MTI Anti Malware Security Managed Service

MTI's Anti-malware solution provides next generation Hybrid Cloud Server & End Point protection that combines a Gartner leading technology platform with MTI's 24*7*365 UK based security team.

1. Trend Micro Deep Security-as-a-Service – for server protection
2. Trend Micro Apex One-as-a-Service – for endpoint protection

The solution is:

- A world leading Next Generation anti-malware product
- Fully hosted in the cloud
- Fully deployed, configured and managed by MTI Technology
- Includes managed malware response in line with pre-agreed actions using anti-malware software
- Fully managed from MTI's UK based 24*7*365 Security Operations Centre

MTI Managed Security Services will plan, integrate, and configure the full deployment of both products to all servers and endpoints and assume responsibility for every aspect of managing the anti-malware service and software, as well as responding to malware events. In essence, the MTI Managed Service Desk will become a helpdesk extension our customers, with the end user contacting MTI directly for any anti-malware help, such as unblocking a file, URL, application etc in line with our pre-arranged processes with you and also includes the response to malware outbreaks in line with agreed actions.

Regular Service Delivery meetings will be held with you to ensure the service is being delivered to expectations and full regular and ad-hoc reporting will be implemented to provide you with any information required, such as users constantly violating policies, clicking URL's etc.

Why Trend Micro?

Trend Micro has a strong history of constant innovation to provide the most effective and efficient security technologies and are always looking ahead to develop the technologies needed to fight tomorrow's ever-changing threats.

- Over 30 years of security innovation
- Protects over 250 million endpoints
- Trusted by 48 of the top 50 global corporations as the primary anti-malware protection
- Clear leader in the 2019 Gartner Magic Quadrant for Endpoint Protection Platforms (EPP), and every year since 2002

MTI have been a Gold partner with Trend Micro for over 15 years and have installed, configured and managed hundreds of complete anti-malware deployments for public and private sector clients across the globe.

A strong integration between the different Trend Micro products means that consistent security polices and protections can be applied across all endpoints, servers, networks and applications. Many enhancements can be utilised with other components within the Trend Micro suite of protections in the future if specific needs arise, such

as automated incident response, network traffic inspection and a world leading network-based Intrusion Prevention System (IPS).

All Trend Micro products in our solution are Next Generation and include:

- Advance Threat Detection
- Global and Local Threat Intelligence Updates
- Machine Learning
- Known and Unknown Vulnerability Protection
- Exploit Protection
- Application control (whitelisting / blacklisting)
- Reputation based analysis of suspicious objects
- Data Loss Prevention Controls
- Hard Drive Encryption (if required – at no extra license cost)
- Virtual Patching for unsupported and supports software and Operating Systems

Trend Micro solutions incorporate many protection techniques, including highly effective traditional approaches like anti-malware, intrusion prevention, whitelisting, encryption and data loss prevention. They also include new state-of-the-art techniques like high-fidelity machine learning and behaviour analysis to catch advanced threats like ransomware.

Benefits of Trend Micro Protection

Trend Micro products are powered by their unique XGen technology. This delivers a blend of threat defence techniques that are **Smart, Optimised** and **Connected** to protect endpoints, servers and applications across the enterprise, all while preventing business disruptions and helping with regulatory compliance.

Smart

Protects against the full range of known and unknown threats using a range of sophisticated threat defence techniques, which apply the right detection and prevention technique at the right time, powered by global threat intelligence. This means if a new malware attack is detected anywhere in the globe, the Threat Intelligence database is updated and all your Trend Products will know about the attack and how to best stop it. This Threat Intelligence is shared amongst all Trend Micro customers who utilise their XGen products to provide almost real-time protection against new threats and attacks as soon as they are detected, and also take in multiple other threat update feeds from government agencies, such as NCSC, NSA and other leading anti-malware vendors. This all combines to provide effective protection against new variants of malware, ransomware and other attacks as soon as they are detected “in the wild”.

Optimised

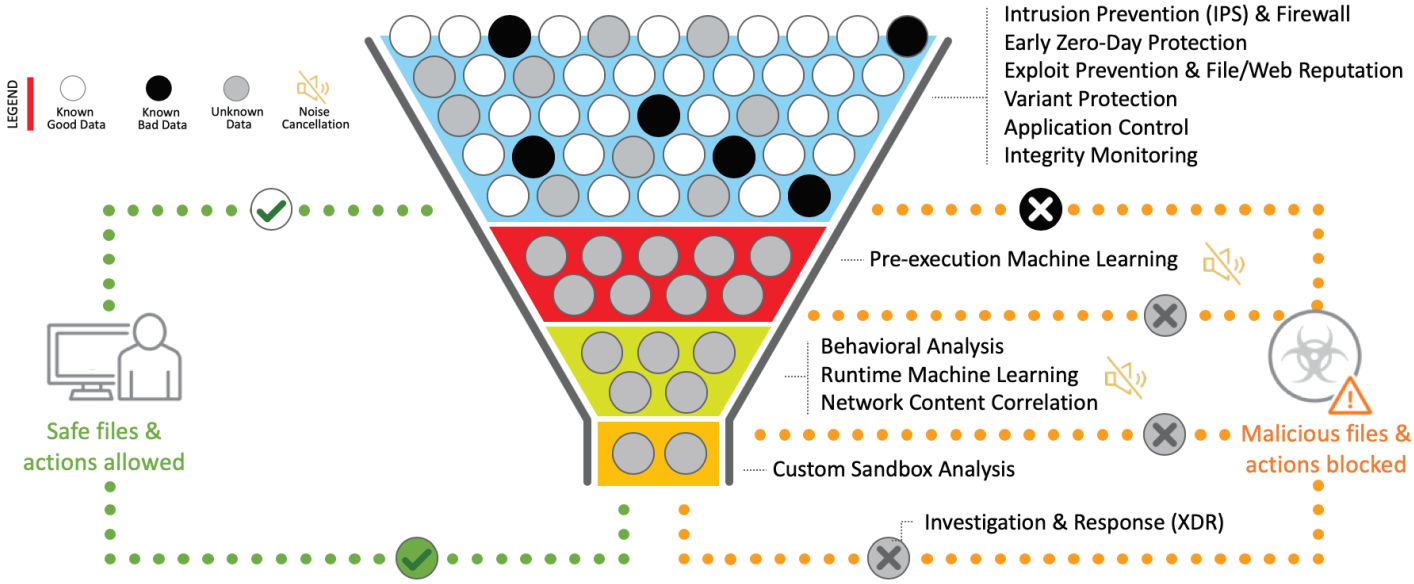
The Trend security solutions protect users, networks and hybrid cloud environments; all designed specifically for and tightly integrated with leading platforms and applications such as VMware, Amazon Web Services, Microsoft Azure, Google Cloud, Office365 and more. This ensures seamless protection as the Trend products are specifically designed to integrate into the applications and environment that your users will utilise every day.

Connected

Automatic sharing of threat intelligence across security layers and centralised visibility and control significantly speeds up time to response. XGen security uses proven techniques to quickly identify known good or bad data, freeing advanced techniques to identify unknown threats quickly and accurately. This identification, in rapid

succession with right-time technology, regardless of location and device across a connected system, maximises both visibility and performance. This core set of techniques powers each of the Trend Micro solutions in a way that is optimized for each layer of security: hybrid clouds, networks, and end-user environments.

By using the most appropriate technology at the right time, XGen removes the most obvious / known threats first and then applies more and more advanced techniques to detect more advanced or unknown threats:



- Progressively filter out threats using the most efficient technique for maximum detection without false positives.
- Blends signatureless techniques, including high-fidelity machine learning, behavioural analysis, variant protection, census check, application control, exploit prevention, and good-file check with other techniques like file reputation, web reputation, and Command &Control blocking.
- Trend Micro is the first to infuse high-fidelity machine learning, which uniquely analyses files not only before execution but also during runtime for more accurate detection.
- Noise cancellation techniques like census and whitelist checking at each layer reduce false positives.
- Instantly shares information on suspicious network activity and files with other security layers to stop subsequent attacks.
- Advanced ransomware protection monitors for suspicious file encryption activities at the endpoint, terminates malicious activities, **and even recovers lost files if necessary.**

Smart Protection Network Overview

Smart protection begins with global threat intelligence. Like MTI, Trend Micro take pride in protecting their customers, which is why data is collected around the clock and across the globe through the Trend Micro Smart Protection Network. Receiving over 2.7 trillion queries in 2019, the Smart Protection Network powers high-performance security solutions, while blocking over 52 billion threats and stopping over 61 million ransomware attacks in 2019.

The global research division, Trend Micro Research, continually analyses and identifies new malware, ransomware, malicious URLs, command & control (C&C) locations and domains that could be potentially used in attacks. The team's broad research agenda helps Trend Micro solutions defend millions of customers around the clock, including vulnerability research that is carried out by Trend Micro's Zero Day Initiative (ZDI), the world's largest vendor

agnostic bug bounty program. ZDI allows the identification and disclosure of new vulnerabilities across a wide range of platforms, focusing on positively impacting Trend Micro's solutions as well as the broader industry.

Whenever a new vulnerability is disclosed via ZDI, in Windows Server for example, the Trend Micro products are immediately updated to stop exploitation of this vulnerability on average 120 days before Microsoft will release a patch and 120 days before the updates will appear in Windows ATP. This provides a considerable benefit above other vendors anti-malware products and Microsoft's own ATP protection and provides full protection for vulnerabilities whilst IT teams test and approve vendor patches. Over 2,000 items of software can be protected by this feature, from Operating Systems to Java / Flash and databases such as Oracle and MSSQL. Most new malware is released shortly after a vendor patch is released, as malware authors reverse engineer the patch to identify the vulnerability and hope to utilise it quickly before the patch is widely deployed. MTI's solution will ensure you are fully protected from these zero-day attacks weeks or months before the vulnerability becomes public knowledge.

Over 70% of all Windows Server vulnerabilities are reported to Microsoft via the zero day initiative, this allows customers of Trend Micro products to be protected by early updates released through the zero day initiative programme before Microsoft acknowledge availability or release a Patch.

https://www.thezdi.com/blog/2020/1/30/looking-back-at-the-zero-day-initiative-in-2019

Deep Security-as-a-Service – Server Protection

Trend Micro's Deep Security-as-a-service product is designed to provide advanced server security for physical, virtual, and cloud servers. It protects enterprise applications and data from breaches and business disruptions without requiring emergency patching.

Delivered "as-a-Service", the Deep Security infrastructure is maintained and updated by Trend Micro, with MTI managing the anti-malware configuration and alerting aspects of the service functionality.

Deep Security consists of the following set of core components:

- **Deep Security Manager**, the centralized web-based management console that administrators use to configure security policy and deploy protection to the enforcement components: Deep Security Virtual Appliance and the Deep Security Agent.
- **Deep Security Virtual Appliance** is a security virtual machine built for VMware vSphere environments that is agentless and provides anti-malware and integrity monitoring protection modules for virtual machines in a vShield environment. In an NSX environment, the anti-malware, integrity monitoring, firewall, intrusion prevention, and web reputation modules are available without the need to install an agent.
- **Deep Security Agent** is a security agent deployed directly on a computer which provides application control, anti-malware, web reputation service, firewall, intrusion prevention, integrity monitoring, and log inspection protection to computers on which it is installed.
- The Deep Security Agent contains a **Relay** module. A relay-enabled agent distributes software and security updates throughout your network of Deep Security components.
- **Deep Security Notifier** is a Windows System Tray application that communicates information on the local computer about security status and events, and, in the case of relay-enabled agents, also provides information about the security updates being distributed from the local machine.

1.1 Deep Security Overview

Trend Micro's Deep Security product provides a complete suite of security capabilities to protect your physical, virtual and cloud infrastructure and environments from myriad threats via a multi-faceted approach using technologies including intrusion detection and prevention, firewalling, malware prevention with web reputation, predictive machine learning, sandbox analysis, integrity monitoring, log inspection, and multi-platform application control.

Deep Security provides advanced threat protection for hybrid workloads. As you deploy workloads across physical, virtual and cloud infrastructure, including serverless and containerised deployments, ensuring security is maintained across each platform becomes of paramount importance.

Key Features

- **Instant Protection:** Immediate protection against known vulnerabilities and Zero-Day threats.
- **Next Generation Antimalware:** Blocks malware, including ransomware, that attempts to evade detection
- **Server integrity protection:** Locks down servers to a "known-good" configuration so that no unauthorized applications can run.
- **Secure web filtering:** Ensures servers only communicate with expected systems and safe domains, preventing access to malicious sites and command and control networks.
- **Enterprise Logging and Reporting:** Detects and alerts you of suspicious or malicious activity, and provides detailed, auditable reports that document prevented attacks and policy compliance status.
- **Cost-Effective Compliance:** Addresses major compliance requirements for PCI DSS, as well as HIPAA, NIST, SANS, and SSAE 16

Apex One-as-a-Service – Endpoint Protection

The Trend Micro Apex One Endpoint protection is a Next Generation product that has been designed from the ground up to provide many advanced detection and response capabilities. It is the replacement for what used to be called Trend Micro OfficeScan.

As it is delivered “as-a-Service” it is fully cloud hosted and there are no infrastructure requirements that you need to worry about. Trend Micro take care of all server hosting, patching and licensing, and MTI will manage all aspects of the anti-malware software.

The core components are:

- Advanced Anti-malware protection
- Data Loss Prevention (DLP) controls
- Endpoint Web Filtering
- Application Control
- Endpoint Encryption

Apex One Overview

Traditional signature-based antivirus approaches alone are a weak defence against malware, ransomware and unknown threats, which can often slip through these static protections. Next-generation technologies help with these threats but are not fool-proof and adding multiple anti-malware tools on a single endpoint to try and close and gaps in coverage results in too many products that do not work well together.

Apex One uses a blend of advanced threat protection techniques to eliminate security gaps across any user activity and any endpoint. It will constantly learn, adapt, and automatically share threat intelligence across your own environment. This means that if one your endpoint detects a new malware variant using advanced detection, it will automatically and immediately inform all other Apex One agents and Deep Security agents of the malware; this then becomes a “known threat” in the context of your internal environment and will instantly be detected and blocked across the entire networked estate.

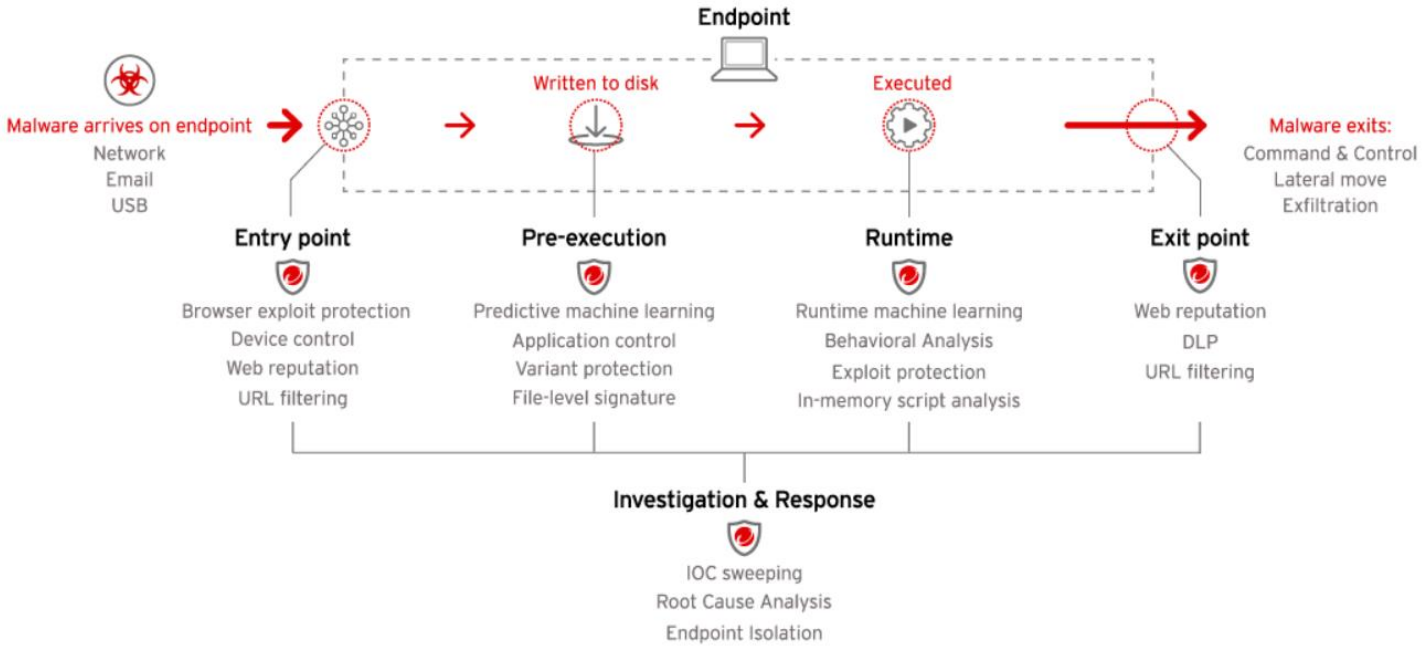
This blend of protection is delivered via an architecture that uses endpoint resources more effectively and ultimately outperforms other anti-malware technologies on CPU and network utilisation, providing you with automatic detection and response against an ever-growing variety of threats, including fileless and ransomware in an all-in-one lightweight agent with deployment flexibility through a security as a service (SaaS) platform.

Key Features:

- **Advanced malware and ransomware protection:** defend endpoints, on or off the corporate network, against malware, trojans, worms, spyware, ransomware, and adapts to protect against new unknown variants and advanced threats like cryptomalware and fileless malware.
- **Detection and response capabilities:** Advanced detection and response capabilities are included as standard with Apex One and will be fully managed by MTI.
- **The industry’s most timely virtual patching:** Trend Micro Apex One Vulnerability Protection virtually patches known and unknown vulnerabilities, giving you instant protection before a vendor patch is available or deployable.
- **Connected threat defence:** Apex One integrates with other security products via Trend Micro’s global cloud threat intelligence to deliver network sandbox rapid response updates to endpoints when a new threat is detected. This enables faster time-to-protection and reduces the spread of malware.

Endpoint Protection Overview

By using the layered approach of the XGen technology, described previously in this proposal, the Apex One’s single Security Agent proactively protects the host from known and unknown threats. The diagram below shows how the different layers of protection are applied by the Apex One Security Agent at the host level to ensure a complete and holistic set of protections are in place on every endpoint:



MTI's Managed Anti-Malware Service

MTI technology propose a fully deployed configured and managed service based on Trend Micro anti-malware software. The overview, scope and remit of this managed service is outlined in the below sections.

The MTI Managed Service Desk consist of many components:

Full Design, Install and Ongoing Management

MTI's Managed Anti-Malware Service is designed, onboarded, configured and managed from the outset to provide comprehensive, layered protection that significantly reduces the risks of malware infections and host compromise using multiple layers of technical controls **and** minimising the effort required by your IT Team in this area.

Our Managed service desk, are focused solely on the Anti-Malware Technology and delivering the managed service, ensuring agents, policies and configurations remain up-to-date, are properly configured and providing the highest level of protection required on ALL in-scope devices at ALL times.

Protected Devices are configured to send logs back to the central Cloud Managed Console, so we are aware of agent enrolment, agent version, anti-malware scanning operation and any significant events or indicators of compromise (IOC's) including areas such as:

- Virus/Malware Detection
- Spyware Detection
- Firewall Exceptions
- Web Reputation Exceptions
- Suspicious Behaviour
- Device Control Events
- Suspicious Connections
- Suspicious Files
- Command and Control Call Back Activity
- Predictive Machine Learning Events

Our team will immediately investigate and start remedial activity and where required deploy updated policies to agents on servers and Windows 10 hosts.

MTI are your Helpdesk Extension

MTI provide full deployment and ongoing managed service that runs effectively as an extension to your Help Desk taking the load away from your over-stretched IT Team who will have very many competing demands.

Day-to Day-Management - We will manage the Anti-Malware Protection to the highest industry standards including that required to be compliant with (CyberEssentials Scheme Plus certification) and deal with all of the day-to-day issues and management so your IT team rarely need to be involved; unless events reach a threshold that we agree during project initiation requires your involvement or approval.

MTI are On-Call 24x7x365 – MTI's team will be "on-Call" 24 hours a day, 7 days a week, 365 days a year to respond to security incidents using the technical controls available within the Trend Apex One and Deep Security solutions, following pre-arranged procedures agreed during project initiation.

Monthly Services Reporting - To evidence the level of service provided we include a Monthly Managed Service Status Report that summarises:

- Security Metrics / Key Events
- Investigations
- Server and Workstation Host Compliance Status
- Capacity
- Trending
- Operational workload
- Agreed Customer service metrics / SLA's

Working to Procedures and Thresholds agreed with you - During project initiation MTI will agree the policies and acceptable working procedures that address all of your needs and provide MTI the authority and framework in which to act on your behalf to respond to events rapidly, and letting you know how we've mitigated any issues or

outbreaks, rather than waiting for consent to be granted for routine events or conducting actions that are appropriate in light of a high risk/high threat situation.

Rules of engagement, approval thresholds and processes will be agreed for reviewing, releasing or blocking access to blocked URLs, Quarantined Files, or Request for relaxation of Application Controls (for example) so that the requests from users can come direct to MTI to deal with in a quick and efficient manner within the parameters agreed with you. MTI will seek explicit approval from the agreed Staff/Roles, for activities and action which are above that which MTI is authorised to do.

Phased Deployment

The service will be delivered in a phased approach as outlined below:

1. **Project Initiation -** MTI will conduct a project initiation meeting with you including all relevant stake holders in order to introduce the project team members and explain roles and responsibilities of each person. We will run through the prerequisites, deliverables, and milestones with you to ensure all parties have a mutual understanding each step, how the overall project will proceed and of the requirements and expectations of the other party.

    - MTI will agree the time scales and delivery dates with you for the roll out and we will highlight the key milestones and targets within the project and how they will be met.
    - This meeting will also provide an opportunity for you to raise any additional questions or queries which have arisen since award of the tender.
    - After the meeting MTI's Project Management Office (PMO) will provide a document containing the agreed dates and list of actions in a format agreed with you.

2. **Design –** MTI will work with you to understand your environment and any other security technology in place to ensure that the new Managed Anti-Malware Service deploys complementary security components to either enhance what is in place ready or where agreed replace them.

3. **Explain Product Capabilities –** MTI will walkthrough and explain all of the security functionality available within the existing licences of the Trend Apex One and Deep Security as a Service suites and agree with you which of those components you wish to deploy under the managed service.

4. **Agree Functionality to be used -** For each of the security components included in the design MTI will discuss with you the appropriate policy configuration to be applied. We will agree with you tailored policies to apply to different groups of Hosts to ensure that the most appropriate protection is applied without adversely impacting the operation of the host.

5. **Baseline Next Gen Malware Scan** – MTI will run a next generation Malware scan across the entire environment to identify the presence of any malicious files, applications or indicators of compromise and agree with you the approach to quarantine and delete any malicious files discovered and to white-list-files or applications which are proven to be safe. This creates a solid baseline from which the new service can be deployed and managed. (Given the legacy anti malware technology this service is replacing, MTI anticipate discovering multiple malicious files and applications. In addition to *on-access* scanning a schedule of malware and recommendations scans will be agreed with you during onboarding (as standard MTI schedule scans to run weekly.)

6. **Pilot and Phased Delivery Approach –** MTI will deliver they roll out of policies to an initial sample per group of hosts to ensure that the controls work effectively without impacting on functionality. MTI will review the logs from the Central Trend Apex One and Deep Security console to identify any errors, in addition to liaising with your project lead to identify if any service impacting issues arising from the newly deployed malware prevention controls. MTI will amend and update the policies and redeploy across the group to incorporate any feedback from this process.

7. **Agree Working Practices, Authorization Processes –** MTI will agree with you the working practises and authorisation process is to be followed in delivery of the service. For example to agree which types of files are up to be released from quarantine or URLs whitelisted, without needing to contact your IT team and at which point / threshold MTI need to obtain explicit authorisation. MTI will capture the roles, staff members and contact details to obtain authorisation both in and outside of working hours.

8. **Agree Reporting Levels and Console Access –** During onboarding MTI will agree:

    a. The level and type of regular reporting

    b. Event / Incident Types you wish to receive a real-time alert for

    c. Whether you would like access to the Central Console for your Managed Service Instance and what you would like to see within it, from the configuration and widgets available.

9. **Agree Emergency / Incident Management Procedure** – MTI will agree with the processes and procedures to follow in the event of an incident arising from malware / malicious files or other host based attack detected by our solution and service. This will clearly define the roles and responsibilities for both your staff and MTI's Managed Anti-malware Service team. Specifically MTI will assist with investigation and incident containment and remediation Remotely, using the technology available within purchased and deployed Trend, across your estate.

    Forensic Incident Response services are not included within the Managed Anti-Malware Service. We are happy to offer these services at additional cost, either on a retainer basis or on a best-endeavour's basis if issues arise.

    It is worth commenting that deploying the Trend technology with its multiple layers of protection and ensuring this is deployed and maintained across the entire state is based on our experience to minimise the occurrence off malware related incidences by orders of magnitude when compared to legacy / signature based solutions.