Endpoint Security Managed Service

Microsoft Defender for Endpoint

Every organisation needs to acknowledge and address the very real dangers posed by cyber threats. It is imperative to not only acknowledge these dangers but also take decisive action to fortify defences against potential breaches and attacks orchestrated by malicious actors. How do you defend your operations effectively at all times and reduce the potential areas of attack from malicious forces?

Microsoft Defender for Endpoint offers comprehensive threat prevention, detection, and response capabilities that enable your enterprise to prevent, detect, and respond to attacks across servers and workstations.

The Service

Our service is designed to manage your anti-malware deployment and ensure your organisation's endpoint security service is healthy and performing at optimal efficiency to deliver best practice security.

Our enterprise endpoint security platform is designed to help prevent, detect, investigate, and respond to advanced threats to your network. The 24x7x365 service integrates MTI's Service Desk as a cost-effective virtual member of your security team, analysing and notifying them of high-risk events and continually tuning the alerting process to ensure only abnormal events are escalated.

What MTI Provides

MTI Technology's managed services team assume all responsibility for the day-to-day operation and configuration of the Microsoft Defender for Endpoint service at all times.

The service provides core Defender vulnerability management, attack surface reduction, next-generation protection, endpoint detection and response, automated investigation, and remediation.

In the event of a security incident or data breach that falls within the scope of the devices monitored by Defender for Endpoint under the Managed Service, the service team will perform automated and/or manual responses to triage the incident and notify the correct contact in line with pre-agreed procedures.

The managed service includes:

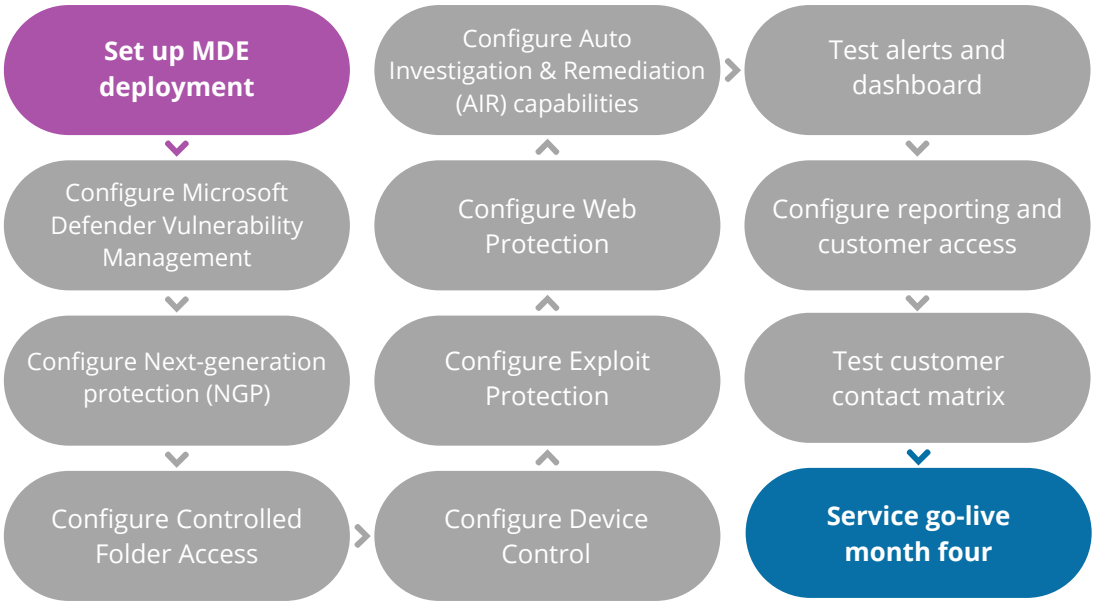
- Automated and immediate email/ticketing alerts in the event of a security incident
- SLA-backed notification of Alerts and Security Events (exact SLAs are agreed during the onboarding process and systematically monitored)
- Full access to Workbooks for data analysis and rich visual reports
- Full Incident handling
- Customer callout/contact matrix to cover 24x7x365 notifications
- Ongoing rule configuration
- Ongoing fine-tuning, incident suppression, data filtering
- Unlimited ad-hoc reporting
- Regular production of required reports from ingested data

Contact MTI
T: +44 (0) 1483 520 200
E: ukmarketing@mti.com
W: mti.com

Service Transition Period

A transition period is vital to implementing a successful Defender solution and will typically last for three months. Defender for Endpoint often exists alongside legacy endpoint security products either indefinitely or during a transition period.

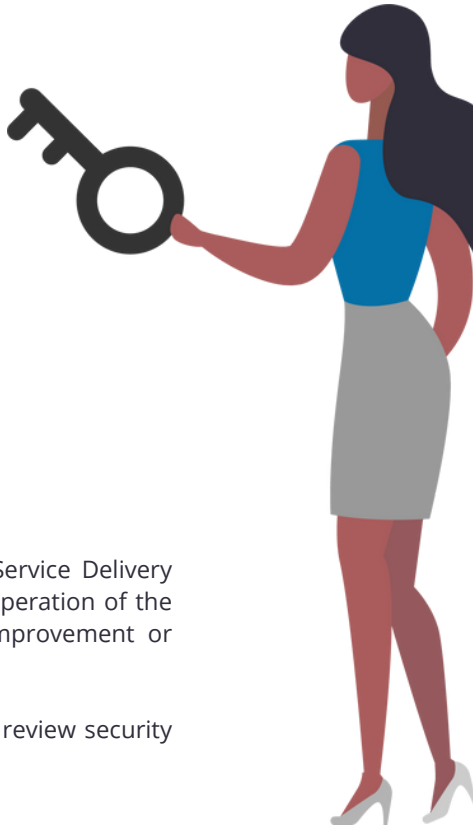
After onboarding devices to enable the endpoint detection and response capability of Microsoft Defender for Endpoint, MTI configures the other capabilities of the service, which include:



Health Checks

Where MTI does not install the products, we perform an initial health check of the existing installed solution to baseline the environment upon the award of the contract. These health checks will be conducted annually.

Once the health check of each product has been completed, we will generate a full report on findings and remediation to ensure awareness is raised of the overall health of the security solutions. Any remediation or changes required will be documented and agreed with you and implemented by our skilled engineers, following approval of a quotation for remediation works.



Service Delivery

After the initial design, onboarding, and transition phase is completed, your dedicated Service Delivery Manager will host regular monthly service delivery management meetings to review the operation of the managed service and ensure it continues to meet your needs. Any suggestions for improvement or additional requirements are factored into the operation of the service.

In addition to monthly service reviews, a bi-weekly technical meeting will be scheduled to review security threats and stay up to date on outstanding actions.

Contact MTI
T: +44 (0) 1483 520 200
E: ukmarketing@mti.com
W: mti.com

Reporting and Performance Reviews

MTI provides a named Service Delivery Manager as a liaison for the services delivered, available for escalations and concerns, and responsible for generating service reports. These reports form a comprehensive monthly reporting suite that serves as the basis for regular performance reviews.

The Monthly IT Service Management report will encompass, but not be limited to, the following:

Monthly ITSM Report

- Performance against agreed KPIs across all disciplines
- Account Relationship Status
- Service Status
- Commercial Status
- Business/IT Transformation Status
- Interpretation and analysis of reports
- Usage of Egress and ServiceNow Dashboard
- Client Feedback
- Incident and Service Request Breakdown
- Change Management reporting as required

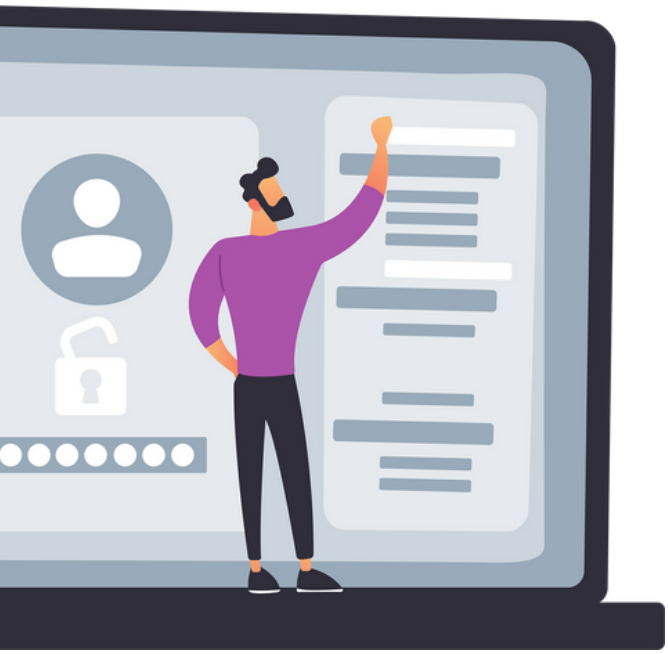
Monthly Technical Report

- Alarm & Threat Summary
- Summaries by Device Group
- Vulnerability Summary
- Microsoft Secure Score for Devices

The MTI Service Delivery Manager will conduct all service reviews, serving as a forum to discuss performance, escalations, risk, issues, and other salient matters.

> “MTI are our strategic cyber security partner of choice. Working together for over 10 years as an extension of our team. Our relationship is built on trust of the people we work with, experts in their field that we know will have our back.”
>
> **Abba Abbaszadi**
> IT Director, Charles Russell Speechlys

Charles Russell Speechlys



Why MTI

With over 20 years of security experience, MTI brings a wealth of expertise to safeguard your organisation's digital assets. As award winners in the field and with extensive experience in security solutions and penetration testing, we offer a comprehensive suite of services designed to fortify your defences.

As a founding member of the global cybersecurity body, CREST, we have developed a deep understanding of the tactics employed by malicious users to infiltrate corporate networks, allowing us to identify and mitigate any risks to your business.