Microsoft Defender Services – Service Definition (DfB)

Microsoft Defender for Business is a new (2022) Endpoint Detection and Response (EDR) cyber security tool designed for smaller organisations (<300 users) and one which many organisations already have access to, via their Microsoft 365 Business Premium license, but aren't necessarily leveraging effectively to reduce cyber risk. A lack of relevant human resource or skills is a major concern for many organisations along with the ability to have eyes on 24/7.

One of the biggest challenges across cyber security is the over-reliance upon technology itself, without due consideration for the people and processes that are needed to make the technology truly effective. The same is true for Microsoft Defender and that's where we come in. It takes many years, and significant spend, to build a Security Operations Centre that can deliver effective cyber security monitoring. Luckily, we have invested in building out that expertise and can support smaller organisations in improving their cyber security and help mitigate their risk at a fraction of the cost of doing it in-house. Whilst bringing Enterprise grade services into the budget of smaller organisations.

Microsoft Defender Service Coverage

The two e2e MDS offerings are targeted at M365BP customers, utilising one or more of the relevant Microsoft Defender services. Defender for Business forms the core service, to which further Defender services can be added as per the illustration below.

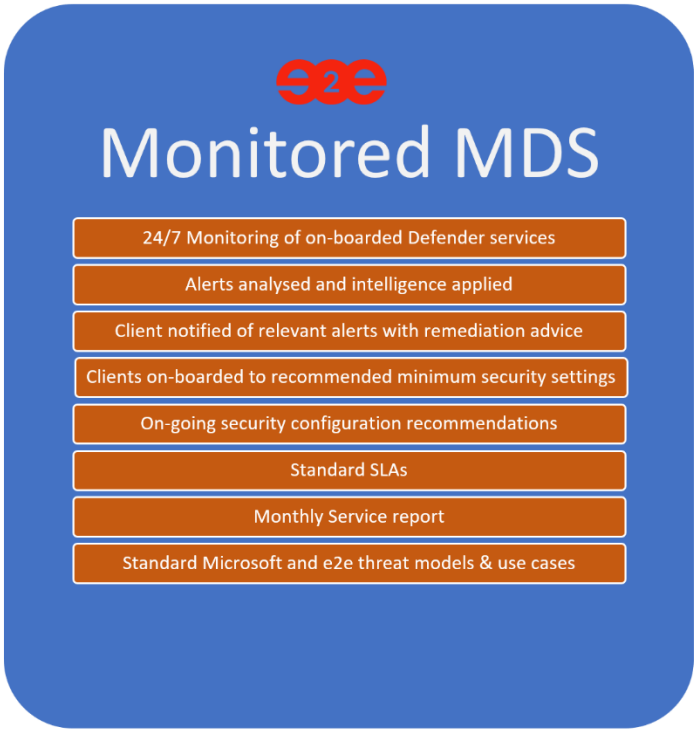
The e2e Microsoft defender Services (MDS) are available at two levels dependent upon the customers attitude to cyber risk and budget. Both services have Security Cleared e2e expert analysts monitoring the customers environments 24/7, these are Monitored and Managed.

Monitored MDS

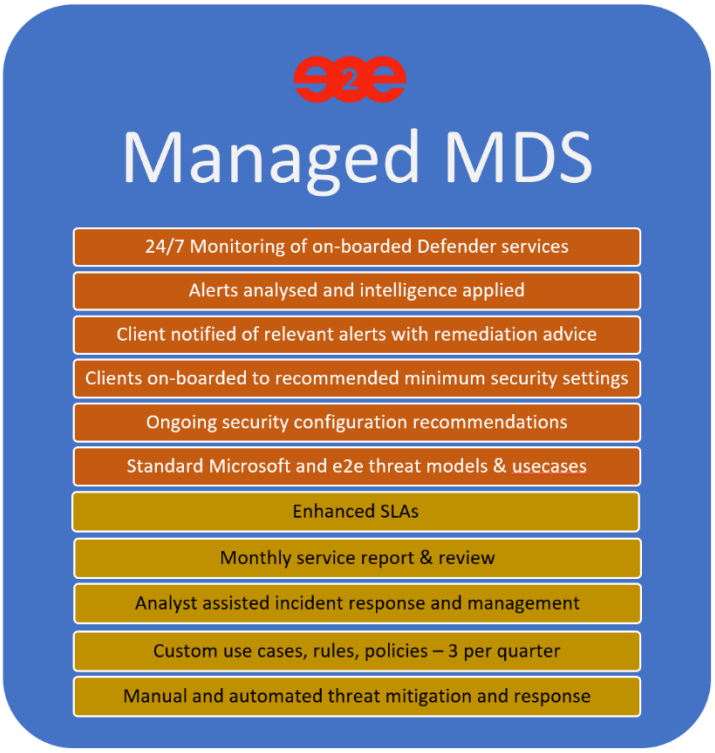
The e2e Monitored MDS service is designed to give base-line coverage of the Defender toolset whilst providing all the functionality listed on the right.

Remediation advice is delivered in a time relevant manner through the Microsoft Teams app.

A monthly report, covers both the service itself, including SLAs, and looks at security events which occurred during that month. This is complimented with advice on improving the customers security posture going forwards. This leverages both the Microsoft Defender toolset capabilities and the e2e proprietary management platform.



MANAGED MDS



The e2e Managed MDS service looks to build upon the features of the monitored service by adding extended functionality and higher service levels.

In addition to delivering the remediation advice the e2e analyst will work alongside the customer to resolve the issue and assist in building out automated responses to certain threats.

The monthly report is delivered by a collaborative Teams session where an analyst or consultant will discuss their findings and help prioritise any broader remediation plans.

Custom rules will also be created to address any customer specific scenarios.

SERVICE LEVELS

There are two constituent parts to the e2e MDS Service levels: Average response Time - to alerts, and the Uptime of the service.

Average Response Time (ART)

e2e categorise alerts into the four same categories as Microsoft. Generally High alerts require a response as soon as possible and informational are just that.

Microsoft Defender Service Levels			
Minutes		Monitored	Managed
High	ART	60	30
Medium	ART	90	60
Low	ART	90	60
Informational	ART	360	240

Note:
Average is calculated monthly per customer, based on all alerts we either closed or surfaced to the customer (including auto response from Defender)
SLAs are dependent upon a minimum number of alerts being generated
Resolution is customer's responsibility

Service Uptime

Both the Monitored and Managed services have a 99.9% uptime guarantee.
Note the Microsoft defender uptime SLA is 99.9%

PRICING

Pricing is on a per user per month basis, based upon the required service, Monitored or Managed. This is typically less than £6 pupm but is dependent upon numbers of users, numbers of services and is subject to a minimum spend.