FORDWAY

fordway.com
Feb 2024

## Service Description

# Complete Cloud Security Management

Microsoft Solutions Partner
Infrastructure
Azure

## Why do you need this?

Fordway's Complete Cloud Security ensures your organisations' security capability meets Cyber Essentials.

With optional external audits to meet Cyber Essentials PLUS, it aligns your security practices with CIS Controls to implement and manage effective security, and provides manned 24 x 7 security monitoring across your entire estate, with event correlation and management, incident response, containment and remediation where required.

## Contents



## 01 Why you need this?...continued

Fordway's Complete Cloud Security ensures any mid to large organisation will have comprehensive security in place, making best use of your Microsoft 365 subscription plus Azure's security capabilities and all third party security tools you have in place. The service has three steps; understand your requirements and help you articulate them at board level; implement the required improvements; ensure comprehensive 24 x 7 security monitoring, event analysis and incident response where needed. It includes an optional vCISO (virtual Chief Information Security Officer) to ensure the smooth running of the service and its continued compliance and protection against new threats and vulnerabilities as your business evolves.

## 02 What is cyber essentials?

Cyber Essentials is a UK government endorsed initiative operated by the NCSC National Cyber Security Centre. It describes 5 key technical controls that organisations should put in place to help prevent cybercrime and is designed to be simple and easy to operate for businesses.

- Boundary firewalls & Internet gateways
- Secure configuration
- Access control
- Malware protection
- Patch management

## 03 What are CIS Controls?

The Centre for Internet Security (CIS) Critical Security Controls are a set of 20 recommended actions that provide specific and actionable ways to stop many of today's most pervasive and dangerous cyber-attacks.

The principal benefit of these controls is that they focus on and prioritise a small number of actions that provide the highest payoffs for security. These controls are based around 5 groups that describe their function rather than their technology:

Identify – the assets which need protection

Protect – the identified assets

Detect – threats in real time

Respond – stopping breaches & limit damage

Recover – repairing damage & bring business back online

# 04 Cyber essentials, CIS Controls & Security Service alignment

| Cyber Essentials Control | CIS Function | CIS Category | CIS Control | Fordway Security Service |
|---|---|---|---|---|
| | Identify | Asset Management | Hardware Inventory<br>Software Inventory | Phase 1 |
| | | Business Environment | | Phase 1/vCISO |
| | | Governance | | Phase 1/vCISO |
| | | Risk Assessment | Secure H/W & S/W Configuration | Phases 1 & 2 |
| | | Risk Management Strategy | | Phase 1/vCISO |
| | | Supply Chain Risk Management | | Phase 2/vCISO |
| Boundary Firewalls & Internet Gateways<br>Secure Configuration<br>Access Control | Protect | Identity Management, Authentication & Access Control | Continuous Vulnerability Assessment & Remediation<br>Network Access Control<br>Secure Network Infrastructure Configuration<br>Boundary Defence<br>Data Protection<br>Access Control – Need to Know<br>Account Monitoring & Control | Phase 2 |
| | | Awareness Training | Continuous Vulnerability Assessment & Remediation<br>Security Skills Assessment & Training (Fordway) | Phase 2 |
| | | Data Security | Hardware Inventory<br>Software Inventory<br>Data Protection<br>Controlled Access – Need to Know<br>Application Security | Phase 2 |
| | | Information Protection Process & Procedure | Secure H/W & S/W Configuration<br>Administrator Privilege Control<br>Email & Web Protection<br>Data Recovery Capability<br>Secure Network Infrastructure Configuration | Phase 2 |
| Patch Management | | Maintenance | Continuous Vulnerability Assessment & Remediation<br>Boundary Defence | Phase 2 |
| | | Protective Technology | Continuous Vulnerability Assessment & Remediation<br>Maintenance, Monitoring, & Analysis<br>Secure Network Infrastructure<br>Data Protection<br>Controlled Access – Need to Know<br>Account Monitoring & Control | Phase 2 |
| | Detect | Anomalies & Events | Maintenance Monitoring & Analysis<br>Network Access Control<br>Boundary Defence<br>Incident Response & Management | Phase 2 |
| Malware Protection | | Secure Continuous Monitoring | Secure H/W & S/W Configuration<br>Malware Defences<br>Incident Management & Response | Phase 2/vCISO |
| | | Detection Processes | Maintenance Monitoring & Analysis | Phase 2 |
| | Respond | Response Planning | Incident Management & Response | Phase 3 |
| | | Communications | Incident Management & Response | Phase 3 |
| | | Analysis | Secure H/W & S/W Configuration<br>Incident Response & Management | Phase 3 |
| | | Mitigation | Secure H/W & S/W Configuration<br>Incident Response & Management | Phase 3 |
| | | Improvement | Incident Response & Management | Phase 3 |
| | Recover | Recover Planning | Incident Response & Management | Phase 3 |
| | | Improvements | Incident Response & Management | Phase 3 |
| | | Communications | Incident Response & Management | Phase 3 |
| | | | Penetration Testing & Vulnerability Scanning | Phase 2 – Optional |

- vCISO – Adds an extra layer of human interaction working on your behalf to articulate cyber risk
- Manage Continual Security Improvement Process
- Present reports and be a single point of contact for security related concerns both inside Fordway and your organisation
- Leads any security incident remediation and recovery
- An option on Phase 2 Complete Cloud Security
- Penetration Testing – Fordway provides vulnerability scanning as part of the Complete Cloud Security service. Optional independent Penetration testing can be organised on a quarterly, bi-annually, or annual basis through the vCISO.

## 05 Complete Cloud Security approach

Based around the 20 CIS controls Fordway's Complete Cloud Security service is consumed in 3 steps, leveraging Microsoft's M365 and Azure licences and security capabilities plus associated 3rd party products to ensure a comprehensive security package can be built around your specific requirements.

**Service Consumption**:

There are three stages in the lifecycle of a security program. First, understanding and testing the current environment and undertaking a risk analysis to identify what improvements are needed and where; secondly, remediation of any identified vulnerabilities and implementation of enhanced capabilities, processes and security tools to ensure complete security coverage. Thirdly, implementation of 24 x 7 monitoring, reporting and analysis to identify ongoing security issues with continual improvement of your security posture and processes. Each of these three elements can be purchased separately or in isolation but the most effective method is to commit to the complete service.

**Phase 1: Cloud Security Baseline – please see separate Service Description for greater detail**

- Discovery & Inventory of hardware & software assets
- Business Environment Assessment
- Security & Risk Governance Assessment
- Overall Risk Assessment
- Risk Assessment Report
- Security scan and 3rd party penetration test

**Phase 2: Cloud Security Improvement**

- Phase 1 Cloud Security Baseline is a prerequisite of Phase 2
- Fordway will design, implement and configure the tools, processes and reports needed to implement CIS CSS controls appropriate to your organisation from the table above
- We will help implement continuous monitoring and improvement of your security posture through real-time event analysis and security incident reporting via Azure Log Analytics data collection and Azure Sentinel analysis and dashboard for historical events & real time updates
- Monthly reporting of security compliance, incidents, threats and risks

- Can include optional virtual CISO to run day to day security tasks

**Phase 3: Cloud Security Management**

- Managed Security Operations Centre (SOC) providing ongoing 24 x 7 security monitoring, threat analytics, event analysis with security incident response, containment and optional remediation service
- Virtual CISO/Security Incident Manager to oversee
- Communications
- Threat removal & mitigation
- Recovery and return to BAU

# 06 What Complete Cloud Security provides

Fordway's Complete Cloud Security uses Microsoft 365 Business Premium, E3 and ideally E5/E5 Security add on licences, together with Azure and 3rd party security features, and requires an Azure Sentinel and Azure Log Analytics subscription.

It can cover your whole IT estate from the user, their desktop and browsing habits, email security to Azure services, and on premises services, hybrid, or legacy systems.

# 06

Fordway's Complete Security Service provides Cyber Essentials review and remediation services that bridge the requirements with CIS (Centre for Internet Security) controls and aligns the business needs with other regulation and standards such as GDPR and ISO27001 where value can be realised. Fordway have a range of services based around providing complete security across the entire breadth of solutions any organisation may have. There are four elements that

Fordway's Complete Cloud Security assists with:

- Managed Security for Microsoft 365
- Managed Security for Microsoft Azure
- Managed Security for On-premise environments
- Managed Security for non-Microsoft cloud services and products

Fordway have detailed understanding of IT security founded on over 30 years of knowledge and experience securing IT infrastructure. Fordway have a dedicated security team, who can provide independent and validated security advice and application recommendations, for all business types. From simple commercial requirements to complex governmental security for CIS and Cyber essentials plus.

Fordway's Complete Cloud Security provides 24 x 7 x 365 monitoring, analysis and response services for the following:

**M365 Defender for Endpoint (Plan 2)**

Fordway will monitor, investigate, contain, and resolve incidents identified by Defender for Endpoint including:

- 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

**M365 Defender for Office 365**

Fordway will monitor, investigate, contain, and resolve incidents in the Office 365 environment categorised as threat Management that includes:

- 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.

06

- Quarterly review of Advanced Anti-Phishing policy
- Incident Analyses
- Provide Threat Tracking Reports

**Microsoft Defender for Identity**

Fordway will setup, monitor and manage your Defender for Identity environment providing:

- 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 Apps**

This is a fully featured Cloud Access Security Broker, providing control and management of access to SaaS services and other Web applications, inspection of data transferred between cloud services and security analytics including web ser vice whitelisting and blacklisting. Fordway will setup and assess the usage of your cloud apps against approved cloud services, preventing data leaks to non-compliant apps and limit access to unauthorised services.

For the above-mentioned services Fordway will:

- Setup and manage alerts
- Provide a monthly report on cloud app usage including MS risky application scoring
- Review user and endpoint compliance against Microsoft Secure Score and assist with remediation where applicable and appropriate
- Customer alerting for all services once an approved list agreed
- Monthly Report of all users who have cloud app integrations setup
- Reporting on who has authorised access to your Office 365 tenant
- Where applicable, review and respond to Azure Sentinel analytics for M365 services and security

06

**Azure Advanced Security Service**

For Azure Security we provide the following:

- We will monitor alerts raised in the ASC/Sentinel portal
- Agreed alerts will be sent to our 24x7 monitoring team to be actioned
- Monthly review of Security Score
- Management of Security Policies
- Management of Azure Defender alerts - 5 maximum
- Workflow automation
- Integration with Azure Monitor
- Optional Kusto (KQL) script development and customised reporting

**Defender products reporting into Azure Sentinel**

- Microsoft Defender for Cloud
- Azure Defender for Identity
- Azure Defender for Servers
- Azure Defender for App Service
- Azure Defender for Storage
- Azure Defender for SQL
- Azure Defender for Kubernetes
- Azure Defender for container registries
- Azure Defender for Key Vault
- Azure Defender for Resource Manager
- Azure Defender for DNS
- Azure Defender for open-source relational databases

**Office 365 Cloud App Security**

Fordway will setup and assess the usage of your cloud apps against approved cloud services, preventing data leaks to non-compliant apps and limit access to unauthorised services.

Fordway will:

- Setup and manage alerts
- Provide a monthly report on cloud app usage including MS risky application scoring
- Customer alerting for all services once an approved list agreed
- Monthly Report of all users who have cloud app integrations setup
- Reporting on who has authorised access to your Office 365 tenant

06

### Microsoft Azure Sentinel analysis

Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) solution that enables security analytics across your IT landscape. Fordway will integrate Azure Security Centre, Defender consoles and Microsoft 365 Security Centre into the Sentinel service, enabling Fordway to deliver a unified security management service that will further enhance the ability to provide comprehensive alert detection, threat visibility, proactive hunting, and threat response.

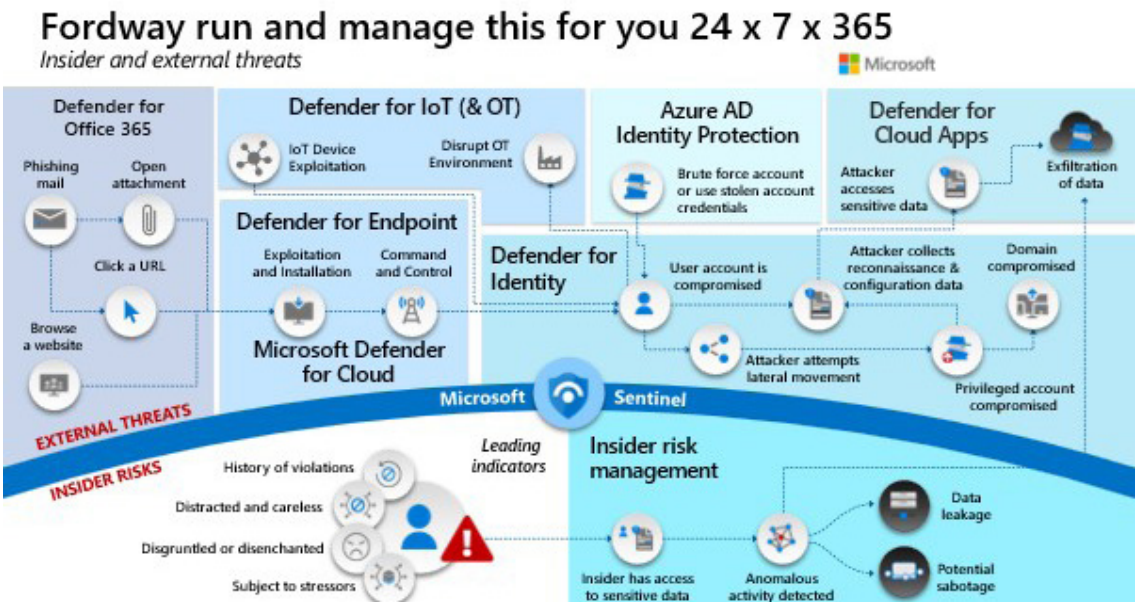
The service includes:

- Data aggregation from Azure Security Centre and all associated Defender products reporting into it, Defender for Cloud Apps, Defender for Endpoint, Defender for Identity and Defender for Office 365
- Upload of data from syslog servers for on premise and 3rd party services, plus implementation and configuration of vendor specific Azure Sentinel connectors where available
- Create default alerts determined by data sources collected
- Review of top 5 behavioural activities in week
- Deeper insight into alerts
- The ability to cross-reference information to build timeline of activity

### Microsoft Log Analytics

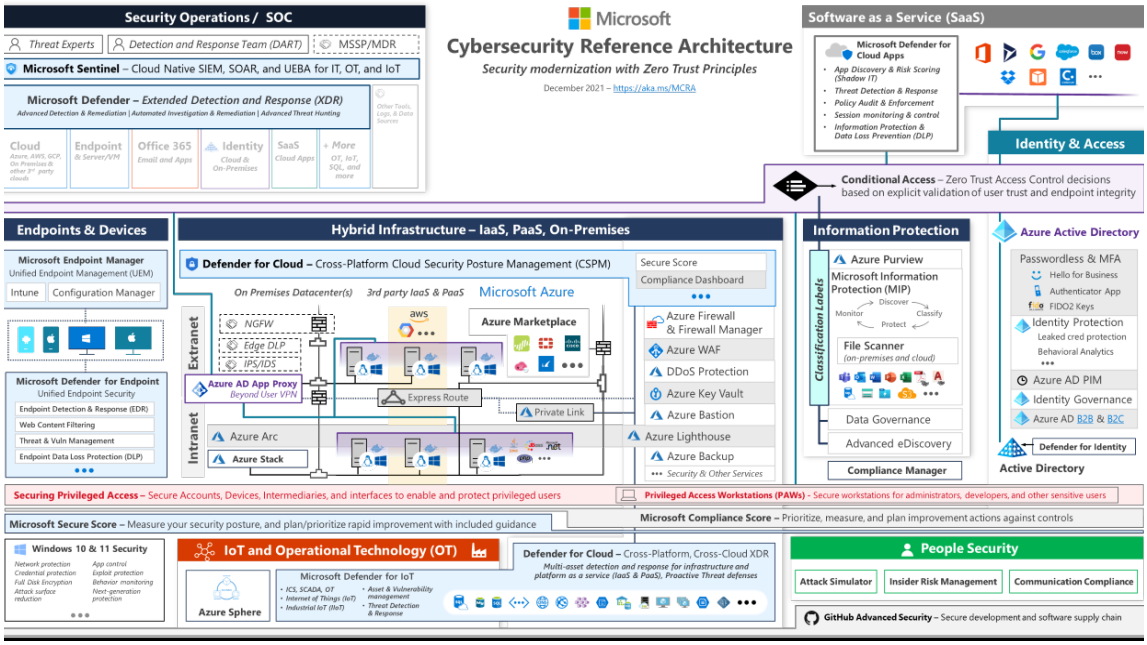
All events for all monitored elements, including on premise equipment and other providers which can forward events, plus Syslog servers from on premise environments and other cloud services, are ingested into a customer specific Log Analytics workspace. Using the Kusto query language customer specific queries and reports can be run, analysed and provided. All logs are then processed and forwarded into Azure Sentinel and Microsoft Secure Score, with output reviewed and shared with the client.  Any recommended enhancement or remediation actions are discussed, agreed and scheduled.

### Fordway Complete Cloud Security – Service Coverage Diagram



## 06

The tools form core components of the overall Microsoft Cyber Security Reference Architecture, shown below.




## 07

# Key Benefits

- **End to end organisation security –** Use the Fordway expertise and knowledge of providing comprehensive, tailored security solutions, to enhance security and protection
- **Proactive Implementation –** Fordway's knowledge can turn reactive, knee jerk reactions to security breaches, into a proactive, automated, policy and risk-based response that ensures all threats are dealt with in a professional manner
- **Independent –** Fordway will provide independent feedback on the benefits and limitations of Security platforms and align with other products if necessary.
- **Experienced Personnel –** From business, project management and technical viewpoint, Fordway have multi-years of experience of real-world deployments and operational requirements
- **Comprehensive Security Assessment –** Fordway will perform a detailed analysis against the existing security measures and portfolio 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 Security Management Tools –** Fordway have extensive knowledge of the Defender and Sentinel tools, also how to integrate them with other complimentary Microsoft products, including Lighthouse, Monitor and Arc. These can be configured to deliver the necessary statistics and dashboard for each organisation.
- **Understand Legacy –** Fordway know companies have legacy systems with potential integrations that cannot just be ignored
- **Clear Recommendations –** Fordway will produce a set of costed recommendations on how to get the best security solution out of the licences held and how to migrate any systems over.

# 08 Key Features of Fordway's Approach

Fordway's approach, is ultimately flexible but the generic steps taken for every engagement are:

- Create and sign off Project Initiation Document
- Review existing security and protection products
- Design new security and compliance capabilities
- Agree on optimisations
- Install and configure
- Migrate from any existing tools
- Monitor and analyse new capabilities
- Create dashboards and reporting
- Operate and manage the environment

The duration and complexity involved in each of the high-level steps listed above is dependent on the nature of the engagement. If needed, full project controls and documentation will be supplied as part of the engagement (Project Manager, RAID, Exception, Highlight logs/reports).

# 09 Service Terms

## Service Initiation (on-boarding)

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

# 09

**Service Levels**

As the service is hosted and run from Microsoft Azure, the service levels will be defined by the underlying Microsoft SLAs for Azure, in line with the resilience configured in the environment.

**Service Management**

Service Management is provided as part 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.

**Financial Recompense**

Fordway offers service credits if the Fordway provided elements of the service do not consistently meet the SLA. Interruption or failure of underlying Azure and M365 infrastructure is covered by Microsoft's Service Credits.

**Service Connectivity**

The Service is Internet based, the customer will need suitable capacity and quality Internet connectivity to allow VPNs to be created to access the Azure resources. The customers Azure tenancy will be managed through Fordway's Azure Lighthouse/Azure Resource Manager tenancy management framework for the duration of the service.

**Trial of Service**

Not applicable to this service, although elements of the transition will be tested and can be implemented as a pilot. These requirements will be determined as part of the Project Initiation Document.

**Data Security**

Fordway is Cyber Essentials Plus accredited. Customer data is managed to ISO27001, 27017 and 27018 certified procedures. All data is stored, processed and managed in Azure. Where applicable Fordway will recommend, implement and operate suitable Azure Backup and Recovery procedures for the environment. Azure costs for these will be charged to the customer's Azure accounts.

**Training**

Fordway will provide skill transfer where applicable and documentation as part of the service onboarding. Formal training and courses can be provided if required.

**Customer Responsibilities**

Fordway will apply data access restrictions and other information security policies as mandated by the customer and required within Fordway's own organisational security controls. The customer is required to provide the necessary resources and information to allow Fordway to achieve the service deliverables as agreed within the Project Initiation Document.

**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**

Where Fordway have the responsibility for maintaining and managing the customer backups, this will be included in the service. Where the customer chooses to manage their own backups, they will be accountable for this function.

# 10 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 Solutions Partner
Infrastructure
Azure

FORDWAY

Charterhouse Suite
Ground Floor
Mill Pool House
Mill Lane
Godalming
Surrey
GU7 1EY