fordway.com

Service Description

Microsoft 365 Management and Security

Contents

Why you need this?

The Microsoft 365 suite provides comprehensive tools and capabilities, whether you have subscribed for the E3 or E5 licence.

Fordway offer a comprehensive range of services to assist organisations make best use of and manage their Microsoft 365 (M365) Enterprise subscription. As an organisation, it is essential to make effective use of the licences you subscribe for, and to ensure that you have not purchased licences from various vendors that provide the same capability.

M365 is Microsoft's combined suite of products, comprising Windows 11 Enterprise (allowing downgrade rights to Windows 10), Office 365, and Enterprise Mobility and Security. Enterprise licences are E3, E5, F3/F5 (for frontline workers) plus A3/A5 for Education and N3 for the NHS. Smaller organisations under 300 staff can use M365 Business Standard and Business Premium; Business Premium offers comparable capabilities to the E3 licence.

All M365 subscriptions offer considerable capability, but when you subscribe you simply receive the capability.

To provide an effective service for your organisation each of the tools in the subscription needs to be correctly implemented, configured and managed. The key to gaining benefit from it is to understand and use the components to simplify your environment, retiring other products to create savings; implementing the chosen elements correctly to maximise utility; and manage the capabilities to improve productivity whilst securing and protecting your services.

Fordway's Microsoft 365 Management and Security delivers the 24 x 7 capability your organisation needs to realise the full value of your Microsoft 365 subscription.

01 Fordway's Services for M365 Enterprise

Fordway offer a range of services for Microsoft 365, dependent on your current or planned M365 subscription.

Fordway M365 Managed Desktop

This service is for customers with Business Premium, E3 and E5 subscriptions (plus A3/A5, N3 and F5) and provides a managed Windows 10/11 desktop or laptop/convertible using MS Intune integrated into Microsoft Endpoint Manager to manage the device, allowing non-domain joined management.

The service provides full warranty management including hardware break/fix and optional advance hardware replacement using the vendor supplied warranty or extended warranty service. It also provides and installs device, OS, security and application updates to the device. It includes PatchMyPC, which integrates automatically patches and updates over 450 common third party applications from a range of vendors including Adobe, Apple, Cisco, Citrix, Google, Mozilla, Oracle and Tableau.

Fordway M365 Managed Desktop provides the following:

• Patching services through Microsoft Endpoint Configuration Manager using Intune delivery

• Fordway configure the following on managed devices: device enrolment, device and user profiles, base applications to be installed, application protection policies, security settings and enrolment restrictions

• Device build, deployment and reimaging service using Microsoft Autopilot

• Device security configured through Windows Information Protection and BitLocker

• Malware protection enabled through Microsoft Defender for Endpoint Plan 1

• Exchange Online Protection configuration

• Set up and manage Multi Factor Authentication for secure login using Microsoft's MFA solution using MS Authenticator

• Assigned Customer Success Manager providing Account Management

• Azure AD Conditional Access configuration and management to support the service

• Automated 3rd Party Application deployment, management and patching using PatchMyPC

• Secure Remote access using Direct Access or Customer specified VPN solution

• CSP Billing Management where Fordway provide the licensing subscription

• Microsoft 365 Tenant Management including a monthly review of the Secure Score for the Microsoft 365 tenant

As an option, for a small additional monthly charge customers can add M365 Mobile Device Management for Android and iOS mobile phones and Tablets which uses the same Intune service as is used for the Windows device management. This provides the following:

• Option for either fully managed corporate device or demarcation configured on device for separation of corporate Work profile and personal profile

• Deployment, update and management of corporate applications on device

• Deployment, update and management of device security management

• Conditional Access policies applied to Work Profile

• Complete separation on device, no corporate visibility of personal data

• Consolidated dashboard and reporting with other end user devices

The following are not included in the service but can be added at additional cost:

• A Service Delivery Manager

• Access to Fordway's Service Desk for End User and Level 1, 2 and 3 support

• Azure Tenancy Management

• Active Directory Management - this is provided through our Identity Management service

• Advanced security services using Microsoft EDR capabilities. Whilst we update licenced endpoint protection and anti-malware applications on the device, Fordway M365 Managed Desktop does not include active security monitoring, for this you need either our M365 Secure or Secure Plus Desktop service.

• Active Directory Management - this is provided through our Identity Management service

• Advanced security services using Microsoft EDR capabilities. Whilst we update licenced endpoint protection and anti-malware applications on the device, Fordway M365 Managed Desktop does not include active security monitoring, for this you need either our M365 Secure or Secure Plus Desktop service.

Fordway M365 Secure Desktop for E3/Business Premium

Fordway's M365 Secure Desktop service for M365 E3 and related A3/N3 subscriptions plus Business Premium for SMEs enhances the Managed Desktop service by adding Service Management, 24 x 7 Security monitoring and alerting into the Defender Portal from the included Defender components in the E3/Business Premium subscription with qualifying event response, plus End User support provided through Fordway's Service Desk.

M365 Service Management provides:

• Assigned Fordway Service Delivery Manager

• Customer specific Service Charter and Service Improvement Plan

• Monthly service reports plus scheduled Service Review

• M365 Tenancy review including cost optimisation and best practice recommendations

• Single point of contact for escalation

• Monthly reports

M365 Secure Desktop monitoring takes events and alerts from the following M365 E3 products reporting into Fordway's 24 x 7 Security Operations Centre who will respond in event of notifiable security events using the Defender console and alerts:

• Defender for Endpoint Plan 1

• Defender Firewall

• Defender Exploit Guard

• Defender Credential Guard

•Defender for Office 365 Plan 1

M365 End User Support extends the M365 Service management by providing first, second- and third-line support for Fordway M365 Secure Desktop users through Fordway's Customer Portal as well as the M365 Tenancy management. It provides 24 x 7 support for Priority 1 incidents and qualifying Security incidents, with extended working hours support (7.00am to 7.00pm weekdays excluding statutory holidays) for Priority 2, 3 and 4 incidents, plus the following:

• M365 user adds, deletes, moves and changes

• Service Request fulfilment and management

• Azure AD Identity Management updates and changes for M365 Secure Desktop users

• Service Onboarding and Relationship management via Service Delivery Manager

• Dashboards and reporting

Please note Fordway's Secure Desktop does not include Microsoft Log Analytics and Sentinel included in the service, this is available at additional cost and will require the customer to add a Log Analytics and Sentinel subscription to their existing Microsoft subscriptions.

Fordway M365 Secure Plus Desktop for E5 (or E3 plus E5 Security)

Fordway's M365 Secure Plus Desktop for E5 provides the highest level of security available from using the M365 suite. In addition to full management and support of the endpoint, detailed in the M365 Managed and Secure Desktop services, it provides comprehensive security monitoring and management that meets the NCSC's Best security certification against their Blueprint. End user devices are monitored, supported and secured 24 x 7 by Fordway's manned 24 x 7 Security Operations Centre.

Events are imported into a customer specific MS Log Analytics environment, processed and analysed by Microsoft Sentinel for real time reporting and alerting. This predictive analysis and alerting ensures that any suspicious security event is analysed, triaged and acted upon where required within minutes. Ongoing compliance is reviewed through Microsoft Secure Score.

Fordway's M365 Secure Plus desktop provides the following monitoring and analysis. Fordway will Monitor, investigate, contain and resolve threat management incidents:

Defender for Office 365 Plan 2:

- Suspicious email sending patterns
- Email messages containing malware removed after delivery
- Malware campaigns detected and blocked
- Email reported by a user as malware or phishing
- Quarterly Phishing Campaigns, with the ability to direct users to follow-up training and guidance material
- Quarterly review of Advanced Anti-Phishing policy
- Incident Analyses
- Provide Threat Tracking Reports

Defender for Endpoint Plan 2:

- Malware detection for zero-day threats
- Manage and leverage the integration between Defender for Endpoint, Defender for Cloud Apps, Defender for Identity and Defender for Office 365
- Use software inventories to assist with prioritising unmanaged software patching
- Leverage Intune integration to provide security baseline and hardening recommendations

Defender for Cloud Apps:

- Cloud Security Posture Management for access to SaaS services
- Access and authentication management for SaaS providers
- Secure scanning of data transfer into and out of SaaS
- Setup and manage alerts

Defender for Identity:

- Audit and reporting of user behaviour and activities
- Protect user identities
- Identify suspicious activities and advanced attacks across the cyber-attack kill-chain
- Perform reconnaissance to identify rogue activity
- Identify compromised credential information post attacks
- Report on lateral movements within the network
- Suspicious activity alerting and investigation

Microsoft Defender for Cloud is a Cloud Security Posture Management (CSPM) and Cloud Workload Protection (CWP) solution. Features include:

- Find weak spots in cloud configurations
- Strengthen security posture
- Protect workload across multi-cloud and hybrid environments
- Manage compliance

Microsoft Sentinel and Log Analytics are included in the service price, collectively they provide Security Information Event Management (SIEM), unified management including alerts from all the Defender products, to provide comprehensive alert detection, threat visibility, proactive hunting, and threat response:

- Data aggregation from Azure Security Centre, Defender for Cloud Apps, Defender for Endpoint, Defender for Identity and Defender for Office 365
- Create default alerts determined by data sources collected
- Provide input into Microsoft Secure Score and proposed remediation plans
- Review of top 5 behavioural activities each week
- Deeper insight into alerts and suggested response or remediation
- The ability to cross-reference information to build timeline of activity
- Customer specific reports and analysis using Kusto query language to interrogate Log Analytics

Where non-Microsoft 365 logs and events are analysed by Sentinel as part of the service this is charged in addition – please see Fordway's Cloud Security Management for service details and costs.

NCSC Service Alignment

Fordway's Secure Desktop and Secure Plus Desktop services are aligned to the National Cyber Security Centre Blueprint for Secure Configuration Alignment for M365. Our Secure Desktop offering meeting the NCSC certified Good controls, our Secure Plus Desktop meets NCSC Certified Best controls.

Good Controls	Better Controls	Best Controls
Highest Residual Risk	Lower Residual Risk	Lowest Residual Risk
M365 E3	M365 E3 + SCP or M365 E3 + E5 Security	M365 E5 or M365 E3 + E5 Security & E5 Compliance
• Enable audit logging • Enable mailbox auditing • Use Secure Score • Implement Cloud authentication • Enable MFA • Implement Conditional Access • Control access to managed devices • Block legacy authentication • Do not expire passwords • Disable accounts not used in last 30 days • Use dedicated accounts to perform Administrative Tasks • Configure Microsoft 365 Global Administrator role members • Use non-global admin accounts to perform O365 administrative tasks • Configure break glass accounts in Azure AD • Enforce MFA for all Global Admins • Enable Client Rules Forwarding Block • Do not allow anonymous calendar sharing • Configure Transport rule for ransomware • Configure anti-malware protection in your tenant • Secure external mail flow • Microsoft Teams External Access (Federation) • Microsoft Teams Guest Access • Allow SharePoint users to invite and share with new and Existing Guests • Configure data loss prevention (DLP) • Enable Office 365 Cloud App Security • Application Consent for Data Access	• Azure AD Identity Protection • Monitor user accounts for suspicious activity • Azure AD Privileged Identity Management • Schedule access reviews for privileged roles • Azure AD Entitlement Management • Configure Office 365 Advanced Threat Protection Safe Attachments feature • Configure Office 365 Advanced Threat Protection Safe Links feature • Azure Information protection - Labelling/Visible marking • Perform a simulated Attack campaign • Connect Microsoft Defender for Office to Azure Sentinel	• Enable Customer Lockbox to control Microsoft's access to organisational data. • Insider risk management • Endpoint Data Loss Protection • Extend data loss prevention to Teams chat and channel messages • Protect against data loss from cloud apps using Microsoft Cloud App Security • Restrict access to content by using sensitivity labels
Privileged Administration		
Zero Trust Security, Azure AD mastered administration accounts, Devices managed for Microsoft 365		

02 How can Fordway help?

Fordway's Microsoft 365 Security and Management uses our 30 years' experience of delivering tailored solutions, to operate and manage components that organisations, simply don't have the time or resources to devote to themselves.

Each solution is bespoke to an organisation to ensure all their unique challenges are met. Fordway have extensive knowledge of the Microsoft products and can assist any business unlock the full potential of what has been purchased. Our in-house expertise and existing service desk capabilities, positions Fordway well to meet the operational challenges for other organisations.

For any/all of the components above Fordway strategy, business and technical consultants will work with the organisation to:

- Understand the capabilities pertaining to the business
- Produce analysis recommending additional tool implementation
- Configure new toolsets including management
- Migrate any systems or devices to use the new toolset
- Provide operational monitoring and management as required

03 Key Benefits

- **Comprehensive Operational Capabilities –** Fordway have been operating and managing multi-cloud solutions for many years
- **Get the best from M365 –** Enable the full cost benefits of using the entire suite of products available.
- **Secure and Secure Plus Desktops –** Ability to deliver secure desktop solutions up to OFFICIAL with additional controls in place to meet OFFICIAL-SENSITIVE
- **Certified staff –** all staff are BPSS checked with key technical, operational and commercial staff SC cleared and vetted
- **Independent –** Fordway will provide independent feedback on the benefits and limitations of the M365 product set against other products.
- **Experienced Personnel –** From business, project management and technical viewpoint, Fordway have multi-years of experience of real-world deployments and operational requirements
- **Licence Assessment –** Fordway will perform a detailed analysis against the licences held and where real benefits can be gained
- **Collaboration –** Fordway's personnel will work alongside your IT staff and any third parties collaboratively, as each has skills necessary.
- **Detailed Knowledge of Management Tools –** Fordway have extensive knowledge of the Microsoft management tools, including Lighthouse, Sentinel, Monitor and Arc. These can be configured to deliver the necessary statistics and dashboard for each organisation.

04 Service Onboarding

The service onboarding is a professional services engagement. The following procedure will be used to commence the service:

- Understand the work requirements
- Sign Non-Disclosure Agreements
- Provide a combination of Project Manager, consultants and engineers relevant for the work profile
- Review the customer requirements and determine the contractual requirements
- Agree the scope of the engagement with the customer and provide a Project Initiation Document which will define the engagement.
- Schedule work
- Commence engagement
- Provide deliverables
- Complete engagement

Suitable resources are likely to be required from the customer and potentially third-party organisations to initiate the service, working alongside Fordway staff. The actual roles and responsibilities will be finalised and agreed in the Project Initiation Document.

Service Levels

As the service is hosted and run from Microsoft 365, the service levels will be defined by the underlying Microsoft SLAs for M365.

Service Management

Service Management is provided as part of the Secure and Secure Plus versions of the service. Customers will have an assigned Service Delivery Manager, access to Fordway's Customer Portal for service incidents and request management, plus monthly service reports and scheduled service reviews. All service is delivered to ISO20000 and aligned to the ITIL best practice framework.

Service Connectivity

The Service is Internet based, the customer will need suitable capacity and quality Internet connectivity to allow access to M365.

Change Management

All changes will be delivered through the Change Management process defined and configured in Fordway's Customer Portal. The process and toolset can interface with the customers Change Management processes.

Data Migration

Where data migration is required, this can either be done as a chargeable element of the service onboarding by Fordway or undertaken by the customer as part of their responsibilities.

Backup and Restore

M365 does not include data backup. We recommend customers take Fordway's Backup Service for Microsoft 365 to provide a M365 independent backup and recovery service for their M365 files and data.

05 Ordering

Fordway services can be ordered by contacting your Fordway account manager or other members of our team on **01483 528200**, emailing **sales@fordway.com** or using the contact form on **www.fordway.com**.

Our Accreditations

ISO 9001
ISO 14001
ISO 27017
ISO 27018
ISO 20000
ISO 27001

Cyber Essentials Plus

PSN Public Services Network

HSCN Health & Social Care Network Compliant

Microsoft Partner
Microsoft
Gold Cloud Productivity
Gold Cloud Platform
Gold Datacenter
Silver Security
Silver Small and Midmarket Cloud Solutions

FORDWAY

Fordway Solutions Ltd,
Charterhouse Suite Ground Floor
Mill Pool House, Godalming
Surrey, GU7 1EY