Take a seat, we'll be starting shortly

PRIVACYENGINE

WEBINAR

Best Privacy Practices for Microsoft 365 - Empowering the DPO

Thursday 25th Jan 2024

12:00 GMT

Mike Morrissey
CISO and Co-Founder
PrivacyEngine

Nollag Conneely
Head of Consultancy
PrivacyEngine

Information Classification: Unclassified

PRIVACYENGINE

Structure

- The importance of Office 365 in organisations today
- The scope of services provided by Office 365
- Why Office 365 matters to DPOs
- Providing DPOs with high level knowledge that allows them engage productively with business and IT decision makers around privacy risks relating to Office 365

www.privacyengine.io

High Performer EMEA WINTER 2024

Best Support WINTER 2024

High Performer WINTER 2024

Best Meets Requirements WINTER 2024

Momentum Leader WINTER 2024

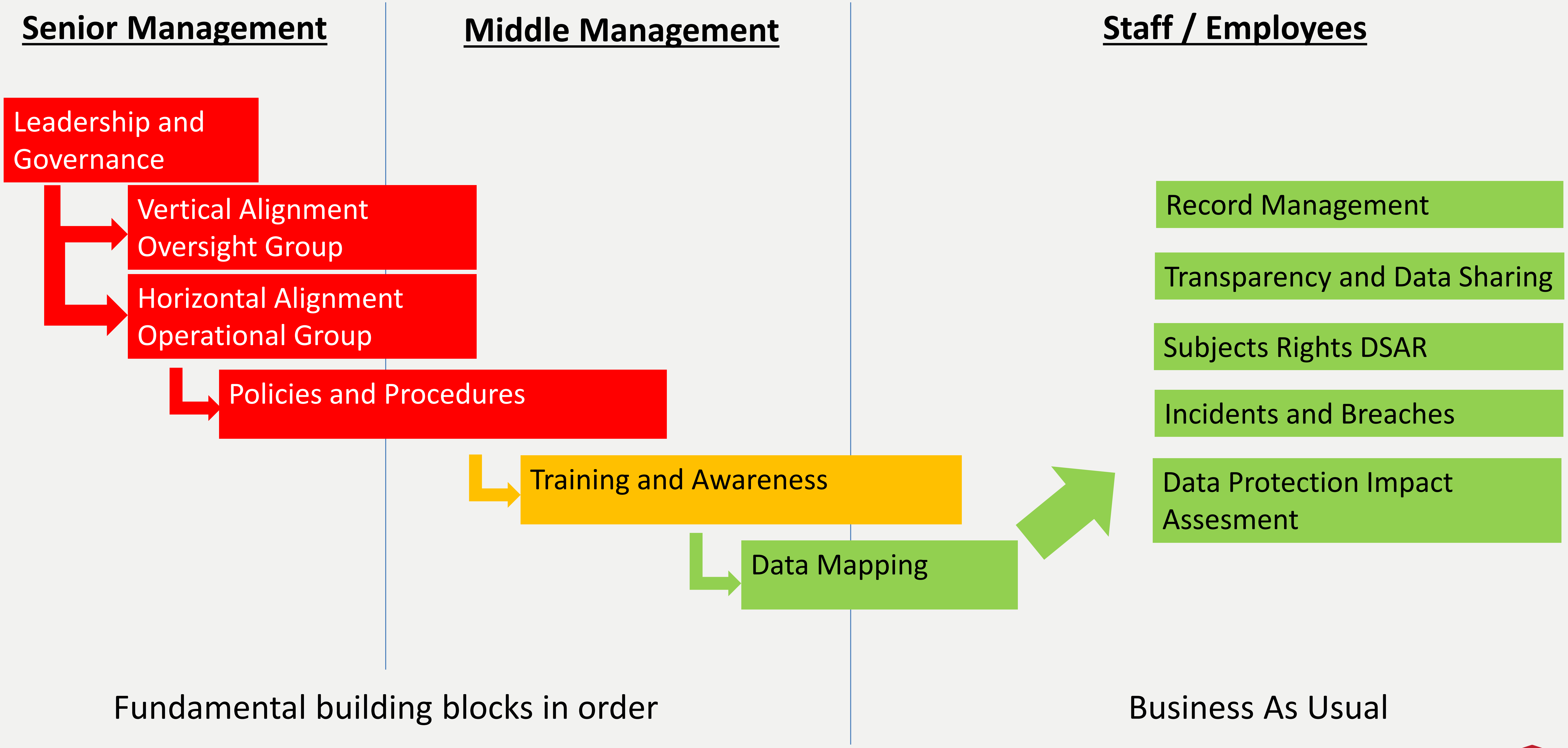
Fastest Implementation WINTER 2024

Easiest To Do Business With WINTER 2024

High Performer Europe WINTER 2024

Information Classification: Unclassified

Privacy Plan on a Page



Senior Management

Middle Management

Staff / Employees

Leadership and Governance

Vertical Alignment Oversight Group

Horizontal Alignment Operational Group

Policies and Procedures

Training and Awareness

Data Mapping

Record Management

Transparency and Data Sharing

Subjects Rights DSAR

Incidents and Breaches

Data Protection Impact Assesment

Fundamental building blocks in order

Business As Usual

Alignment 33 KPIs	Policies & Procedures 17 KPIs	Training 21 KPIs	ROPA 33 KPIs	Individual Rights 42 KPIs	Transparency 31 KPIs	Contracts & data Sharing 31 KPIs	Risks & DPIAs 29 KPIs	Records Management 63 KPIs	Breach Response 39 KPIs
Organisational Structure	Direction and Support	Comprehensive Staff Training	Data Mapping	Informing individuals and identifying requests	Privacy Notice Content	Data Sharing Policies and Procedures	Identifying, Recording, and Managing Risks	Creating, Locating, and Retrieving Records	Detecting, Managing, and Recording Incidents and Breaches
Appointing a DPO	Review and Approval	Induction and Ongoing Education	Records of Processing Activities (ROPA)	Resources	Timely Privacy Information	Data Sharing Agreements	Data Protection by Design and by Default	Security for Transfers	Assessing and Reporting Breaches
Appropriate Reporting	Staff Awareness	Specialized Role Training	ROPA Requirements	Logging and tracking requests	Effective Privacy Information	Restricted Transfers	DPIA Policy and Procedures	Data Quality	Notifying Individuals
Operational Roles	Data Protection by Design and by Default	Monitoring and Verification of training	Good Practice for ROPAs	Timely Responses	Automated Decision-making and Profiling	Data Processors	DPIA Content	Retention Schedule	Reviewing and Monitoring
Oversight Groups		Proactive Awareness Building	Documenting Lawful Basis	Monitoring and Evaluating Performance	Staff Awareness	Processor Due Diligence Checks	DPIA Risk Mitigation and Review	Destruction	External Audit or Compliance Check
Operational Group Meetings			Lawful Basis Transparency	Inaccurate or Incomplete Information	Privacy Information Review	Processor Compliance Reviews		Information Asset Register	Internal Audit Programme
			Consent Requirements	Erasure	Tools Supporting Transparency and Control	Third Party Products and Services		Rules for Acceptable Software Use	Performance and Compliance Information
			Reviewing Consent	Restriction		Purpose Limitation		Access Control	Use of Management Information
			Risk-based Age Checks and Parental/Guardian Consent	Data Portability				Unauthorised Access	
			Legitimate Interest Assessment (LIA)	Rights Relating to Automated Decision-making and Profiling				Mobile Devices, Home or Remote Working, and Removable Media	
				Individual complaints				Secure Areas	
								Business Continuity, Disaster Recovery, and Back-ups	

Privacy Engine's 'Plan on a Page' is supported by 76 Goals/Initiatives outlined above.

These are monitored, measured and reported utilising 339 metrics to assess Goals/Initiatives under the 10 headings above.

64 Metrics relate to the 12 Record Management Initiatives

DPC Case studies

- Article 5
  - Integrity and Confidentiality
  - Cybersecurity Triad CIA
- Article 32
- Microsoft 365 (A1) licence being utilised did not provide a level of security appropriate to the risk associated with the type of personal data it processes in its role as a professional standards body
- I find that you failed to regularly assess and evaluate the effectiveness of technical and organisational measures for ensuring the security of the processing of personal data, in accordance with Article 32(1)(d)
- I find that you failed in your obligation to ensure appropriate organisational and technical measures where the state of the art is significantly more advanced than the systems in use at the time of the breach

DPC Case studies

- I find that an appropriate level of security includes the implementation of 2FA (two factor authentication) in Office 365 for all users
- I find that you should implement Advanced Threat Protection (ATP) in Office 365
- I find that you should mandate annual data protection and cyber security training for all staff. This measure should assist users in identifying emails from malicious actors and require them to report any such emails to IT staff.
- By paying Office 365 license fees appropriate to the level of a professional standards body such as the Council, would not impose a disproportionate cost on Council with regard to its obligation to implement a level of security appropriate to the risk presented.
- The organisation ought to have been aware of the data breach if it had used all appropriate technological and organisational measures to establish the cause of the initial, second and third security alerts as it was obliged to do.
- I find that all appropriate technological protection and organisational measures had not been implemented to establish within a reasonable period of time whether a personal data breach had taken place.

DPC Case studies

- I find that an appropriate level of security must also include a policy that mandates password protection for sensitive personal data transmitted by email.
- Although default email settings for Microsoft 365 only stores log files for 90 days, system administrators may increase the mailbox's AuditLogAgeLimit value and retain log records for longer than the 90 day period
- Legacy Authentication protocols in Office 365 should be disabled for all users;
- A policy of encryption and password protection on all data spreadsheets containing personal data in their possession, for both for internal and external document sharing;

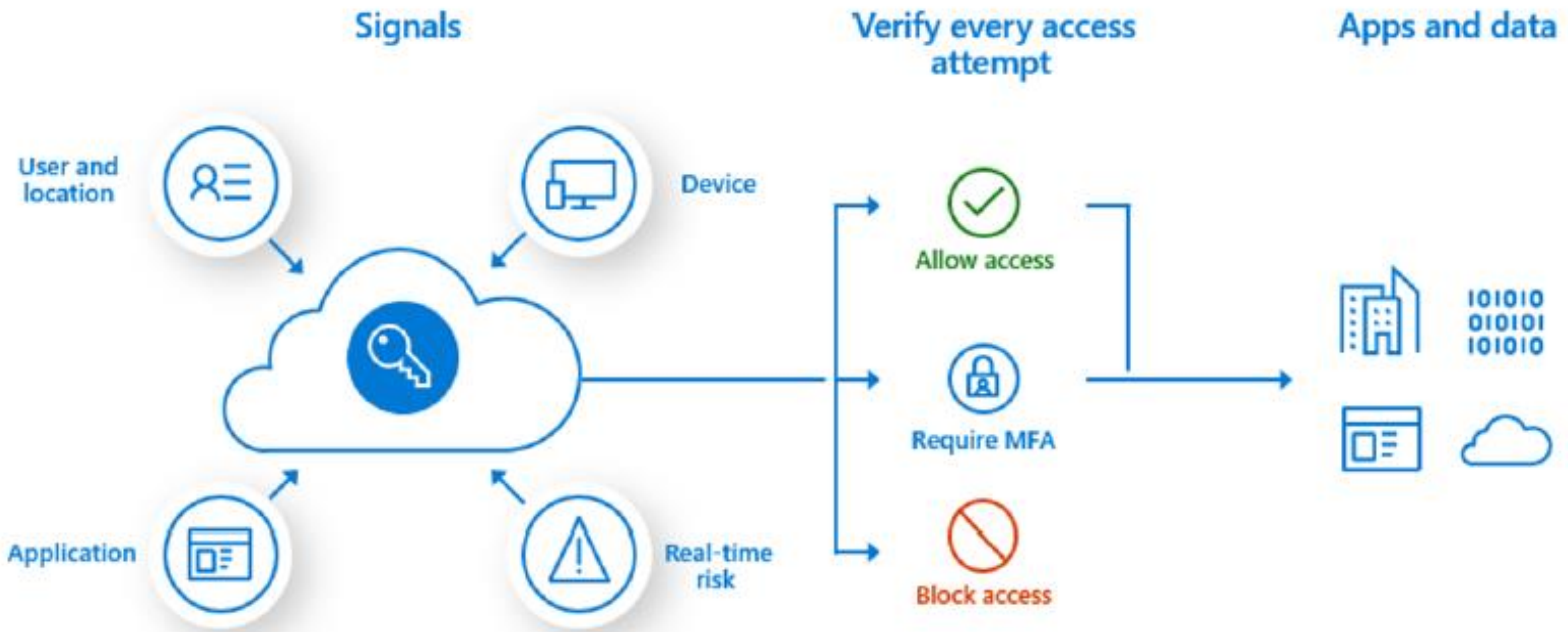
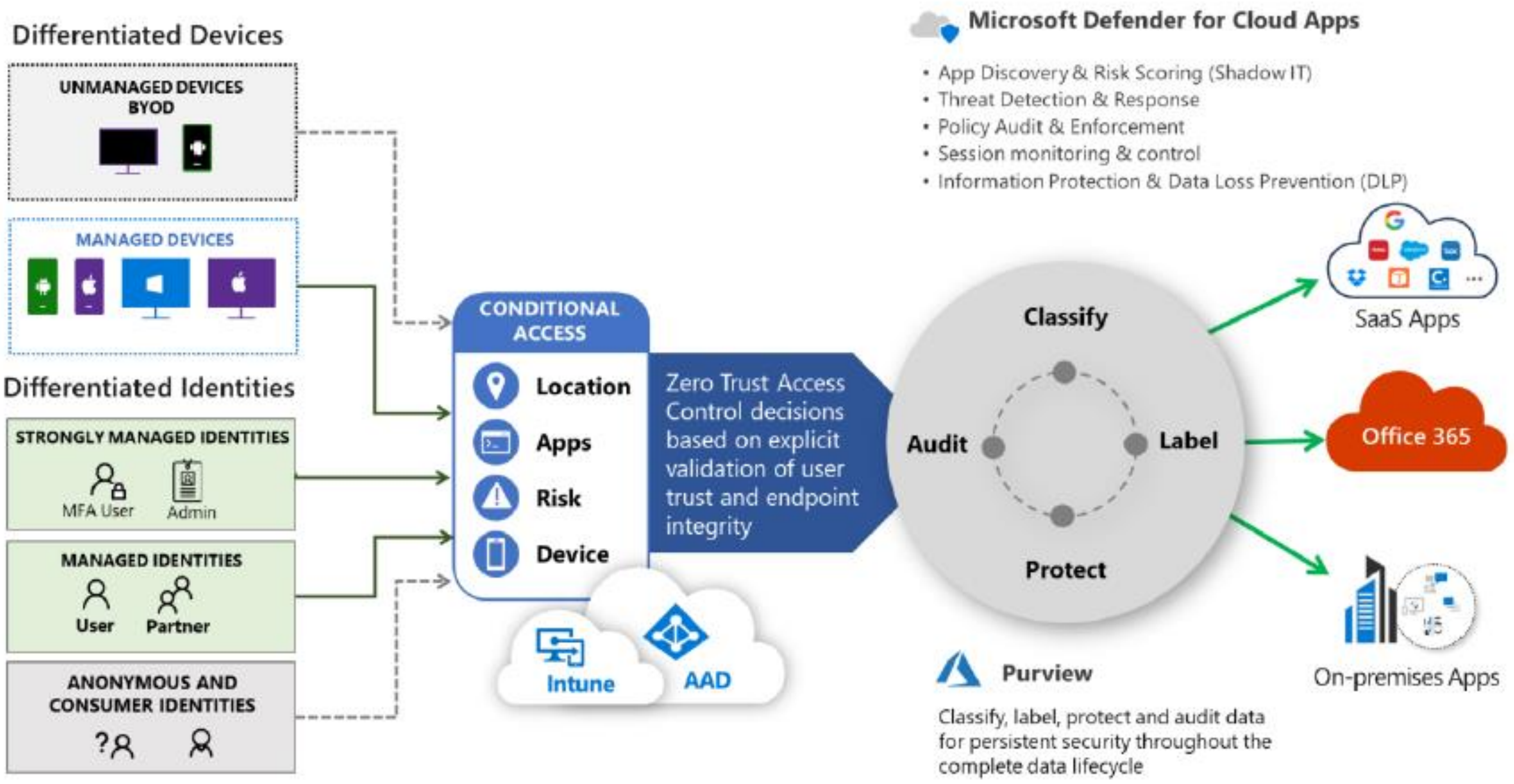


Figure 3 – Zero Trust Principles



Zero Trust Access Control decisions based on explicit validation of user trust and endpoint integrity

Microsoft Defender for Cloud Apps

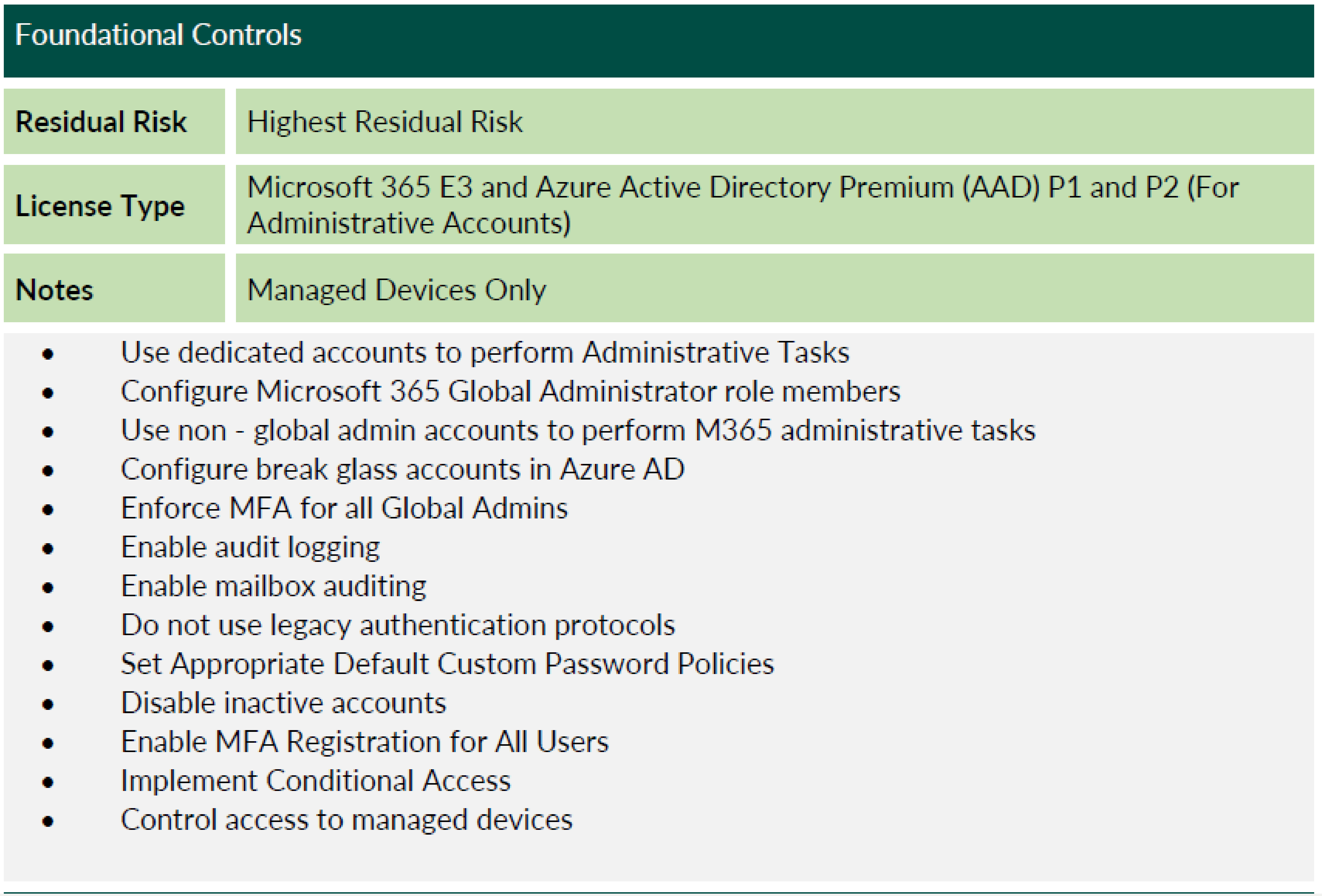
- App Discovery & Risk Scoring (Shadow IT)
- Threat Detection & Response
- Policy Audit & Enforcement
- Session monitoring & control
- Information Protection & Data Loss Prevention (DLP)

Purview

Classify, label, protect and audit data for persistent security throughout the complete data lifecycle

Figure 4 – Data Protection through conditional access and zero trust principles

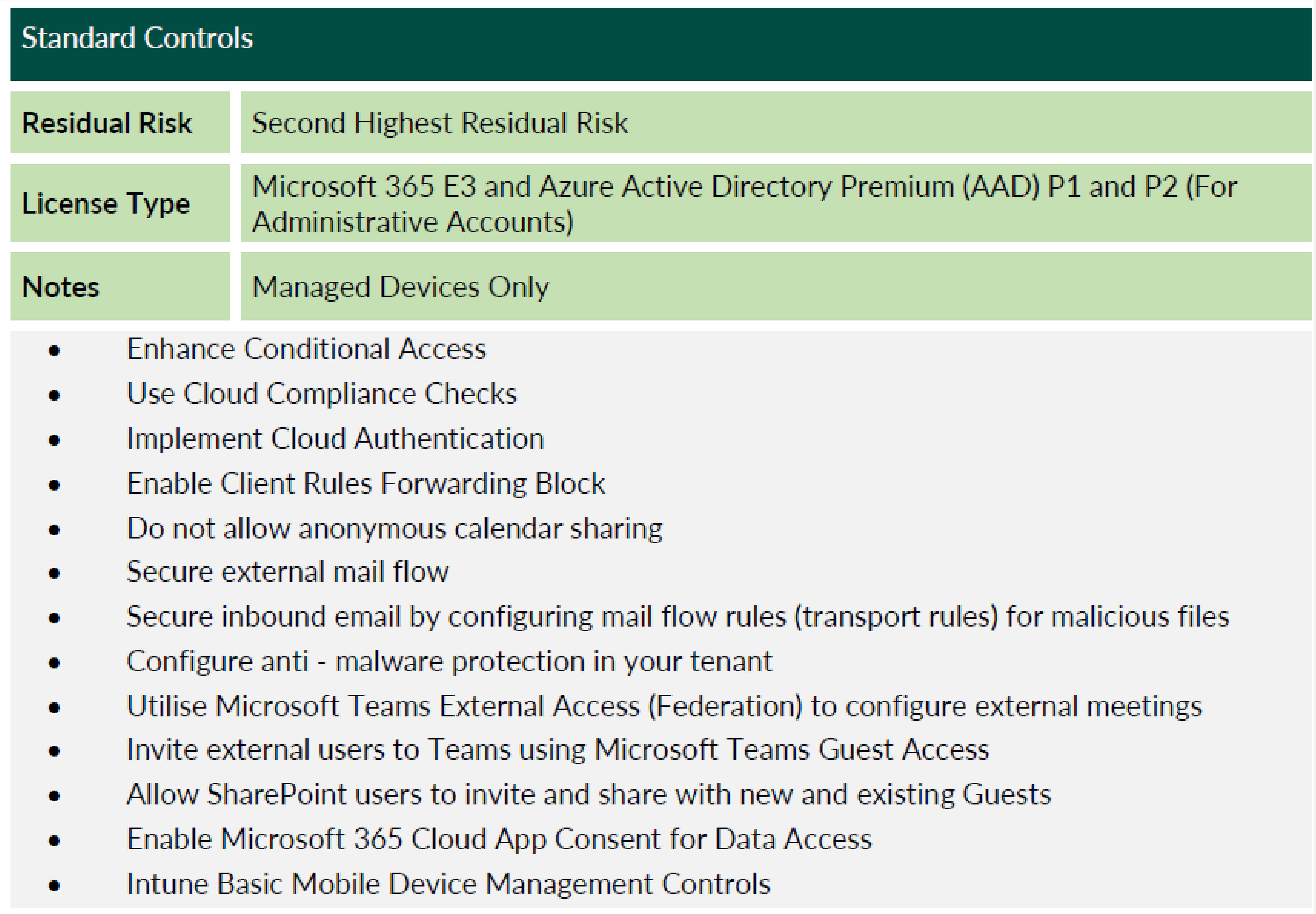
Control Levels



Foundational Controls	
Residual Risk	Highest Residual Risk
License Type	Microsoft 365 E3 and Azure Active Directory Premium (AAD) P1 and P2 (For Administrative Accounts)
Notes	Managed Devices Only

- Use dedicated accounts to perform Administrative Tasks
- Configure Microsoft 365 Global Administrator role members
- Use non - global admin accounts to perform M365 administrative tasks
- Configure break glass accounts in Azure AD
- Enforce MFA for all Global Admins
- Enable audit logging
- Enable mailbox auditing
- Do not use legacy authentication protocols
- Set Appropriate Default Custom Password Policies
- Disable inactive accounts
- Enable MFA Registration for All Users
- Implement Conditional Access
- Control access to managed devices

Control Levels



Standard Controls	
Residual Risk	Second Highest Residual Risk
License Type	Microsoft 365 E3 and Azure Active Directory Premium (AAD) P1 and P2 (For Administrative Accounts)
Notes	Managed Devices Only

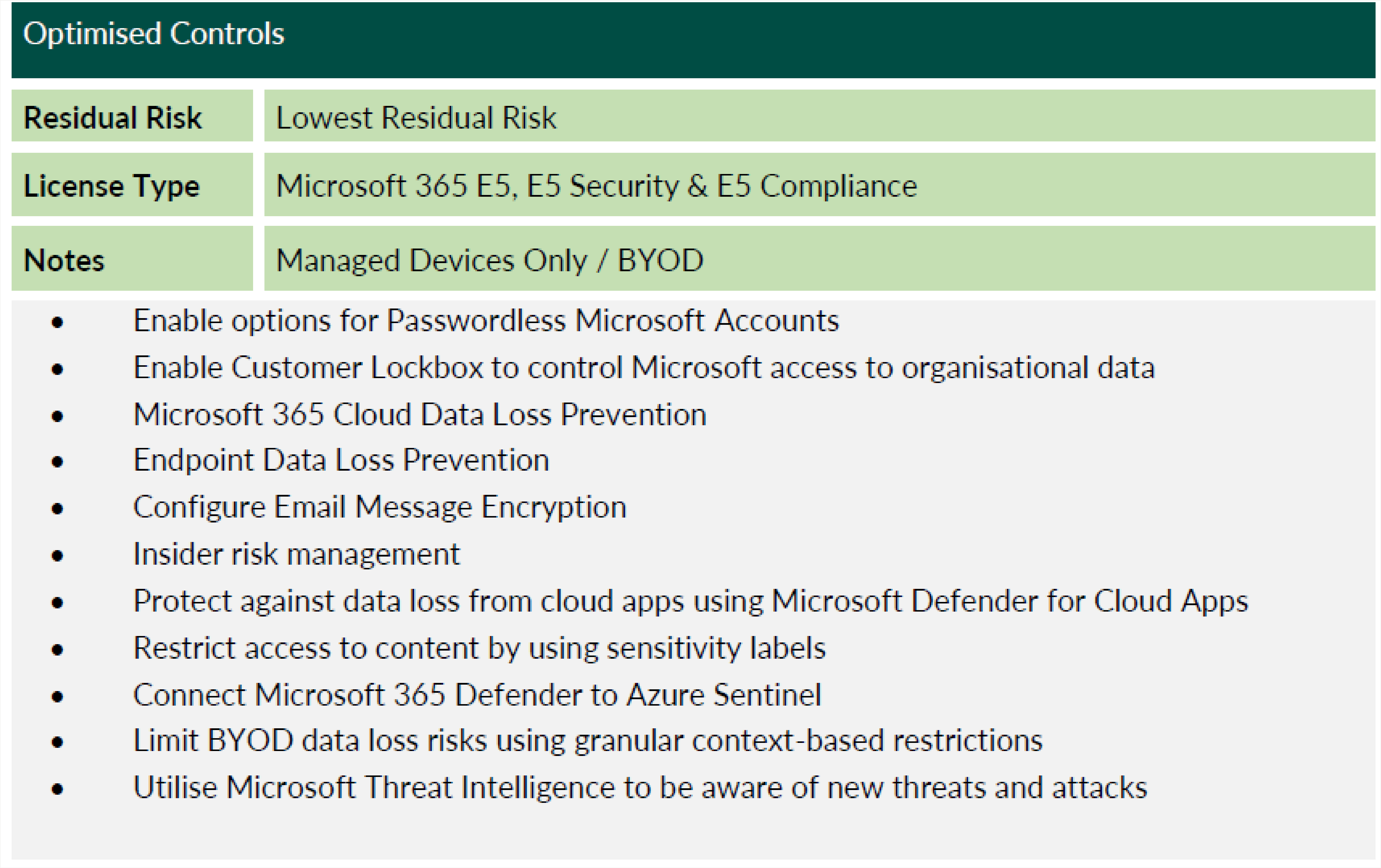
- Enhance Conditional Access
- Use Cloud Compliance Checks
- Implement Cloud Authentication
- Enable Client Rules Forwarding Block
- Do not allow anonymous calendar sharing
- Secure external mail flow
- Secure inbound email by configuring mail flow rules (transport rules) for malicious files
- Configure anti - malware protection in your tenant
- Utilise Microsoft Teams External Access (Federation) to configure external meetings
- Invite external users to Teams using Microsoft Teams Guest Access
- Allow SharePoint users to invite and share with new and existing Guests
- Enable Microsoft 365 Cloud App Consent for Data Access
- Intune Basic Mobile Device Management Controls

Control Levels

Advanced Controls	
Residual Risk	Second Lowest Residual Risk
License Type	Microsoft 365 E3 and Azure Active Directory Premium (AAD) P1 and P2 (For Administrative Accounts) or Microsoft 365 E5 and E5 Security
Notes	Managed Devices Only / BYOD

- Security Azure AD Identity Protection
- Monitor user accounts for suspicious activity
- Azure AD Privileged Identity Management access reviews for privileged roles
- Azure AD Entitlement Management
- Enhance External Mail Flow
- Configure Microsoft 365 Advanced Threat Protection Safe Attachments feature
- Configure Microsoft 365 Advanced Threat Protection Safe Links feature
- Microsoft Purview Information Protection Labelling / Visible marking
- Perform a simulated Attack campaign
- Advanced Intune Endpoint Reporting
- Intune Advanced MAM/MDM rules
- Advanced Privileged Access Controls
- Advanced Teams Security Configuration
- Enhanced SharePoint Controls

Control Levels



Optimised Controls	
Residual Risk	Lowest Residual Risk
License Type	Microsoft 365 E5, E5 Security & E5 Compliance
Notes	Managed Devices Only / BYOD

- Enable options for Passwordless Microsoft Accounts
- Enable Customer Lockbox to control Microsoft access to organisational data
- Microsoft 365 Cloud Data Loss Prevention
- Endpoint Data Loss Prevention
- Configure Email Message Encryption
- Insider risk management
- Protect against data loss from cloud apps using Microsoft Defender for Cloud Apps
- Restrict access to content by using sensitivity labels
- Connect Microsoft 365 Defender to Azure Sentinel
- Limit BYOD data loss risks using granular context-based restrictions
- Utilise Microsoft Threat Intelligence to be aware of new threats and attacks

Questions?

Information Classification: Unclassified

PRIVACYENGINE

Thank You!

Visit: https://www.privacyengine.io/services/
Email: nollag.conneely@privacyengine.io

Nollag Conneely
Head of Consulting
Consultancy | PrivacyEngine

www.privacyengine.io

High Performer EMEA WINTER 2024

Best Support WINTER 2024

High Performer WINTER 2024

Best Meets Requirements WINTER 2024

Momentum Leader WINTER 2024

Fastest Implementation WINTER 2024

Easiest To Do Business With WINTER 2024

High Performer Europe WINTER 2024

Information Classification: Unclassified