AllyCare Guardian

Service Guide

Solution Description

The AllyCare Guardian solution provides continuous security hardening, monitoring, and breach detection for Microsoft 365 and Azure tenants. The service builds on Microsoft 365 E5/G5/A5 licensing to maximize available security features, reduce redundancy, and ensure proactive compliance alignment. AllyCare Guardian is delivered as a recurring service focused on reviewing, implementing, and updating workloads across the Microsoft ecosystem while incorporating MAD365 for advanced breach detection and monitoring.

Table 1: Scoping Worksheet

Item	Core System / Service Component	Scope Parameters
1	Microsoft 365 Tenant Workloads	Azure AD, Purview, Defender for Cloud Apps, Defender for Endpoints, Exchange Online, Intune, OneDrive, SharePoint, Teams
2	Security Review & Hardening Cycle	Initial assessment (6 months) followed by ongoing quarterly reviews
3	MAD365 Identity Breach Protection	Daily log ingestion, anomaly detection, and engineer-led analysis
4	Security Policy Implementation	Conditional Access, MFA, DLP, Retention, Anti-Spam/Phishing/Malware policies
5	Monitoring & Alerting	Continuous monitoring, high-risk escalation to client, remote technical support

Services Provided

The Service Provider will employ the BlueAlly solution delivery methodology as the framework to deliver AllyCare Guardian. Project phases are described below:

Project Initiation

- Conduct kickoff meeting and review scope
- Request and validate system access
- Develop project plan/schedule

Discovery and Assessment

- Perform initial assessment of Microsoft 365 tenant security posture
- Review Azure AD, Purview, Defender, Exchange, Intune, OneDrive/SharePoint, Teams
- Deliver findings and prioritized timeline

Implementation and Hardening

- Implement agreed-upon security changes in working sessions
- Apply MFA, Conditional Access, DLP, Safe Links/Attachments, and retention policies
- Provide support immediately following implementation

MAD365 Breach Detection & Monitoring

- Daily review of Microsoft Defender for Cloud Apps logs
- Anomaly detection: impossible travel, anonymous IPs, failed logins, suspicious activity
- Engineer review and escalation of high-risk issues

Ongoing Review and Optimization

- Quarterly reviews and compliance alignment
- Continuous updates for new Microsoft security features
- Recommendations for additional controls and configuration improvements

Deliverables

- Security Assessment Report
- Prioritized Implementation Plan
- Quarterly Security Review Reports
- MAD365 Dashboard & Alerts
- Configuration and Policy Documentation

Period of Performance

The Period of Performance is twelve (12) to twenty-four (24) months from the date of Project Kickoff, depending on the option selected. Working sessions are scheduled in one-hour blocks. Remote delivery is assumed unless otherwise agreed.

Project Assumptions

- Client must hold Microsoft 365 E5/G5/A5 licensing to leverage all features
- Client SMEs and stakeholders are available for workshops and reviews
- Client provides secure remote access and IAM permissions to BlueAlly engineers
- Additional functionality outside scope requires a Change Authorization

Client Responsibilities

- Assign stakeholders and establish a single point of contact (SPOC)
- Provide required system access and documentation
- Participate in working sessions and approve deliverables
- Maintain licensing and ensure environmental readiness

Service Provider Responsibilities

- Lead kickoff, discovery, implementation, and quarterly review activities
- Provide security assessment, design, and implementation support
- Monitor MAD365 logs and escalate high-risk events
- Deliver quarterly reporting and recommendations
- Maintain project documentation and communicate updates

Out of Scope Services

This guide outlines the services provided. Any services not explicitly detailed within this guide are considered beyond the scope of this service. Requests falling outside the scope may necessitate adjustments to the existing contract, denial of service, or additional billing on an hourly basis. Before any billing for services outside the agreed scope, customer approval is mandatory.

The following services are out of scope and require separate engagement or contract modification:

- Network infrastructure redesign
- On-premises systems not related to Microsoft 365 integrations
- Custom development or third-party security platform integration
- Support for non-Microsoft cloud platforms