https://www.e2e-assure.com/services-microsoft-defender

Microsoft Defender Services

Maximise your investment in Microsoft Defender

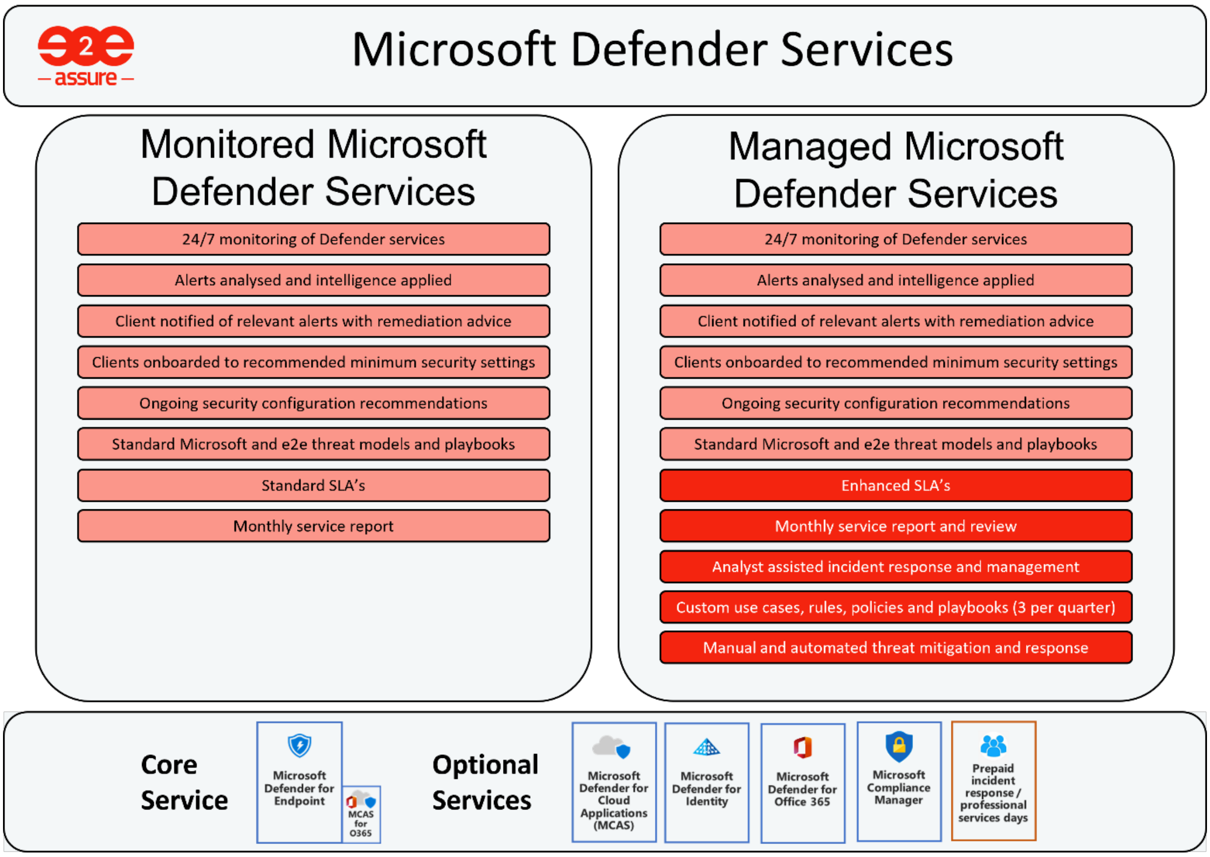
Microsoft Defender for Endpoint is one of the leading Endpoint Detection and Response (EDR) tools and one that many organisations have access to (via various Microsoft 365 licence options) but aren't getting the best out of. A major concern for most organisations is the ability to have eyes on it 24x7.

One of the biggest challenges in cyber security is the reliance upon technology, 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've spent a lot of time and money building out that expertise and can support all organisations in improving their cyber security and mitigating their risk at a fraction of the cost of doing it in-house.

What is the service?

We have two levels of service available, depending on your requirements, in-house teams and budget. The services are based on a simple per-user, per-month pricing, giving you flexibility as you grow, only paying for what you need today. The core services focus on monitoring and/or managing Microsoft Defender for Endpoint.

A top-level overview of the services is below, for more details, including SLA's, please ask for our service description document.



Microsoft Defender Services

Monitored Microsoft Defender Services

- 24/7 monitoring of Defender services
- Alerts analysed and intelligence applied
- Client notified of relevant alerts with remediation advice
- Clients onboarded to recommended minimum security settings
- Ongoing security configuration recommendations
- Standard Microsoft and e2e threat models and playbooks
- Standard SLA's
- Monthly service report

Managed Microsoft Defender Services

- 24/7 monitoring of Defender services
- Alerts analysed and intelligence applied
- Client notified of relevant alerts with remediation advice
- Clients onboarded to recommended minimum security settings
- Ongoing security configuration recommendations
- Standard Microsoft and e2e threat models and playbooks
- Enhanced SLA's
- Monthly service report and review
- Analyst assisted incident response and management
- Custom use cases, rules, policies and playbooks (3 per quarter)
- Manual and automated threat mitigation and response

Core Service

- Microsoft Defender for Endpoint
- MCAS for O365

Optional Services

- Microsoft Defender for Cloud Applications (MCAS)
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Compliance Manager
- Prepaid incident response / professional services days

info@e2e-assure.com

e2e-assure ltd

e2e-assure.com

@e2e-assure

Microsoft Partner Silver Security

https://www.e2e-assure.com/services-microsoft-defender

Whilst our core service offers a good starting point for many organisations by focusing on endpoints, we are aware that many organisations also deploy other Defender services. As part of the expanded services, we can leverage other Defender tools to improve the correlation of security events and enrich the data Analysts can investigate. Additional options include coverage for:

- Microsoft Defender for Cloud Applications (MCAS)
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Compliance Manager

As well as optional pre-paid incident response / professional service days.

We also have a roadmap to move customers to a bespoke managed Microsoft Sentinel service when they are ready, to both further improve their cyber security and maximise their investment in Microsoft technologies. As we don't sell Microsoft licensing, our only objective is to improve our customer's security and so we work with you to build a cyber roadmap, prioritising spending and proving ROI before investing in any future improvements.

How does it work?

With our monitored service, e2e's UK Security Cleared Analysts monitor your Microsoft Defender environment, 24x7, using their expert knowledge and standard processes to investigate alerts. With any alerts that require further investigation and/or remediation, this information is passed onto the customer, with remediation advice. A monthly report is also provided providing insight into the alerts and threats seen, with trends, that is used to improve the service and reduce noise for the customer.

With our managed services, customers get the same base service, with the addition of enhanced SLA's, a monthly review (on top of the report) and the addition of 3 bespoke processes (playbooks) per quarter. On top of this, our Analysts will also assist with incident response and management, should the customer wish, including manual and automated threat mitigation and response, in line with pre-agreed processes.

Who is it for?

In short, anyone who's looking to get the most out of their Microsoft Defender investment. Our Microsoft Defender Services focus on levelling the playing field of cyber security: aimed at smaller organisations looking to deploy cyber security monitoring on a budget and get started on the journey of continuous cyber improvement.

So what? Benefits and outcomes

We align the outcomes any of our services with best practice, such as the UK NCSC's CAF and US NIST frameworks. Whilst we offer advice on all elements of cyber security identified by these organisations, our core Microsoft Defender Services actively support with two key areas:

- **Detecting cyber-attacks** – customers of our Microsoft Defender Services benefit from additional e2e intelligence in enriching the data provided to your in-house team. This gives a broader view of the threat landscape and we help you focus on the most important cyber risks for you to remediate.
- **Responding to cyber-attacks** – whilst our Monitored Microsoft Defender Service doesn't offer active response from e2e, our Managed Microsoft Defender Service offers analyst assisted incident response, custom rules and processes plus a monthly review.