicious the user will be blocked from exiting the container meaning those macros will never be able to run.
- Microsoft Endpoint Manager or Active Directory Group Policy can be used to configure attack surface reduction rules and specific configuration settings for Microsoft 365 Apps for Enterprise. The Office cloud policy service can be used to enforce policy settings on Office applications even if the device is not domain-joined or otherwise managed.

User application hardening

User application hardening refers primarily to the configuration of web browsers, Microsoft Office applications, and PDF software. Maturity Level One calls for basic controls over the browser, Level Two adds specific blocking rules for Office, and Level 3 adds restrictions on PowerShell and .NET Framework.

The ACSC provides a guide for **Hardening Windows 10** at https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-microsoft-windows-10-version-21h1-workstations and for **Hardening Microsoft 365, Office 2021, Office 2019 and Office 2016** at https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-microsoft-365-office-2021-office-2019-and-office-2016.

Primary controls:

- Microsoft Defender for Endpoint includes Attack Surface Reduction rules that can limit the behaviors available to Microsoft Office and other applications such as Adobe Reader. Rules need to be enabled individually and should be configured in Audit mode to determine impact to users before being enforced. Currently there are 16 rules that can be configured including "Block Adobe Reader from creating child processes", "Block Office applications from injecting code into other processes", "Block executable content from email client and webmail" and "Block Win32 API calls from Office macros".
- Application Guard for Microsoft Edge uses hardware isolation to launch untrusted sites within a protected container. Administrators define trusted sites, cloud resources, and internal networks, and anything not listed is considered untrusted and kept isolated from the corporate network and data on the user's device.

- Microsoft Edge is built on top of the Chromium open source project and further enhanced with built-in defenses against phishing and malware, and native support for Microsoft 365 security and compliance services. Microsoft Edge also includes native PDF reader support, eliminating the need for third-party software.

Supporting controls:

- Microsoft Endpoint Manager or Active Directory Group Policy can be used to configure attack surface reduction rules and specific configuration settings for Microsoft 365 Apps for Enterprise. The Office cloud policy service can be used to enforce policy settings on Office applications even if the device is not domain-joined or otherwise managed.

Restrict administrative privileges

To reduce the possibility of administrative credentials being compromised through standard user activity separation of privileged and unprivileged resources and strict adherence to the principals of least privilege is recommended. Users should not use the same account for managing systems as they use for accessing the Internet or reading e-mail, and accounts should not have permanently-assigned administrative permissions. While some customers make a risk-based decision to use a single account with just-in-time privilege elevation through the use of Privileged Identity Management/Privileged Access Management solutions, the ACSC through the Maturity Model requires complete separation between accounts and operating environments. Higher maturity levels list requirements for stricter monitoring and alerting as well as just-in-time elevation.

The ACSC provides a guide for **Restricting Administrative Privileges** at https://www.cyber.gov.au/acsc/view-all-content/publications/restricting-administrative-privileges.

Primary controls:

- In general, Microsoft 365 does not require a license for a second account used for administrative purposes, provided the account does not need a mailbox or access to productivity services.
- Conditional Access as part of Azure Active Directory provides the security policy enforcement engine for Microsoft's Zero Trust Model and can be used to enforce multi-factor authentication requirements to federated services based on conditions such as the user's identity, location, or device state. In the context of this strategy, Conditional Access could be used to prevent administrative accounts logging in from unmanaged devices or locations, and multi-factor authentication requirements could be enforced.
- Azure AD Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources. Instead of users having permanent role assignments such as Global Administrator, users can instead be configured as eligible for the role with the requirement to request just-in-time elevation through the Azure portal when required. Access requests can require a justification and approval and would typically be granted for a limited period of time.
- Microsoft Defender for Servers includes just-in-time virtual machine access for Windows and Linux servers hosted in Azure. Users must request access to a JIT-enabled VM programmatically or through the Azure portal, at which point the appropriate Network Security Group or firewall rules are configured to allow access to the RDP or SSH ports for a specified period of time from specific source IP addresses. All requests are audited and can include a justification for why the request was made.
- Azure Bastion is a fully platform-managed PaaS service that provides secure and seamless RDP/SSH connectivity to Azure-hosted virtual machines directly from the Azure portal over TLS using a HTML5-based web client. Virtual machines do not need a public IP address, agent, or special client software, and there is no need to expose RDP/SSH ports to the outside world.
- Windows Defender Credential Guard in Microsoft Defender for Endpoint uses virtualization-based security to isolate secrets so that only privileged system software can access them. Unauthorized access

to these secrets can lead to credential theft attacks, such as Pass-the-Hash or Pass-The-Ticket. Windows Defender Credential Guard prevents these attacks by protecting NTLM password hashes, Kerberos Ticket Granting Tickets, and credentials stored by applications as domain credentials. Windows Defender Remote Credential Guard helps protect credentials over a Remote Desktop connection by redirecting Kerberos requests back to the device that's requesting the connection. It also provides single sign-on experiences for Remote Desktop sessions. By using Windows Defender Remote Credential Guard to connect during Remote Desktop sessions, if the target device is compromised, your credentials are not exposed because both credential and credential derivatives are never passed over the network to the target device. User Account Control (UAC) helps prevent malware from damaging a PC by ensuring applications and tasks run in the security context of a non-administrator account unless specifically authorized. Users are granted standard user permissions at sign-in, and if an application needs anything higher UAC seeks consent and runs only that application with elevated privileges.

- Privileged Access Workstations (PAWs), sometimes also referred to as Secure Admin Workstations (SAWs), are dedicated devices used for administration of privileged systems. PAWs should start with a hardware root of trust and come directly from the manufacturer in a known-good state such as with Secured-core PCs. PAWs should be strictly controlled and not used for anything other than administration, with all Internet access denied except for a specific list of URLs required for management. Depending on an organization's risk tolerance, in order to save users from carrying two physical devices PAWs sometimes run virtualized environments where normal user activities such as email and web browsing can be completed, however the privileged environment should never run as a virtual machine on an unprivileged system due to the potential for compromise of the firmware or host operating system. Cloud PC solutions such as Azure Virtual Desktop or Windows 365 can also be used to provide an unprivileged OS environment.

Supporting controls:

- Microsoft Endpoint Manager or Active Directory Group Policy can be used to configure policies for Windows security features such as Credential Guard. In addition, Microsoft Endpoint Manager is recommended for the provisioning and ongoing management of Privileged Access Workstations including deployment through Windows Autopilot.
- Microsoft Defender for Identity monitors and analyzes user activities and information across your network, such as permissions and group membership, creating a behavioral baseline for each user. Defender for Identity then identifies anomalies with adaptive built-in intelligence, providing insights into suspicious activities and events, revealing the advanced threats, compromised users, and insider threats facing your organization.
- Microsoft Defender for Cloud Apps analyzes data captured across SaaS applications and cloud services, combining multiple detection methods including anomaly, behavioral analytics (UEBA), and rule-based activity detections, to provide a broad view of user activity in your environment. Alerts can be raised for events such as activity from a suspicious IP address, multiple failed login attempts, unusual administrative activity, or impossible travel.

Patch operating systems

The requirements and solutions for patching of operating systems are very similar to those for patching applications, with the biggest difference being in regards to currency: while the strategy for patching applications notes in Maturity Level Three that applications no longer supported by the vendor should be removed, this requirement is in place for operating systems even at Maturity Level One. In addition, Maturity Level Three for patching operating systems requires the latest or previous release of the OS be used by all workstations, servers and network devices.

The ACSC provides a guide for **Assessing Security Vulnerabilities and Applying Patches** at https://www.cyber.gov.au/acsc/view-all-content/publications/assessing-security-vulnerabilities-and-applying-patches.

Primary controls:

- Microsoft Endpoint Manager includes capabilities to manage updates and patching in the cloud and on-premises. Endpoint Manager combines services you may know and already be using, including Microsoft Intune, Configuration Manager, co-management, and Windows Autopilot. In addition, the Microsoft Desktop Analytics and Office 365 Client Dashboard can provide further insight into application inventory and compatibility. Co-management enables you to concurrently manage Windows 10 or later devices by using both Configuration Manager and Microsoft Intune.
- Microsoft Defender for Endpoint includes Threat and Vulnerability Management which provides continuous discovery of vulnerabilities and misconfigurations, prioritization based on business context, and built-in remediation processes through unique integration with Microsoft Endpoint Manager. Email alerts can be configured to notify security personnel of newly detected vulnerabilities.
- Microsoft Defender for Cloud provides reporting of missing OS patches and security misconfiguration assessments for Windows and Linux machines in Azure and other servers managed through Azure Arc. With Microsoft Defender for Servers enabled, Microsoft Defender for Cloud can display results from the integrated Qualys vulnerability scanner or Threat and Vulnerability Management in Microsoft Defender for Endpoint.

Supporting controls:

- Attack surface reduction in Microsoft Defender for Endpoint provides controls to target software behaviors that can be exploited by an attacker to compromise your devices. These behaviors are sometimes seen in legitimate applications, such as launching executable files and scripts that attempt to download or run files, however by restricting these capabilities wherever they are not required to meet a business function you can increase the security posture of your devices. Rules can be implemented in audit mode to assess the impact to your users, and Microsoft Defender for Endpoint can recommend rules to enable based on observed patterns of behavior.
- Exploit protection in Microsoft Defender for Endpoint helps protect devices from malware that uses exploits to spread and infect other devices. Mitigation policies can be applied to either the operating system or individual applications. Exploit protection is enabled by default in Windows 10, and each mitigation can be controlled individually or set to audit mode to test policies without impacting normal system function. Examples of exploit protection include Control Flow Guard (CFG) and Data Execution Prevention (DEP).
- Azure Automation Update Management can be used to manage operating system updates for Windows and Linux virtual machines in Azure or other platforms including on-premises servers through the use of Azure Arc. The machines assigned to Update Management report how up to date they are based on the source they are configured to synchronize with. Windows machines need to be configured to report to either Windows Server Update Services or Microsoft Update, and Linux machines need to be configured to report to a local or public repository. You can also use Update Management with Microsoft Endpoint Configuration Manager.

Multi-factor authentication

Even the most complex passwords aren't enough to protect against the countless methods attackers have at their disposal for stealing credentials and gaining unauthorized access to systems. Microsoft estimates 99.9% of account compromise incidents could have been blocked by a multi-factor solution, so this is clearly one of the most important strategies to implement. The Maturity Models call for multi-factor authentication when accessing third-party or Internet-facing systems at a minimum, with the higher levels adding requirements

around the strength of the MFA implementation, use with privileged accounts, and centralized monitoring and reporting.

The ACSC provides a guide for **Implementing Multi-Factor Authentication** at https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-multi-factor-authentication.

Primary controls:

- Conditional Access as part of Azure Active Directory provides the security policy enforcement engine for Microsoft's Zero Trust Model and can be used to enforce multi-factor authentication requirements to federated services based on conditions such as the user's identity, location, or device state.
- With Azure AD Identity Protection, Conditional Access gains the ability to evaluate session risk in real-time based on signals from each sign-in, providing the capability to mitigate risky sign-ins by selectively blocking access or requiring MFA.
- On-premises web applications can be enabled for MFA by publishing them using the Azure AD Application Proxy. Unlike reverse proxy solutions that require you to allow inbound connections through your firewall, the Application Proxy Connector running on a Windows Server inside your network uses stateless outbound connections to the Application Proxy Service for communication between the requesting user and the on-premises application.
- MFA can be enforced on sign in to Remote Desktop services using the Network Policy Server extension for Azure MFA and enabling RADIUS authentication. The same configuration can be leveraged to provide MFA for VPN connections.
- Windows 10/11 includes biometric factors (Windows Hello for Business), TPM, physical/virtual Smartcard technologies, and support for FIDO2 tokens, all of which, all of which can be used to eliminate the need for passwords entirely. Passwordless authentication is by definition multi-factor authentication, and as a result users who sign in to the device using a solution such as Windows Hello will not be prompted with a separate MFA challenge when accessing Azure AD-enabled applications. With a Temporary Access Pass users can be issued with a time-limited passcode that can be used to onboard other authentication factors such as a FIDO2 security key or Microsoft Authenticator app.

Supporting controls:

- Microsoft Defender for Identity monitors and analyzes user activities and information across your network, such as permissions and group membership, creating a behavioral baseline for each user. Defender for Identity then identifies anomalies with adaptive built-in intelligence, providing insights into suspicious activities and events, revealing the advanced threats, compromised users, and insider threats facing your organization.
- Microsoft Defender for Cloud Apps analyzes data captured across SaaS applications and cloud services, combining multiple detection methods including anomaly, behavioral analytics (UEBA), and rule-based activity detections, to provide a broad view of user activity in your environment. Alerts can be raised for events such as activity from a suspicious IP address, multiple failed login attempts, unusual administrative activity, or impossible travel.

Regular backups

Under the Shared Responsibility Model data governance is always the responsibility of the customer, but that doesn't necessarily mean taking a copy of everything stored within Microsoft 365. Microsoft services are designed to be highly resilient with redundancy built directly into our cloud services. Additional controls are available to manage retention requirements unique to each customer, and external backup solutions can be employed where necessary for critical data. All of the Maturity Levels require data, software and configuration settings to be backed up in accordance with business continuity requirements and restoration tested

periodically; higher levels further restrict which privileged and unprivileged accounts should be able to access backups.

Primary controls:

- Microsoft 365 allows for control of data stored within the tenant through the use of Retention policies and retention labels. Retention policies control retention settings at a site or mailbox level, while retention labels can apply settings to an individual item (folder, document, email) and may travel with the content if it's moved to a different location. Retention settings ensure content will remain available within the platform subject to your preservation requirements, even if it may appear deleted to end users, and with multiple versions of items stored by default any permitted changes to items are also captured. Retention labels can be applied automatically based on the content through the use of Sensitive Information Types and Trainable Classifiers, ensuring different retention and disposition schedules based on the importance of the data. To ensure administrators cannot alter retention policies or label policies the Preservation Lock feature prevents all changes except adding locations or increasing the retention period. Marking an item as a regulatory record can further prevent changes to labels in locked policies.
- The Azure Backup service provides a simple, secure and cost-effective solution to back up and recover on-premises and cloud-based data from within Microsoft Azure. Native controls in Azure enable backups of Windows/Linux VMs, Azure Managed Disks, Azure Files shares, SQL databases, SAP HANA databases, and Azure Blobs. The Microsoft Azure Recovery Services (MARS) agent provides the ability to back up files, folders and system state from on-premises or virtual machines, as well as integration with on-premises Azure Backup Server (MABS) or System Center Data Protection Manager (DPM) servers. Azure Backup includes extensive security capabilities to protect data in transit and at rest, including fine-grained role-based access controls, encryption of data, protection from unintentional deletion, and monitoring and alerting of suspicious activity.

Supporting controls:

- Microsoft 365 data resiliency principles ensure customer data remains intact and unaffected regardless of what may fail within the environment. Multiple copies of customer data are stored across fault domains and protected from corruption. Microsoft 365 also provides a graphical interface for customers to restore deleted items on their own, whether that's end-user recovery of deleted items in SharePoint, OneDrive and Outlook, or administrators recovering purged files through eDiscovery solutions.
- OneDrive for Business and Outlook as part of Microsoft Office Apps for Enterprise both store copies of data synchronized with the cloud services on a user's local machine. While not intended as a primary backup/restore solution, this cached information can be used to ensure availability when a connection to the cloud service is unavailable.
- Windows Autopilot is a collection of technologies used to set up and pre-configure new devices. In the context of this strategy, Windows Autopilot can be used to provision new Windows 10 and 11 devices in a "business-ready" state that includes all appropriate applications, policies and settings. Autopilot can also be used to reset a device to the business-ready state in the event of problems or for repurposing. Combined with data stored in cloud services and synchronized on demand, Autopilot can help restore a user's environment in the event of loss or corruption.

Summary

The solutions provided in the Microsoft 365 E5 suite offer extensive functionality to meet the requirements of the Essential Eight across your end user identities and devices, and with the addition of Microsoft Defender for Cloud these capabilities extend across your server fleet regardless of where the servers may be hosted.

This document aimed to provide a sufficient level of detail to determine how the Microsoft solutions can be utilized, with more information available through the various hyperlinks included within the text or from the companion whitepapers for Security and Compliance with links available in the introductory section on Page 3. In particular, Microsoft encourages review of the Desktop-as-a-Service solutions available through Microsoft Managed Desktop, Azure Virtual Desktops, and Windows 365, as well as the new Essential Eight premium assessment templates for Microsoft 365 Compliance Manager. The Essential Eight workbook for Microsoft Defender for Cloud provided through the Office of Digital Government can also assist with monitoring progress against the Essential Eight requirements.

However, compliance with the Essential Eight Maturity Levels requires more than just deploying technical solutions and turning on features. Any restrictions implemented to reduce the exploitable surface area may result in a negative user experience as functions users depend on are also impacted. Microsoft recommends Agencies work with a Certified Partner to determine a strategy that weighs their security requirements against the functionality needs of the user base and seeks to minimize exceptions to the security baseline. Any exceptions should be properly documented and reviewed on a regular basis, with the goal to eliminating them as business requirements or technology limitations change.

Finally, remember you are not alone – all government agencies in Western Australia will be working towards alignment with the Essential Eight, as will other state and federal agencies and commercial organizations of all sizes. Look out for opportunities to connect with your community and share experiences through webinars, training, or user groups.

For more information on any of the capabilities described in this whitepaper, or to share feedback and request topics for future updates, please contact your Microsoft Account Team using the details at the beginning of the document.

Appendix A: Essential Eight Technology Mapping Summary

	Defender for Endpoint / Windows Security	Microsoft 365 Apps for Enterprise	Defender for Office 365	Azure AD Premium	Microsoft Endpoint Manager	Defender for Identity / Defender for Cloud Apps	Defender for Cloud Apps	Other
Application Control	**Application Control** **AppLocker** **Event Collection**				Policy management		Adaptive Application Control	
Patch Applications	Attack Surface Reduction Exploit Protection **Threat and Vulnerability Management**				**Patch management**		Azure Update Management	
Configure Office macro settings	**Attack Surface Reduction** **AppGuard for Office** **Antimalware Scan Interface** **EDR**	Configure Office Client Policies	Safe Attachments Safe Documents		Policy management			
User application hardening	**Attack Surface Reduction** **AppGuard for Edge** EDR	Configure Office Client Policies			Policy management			**Microsoft Edge**
Restrict administrative privileges	**Credential Guard** **User Account Control** **LAPS** **PAW**			**Conditional Access** **Privileged Identity Management** **Access Reviews**	Policy management	Defender for Identity Defender for Cloud Apps	**Just-in-time VM Access** **Azure Bastion**	
Patch operating systems	Attack Surface Reduction Exploit Protection **Threat and Vulnerability Management**				**Patch management**		**Security Recommendations** Azure Update Management	
Multi-factor authentication	**Windows Hello for Business** **FIDO2 Authentication**			**MFA** **Conditional Access** **Identity Protection** **Application Proxy**	Policy management	Defender for Identity Defender for Cloud Apps		
Regular backups		OneDrive for Business Outlook			Windows Autopilot		**Azure Backup**	**Retention policies and labels** Native Microsoft 365 Service Resilience

Service Compliance: Microsoft 365 Compliance Manager with premium assessment templates for Essential Eight Maturity Level One, Two, and Three
Monitoring: Microsoft Sentinel workbooks / Power BI

Appendix B: Microsoft Training and Certification

Microsoft Enterprise Agreement Yammer Group
Administered by the WA Department of Finance, this invitation-only group is available to approved agencies and provides a means to communicate between Microsoft and agencies in the Whole of Government agreement. The group hosts announcements on training opportunities and recordings of previous sessions.

Microsoft Snackable Series for WA Government
The Microsoft Snackable Series offers short webinars delivered through Microsoft Teams by Microsoft experts on both technical and non-technical subjects. These sessions cover popular topics and provide overviews, updates, and tips. Attendance is open to all agencies under the Whole of Government agreement and recordings are posted to the Yammer group.

Microsoft Security Webinars
http://aka.ms/securitywebinars

Public deep-dive webinars conducted by the Engineering teams on new and upcoming features. Presentations are recorded and decks and videos are available for all past sessions.

Microsoft Certified: Security, Compliance, and Identity Fundamentals
https://docs.microsoft.com/en-us/learn/certifications/security-compliance-and-identity-fundamentals/

This certification is intended for those looking to familiarize themselves with the fundamentals of security, compliance and identify across cloud-based and related Microsoft services. This exam and associated Learning Path will help you understand the solutions available in E3 and E5 licensing and when you would use each capability. This is a great place to start for IT Professionals and business users alike.

Microsoft Certified: Security Operations Analyst Associate
https://docs.microsoft.com/en-us/learn/certifications/security-operations-analyst/

This certification is intended for people responsible for securing information technology systems for the organisation. The exam and learning path are focused on investigating, responding to and hunting for threats using Microsoft Azure Sentinel, Microsoft Defender, Microsoft 365 Defender, and other third-party security products.

Microsoft Certified: Identity and Access Administrator Associate
https://docs.microsoft.com/en-us/learn/certifications/identity-and-access-administrator/

This certification is intended for people responsible for implementing, and operating an organisation's identity and access management systems by using Azure AD. The exam and learning path are focused on Azure AD capabilities including general administration and implementation of hybrid identity, Azure AD Identity Protection, and Identity Governance.

Microsoft Certified: Information Protection Administrator Associate
https://docs.microsoft.com/en-us/learn/certifications/information-protection-administrator/

This certification is intended for people responsible for planning and implementing controls to meet organisational compliance needs. The exam and learning path are specifically focused on Microsoft Information Protection, Data Loss Prevention, and Information Governance.