A RICOH Company

29 January 2026

Trend Micro Vision One MTI Managed XDR Service

Ref no: G-Cloud 15

PREPARED BY

MTI Technology

COPYRIGHT

TABLE OF CONTENTS

1.0 SERVICE OVERVIEW

- **1. Service Summary**

MTI's Trend Vision One Security Managed Service provides 24/7/365 operational management of Trend Micro Trend Vision One for endpoint protection, detection and response. The service combines continuous monitoring, incident triage and response, policy and sensor tuning, cyber risk exposure reporting, and regular service reviews to maintain a healthy, effective endpoint security service.

- **1.1 Customer outcomes**
  - Reduced time to detect and respond to endpoint threats through 24/7 monitoring and triage.
  - Improved security posture through continuous visibility, risk scoring and prioritised remediation guidance.
  - Consistent application of endpoint security policy and configuration across the estate.
  - Clear, actionable reporting for operational and governance stakeholders.
  - A defined and auditable incident handling process with agreed communications and escalation paths.

- **1.2 Underpinning technology (Trend Vision One)**

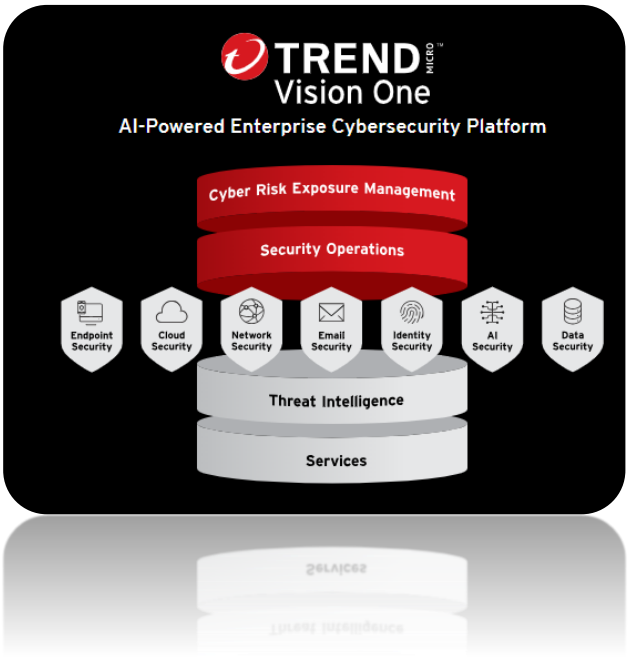
Trend Vision One is a cloud-native cybersecurity platform that centralises endpoint security, security operations (XDR), and cyber risk exposure management. This managed service uses the Trend Vision One console to manage endpoint inventory, detections, response actions, policies, and reporting.

- **1.3 Service components (within purchased entitlements)**

Area	Description
Endpoint Security	Layered endpoint protection with integrated EDR/XDR for faster detection and response
Security Operations	Investigation and response workflows supporting alert triage, correlation, and incident handling
Cyber Risk Exposure Management (where licensed)	Attack surface discovery and risk visibility to support prioritised remediation planning
Automation and Response Management	Execution of supported response actions and playbooks, subject to approvals

2.0 SCOPE OF DELIVERY

- **2.1 In-scope assets**

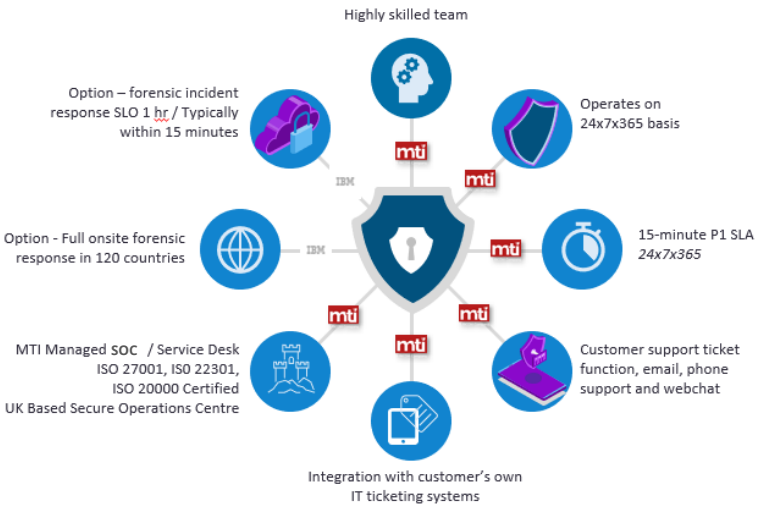


Endpoints and servers with Trend Vision One endpoint security sensors/agents installed and reporting.

Associated Trend Vision One telemetry and detections generated by those assets.

Optional: additional sensors (email, network, collaboration, cloud) where included in the customer's Trend Vision One licensing and explicitly added to scope.

- **2.2 Included**
- Service onboarding and transition (health check of existing deployment, operational readiness, and tuning).
- Configuration and day-to-day management of Trend Vision One XDR Security policies and sensors (within entitlements/credits).
- 24/7/365 monitoring of alerts and detections, including triage, validation, and customer notification.
- Incident handling for in-scope assets, including supported automated and manual response actions via Trend Vision One.
- Ongoing policy tuning, suppression management, and data filtering to reduce noise and improve signal quality.
- Configuration of dashboards and scheduled reporting packs; unlimited ad-hoc reporting within reasonable use.



- Service management, including a named Service Delivery Manager and regular service review meetings.

- **2.3 Exclusions**

End-user device build/refresh activities and general desktop support not directly related to endpoint security.

Remediation activities that require changes outside Trend Vision One (for example, OS rebuild, application patching, identity platform changes), unless separately scoped as professional services.

Forensic investigation and recovery services beyond initial triage/containment (optional add-on – see Section 9).

Endpoint agent deployment at scale where the customer retains tooling and ownership (optional MTI professional services can be provided).

Third-party product administration unless explicitly included as an integration and covered by agreed runbooks.

- **2.4 Service assumptions and dependencies**

The customer maintains valid Trend Vision One licences/credits for the required features and sensor coverage.

The customer provides appropriate administrative access (least privilege) for MTI to operate Trend Vision One and execute agreed response actions.

Endpoints can communicate with Trend Vision One services (network routes, firewall exceptions, proxy settings and DNS).

A customer ticketing integration (or agreed alternative) is available to create/update incidents and service requests.

A customer call-out/contact matrix is agreed and maintained to support 24/7 notifications.

The customer nominates a service owner and technical contacts to support governance, change approvals and remediation actions.

3.0 SERVICE OPERATING MODEL

- **3.1 Service hours**

Monitoring, triage, and incident notification are provided 24/7/365. Service management activities (service reviews, reporting walkthroughs, change planning) are typically delivered during UK business hours unless otherwise agreed.

- **3.2 Roles and responsibilities (high level)**

The service is delivered as a shared responsibility model:

Stakeholder	Responsibilities
MTI Managed Services	Operate Trend Vision One per service definition; monitor, triage, respond, and report; maintain service documentation and runbooks
Customer IT/Security	Own business decisions and risk acceptance; approve/authorise response actions; perform out-of-tool remediation (patching, rebuilds, account actions); provide timely inputs
Trend Micro	Provide product support, platform availability, and product updates as per customer agreement

- **3.3 RACI (summary)**

RACI key: R = Responsible, A = Accountable, C = Consulted, I = Informed

Activity	MTI	Customer	Trend Micro
Platform configuration and policy management	R	A/C	
24/7 monitoring and alert triage	R	A/C	
Incident notification and comms	R	A/C	
Execute Trend Vision One response actions	R	A (approve)/C	
Out-of-tool remediation (patching/rebuilds/account admin)	C	R/A	
Service reviews and reporting	R	A/C	
Product support case with vendor	A	C/I	R
Annual health check	R	A/C	

- **3.4 Customer access and visibility**

The customer retains access to the Trend Vision One console (role-based access). MTI will agree visibility scopes, reporting requirements and access for operational and governance stakeholders.

- **3.5 Service requests and change control**

All service requests and changes are logged and tracked. Changes that may materially affect security posture, user experience, or availability are subject to change control and, where appropriate, customer approval. Emergency changes may be implemented to contain active threats and will be documented retrospectively.

4.0 MONITORING, ALERTING AND INCIDENT MANAGEMENT

- **4.1 Alert intake and triage**

MTI monitors Trend Vision One alerts and detections for in-scope assets. Each alert is triaged to determine scope, severity, confidence, and required response. MTI uses available correlated context and investigation views to reduce false positives and prioritise actions.

- **4.2 Ticketing and customer notification**

When an incident is confirmed or requires customer action/awareness, MTI will open a ticket and notify the appropriate customer contacts in line with the agreed contact matrix. Notifications include severity, affected assets, summary of observed activity, actions taken (if any), and recommended next steps.

- **4.3 Configuration Management, Monitoring, Investigation**

After transition, health check and any required platform remediation are complete, MTI will take on all day-to-day configuration management, investigation/triage, and response to alerts and incidents. Examples of key areas managed by MTI through our MXDR service include:

Activity Area	Managed XDR Activities (Trend Micro Vision One)
Identity Telemetry & Access Context	Monitoring user identity signals, access events, and authentication context to support threat detection and investigation.
Endpoint Fleet Oversight	Onboarding, monitoring, and health management of endpoints providing telemetry into the XDR platform.
Endpoint Protection Operations	Managing endpoint security policies, prevention controls, and configuration baselines aligned to best practice.
Workload Protection Operations	Securing and monitoring server, virtual, and container workloads integrated into XDR detection and response workflows.
Endpoint Detection & Response (EDR)	Continuous monitoring of endpoint telemetry, threat detection, investigation, and guided or automated response actions.
Network Threat Visibility	Correlating network telemetry and detections to identify lateral movement, command-and-control, and network-based threats.
Cloud Security Monitoring	Ingesting cloud workload, posture, and activity telemetry to detect misconfigurations and cloud-based attack paths.
Email & Collaboration Threat Detection	Monitoring email and collaboration signals to identify phishing, malware, and account compromise activity.

Security Policy Lifecycle Management	Implementing, tuning, and maintaining security policies to balance protection efficacy and operational impact.
Alert Triage & Prioritisation	24×7 monitoring, enrichment, severity assessment, and escalation of XDR alerts and incidents.
Threat Detection, Investigation & Response	Correlating cross-domain telemetry, validating incidents, and executing containment or remediation actions.
Subscription & Feature Management	Managing platform entitlements, feature enablement, and licence utilisation to maximise service coverage.
Platform & Service Health Monitoring	Monitoring sensor health, data ingestion, and service availability to maintain effective detection coverage.
Integration & Automation Enablement	Managing integrations with SIEM/SOAR and leveraging automation and playbooks to accelerate response.

- **4.3 Response actions (containment and remediation)**

Where agreed and supported, MTI can execute Trend Vision One response actions to contain and remediate threats. Actions are performed in line with pre-agreed runbooks and the customer's response approval settings. Examples include:

Response Action	Description
Add to Block List	Block supported indicators such as hashes, URLs, IPs, and domains for subsequent detections
Isolate Endpoint	Disconnect the endpoint from the network except for Trend Micro management; restore connection when safe
Terminate Process	Stop an active malicious process on affected endpoints
Scan for Malware	Trigger a one-time scan for file-based threats
Collect Evidence / Collect File	Gather artefacts to support investigation and incident response (subject to approvals)
Disable User Account	Sign the user out and prevent new sessions where supported and in scope
Quarantine Message	Quarantine inbound messages where email/collaboration sensors are in scope

- **4.4 Communications and escalation**

MTI follows the agreed call-out matrix for out-of-hours notifications. P1 and P2 incidents typically require phone call escalation 24/7/365, with P3/P4 handled as agreed (for example, email out of hours). Escalations to customer leadership and third parties are performed as per agreed procedures.

- **4.5 Evidence and audit trail**

All investigation steps, notifications, and response actions are recorded in the incident ticket to provide a clear audit trail. Evidence collection requests are handled in line with customer approvals and data handling requirements.

- **4.6 Incident severity model**

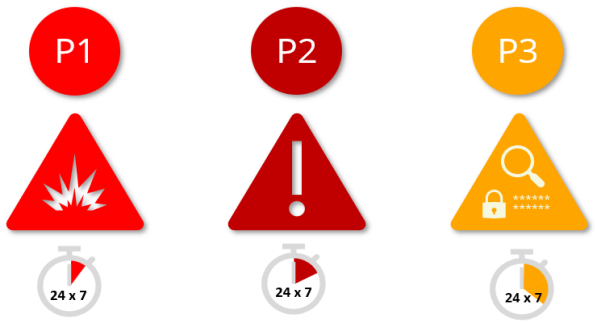
Incident severity is agreed during onboarding. As a default, MTI uses the following interpretation:

Priority	Description
P1 – Critical	Active compromise, widespread malware or ransomware, or imminent business impact requiring immediate containment
P2 – High	Confirmed malicious activity with limited impact or scope, or high likelihood of escalation if not quickly contained
P3 – Medium	Suspicious activity requiring investigation and/or customer action, with limited immediate impact
P4 – Low	Informational events, benign positives, or hygiene items tracked for trend reporting

5.0 SERVICE LEVELS AND KPIS

- **5.1 Service level targets (SLAs)**

SLAs are agreed during onboarding and are measured from alert receipt/visibility to customer notification for confirmed or actionable incidents. Default SLA targets include:



Alert SLA:	15 mins	15 mins	1 hour
Response SLA:	+15 mins	+30 mins	+1 hour

Incident Level	Detect (within)	Respond (within)	Resolve/ Mitigate (within)	Customer Notification (within)
P1 – Critical	15 minutes	15 minutes (from detection)	4 hours	Immediate (updates every 30 minutes)
P2 - High Priority	15 minutes	30 minutes (from detection)	8 hours	Immediate (updates every 2 hours)
P3 – Medium/Low Priority*	1 hour	1 hour (from detection)	24 hours	1 hour (updates every 4 hours)
P4 - Informational*	24 hours	8 hours (in-office hours)	5 business days	1 business day

* Out-of-hours response will only be initiated for Severity 3 and Severity 4 alerts where such action has been explicitly identified and agreed as a customer requirement during the transition process. All other Severity 3 and 4 alerts not classified as critical will be addressed during standard business hours on the next working day. This policy ensures alignment with agreed service levels, prevents unnecessary escalation, and enables priority to be placed on genuinely critical events during periods when customer resources are limited. Low Risks are summarised in a scheduled report, which can be run at any interval preferred by the customer agreed during transition. Most customers settle on a monthly report for Low Priority alerts. SLA exclusions may apply where customer approvals, third-party dependencies, or endpoint connectivity prevents timely execution. MTI will document any SLA-affecting constraints within the incident record.

- **5.2 Key performance indicators (KPIs)**

KPIs are reviewed during monthly service reviews and tailored to customer priorities. Typical KPIs include:

Metric	Description
Coverage	Percentage of in-scope endpoints onboarded and reporting
Sensor Health	Percentage of endpoints reporting expected telemetry and protection modules
SLA Compliance	Percentage of incidents notified within SLA, by priority
Noise Reduction	Trend in false positives and suppressed alerts over time
Response Effectiveness	Response actions executed and time-to-contain P1/P2 incidents
Remediation Closure	Percentage of agreed actions closed within target timeframes

6.0 ONBOARDING, TRANSITION AND ACCEPTANCE

MTI follows a structured onboarding approach designed to establish visibility, validate sensor coverage, agree operational processes, and tune detections before service go-live.

- **6.1 Transition timeline**

The transition period typically lasts three months, with service go-live in month four, subject to successful operational readiness and sensor coverage.

- **6.2 Onboarding deliverables**
  - Confirmed scope and endpoint inventory (in-scope device groups).
  - Agreed contact matrix and escalation paths.
  - Agreed incident severity model and runbooks.
  - Configured Trend Vision One tenant/console settings (RBAC, visibility scopes, reporting access).
  - Validated sensor/agent coverage and endpoint protection policy baseline.
  - Operational readiness sign-off and go-live plan.

- **6.3 Onboarding activities**
  - Kick-off and discovery: confirm scope, endpoint inventory, stakeholder contacts, and existing controls.
  - Deployment planning: confirm agent/sensor deployment method, network requirements, and any coexistence constraints.
  - Tenant/console configuration: roles, permissions, access controls, and customer access.
  - Sensor enablement and coverage validation: confirm endpoints are reporting; validate telemetry and key security features.
  - Policy baseline: align endpoint protection policies and exception lists to organisational requirements.
  - Alert workflow configuration: ticketing integration, severity mapping, notification routing, and response approval settings.
  - Runbook creation and testing: validate alert generation, response actions, dashboards, and call-out procedures.
  - Tuning period: iterative reduction of noise and alignment of detections with customer context.
  - Service go-live and steady-state handover to BAU operations.

- **6.4 Acceptance criteria (go-live)**
  - In-scope endpoints are onboarded and reporting at an agreed coverage threshold.
  - Alert-to-ticket workflow is validated end-to-end (including customer ticketing integration).
  - Call-out/contact matrix is tested and confirmed.
  - Response action approvals and runbooks are agreed and tested (where applicable).
  - Reporting pack format and cadence are agreed.
  - Initial tuning backlog is agreed with owners and timescales.

- **6.5 Coexistence and cutover**

Where migrating from an existing endpoint security product, MTI will support an agreed coexistence/cutover plan, including phased deployment, policy alignment and reporting to demonstrate equivalent or improved control coverage.

7.0 REPORTING, DELIVERABLES AND SERVICE REVIEWS

- **7.1 Core deliverables**
  - 24/7/365 monitoring and incident triage for in-scope assets.
  - Incident tickets and customer notifications aligned to the contact matrix.
  - Execution of agreed response actions (subject to approvals).
  - Monthly service report pack and monthly service review (SDM).
  - Bi-weekly technical review (where required/contracted).
  - Annual health check report and improvement plan.

- **7.2 Monthly reporting pack (typical content)**
  - Service performance against KPIs and SLAs.
  - Incident and service request breakdown (volumes, severity, trends, response actions taken).
  - Threat summary (top detections, attack techniques observed, recurring sources).
  - Endpoint coverage and sensor health (onboarded vs expected; failures and gaps).
  - Cyber risk exposure highlights (for example, risky devices, accounts and internet-facing assets where licensed).
  - Recommendations and prioritised actions for risk reduction.

- **7.3 Service review cadence**

A named Service Delivery Manager (SDM) provides monthly service review meetings. A bi-weekly technical meeting may also be scheduled to review threats, outstanding actions, and tuning activities, where required.

- **7.4 Ad-hoc reporting (reasonable use)**

Ad-hoc reporting is provided on request. Requests that require significant bespoke development or third-party data enrichment may be treated as a separate professional services activity.

8.0 HEALTH CHECKS AND CONTINUOUS IMPROVEMENT

Health checks validate that Trend Vision One endpoint protection, sensors, and operational workflows remain effective. Where MTI does not perform the initial deployment, an initial baseline health check is completed at service start.

- **8.1 Frequency**

Baseline on service start (where applicable) and annually thereafter, or more frequently by agreement.

- **8.2 Health check coverage (typical)**

A Brief overview of the Health Check areas is shown below for brevity. Full details are shown in *Appendix - Trend Micro Vision One Health check.*

Area	Description
Endpoint Inventory and Coverage	Confirm all in-scope endpoints are reporting and have required protection modules enabled
Security Feature and Sensor Coverage	Review enabled features and XDR sensors to ensure adequate telemetry for detection and investigation
Policy Assurance	Review endpoint protection policies, exclusions, and exception handling
Response Readiness	Validate approvals, runbooks, and access controls for response actions
Risk Posture (where licensed)	Review discovered assets and prioritised remediation opportunities
Reporting and Audit	Validate report outputs and evidence trails in incident tickets

- **8.3 Outputs**

  - Health check findings report (configuration gaps, coverage gaps, and risks).
  - Prioritised remediation plan with recommended actions and owners.
  - Agreed improvement backlog for ongoing optimisation.

9.0 OPTIONAL ADD-ONS

- **9.1 Emergency Incident Response (forensics and recovery)**

To complement the managed service, MTI offers an optional Emergency Incident Response service for P1/critical cyber incidents. The service is delivered via MTI's trusted partner IBM, who provide global incident response teams and a network of global SOCs to deliver remote and on-site forensic investigations and support.

- Access to a global incident response team for rapid triage (target within one hour).
- On-site support typically within 24 to 48 hours (location dependent).
- Forensic investigation to determine attack timeline, access obtained, and potential data exposure.
- Remediation advice and guidance on technical fixes and hardening actions.

When purchased with MTI's managed service, MTI will work with the investigators and the customer throughout the incident, providing relevant data and executing authorised Trend Vision One response actions as needed.

10.0 SECURITY, PRIVACY AND COMPLIANCE

- **10.1 Access control and auditability**

MTI operates the service in line with agreed security requirements and least privilege access principles. Access to the Trend Vision One console is role-based and auditable.

- **10.2 Data handling and retention**

Customer data processed within Trend Vision One remains the customer's data. MTI will not export customer data except where required for incident handling, reporting, or at the customer's request, and in line with agreed data handling requirements. Data retention is governed by the customer's Trend Micro entitlements and configuration choices.

11.0 GLOSSARY

Term	Description
Trend Vision One	Trend Micro's cloud-native platform centralising cyber risk management, XDR, and layered protection
XDR (Extended Detection and Response)	Correlates telemetry across multiple security layers for higher-fidelity detections and incident context
EDR (Endpoint Detection and Response)	Endpoint-focused detection and investigation capabilities
Sensors	Telemetry and protection components providing visibility and detection coverage within Trend Vision One
Response Actions	Approved actions executed via Trend Vision One to contain or remediate threats (e.g., isolate endpoint, terminate process)
CREM (Cyber Risk Exposure Management)	Capabilities for asset discovery, risk scoring, and exposure visibility (licence/credits dependent)

12.0 APPENDIX - TREND MICRO VISION ONE HEALTH CHECK

As part of the onboarding process, MTI conduct a health check of the platform to be onboarded into the managed service. MTI's Health Check delivers a comprehensive review of the Trend Vision One deployment, conducted remotely via secure access to the platform's console. The review will examine key configuration areas and policies directly within the console, ensuring alignment with best practices and organisational requirements. As part of this process, a sample of alerts and detections will be assessed to confirm that threat monitoring and alerting functions are performing effectively.

- **12.1 Assessment Areas**

The review is conducted across licensed elements within the Trend Vision One platform, as relevant and applicable to your environment and may include the following areas:

Category	Assessment Areas
User & Access Management	• User Accounts • User Roles and Permissions (RBAC) • Single Sign-On (SSO) integration • Access Control
Device Management	• Endpoint Inventory • Grouping & Tagging • Agent Deployment Coverage • Agent Health • Device Visibility in Vision One • Orphaned Devices Review
Endpoint Security	• Endpoint Coverage • Security Policy Configuration • Malware, Ransomware, Exploit Protection • Application Control / Device Control • Behaviour Monitoring • Pattern File & Engine Updates
Workload Security	• Workload Inventory • Agent / Agentless Deployment • Policy Enforcement • Update & Patch Compliance • Cloud Connector Integrations • Visibility of Unprotected Workloads
Endpoint Sensor (EDR)	• Sensor Coverage & Deployment Status • Telemetry Quality & Event Visibility
Network Security	• Proxy & Network Configuration • Network Sensor Deployment • IPS/IDS Rule Sets

Cloud Security	• Cloud Account Linking (AWS, Azure, GCP) • Posture Management (misconfigurations, compliance templates) • Workload & Container Discovery • Runtime Protection (container/Kubernetes) • Cloud Event Visibility in Vision One • Threat Detection & Response in Cloud Workloads
Email & Collaboration Security	• Integration with M365 / Exchange • Collaboration App Coverage (Teams, SharePoint, OneDrive) • Reporting on blocked/phished mail and collaboration threats
Policy Management	• Security Policies per module (Endpoint, Workload, Network, Email, Cloud) • Policy Tuning & Exclusions • Policy Enforcement Status & Gaps
Alerts & Notifications	• Alert Settings & Thresholds • Notification Channels
Threat Detection & Response	• Incident & Threat Investigation Workflows • XDR Correlation across Endpoint, Email, Network, Cloud • Sensor Telemetry Quality • Automated Response Actions • Playbook Testing & Validation
Subscription & Licensing	• Tenant Subscription Details • License Usage and allocation by module • Unused entitlements review
Platform & Service Health	• Platform Status Overview • API Health & Connectivity • System Performance & Reliability
Integration & Automation	• SIEM & SOAR Integrations • API Credential & Key Management • Automation Jobs & Playbooks • Integration with ITSM • 3rd Party Threat Intelligence Feed Ingestion

- **12.2 Formal Report Output**

The findings of the health check will be documented in a formal report. This will include:

- An Executive Summary section providing concise, high-level insights for leadership and stakeholders
- An Issue Matrix of Identified Issues comprising: Area, Issue Title, Risk/Severity, and Remediation Action Title
- Results and observations against platform health, configuration status, and alert handling
- Detailed recommendations for optimisation, remediation, or further action, including [where available] links to specific vendor documentation to assist with resolution.

13.0 ABOUT MTI

MTI Technology is a technology services and solutions provider with over 200 staff, operating across EMEA with offices in the UK and Germany. Over the last 36 years, MTI has helped thousands of organisations transform their IT operations, enabling them to leverage the latest technologies, reduce operating costs, become more flexible, and mitigate risk.

MTI has considerable experience in designing, delivering, and managing cybersecurity and data centre solutions for our customers across various industry sectors, including Commercial, NHS, central government, local government, Banking, Defence, Finance, and Insurance. This extensive experience ensures your solution is designed and installed by industry-leading MTI experts, guaranteeing a smooth, accurate, and on-time project delivery.

MTI specialise in cybersecurity, data centre modernisation, IT managed services and IT transformation. By employing proven methodologies and best practices, and adopting a consultative approach, MTI helps its customers solve business challenges and provides secure, compliant management of their applications, data, infrastructure, and system environments.

13.1. ACCREDITATIONS

MTI hold the following ISO Standards and Certifications

- ISO 27001 Information Security Management system
- ISO 9001 Quality Management System
- ISO 20000 IT Service Management
- ISO 45001 Occupational Health and Safety Management
- ISO 22301 Business Continuity Management System
- ISO 14001 Environmental Management System
- Cyber Essentials & Cyber Essentials Plus
- NCSC CHECK Scheme Member (CHECK 'Green Light' company since 2003)
- CREST Scheme Member

13.2. AWARDS

Our dedication to maintaining high standards is reflected in our numerous industry awards, including Dell Specialist Partner of the Year 2024, Dell Exceptional Services Delivery Performance 2024, Dell Advanced Services Delivery Partner 2024, Cyber Security Customer Service Award at the Computing Security Awards 2024, Cybersecurity/Data Protection Partner of the Year Award at the CRN Awards 2024, CRN MSSP/Security Reseller of the Year 2023, CRN Security Value Added Reseller (VAR) of the year for 2018, 2019, and 2020, and Penetration Tester of the Year for 2018 and 2020. We have won the UK Service Partner of the Year award twice for excellence in service delivery, in 2023/2024. MTI is committed to delivering exceptional customer service, which is why we have an industry-leading 98% customer satisfaction rating.

13.3. KEY PLATFORMS

MTI is proud to be a Dell Technologies Titanium Black Partner, the highest tier in Dell's Global Partner Program. This elite recognition positions MTI among a select group of global partners that demonstrate exceptional technical expertise, strategic alignment, and a consistent ability to deliver transformational outcomes for customers in today's data-driven, multi-cloud world.

Other key partners include:

13.4. ENVIRONMENTAL, SOCIAL AND GOVERNANCE (ESG), CSR & SOCIAL VALUE

MTI integrates ESG, CSR and Social Value principles into our business values and operations to meet the expectations of customers, employees, investors, suppliers, the community, and the environment. Our Policy governs responsible and ethical conduct, a positive working environment, support for local communities, fair dealings with suppliers, and respect for human rights.

Environmental Management

MTI maintains a documented Environmental Policy Statement, approved by senior leadership, and reviewed annually. Our **ISO 14001 Environmental Management System** incorporates policies and procedures to manage, reduce, and report environmental impacts. We are committed to **Net Zero by 2050** and have achieved **EcoVadis Gold** standard for Social Value policies and procedures.

Sustainability Activities and Achievements

- **Planting of ~600 trees annually** to neutralise our carbon footprint (in partnership with Treedom). Treedom plants a tree on our behalf across Africa, South-East Asia and South America to offset MTI's carbon emissions. They are a certified B Corporation, and every tree on their site has its own online page for tracking. To date, MTI has planted 3,299 trees, resulting in a 6.17 mt CO2e reduction and driving positive social and environmental impact.
- Reduction targets for business travel, including a digital-first approach, increased virtual meetings, and reduced travel emissions.
- **In 2023, we took one step closer as we are proud to say all our company vehicles are electric.**
- Transition to homeworking/hybrid models, reducing commuting and office energy consumption.
- Use of renewable energy sources for office electricity and optimisation of lighting, heating, and cooling systems.
- Eradication of single-use plastics in all offices.
- Implementation of cloud-based applications to reduce energy consumption.
- Collaboration with carbon-neutral suppliers and annual Supplier Sustainability Assessments.
- Comprehensive waste management systems, with recycling and mandatory staff training.
- Ongoing achievement of ISO 14001:2015 Certification.

Social Responsibility and Value Creation

- Dedicated ESG committee overseeing strategy, risk management, compliance, stakeholder engagement, and continuous improvement.
- Social Value Development Plan tracked by an ESG Manager, with regular reviews and reporting.
- Employer-supported volunteering, offering employees charity days tracked via our ESG application. MTI employees have completed 1,088 hours of volunteering.
- Initiatives supporting disadvantaged groups, including participation in the Disability Confident Scheme.

- Commitment to equal opportunity, diversity, and inclusion in the workplace.
- MTI support Cystic Fibrosis Charity through fundraising events, employee challenges and donations.

Governance and Assurance

- Regular supplier assurance activities and annual Supplier Code of Conduct refresh.
- Compliance with ILO standards, UN Global Compact, and Universal Declaration of Human Rights.
- Board-level reporting of CSR compliance and performance.

Public Disclosure and Transparency

- Annual publication of Carbon Reduction Plan/ESG Report on MTI's website - https://mti.com/about/corporate-social-responsibility/
    - https://mti.com/wp-content/uploads/2025/10/MTI_Carbon-Reduction-Plan_FY2024.pdf
- Enhanced reporting of ESG performance and promotion of industry certifications - https://mti.com/wp-content/uploads/2025/12/ESG-Report-FY24.pdf

Head Office

MTI Technology Limited

3 Lotus Park First Floor

The Causeway

Staines-Upon-Thames

TW18 3AG

Reception: +44 (0) 1483 520 200

Service Desk: +44 (0) 1483 520 349

Web: www.mti.com

About MTI

MTI provides award-winning, end-to-end technology solutions and services across cybersecurity and data centre infrastructure, supporting customers for over 35 years. With over 250 specialists across the UK, France and Germany, we deliver expert consultancy, project delivery, and scalable managed services.

Our mission is to build a secure digital future for our customers. We do this by combining deep technical expertise with a consultative, proven approach – helping organisations accelerate and de-risk transformation while ensuring secure, compliant management of applications, data and IT systems.