Service Description

Security Posture Management (SVM)
August 2025

transparity

Contents

1. Service Overview

The Security Posture Management (SPM) service provides ongoing security platform, framework, and organisational process improvements to proactively address future issues and challenges.

Delivered primarily by our expert-level Security Consultants, SPM aims to move your organisation into the anticipatory phase of your cyber security maturity model by combining advanced technology, Threat and Vulnerability Management (TVM), Attack Surface Reduction (ASR), continuous exposure management, and platform enhancements.

Additional information may be included in your Order Form or Statement of Work.

2. Service Features

Feature
Retained Security Consultancy
Continuous Exposure Management
Threat and Vulnerability Management (TVM)
Attack Surface Reduction (ASR)
Platform Enhancements
Attack Simulations
Service Delivery Management
Inclusive Security Advice
Threat Advisories
Security Reporting

2.1 Retained Security Consultancy

- Our security team provides expert-level consultancy to enhance your security posture[1], prioritising improvements within the scheduled, contracted monthly days.
- Our security consultants will work in collaboration with your technical team to provide routine security posture management[2] through any of the below defined activities depending on the contracted monthly days.
- Any other defined security-related activities not defined below, aimed at improving your organisation's security posture.

2.2 Continuous Exposure Management

- Identify cyber security weaknesses
- Apply posture hardening recommendations
- Implementation of security controls towards common security standards
- Asset inventory and management
- Prioritisation of security efforts and investments
- Reporting and insights into security events, recommendations, metrics and security initiatives
- Attack path analysis

[1] Where prerequisite security tooling is in production to be used by our security consultants.
[2] Security posture improvements are managed and implemented on a rolling top 10 basis.

- Secure Score management

This service utilises Microsoft Security Exposure Management, which can be deployed using our Secure by Default security blueprints or aligned to our blueprints if already in production and maintained as part of the service.

This service includes change control for the existing platform configuration, and product support for Microsoft Security Exposure Management.

2.3 Threat and Vulnerability Management (TVM)

- Vulnerability assessments of your network-connected assets across public, private and OT / IoT networks (depending on the agreed scope)
- Vulnerability analysis and prioritisation
- Remediation of high and critical vulnerabilities (depending on the contracted monthly days)

This service utilises industry standard tooling, which can be deployed using our Secure by Default security blueprints or aligned to our blueprints if already in production and maintained as part of the service.

This service includes change control and product support for our preferred Threat and Vulnerability Management tooling.

2.4 Attack Surface Reduction (ASR)

- Digital attack surface discovery and mapping
- Continuous inventory analysis
- Implementation and management of ASR rules
- Ongoing reduction of your organisation's attack surface

This service utilises Microsoft External Attack Surface Management, Microsoft Defender for Endpoint P2 and the ASR capabilities in the Microsoft Windows operating system[3], which can be deployed using our Secure by Default security blueprints or aligned to our blueprints if already in production and maintained as part of the service.

This service includes change control and product support for Microsoft External Attack Surface Management, Microsoft Defender for Endpoint P2 and the ASR capabilities in the Microsoft Windows operating system[4].

2.5 Platform Enhancements

- Implement advanced product features and capabilities beyond the core functionality:
  - Microsoft Entra ID P2
    - Risk-Based Conditional Access
    - Access Reviews
    - Entitlement Management
    - MFA Registration Policy
    - Privileged Identity Management (PIM)
    - Multi-Factor Authentication (MFA)
    - Password Protection
    - Password less Authentication / Windows Hello for Business
    - Self-Service Password Reset (SSPR)
    - Single Sign-On (SSO)
    - Temporary Access Pass (TAP)
    - App Proxy

[3] Requires a supported operating system, details available on request.
[4] Requires a supported operating system, details available on request.

- Microsoft Defender for Office 365 P2
  - Advanced Anti-Phishing
  - Exchange Online Protection (EOP)
  - Safe Attachments
  - Safe Links
  - Attack Simulation Training
  - Automated Investigation and Response (AIR)
  - Compromised User Detection
  - Teams Message Quarantine
- Microsoft Defender for Endpoint P2
  - Microsoft Information Protection Integration
  - Vulnerability Management
  - Asset management
  - Network discovery

Transparity's security teams constantly review recommendations from industry standard security governing bodies such as the NCSC, CIS, NIST, CISA, and MITRE. They also review and test product enhancements, improvements and features from Microsoft for their security tooling. The results of these reviews drive our security blueprints.

This service ensures that all Microsoft Security tooling deployed as part of the Transparity Managed Extended Detection and Response and / or Security Posture Management services are continually aligned to our Secure by Design blueprints[5] ensuring that your organisation is benefitting from an evergreen security configuration, rather than a set-and-forget approach to product maintenance.

The enhanced capabilities of the Microsoft Security products[6] can be enabled / deployed / realigned to our security blueprint framework enabling you to onboard your devices and users.

2.6 Attack Simulations

- Phishing-based simulations based on various social engineering techniques
- Tailored payload and composition
- Simulation reports and insights
- Training campaigns
- How-to guides

This service utilises industry standard tooling, which can be deployed using our Secure by Default security blueprints or aligned to our blueprints if already in production and maintained as part of the service.

This service includes change control and product support for our preferred attack simulation tools.

2.7 Service Delivery Management[7]

As part of your account team, you will be allocated a Service Delivery Manager. They will serve as your primary contact(s) for day-to-day management and interaction for this Service. In addition, the Service Delivery Manager will act on your behalf to ensure we adhere to our processes and standards to meet contracted obligations and provide advice and guidance on your Cyber Security Service.

[5] Customer can choose to opt out of the security blueprint alignment if required and will be logged on the risk register.
[6] In scope Microsoft Security tooling / products are listed in section 2.11 of this document.
[7] Where you also contract our Managed Extended Detection and Response (MXDR) service. Non-MXDR contracted customers are not eligible for this service feature.

Your aligned Service Delivery Manager will host monthly service review meetings with your nominated contacts to run through the following activities:

- Provide you with your monthly service report.
- Discuss your service and run through the report content.
- Discuss and agree actions on any outstanding service tickets, change requests or risks.
- Review the Risk Register backlog.
- Any other business.

2.8 Inclusive Security Engineering[8]

Delivered by our Security Engineering team. This service includes up to five (5) hours of Security Engineering per month.

2.9 Threat Advisories

Threat advisories are reports that provide information about significant new trends or developments regarding potential or existing cyber threats, including analytical insights into the tactics, techniques, and procedures (TTPs) of adversaries.

This service offers detailed reports and advisories for impactful and emerging threats being tracked by our SOC.

2.10 Security Reporting

Providing holistic visibility into the status of your organisation's security service through robust reporting (where tooling is deployed and managed within this service) monthly.

2.11 Microsoft Security Tooling

This service can utilise some or all of Microsoft's Security tooling, any of which can be deployed using our Secure by Design security blueprints or aligned to our blueprints if already in production and maintained as part of the service.

This service includes change control for the existing platform configuration, and product support for any / all the following Microsoft Security products:

- Microsoft Defender for Office 365 P2
- Microsoft Entra Identity Protection
- Microsoft Defender for Endpoint P2
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Identity
- Microsoft Defender for Enterprise IoT
- Microsoft Defender for Cloud – Cloud Workload Protection (CWP)
    - Microsoft Defender for Servers
    - Microsoft Defender for Storage
    - Microsoft Defender for Azure SQL Databases
    - Microsoft Defender for SQL servers on machines
    - Microsoft Defender for Open-source relational databases
    - Microsoft Defender for Azure Cosmos DB
    - Microsoft Defender for Containers
    - Microsoft Defender for App Service
    - Microsoft Defender for Key Vault
    - Microsoft Defender for Resource Manager

[8] Where you also contract our Managed Extended Detection and Response (MXDR) service. Non-MXDR contracted customers are not eligible for this service feature.

    - Microsoft Defender for AI Workloads
    - Microsoft Defender for APIs
- Microsoft Defender for IoT
- Microsoft Purview suite
- Microsoft External Attack Surface Management
- Microsoft Entra Private Access
- Microsoft Entra Internet Access
- Microsoft Windows Enterprise
- Microsoft Intune Endpoint Security
- Microsoft Sentinel
- Microsoft Entra P2
- Microsoft Entra ID Governance

3. Service Operations

Please refer to our Operations Manual for further information on incident management, requests for change and information requests.

3.1 Service Hours

We will provide the following service hours: -

Security Posture Management	Business Hours GMT 08:30-17:30	Sat / Sun / Bank Holidays GMT 08:30-17:30	Mon-Sun GMT 17:30-08:30
Consultancy	In-Scope	Out-of-Scope	Out-of-Scope

We deliver Security Posture Management activities on an agreed cadence, ensuring alignment to your purchased service days. The exact schedule and scope will be outlined in your Statement of Work.

4. Billing

4.1 Additional Charges

We reserve the right to charge additional fees in the following situations:

- Implementation work carried out outside Business Hours; and
- Any change in your requirements occurring after the implementation of the Service and outside the scope of the contract (as described in the MSA).

5. Dependencies

We will provide the service subject to the following dependencies:

5.1 Customer Obligations

- You will provide us reasonable assistance in the performance of the Service(s) including, but not limited to, providing all technical and licence information that we may require to perform the Service(s).
- You will provide named contacts who will be authorised to submit support requests on behalf of your company (“Nominated Contacts”). They will be the designated people with whom all contact is made regarding all requests.

- You will provide us with access to the in-scope subscriptions, accounts, and tenants. This access will be used by our support staff and tooling.
- B2B guest access.
  - Azure Lighthouse relationship and delegations.
  - Service Principals.
  - Administration break-glass accounts.
- You will provide us with reasonable advance notice of any:
  - Intent to perform planned maintenance activities (including upgrades, deployments, patching).
  - Additional resources that you will deploy into the Supported Public Cloud Platform.
  - Penetration tests to be completed and defined rules of engagement during the testing period.
- It is your responsibility to comply with your data sovereignty controls, policies, and procedures.

5.2 Prerequisites

Transparity's Security Consultants will require access to various systems, resources, and stakeholders within your organisation throughout the course of this engagement to ensure a smooth and successful delivery. The required level of access, permissions and resource alignment for collaboration will be provided ahead of the project commencement.

6. Exclusions

The creation of bespoke code or integrations for 3rd party systems is not included as part of this service; we can provide a separate quotation for any bespoke code or integration work.

6.1 Third Party Related

- Managing incident maintenance for:
  - 3rd party systems,
  - Software, and/or
  - SaaS services.
- Specifically, if the above items are not covered by a third party's warranty, support agreement, or terms of use.
- Management, configuration, maintenance, administration of third-party appliances, Customer applications, and any code used to create, update, or deploy applications from third parties or by the Customer is excluded from this Service.

7. Definitions and Acronyms

In this document "we" or "us" refers to the Supplier, and "you" refers to the Client.

7.1 Terms

The terms listed have the following meanings:

Term	Meaning
Event Management Platform	The tooling Transparity uses to monitor and alert on the Supported Public Cloud Platform
Statement of Work	This means a document that defines project-specific or Customer-specific activities, deliverables, and/or timelines for providing services to that Customer.

7.2 Acronyms

Acronym	Meaning
TVM	Threat and Vulnerability Management
ASR	Attack Surface Reduction
KSAT	KnowBe4 Security Awareness Training
MXDR	Managed Extended Detection and Response
TTPs	Tactics, Techniques, and Procedures
CWP	Cloud Workload Protection
TI	Threat Intelligence

8. Service Level Agreement and Operational Targets

8.1 Consultancy

	Security Posture Management Request
Hours of Cover	08:30-17:30
Response	1 Working Day