FORDWAY

fordway.com

Service Description

Microsoft Sentinel Managed Service

Gold Microsoft Partner

Contents

01	Microsoft Sentinel	**1-3**
02	What Fordway Provide	**3-7**
03	On premise infrastructure and applications	**9**
04	Other public cloud and SaaS services	**9**
05	About Fordway	**10**
06	Ordering	**10**
07	Our Accreditations	**10**

Microsoft Sentinel

Microsoft Sentinel is Microsoft's SIEM (Security Information Event Management) and SOAR (Security Orchestration Automated Response) solution that is cloud-native, available with your Azure subscription, massively scalable and with integration with almost all known IT security tools.

It delivers organisation-wide threat intelligence and security analytics through a single interface dedicated to event analysis, alert detection, threat visibility with proactive hunting and threat response, containment and remediation.

01

With the advanced SIEM and SOAR capabilities, Microsoft Sentinel plus Fordway's 24 x 7 Security Operations Centre (SOC) to provide round the clock security with a human face to keep every organisation secure against different cyber threats and attacks.

Fordway's 24 x 7 SOC plus Sentinel allows you to:

- **Respond:** with the help of Fordway's proven expertise and depth of resources, our services ensure you maintain security and compliance whilst knowing that you have a team of experts to respond quickly and calmly where needed.
- **Investigate:** Sentinel provides AI capabilities for advanced threat identification and pattern matching, enhanced with optional MS Security Co-pilot, ensuring hunting and investigating suspicious activities and identifying threats at scale is considerably easier and faster.

01

- **Detect:** Sentinel is powered by and learns from Microsoft's global security analytics to recognise threats and minimise false positives using Microsoft's threat intelligence and analytics.
- **Collect:** with Sentinel, collecting data across infrastructure, applications, devices, and users, both on-premises and multiple clouds, analysing and reporting on it is a straightforward process.

02 What Fordway Provide

Using MS Sentinel and MS Log Analytics plus the security tools that your organisation already has implemented, reporting into our 24 x 7 SOC,
Fordway use these to provide comprehensive, end to end security for any sized organisation.

There are **six main areas** that **Fordway's 24 x 7 Security Operations** assist with:

1. Managed security for end users using Microsoft 365
2. Managed security for Microsoft Azure subscriptions
3. Managed security for on-premise environments
4. Managed security for non-Microsoft cloud services and SaaS applications
5. Security incident response and management
6. Security breach containment and remediation

Microsoft Azure Sentinel Analysis

Fordway integrate Azure Security Centre, Microsoft 365 Security Centre, 3rd party devices, tools and syslog servers into the Sentinel service, and provide our 24 x 7 SOC staffed with qualified IT Security experts to investigate, respond and contain or remediate any identified security incident.

The service includes:

- Manned 24 x 7 SOC staffed with qualified IT Security specialists
- Incident response and corrective actions to defined and agreed SLAs

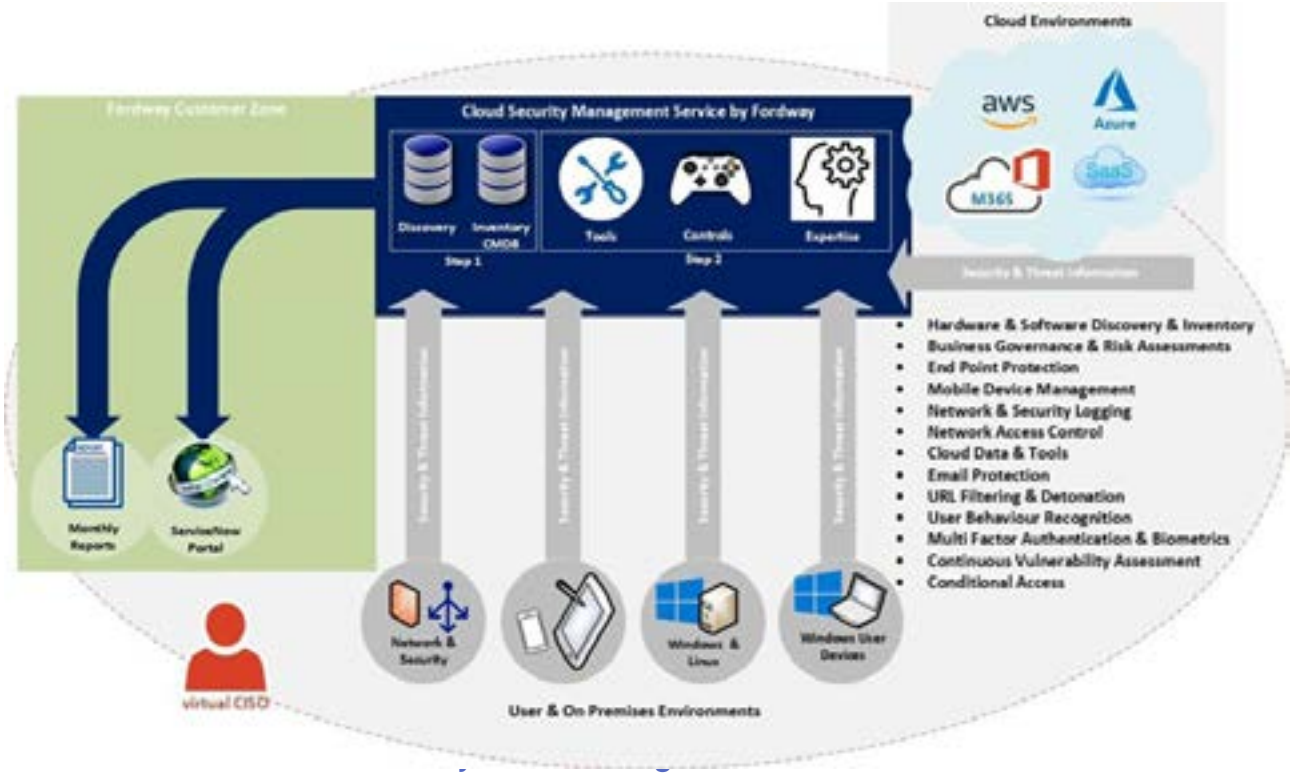
- Data aggregation from Azure Security Centre and all associated Defender products reporting into it, Defender for Cloud Apps, Defender for Endpoint, Defender for Identity and Defender for Office 365.
- Create default alerts determined by data sources collected
- Review of top 5 behavioural activities in week
- Deeper insight into alerts
- The ability to cross-reference information to build timeline of activity for advanced threat hunting and continual service improvement 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 for advanced threat hunting and continual service improvement

Microsoft Log Analytics

Events for all monitored elements, including on premise equipment 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 against the ingested data and analysed. Event 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.



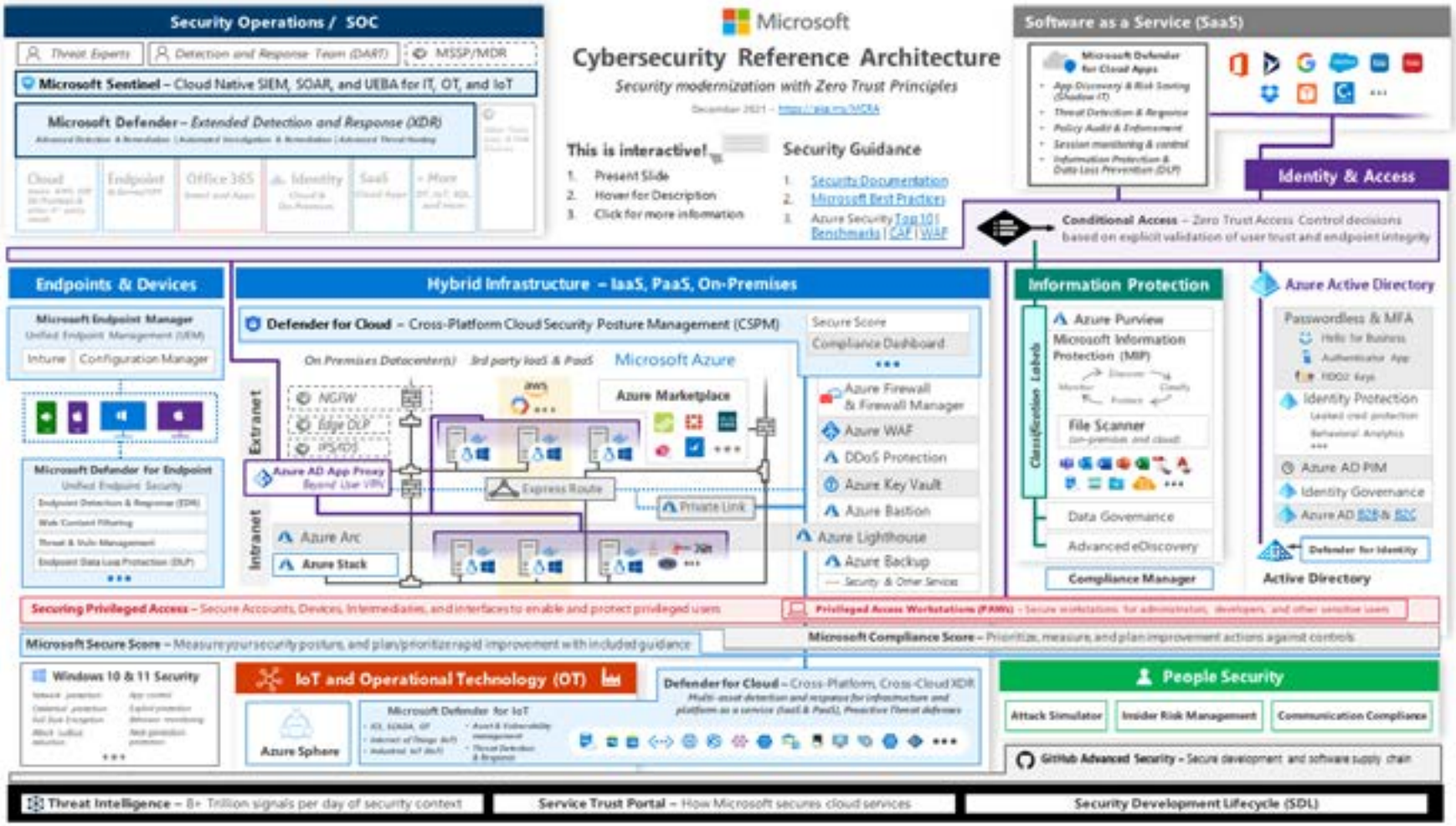
Microsoft have a comprehensive set of security applications, meaning that if an organisation has a Microsoft business licence, there are tools included that can provide comprehensive security and protection controls. The main ones being:

- **Microsoft Sentinel** – SIEM for analysis, alerting and dashboards with SOAR capabilities for automated event response and remediation
- **Microsoft Log Analytics** – event log consolidation, correlation, storage and reporting
- **Microsoft 365 Defender** – security for End Users, identities and applications
- **Microsoft Defender for Azure** – security for servers, storage and core infrastructure
- **Microsoft Defender for Cloud** – Security for Cloud applications and components

These products protect all major cloud and hybrid environments, including Azure, AWS & Google Cloud. Defender XDR (eXtended Detection and Response) is designed to provide integrated,

These products protect all major cloud and hybrid environments, including Azure, AWS & Google Cloud. Defender XDR (eXtended Detection and Response) is designed to provide integrated, intelligent and automated security to any location.

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



02 For each monitored element Fordway provide the following...

M365 Defender for Endpoint

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

M365 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

02

M365 Defender for Cloud Apps

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

Azure Advanced Security Service

Azure Security Centre

- We will monitor alerts raised in the ASC 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

Defender products reporting into Azure Security Centre

- 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

03 On premise infrastructure and applications

Fordway will configure and test native integration of your organisations' existing tools and services with Sentinel where available, with defined event and alerting thresholds. Where native integration is not available system events will be collected by syslog servers, Common Event Forwarding or Rest API integration for correlation and forwarding into the customer specific Log Analytics workspace for Sentinel ingestion and analysis.

04 Other Public Cloud and SaaS Services

Sentinel offers AWS CloudTrail, Google Cloud Monitoring, Oracle Cloud Infrastructure and Salesforce Service Cloud data connectors along with (currently) 135 other vendors and SaaS providers including Cisco, Juniper, Palo Alto, Fortinet and VMware.

Where data connectors exist we will use them, otherwise we will forward events using syslog, Common Event Forwarding or API integration where available to integrate the service and analyse events with Sentinel.

05 About Fordway

Fordway offers over 30 years' experience advising and delivering strategic IT infrastructure and IT service delivery change to complex enterprises.

Fordway's consultancy helps inform your strategy and review the options relevant for your organisation. Our advice will be aligned to your business requirements. We can then assist with the ongoing migrations, operational management and optimisation of the resulting cloud service, based on best practice defined by the ITIL service management framework.

06 Ordering

Fordway's 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

07 Our Accreditations

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

Cyber Essentials Plus

PSN

HSCN Health & Social Care Network Compliant

Microsoft Partner