itps

intelligent technology. practical solutions.

itps.co.uk

# MANAGED DETECTION AND RESPONSE (MDR)

## SERVICE DESCRIPTION

Get in touch with us today, we'd love to hear from you...
+44 (0)191 442 8300 | enquiries@itps.co.uk

Crown Commercial Service Supplier

Technology for a brighter tomorrow.

## Contents

## 1.0 ABOUT THIS DOCUMENT

This guide provides an overview of our Managed Detection and Response (MDR) service. We're here to show you how we help protect your organisation from today's security threats, leveraging the tools you already own. In this document, we'll cover the key features of our MDR service, explain how it works, and highlight the benefits it brings to your security strategy. Let's explore what our MDR service can do for you!

| SECTION | DESCRIPTION |
|---|---|
| **Service Overview** | What Managed Detection and Response (MDR) is and the unique value our MDR service delivers in your organisation. |
| **Technology Stack** | The technology deployments and licenses that are prerequisites to consuming our MDR Service. |
| **Service Deliverables** | The precises set of deliverables we offer to customers of our service. |
| **Service Level Agreement** | The Service Level agreement (SLA) we commit to as part of our service. |
| **Service Launch** | The details of how we operationalise the service for you through a set of carefully defined launch workstreams. |



+44 (1)191 442 8300 | enquiries@itps.co.uk

# 2.0 SERVICE OVERVIEW

## 2.1 Managed Detection and Response (MDR)

Managed Detection and Response (MDR) provides you with 24/7 threat monitoring, detection, and response services, keeping your systems safe around the clock. Our comprehensive service combines cutting-edge technology at both the host and network levels with advanced analytics, rich threat intelligence, and the deep expertise of our team.

MDR has become a key player in recent years, stepping up where traditional Managed Security Service Providers (MSSPs) have fallen short. Unlike MSSPs, which often just send out alerts—sometimes without sorting the real threats from the false alarms—our MDR service takes care to sift through these alerts, ensuring we only flag the real concerns. And we don't just stop at detection; our proactive response capabilities mean that we're always on hand to help you tackle any threats head-on, giving you peace of mind and robust protection.

## 2.2 Benefits with ITPS MDR

Our MDR service makes the most of the powerful Microsoft Sentinel and Defender suite, so you don't have to worry about buying or managing any extra security tools. This approach maximises your current licences and investments, focusing on the Microsoft security ecosystem to boost detection accuracy and response capabilities. Unlike other services that just integrate with Microsoft technologies, we dive deep to give you superior protection.

Our Managed Detection and Response services are looked after by our dedicated Cyber Team, available 24/7 right here in the UK. This ensures top-notch security that's usually only available to the most advanced organisations. At the core of what we do are our Security Operations Centres (SOCs), providing non-stop, thorough security coverage.

Our team is made up entirely of seasoned professionals, each extensively trained in their field. This means our service is not only continuous but also proactive. Managed entirely from our UK-based centres, our operations are streamlined to avoid night shifts and are more resilient to local disruptions.

Beyond constant security monitoring, you'll also get the personalised touch of a dedicated security engineer. This engineer will work closely with you, getting to know your environment inside out and carrying out proactive threat hunting to stop incidents before they start.

We've also boosted our capabilities with a cutting-edge platform that integrates automation artificial intelligence and leading threat intelligence feeds. This enhances our security effectiveness and operational efficiency, keeping you safer and more secure.



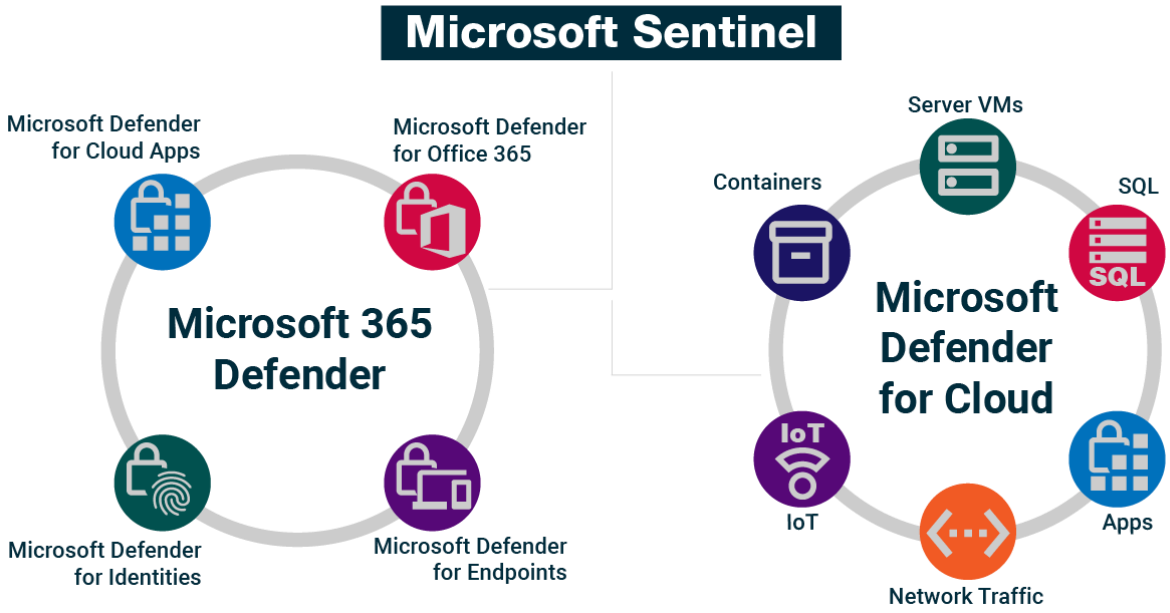
+44 (1)191 442 8300 | enquiries@itps.co.uk

# 3.0 TECHNOLOGY STACK

## 3.1 Technology Overview

Our MDR Service is based on the following core components.

Microsoft 365 Defender Services are:




**Microsoft Defender for Endpoints**: (Previously known as Windows Defender for Endpoint, Microsoft Advanced Threat Protection, Window Advanced Threat Protection) is a unified endpoint platform for preventative protection, post-breach detection, automated investigation, and response for endpoints.

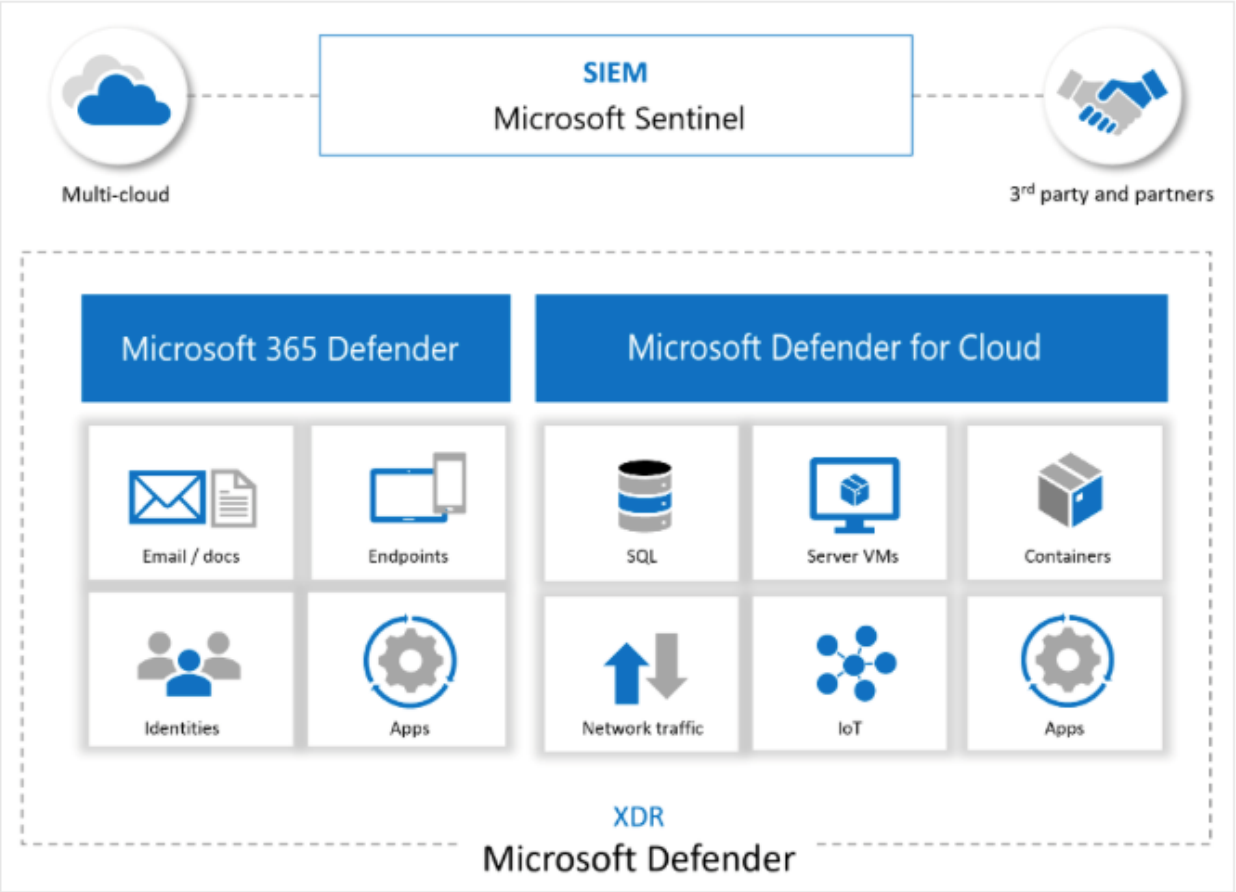
**Microsoft Defender for Office 365**: (Previously known as Office 365 Advanced Threat Protection) is the platform to protect against threats targeted using malicious emails, links, attachments, phishing to email, and collaboration tools.

**Microsoft Defender for Identity**: (Previously known as Azure Advanced Threat Protection) is the cloud-based security solution for on-prem Active Directory identities. Active Directory Forest is connected to Microsoft Defender to Identity using gMSA (Group Managed Service account), Microsoft Defender for Identity sensors installed on domain controllers and ADFS servers then send security signals to Microsoft Defender for Identity

**Microsoft Cloud App Security**: is Microsoft's CASB (Cloud Access Security Broker) solution. CASB is security software that acts as an interface between users and cloud resources. CASB examines cloud traffics and enforces security policies defined by the organization.

**Microsoft Sentinel** is a cloud-native solution that combines Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR)

capabilities built to collect and analyse data at scale, al- lowing automated analysis and response actions. It is a required component of our MDR+ service, serving as the central location where log sources of all types are ingested.



## 4.0 SERVICE DELIVERABLES

**Optimised Business-Oriented Security Setup, Configuration and Management:**

- Tailoring detection logic and response actions based on a provided inventory of high-value assets ensures that our services are closely aligned with your organisation's priorities.
- Establishing clear escalation procedures and rules of engagement provides total clarity on roles and responsibilities across all scenarios, from routine operations to emergency responses.

**24x7 proactive detection and response by security experts:**

- Automation of routine security operations activities frees up your security teams to concentrate on strategic initiatives.
- Immediate investigation, escalation, and response to verified threats, as pre-agreed, ensures swift action.
- Access to unlimited escalations, tickets and supports calls with skilled security experts guarantees expert assistance whenever needed.
- Integration of curated threat intelligence enhances detection capabilities, keeping your defences ahead of potential threats.

**Continual Service Improvements:**

- Ongoing tuning to minimise false positives, ensuring more accurate threat detection.
- Regular updates on new use cases to stay ahead of the rapidly changing threat landscape.

**Reporting, Continual Service Improvements:**

- Monthly service meetings with ITPS Security Operations Manager.
- Monthly Reporting from our Security Operations Centre
- Realtime auditability of all incidents through an integrated ticketing system
- Access to an ITPS SOC Incident co-ordinator for improved visibility and responses during incidents.
- ITIL / ISO27001 Aligned Change Management Processes

## 5.0 SERVICE LEVEL AGREEMENT

**Introduction to Service Operations**

ITPS MDR Service is available 24 hours a day; 365 days a year. The table below shows how incidents are classified and the associated response times.

| INCIDENT SEVERITIY | DESCRIPTION | RESPONSE TIMES | RESPONSE DEFINITIONS |
|---|---|---|---|
| **P1 - HIGH** | A major breach of security has occurred, which requires immediate attention e.g. unauthorised access has been obtained, or ransomware has been deployed. | 15 MINS | Incident acknowledge by ITPS SOC; containment activity automatically initiated |
| **P2 - MEDIUM** | A medium risk of security may have occurred, which requires prompt attention. E.g. Account brute force attempt, Admin permissions assigned outside of PIM. | 30 MINS | Incident acknowledged by ITPS SOC. The client is given the option to initiate containment. |
| **P3 – LOW** | An attempt to breach security may have been made, this was unsuccessful. | REAL TIME REPORTING | Incident triaged and fed in to live reporting dashboard |

| | | | |
|---|---|---|---|
| **P4 – INFORMATIONAL** | An informational alert may have occurred which requires attention. | REAL TIME REPORTING | Incident triaged and fed into live reporting dashboard |

# 6.0 SERICE LAUNCH

## 6.1 Service Onboarding Responsibilities

Our ITPS MDR Service is all about working together with you. There might be times when we need to bring in third parties, but these situations are rare. To make sure everything goes smoothly from the start, it's helpful to know who's involved and what their roles are during the onboarding process.

**ITPS**:

- **Security Operations Centre (SOC)**: Our SOC is the heart of the MDR Service, providing operations around the clock every day of the year. This includes continuous monitoring, threat hunting, incident handling, and reporting. During onboarding, our SOC experts will make sure everything is set up correctly to get you started on the right foot.
- **Customer Success**: From the moment you start onboarding, our customer success team is there to ensure the technical implementation of the service is spot on. They work closely with the SOC to make sure our collaboration is a success from day one.
- **Project Management**: Alongside the SOC and Customer Success teams, you'll also have a dedicated project manager. They take charge of coordinating everything between ITPS and you during onboarding, ensuring everything runs smoothly.

**Customer**:

- **CISO (Or equivalent role)**: You'll confirm the high-value assets, overall setup, service focus, and business use cases.
- **IT Security Operations**: Acts as the counterpart for operational MDR engagement.
- **IT Team**: Handles onboarding and installs any necessary customer prerequisites like Microsoft Defender for Endpoint. They also make sure the right access rights are set up, for example, Microsoft Entra.

* ITPS SOC Team (**Optional**): For an extra fee, separate from the MDR Service, our SOC team can also help set up Microsoft-related services, including Sentinel, Log Analytics, and the Defender suite of products.



+44 (1)191 442 8300 | enquiries@itps.co.uk

**Third Parties**:

- **Law Enforcement**: During onboarding, it's important to get the right emergency contacts and procedures in place. ITPS can help by providing access to our own contacts. Having a quick response process for law enforcement is beneficial, particularly in situations like money fraud through business email compromises.

- **Forensics**: Setting up the correct emergency contacts and procedures during onboarding is essential. At ITPS, we're ready to assist with our trusted partners.

- **Incident Response on Demand**: This is an optional service that can be useful for extensive on-site investigations. Some cyber insurance policies may provide support here too. We make sure that the appropriate emergency contacts and procedures are established during onboarding, with ITPS available to help with our resources.

itps

intelligent technology. practical solutions.

itps.co.uk

## Get in touch with us today, we'd love to hear from you...

**Call:** +44 (0)191 442 8300

**Email:** enquiries@itps.co.uk

Crown Commercial Service *Supplier*

Technology for a brighter tomorrow.