ATECH IOMART

# Service Definition Document

## Managed Detection and Response (MDR) and Extended Detection and Response (XDR)

## Contents

# Solution Overview

## What is Managed Detection and Response (MDR)

Iomart's Managed Detection and Response (MDR) providers deliver 24x7 threat monitoring, detection, and response services to clients. This is achieved by leveraging a combination of technologies (deployed at the host and network layers), advanced analytics, threat intelligence, and human expertise. MDR has emerged as a category in recent years because of significant gaps in the Managed Security Service Provider (MSSP) model. The MSSP model simply delivers alert notifications, without establishing whether an alert is a false or true positive. The burden of identifying true positives within the flood of alerts rests squarely on the Client. Even more importantly, in the case of true positives, clients are on their own in terms of response. In contrast, MDR delivers true threat detection capabilities, because alerts are triaged and established as false or true positives. When true positives are identified, the service capabilities of MDR extend all the way through to delivering a response.

## Key Features

- 24x7 monitoring of your security alerts
- Enhance SIEM Visibility using the Microsoft SIEM/SOAR solution in Sentinel.
- Ingestion of log data from across the infrastructure
- Monthly reports covering incidents and threat hunting
- Quarterly service reviews
- Comprehensive reporting for compliance and auditing service benefits
- Standard and customisable detection rules
- Remediation advice and posture enhancements
- Advanced threat hunting by in-house experts across the cyber kill-chain

These features collectively contribute to the MDR Service's role in strengthening an organisations' cybersecurity framework, offering a comprehensive, expert-driven approach to managing and mitigating cyber risks.

## Key Benefits

- improved management of your environment, leading to better security outcomes
- Reduced burden on IT staff
- Improved response times to security incidents
- Access to our specialised security expertise
- Reduced costs associated with building and maintaining a security team
- Custom use case design and development
- Enhanced rule tuning for broader, cleaner, accurate detections
- Flexible and adaptable to emerging threats and increased threat landscape

## Service Overview

The Iomart Guardian service is based on the following components, the service provided is determined be the service level chosen by the Client, with each service level providing a different level of cover.

- Guardian Business MDR
- Guardian Enterprise XDR

| Core capabilities | Guardian Business MDR | Guardian Enterprise XDR |
|---|---|---|
| Rapid Onboarding | ✓ | ✓ |
| 24x7x365 SOC Service | ✓ | ✓ |
| Iomart service hub | ✓ | ✓ |
| Standard Security Reporting | ✓ | |
| Enhanced Security Reporting | | ✓ |
| Investigation for M365/Sentinel security alerts | ✓ | ✓ |
| Security alert containment (connected Sentinel data sources) | ✓ | ✓ |
| Microsoft XDR Complete Threat coverage | | ✓ |
| Security posture improvement | | ✓ |
| Security Remediation hours ② | Optional | ✓ (10 hours p/month) + |

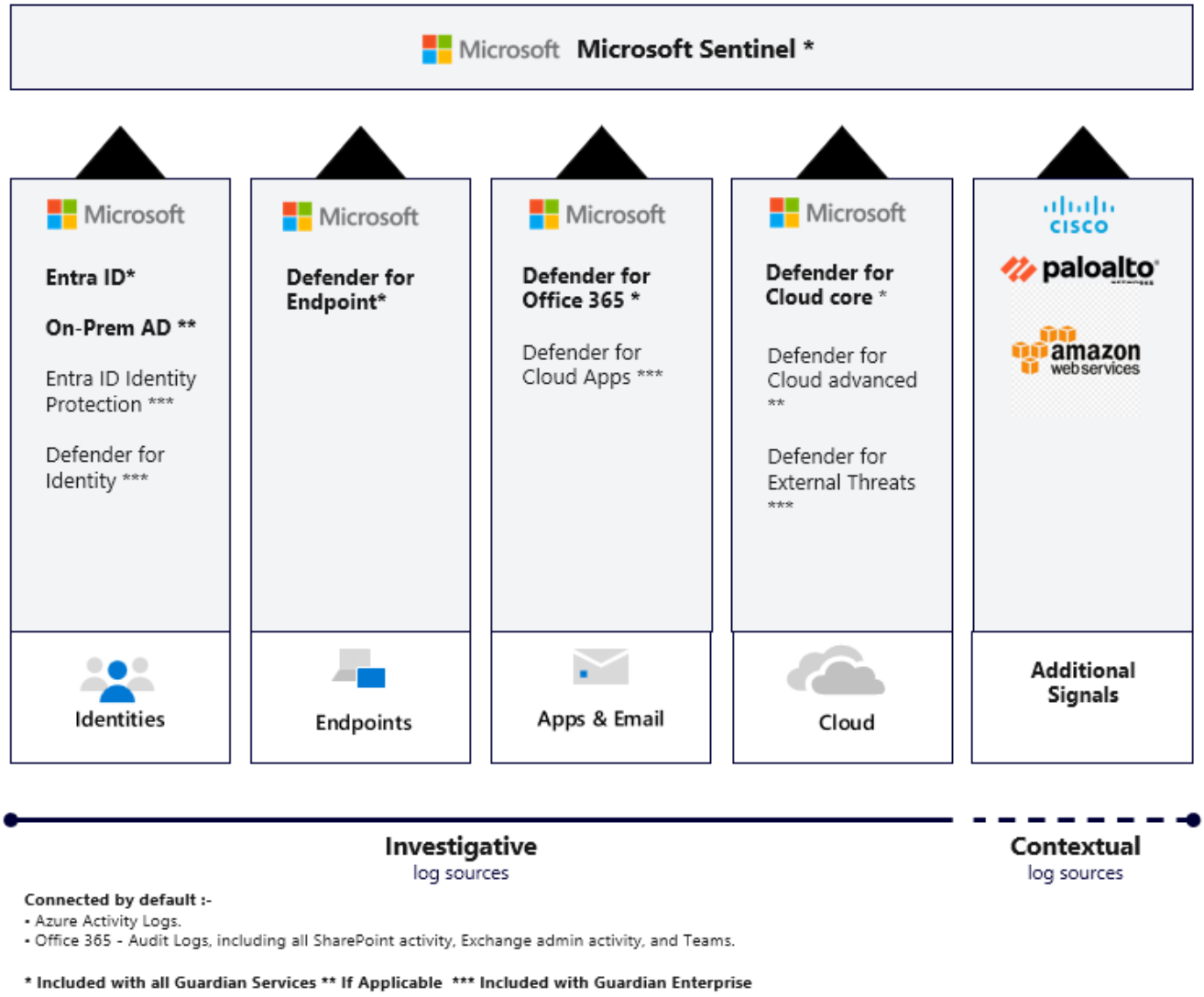
| | | |
|---|---|---|
| | | option to procure more |
| Managed – Endpoint, Detection & Response (Microsoft Defender for Endpoint) | | |
| Conditional Access | ✓ | ✓ |
| Device Compliance | ✓ | ✓ |
| Threat Analytics | ✓ | ✓ |
| Web Content Filtering | ✓ | ✓ |
| Attack Surface Reduction (Initial Audit Mode 30 days – then transfer to Block mode) ③ | ✓ | ✓ |
| Vulnerability management (core) ④ | | ✓ |
| Managed – Cloud Protection (Microsoft Defender for Cloud) | | |
| Cloud workload protection core – includes | | |
| Cloud Security Posture Management (Foundational) | ✓ | ✓ |
| Defender for Cloud workload protection (Servers) | ✓ ⑤ | ✓ ⑥ |
| Defender for Cloud workload protection (Databases) | ✓ ⑦ | ✓ ⑧ |
| Defender for Cloud workload protection (Containers) | ✓ | ✓ |
| Defender for Cloud workload protection (Storage) | ✓ | ✓ |
| Defender for Cloud workload protection (Service Layer) | ✓ | ✓ |
| Cloud workload protection advanced – In addition to the above, also includes | | |
| Cloud Security Posture Management (Advanced) | | |

| | | |
|---|---|---|
| File integrity monitoring | Optional | Optional |
| Just in time access scanning | | |
| Container Image scanning | | |
| Adaptive Application Control | | |
| Adaptive Network Hardening | | |
| SQL Vulnerability Management | | |
| Managed – Email Collaboration (Defender for Office 365) | | |
| Anti-Phishing | ✓ (M365 Business Premium only) | ✓ |
| Real Time Detection | | ✓ |
| Safe Attachments | ✓ (M365 Business Premium only) | ✓ |
| Safe Links | ✓ (M365 Business Premium only) | ✓ |
| Anti-Malware | ✓ (M365 Business Premium only) | ✓ |
| Quarterly Simulated Phishing Attacks | | ✓ |
| Attack Simulation Training for Client | | ✓ |
| Cloud Applications (Defender for Cloud Apps) | | |
| Discovered Apps | ✓ (M365 Business Premium only) | ✓ |
| Cloud App Risk Assessment | ✓ | ✓ |

| | | |
|---|---|---|
| | (M365 Business Premium only) | |
| Anomaly Detection for Discovered Apps | | ✓ |
| App Permissions and Ability to Revoke Access | | ✓ |
| Real-time Session Monitoring and Control | | ✓ |
| Identity Protection (Microsoft Entra ID Identity Protection) | | |
| Identify Anonymous IP Address Use | | ✓ |
| Atypical Travel | | ✓ |
| Malware Linked IP Address | | ✓ |
| Unfamiliar Sign-in Properties | | ✓ |
| Leaked Credentials | | ✓ |
| Defender for Identity (for hybrid AD signals) | | |
| Monitor users, entity behaviour, and activities | | ✓ |
| Protect user identities and credentials stored in Active Directory | | ✓ |
| Identify and investigate suspicious user activities | | ✓ |
| Microsoft Defender for External Threats | | |
| External Attack Service Monitoring ⑨ | | ✓ |
| Managed Microsoft Sentinel | | |
| Sentinel Deployment, configuration, and integration (Including Azure Lighthouse setup and configuration) | ✓ | ✓ |
| Microsoft (out of the box) connector setup | ✓ | ✓ |
| Security baseline | ✓ | ✓ |

| | | |
|---|---|---|
| Monthly Sentinel cost reporting & optimisation | ✓ | ✓ |
| Additional Sentinel (3rd party) connectors | Optional | ✓ |
| Custom Connector integration ⑩ | Optional | ✓ |
| Proactive Threat Hunting | | ✓ |
| Threat intelligence | | ✓ |
| Managed Incident, Detection and Response ⑪ | ✓ | ✓ |

## Technology Overview




**Connected by default :-**
- Azure Activity Logs.
- Office 365 - Audit Logs, including all SharePoint activity, Exchange admin activity, and Teams.

*** Included with all Guardian Services ** If Applicable *** Included with Guardian Enterprise**

Please note: Iomart also include a quarterly M365 baseline audit, this is a managed audit and configuration service to discover and harden security configuration settings in Microsoft 365.

## Technology Pre-requisites

To activate and benefit from Iomart's managed Guardian service(s), you are required to hold certain Microsoft technology licenses as well as having certain Microsoft technology deployed and configured within your environment.

## Service Deliverables

Iomart will deliver the following.

**Best Practices and Business-Needs Driven Guardian Service Setup, Configuration, and Tuning**

- Tuning of detection logic and response actions based on the inventory of High Value Assets & VIP's you provide, to deliver a service tightly aligned to your organisation's priorities.
- Meticulous definition of escalation procedures and rules of engagement, such that there is total clarity on who does what in every major category of situation, from daily operations to emergency responses.
- Initial service setup of Microsoft Sentinel (with applicable data connectors/log sources) *
- Integration of Microsoft Defender for Cloud CSPM (Foundation) and cloud workload protection core
- External attack service monitoring via Microsoft Defender for External Threats, this is included with Guardian Enterprise and is an optional service add-on for Guardian Business clients

* Please note: Additional Client log connectors/data sources will need to go through Iomart's Change Request process (detailed at onboarding and as set out in clause 3.5 of the Agreement) to enable post service go-live. If the connector requires configuration outside of an OOB connector, i.e a custom connector/use case - Atech will provide as estimate for the number of hours required and this will be classed as additional chargeable work.

**24x7x365 Proactive Detection, Education, and Response by Highly Skilled Security Experts**

- Automated handling of mundane security operations activities, allowing your internal IT teams to focus on high value work.
- Investigation, escalation, and response (as agreed upon) in the case of true positives.
- Use of Iomart curated threat intelligence for improved detection capabilities.
- Security awareness training (Guardian Enterprise clients included) this service is optional for Guardian Business users and is charged in addition to the core Guardian service.

**Continual Service Improvements**

- Continual security tuning to reduce false positives.
- Continuous delivery of new security use cases to keep pace with the evolving threat landscape.
- Fast operationalisation of new detection capabilities in Microsoft 365 Defender, Microsoft Defender for Cloud, and other Microsoft Security products (where applicable)

**Reporting, Auditability, and Transparency to Drive Collaboration and Service Effectiveness**

- Monthly enhanced security "Action" Reports (Enterprise clients) delivering insights to drive high-impact actions, key decisions, and communicate information on the progress of the client's security program.
    - Monthly status meetings with your Atech Cyber Defence Centre Security Engineer to guide you through your action report, as well as share any relevant

recommendations to improve your security posture based on observations made during the monitoring of your environment.

- Real-time auditability of all incidents through Iomart's ITSM (IT service management) platform
- Strong Atech security services delegated user authentication and control, with audit trail of all user access.
- Enforced change management processes by comprehensive ticketing system and built-in sign-off procedures.
- Review of change requests by Iomart Cyber Defence Centre Security Engineers, clarifications and feedback provided in the case of any hidden risks.
- Log search capability for all logs collected over a period you define (minimum 90 days, optionally up to 7 years – note that Microsoft retention for logs is free for 90 days, Microsoft costs are applied after this timeframe – Atech will use reasonable endeavours to work with you to understand any additional costs as required).
- Reporting to meet your compliance needs.

**Ongoing Technology Lifecycle Management and Coverage of Risk**

- Continuous security (in scope) monitoring, operation and adaption of all detection and response components on rapidly changing cloud technologies

**Microsoft 365 Secure Audit and Baselining Health Check**

- Performed by a Microsoft certified security expert. Iomart will provide an initial health check baseline and then a deliverable scan each quarter, including recommendations for improvements to harden your M365 security posture. Security remediation hours can be used towards rectifying or implementing the recommendations in the health check. Note that Guardian Enterprise clients get 10 hours per month as part of the service, Guardian Business subscribers do not receive an allowance of hours as part of the core service. You can purchase additional block hours, these come in 100-, 200-, 300- & 400-hour blocks and can be used throughout the duration of the contract (applicable to both Guardian Business & Enterprise)

Please note hours are pooled for the term of the contract, any unused hours can be used the following month(s) – note that hours will be lost at end of the contract if they are not used.

**Security Awareness Training**

- Iomart's security awareness training platform is provided to Guardian Enterprise clients by default, please note that this service is also optional for Guardian Business clients. The security awareness platform includes the following features.
    - Phishing simulation
    - Security awareness training (videos, courses, and quizzes)
    - Gamified interactive testing.
    - Cyber assessments

**Incident Response Automation**

The SOC will utilise the full capabilities of response actions in the available Microsoft Defender suite to contain an ongoing security incident. Possible response actions are described in the terms of engagement, and customers using Guardian can tailor a limited number of responses, based on the entities involved.

Some response and auto-investigations require specific licence enablement.

Our Service Management approach is designed to ensure that you are always informed, involved, and confident in the security measures we are implementing on your behalf. We believe that this collaborative approach is key to delivering a service that accelerates the enhancement of your security posture.

## Objectives of the Service

Key objectives of the Service are:

- **Real-Time Threat Identification**: Through constant surveillance and sophisticated analytics, a MDR service identifies potential security threats in real time, enabling swift mitigation actions before they escalate into serious breaches.
- **Enhanced Incident Response**: One of our standout features is its rapid incident response capability using automated remediation, drastically reducing the time from threat detection to resolution. This not only minimises potential damage but also accelerates recovery, ensuring business continuity.
- **Bespoke Security Insights**: Our objective is to move beyond generic advice, our MDR offers tailored security recommendations, informed by deep analysis of an organisation's specific threat landscape and business context to provide insights to enable strategic security enhancements and informed decision-making to ensure our customers have the best business outcomes from our service.
- **Comprehensive Compliance Management**: With an acute understanding of the regulatory landscape, our MDR Services ensure organisations not only meet but exceed compliance requirements, thereby avoiding potential fines and reputational damage.

- **Advanced Threat Intelligence**: Organisations benefit from cutting-edge threat intelligence, leveraging global insights to pre-emptively address vulnerabilities and defend against emerging threats and keep our customers safe.
- **Scalable Security Posture**: The service aims to flexibly scales in response to an organisation's growth or changing needs, ensuring that the cybersecurity measures evolve in tandem with the organisation's expansion or strategic pivots.
- **User-Friendly Interface**: We understand the importance of user experience. The solution comes with an intuitive interface, making it easy for security professionals to manage and analyse threat data effectively.

## Service Transition

Each Guardian (Business or Enterprise) security service onboarding starts with a project kick-off meeting, led by the Project Manager. The Project Manager takes on the responsibility of project administration and reporting over the entire course of the service onboarding.

At the project kick-off meeting, you'll meet the full onboarding project team, which includes the aligned Project Manager and Security Engineer. The Project Manager will walk you through the full process and present a comprehensive project plan proposal with specific milestones and due dates. The major project tasks and responsibilities will be discussed and jointly defined. The Project Manager will introduce you to the established project management and collaboration tools, gather reporting requirements, and set the meeting cadence for recurring project status meetings. A Guardian service onboarding tool is introduced, and first steps are discussed and assigned to relevant owners.

As soon as the prerequisites are met on your side, the **Iomart** Onboarding Team will work with you on the five onboarding workstreams listed below. These are termed workstreams as they can take place in parallel, with the overall goal of activating the Guardian security service as quickly as possible.

| Guardian Service(s) onboarding workstreams | | | | |
|---|---|---|---|---|
| Client Asset Identification | Service Setup | Escalation Process Definition | Use Case Deployment & Baselining | Acceptance and Go-Live |

| Workstream 1 | |
|---|---|
| Client Asset Identification | Building cyber risk resiliency starts with a clear understanding of what needs to be protected with the highest level of priority. Through the Guardian Security Services Onboarding Tool, you provide us information about your critical business assets (including their technical composition) such as servers, applications, files, software, and data. These critical assets are designated as High-Value Assets & VIP's and help us understand the "crown jewels" of your organisation, serving as foundational information for the Guardian managed Security Service. Beyond this, the inventory of High-Value Assets is also important for recovery plans, to rapidly assess, contain, and recover these assets during any incident. |

| Workstream 2 | |
|---|---|
| Service Setup | This workstream is focused on the setup, configuration, and activation of the various Guardian service components. A key step is connecting/activating your Sentinel instance through Azure Lighthouse. Access to your Microsoft Defender for Endpoint is established. Additional configuration tasks including adjustment of the Active Directory audit policy to conform to best practices, log streaming from all T0 server assets to Microsoft Log Analytics (Guardian Enterprise) enabling any previously defined log connectors and ensuring that all necessary logs and data feeds are working as expected.<br><br>Atech will also plan & undertake the M365 Baseline audit – sharing remediation actions with the Client and will plan work with you to schedule the quarterly reviews (using remediation hours)<br><br>For Guardian Enterprise clients (optionally for business clients), Atech will also work with you to implement and establish the cadence of the security awareness training |

| Workstream 3 | |
|---|---|
| Escalation Process Definition | A key aspect of our Guardian Security service(s) is efficient and effective response. To ensure the effectiveness of response capabilities, we work with you closely during this workstream to ensure that all necessary responsibilities (on both sides) are assigned and "process-activated". In doing so, we create an Incident Escalation Matrix, the complexity (single or multitier) of which may vary, depending on your needs. Along with this we also discuss and agree upon the Rules of Engagement, which define the cases in which we can respond directly, as well as the cases in which we require your explicit approval first. |

| Workstream 4 | |
|---|---|
| Use Case Deployment and Baselining (tuning) | To ensure high-fidelity detection, use cases must take into consideration the specificities of your environment. Upon completion of the Asset Identification and Service Setup workstreams, we have the relevant inputs (your High Value Assets, the setup of your IT environment) to deploy relevant use cases. Once activated, together with you, we fine tune the use cases to your environment. Your input and active collaboration during this baselining process is crucial – please note that during this time SLA timeframes are not active.<br><br>Atech will also enter a period of optimisation & refinement This ensures that the environment enters the live monitoring phase in the best manner possible. Identifying business as usual activity and fine tuning the "noise" allowing analysts to have time to investigate true positives thoroughly.<br><br>This phase also validates the response and communications process between Atech and yourselves, running through proactive scenarios and resilience if the main point of contract was unavailable.<br><br>This penultimate phase aligns the expectations between client and Atech to ensure a harmonious working relationship through the length of the contract. Both parties should be happy before moving to the final workstream, |

| Workstream 5 | |
|---|---|
| Acceptance and Go-Live | This final workstream ensures that all the requirements are met both on the Atech and Client side. This includes successful validation of configuration, acceptance tests, and defined escalation processes clause 11 of the Agreement applies to this workstream 5. Once all this is completed, and with your formal acceptance, the Guardian service is fully activated and handed over to the Atech Cyber Defence Centre (SOC) for the 24x7 operations moving forward. At this point the Onboarding team closes the service onboarding project, and you work with your Account Management team moving forward |

## Incident Management SLAs

Alerts and Incidents are generated based on rules and analytics applied to the logs and telemetry sources from the activated threat detection and response service components. Many of these alerts are triaged automatically via advanced logic developed by our SOC, ensuring swift and efficient response to known potential threats.

High and medium incidents are given priority and are triaged against specific Service Level Agreements (SLAs) to minimise any potential impact. Our alert and incident categorisation and corresponding action times are applicable 24 hours a day, 7 days a week and are as follows:

| **Priority** | **Mean Time to Investigate** (MTTI) | **Mean Time to Advise** (MTTA) | **Description** |
|---|---|---|---|
| P1 (High) | 30 Minutes | 60 Minutes | High risk incident, a suspected, or high probability, of system compromise. Pose an immediate threat to the confidentiality, integrity, or availability of sensitive data or systems. Examples include data breaches & active malware attacks. |
| P2 (Medium) | 60 Minutes | 2 Hours | Increased attack activity including high-priority events that may require further investigation by you (*e.g.,* repeated events or attacks to your network or for an outage of any type). |
| P3 | 2 Hours | 4 Hours | Low-risk incidents indicate the need for increased vigilance in monitoring and will be used to keep you up to date on |

| | | | |
|---|---|---|---|
| (Low) | | | potentially hostile activity. This is an incident which poses no immediate risk of compromise or exposure |
| P4 (Informational) | Weekly Report | N/A | Minimal risk/No Risk activity to which clients would like to be informed about. This typically relates to normal business activity |

The measurement time metrics are defined as follows:

- Mean Time To Investigate (MTTI) - The point from which an Incident has been raised by The System to when it has been triaged.
- Mean Time To Advise (MTTA) - The time taken from an incident being triaged as a True Positive to an analyst undertaking an active response, or onward escalation to a customers' emergency incident response team.

## Billing Enquiries

Iomart's managed Guardian Security services pricing will be determined at the start of the client engagement and includes the following items.

- **Per-user per-month pricing for both Guardian Business and Enterprise services** (active users – identified from customers Entra ID)
- **One off "service onboarding" charge for**
  - Onboarding fees
    - Includes, security baselining, project management, Atech use case deployment and SOC environment tuning.
  - Custom connectors and non Atech use cases (custom)
- **Optional additional service portfolio capabilities (examples include):-**
  - Microsoft Defender "Guardian security services" coverage for
    - Cloud Advanced CSPM coverage *if applicable*
    - Additional Microsoft Defender for Server coverage (in addition to what is included as part of the core service) *if applicable*
    - Additional Microsoft Defender for Database coverage (in addition to what is included as part of the core service) *if applicable*
  - Patch management (Servers and Endpoints) *if applicable*
  - Cyber awareness training *if applicable*
  - **Remediation hours** (included for Guardian Enterprise customers – additional blocks can be purchased)

If the number of users/cloud protected is amended the monthly client per/user per/month and protected cloud asset bill will be updated accordingly and reflected in the next invoice.

Please note: Microsoft consumption/licensing charges do apply in addition to Iomart's managed Guardian support service, these costs vary depending on the consumption/licensing model applied.

## Guardian Managed Services – What's Not Included?

Iomart's managed Guardian services does not include support, SOC coverage and or professional services assistance for anything not detailed or explicitly called out in relevant contracts or Statement of Works – examples of unsupported service support and or direct management are detailed below:

- End of support/life operating systems (Windows Server 2012 R2 or older, Windows 10 20H2 or older and or Linux distributions not supported by Microsoft)
- 3rd party Anti-Virus/EDR solution inclusion (Sophos, McAfee, CarbonBlack, Crowdstrike etc)
- 3rd party SIEM cloud/on-prem hosted solutions (Splunk, QRadar, Logpoint, LogRhythm)
- 3rd party identity management platforms/services support (Okta, Duo etc)
- Microsoft Azure – management and configuration (outside of deployment and management of Microsoft Sentinel)
- Microsoft M365/O365 service management
- Amazon Web Services (AWS) – Management & configuration of Clients AWS tenant
- Google Web Services (Google) – Management & configuration of Clients google tenant.
- Active Directory Management
- Entra ID Management (outside of the scope and what's is required for the managed service)
- Deployment of Azure based services and/or subscription creation/management (outside of the managed service)
- Endpoints where users are members of the local administrators group.
- Endpoints running end of support applications.
- Endpoints excluded from Atech Windows & Defender baseline policies.
- Endpoints that are unmanaged or BYOD (bring your own device)
- 3rd party application/service patching
- Formal Security training, support, or certifications
- Formal Incident response – Atech will use reasonable endeavours to work with the Client to mitigate and respond to a potential breach and will actively attempt to neutralise threats before a potential attacker can penetrate another security layer. Atech will work alongside both the Client and additional 3rd party service providers to integrate our Guardian MDR service into your incident response plan.

## Exit Planning

If you wish to transition to an alternative supplier, Iomart will work with you and the new supplier to ensure an efficient and seamless transition. Like our implementation process, our exit process will ensure that all stakeholders are engaged, risks are identified and mitigated, and that a clear programme of works is documented and communicated.

Upon confirmation of transition, Iomart will engage with you to create a Statement of Work and present a services package that will ensure a successful move.

The topics to be discussed include:

- Data migration
- Simultaneous use (if needed)
- Handover of projects in progress (if applicable)
- Final period report(s)
- Final period invoice(s)

You can be assured of minimal disruption during the transition, therefore allowing you to focus on business-as-usual activities.

Please see our Terms and Conditions for further detail.

## Data Protection & GDPR

Atech, part of the Iomart Group, is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct. Our Data Protection policy sets forth the expected behaviours of Iomart Employees and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to an Iomart Contact (i.e. the Data Subject). Iomart, as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in our Data Protection policy (available on request).

Iomart's leadership is fully committed to ensuring continued and effective implementation of this policy and expects all Iomart Employees and Third Parties to share in this commitment.

Iomart uses the Personal Data of its Contacts for the following broad purposes:

- The general running and business administration of Iomart Entities.
- To provide services to Iomart customers.
- The ongoing administration and management of customer services.
- The use of a contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object.

Each Iomart Entity will Process Personal Data in accordance with all applicable laws and applicable contractual obligations. More specifically, Iomart will not Process Personal Data unless at least one of the following requirements are met:

- The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the Data Subject is party or to take steps at the request of the Data Subject prior to entering a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary to protect the vital interests of the Data Subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.

- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party.

# Why Partner with Atech?

## Credentials and Capability

Atech is the one of the UK's most accredited providers of secure hybrid cloud managed services, delivering deep expertise across Microsoft technologies, data protection, and cybersecurity. We hold Microsoft designations for **Modern Work, Security, Infrastructure (Azure)** and are recognised as an **Azure Expert MSP** - a status achieved by only 60 partners globally and 15 in the UK.

As part of the Microsoft AI Cloud Partner Program, we have validated technical capabilities across the full cloud lifecycle. Our inclusion in the **Azure Expert MSP Program** reflects proven excellence in people, processes, and tools, ensuring sustainable, repeatable, and scalable managed services. This means you can rely on a partner that consistently delivers best practice and operational efficiency.

Partnering with us gives you access to over **200 Microsoft cloud specialists**, including **two Microsoft MVPs**, ensuring unparalleled technical depth and experience.

## Microsoft Endorsements and Specialisations

We hold multiple Microsoft Solutions Partner designations, including:

- Digital & App Innovation (Azure)
- Data & AI (Azure)
- Business Applications


Figure 1: Microsoft Accreditations

In addition, we have achieved advanced specialisations in areas such as:

- Cloud Security
- Identity and Access Management
- Threat Protection
- Infra & Database Migration
- Azure Virtual Desktop
- Enterprise Application Migration to Azure


Figure 2: Microsoft Designations

These credentials validate our ability to deliver complex, secure, and innovative solutions aligned to Microsoft best practices.

## Security and Compliance

Security is at the heart of our services. Atech is **ISO 27001 certified, Cyber Essentials Plus accredited**, and a member of the **Microsoft Intelligent Security Association (MISA)** – an invitation-only program granting access to Microsoft's top security experts. We also hold **CREST accreditation** and participate in the **Microsoft MSSP Program**, one of only 12 partners in the UK, giving our customers direct benefits such as access to product teams and funded workshops.

Further reinforcing our security leadership:

- **Microsoft Gold Partner Status** alongside **Azure Expert MSP**
- **Microsoft MSSP Program** (1 of only 12 UK partners)
- **Microsoft Fastrack Ready Partner** (1 of only 300 globally)
- **Microsoft XDR status**

These credentials provide you with assurance that security is embedded throughout design, migration, and ongoing management. Combined with our advanced specialisations and industry recognition, they demonstrate our ability to deliver secure, compliant, and future-ready solutions.


ATECH IOMART
6 Atlantic Quay, 55 Robertson Street, Glasgow, G2 8JD