Trend Micro, Inc.

System and Organization Controls Report (SOC 3)

Independent Report of the Controls to Meet the Trust Services Criteria for the Security, Availability, and Confidentiality for the Period of October 1, 2024, through September 30, 2025.

Table of Contents

Assertion of Trend Micro, Inc. Management 1

Assertion of Trend Micro, Inc. Management 2

Independent Service Auditor's Report 3

Independent Service Auditor's Report 4

Scope 4

Service Organization's Responsibilities 4

Service Auditor's Responsibilities 4

Inherent Limitations 5

Opinion 5

Trend Micro, Inc.'s Description of Its Trend Micro Apex One as a Service, Trend Micro Cloud App Security, Trend Cloud One, Trend Micro Email Security, Trend Micro ID Protection, Trend Micro Managed XDR, Trend Vision One, and Worry-Free Services System 6

Section A: Trend Micro, Inc.'s Description of the Boundaries of Its Trend Micro Apex One as a Service, Trend Micro Cloud App Security, Trend Cloud One, Trend Micro Email Security, Trend Micro ID Protection, Trend Micro Managed XDR, Trend Vision One, and Worry-Free Services System 7

Services Provided 7

Scope of Assessment 7

Trend Micro Services Overview 7

Customer Engagement – Onboarding 7

Customer Engagement – Client Services 8

Customer Engagement – Offboarding 8

Trend Micro Apex One as a Service 8

Customer Engagement – Onboarding 9

Customer Engagement – Client Services 9

Customer Engagement – Offboarding 9

Trend Micro Cloud App Security 10

Customer Engagement – Onboarding 10

Customer Engagement – Client Services 10

Customer Engagement – Offboarding 10

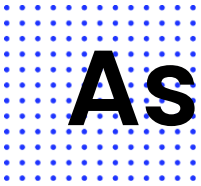
Trend Cloud One 11

Customer Engagement – Onboarding 12

Customer Engagement – Client Services 12

Customer Engagement – Offboarding 12

Trend Micro Email Security 12
Customer Engagement – Onboarding 13
Customer Engagement – Client Services 13
Customer Engagement – Offboarding 13
Trend Micro ID Protection 13
Customer Engagement – Onboarding 14
Data Management – Identity Monitoring 14
Data Management – Vault 14
Data Management – Privacy 14
Customer Engagement – Client Services 14
Customer Engagement – Offboarding 14
Trend Micro Managed XDR 15
Customer Engagement – Onboarding 15
Customer Engagement – Client Services 15
Customer Engagement – Case Management 16
Customer Engagement – Offboarding 16
Trend Vision One 16
Customer Engagement – Onboarding 17
Customer Engagement – Client Services 18
Customer Engagement – Offboarding 18
Worry-Free Service 18
Customer Engagement – Onboarding 18
Customer Engagement – Client Services 18
Customer Engagement – Authentication and Access Control 19
Customer Engagement - Offboarding 19
Infrastructure 19
Software 19
People 19
Data 20
Processes and Procedures 21
Section B: Principal Service Commitments and System Requirements 22
Regulatory Commitments 22
Contractual Commitments 22
System Design 22



Assertion of Trend Micro, Inc. Management

Assertion of Trend Micro, Inc. Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Trend Micro, Inc.'s Trend Micro Apex One as a Service, Trend Micro Cloud App Security, Trend Cloud One, Trend Micro Email Security, Trend Micro ID Protection, Trend Micro Managed XDR, Trend Vision One, and Worry-Free Services system (system) throughout the period October 1, 2024, to September 30, 2025, to provide reasonable assurance that Trend Micro, Inc.'s service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in section A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period October 1, 2024, to September 30, 2025, to provide reasonable assurance that Trend Micro, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Trend Micro, Inc.'s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in section B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period October 1, 2024, to September 30, 2025, to provide reasonable assurance that Trend Micro, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

Independent Service Auditor's Report

Independent Service Auditor's Report

Steven Ryan
Senior Program Manager, Compliance
Trend Micro, Inc.
225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.

Scope

We have examined Trend Micro, Inc.'s accompanying assertion titled "Assertion of Trend Micro, Inc. Management" (assertion) that the controls within Trend Micro, Inc.'s Trend Micro Apex One as a Service, Trend Micro Cloud App Security, Trend Cloud One, Trend Micro Email Security, Trend Micro ID Protection, Trend Micro Managed XDR, Trend Vision One, and Worry-Free Services system (system) were effective throughout the period October 1, 2024, to September 30, 2025, to provide reasonable assurance that Trend Micro, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

Trend Micro, Inc. is responsible for its service commitment and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Trend Micro, Inc.'s service commitments and system requirements were achieved. Trend Micro, Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Trend Micro, Inc. is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements

- Assessing the risks that controls were not effective to achieve Trend Micro, Inc.'s service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Trend Micro, Inc.'s service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

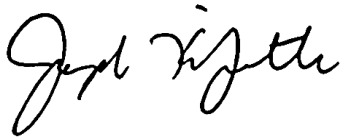
Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Trend Micro, Inc.'s Trend Micro Apex One as a Service, Trend Micro Cloud App Security, Trend Cloud One, Trend Micro Email Security, Trend Micro ID Protection, Trend Micro Managed XDR, Trend Vision One, and Worry-Free Services system were effective throughout the period October 1, 2024, to September 30, 2025, to provide reasonable assurance that Trend Micro, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.



Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

December 3, 2025

Trend Micro, Inc.’s Description of Its Trend Micro Apex One as a Service, Trend Micro Cloud App Security, Trend Cloud One, Trend Micro Email Security, Trend Micro ID Protection, Trend Micro Managed XDR, Trend Vision One, and Worry-Free Services System

Section A: Trend Micro, Inc.'s Description of the Boundaries of Its Trend Micro Apex One as a Service, Trend Micro Cloud App Security, Trend Cloud One, Trend Micro Email Security, Trend Micro ID Protection, Trend Micro Managed XDR, Trend Vision One, and Worry-Free Services System

Services Provided

Scope of Assessment

This report considers the Trend Micro Apex One as a Service, Trend Micro Cloud App Security, Trend Cloud One, Trend Micro Email Security, Trend Micro ID Protection, Trend Micro Managed XDR, Trend Vision One, and Worry-Free Services products within Trend Micro, Inc. (Trend Micro). The controls for the Trend Cloud One platform apply to the following:

- Trend Cloud One – Conformity
- Trend Cloud One – Endpoint & Workload Security
- Trend Cloud One – File Storage Security
- Trend Cloud One – Network Security
- Trend Cloud One – Cloud Sentry

Trend Micro Services Overview

Trend Micro is a global cybersecurity company that offers a range of security solutions for both consumer and enterprise users, providing protection against various cyber threats, including identity theft and malware, and offer tools such as an online scanner to check for compromised email addresses.

Trend Micro's solutions are designed to address the evolving security needs of modern businesses. Trend Micro's cloud-based services and products integrate advanced threat detection capabilities, artificial intelligence (AI), and machine learning to ensures that businesses can stay aware of emerging threats.

Customer Engagement – Onboarding

Trend Micro works almost exclusively through distributors, resellers, and other partnerships to sell their products. In rare cases, Trend Micro can sell direct, but only with prior approval. Once the customer's order has been fulfilled, the customer receives an electronic licensing file with an embedded activation link to the appropriate product, such as Trend Vision One or Trend Cloud One. Each product is integrated with License Activation Service that is central to all Trend Micro products, including both on-premises and cloud-based.

The customer initial account (root account) is created in the Trend Micro Foundation Identity Access Management (IAM) single sign-on (SSO) service common to all Trend Micro products. Trend Micro recommends that the root account is not used for regular tasks, but that a second account is created – or that the customer configures federated logins using SAML in the Foundation IAM service – for all other use cases.

During the initial configuration, the customer chooses the data center location for the subscribed services, and the location is closely related to the cloud provider regions. Customers choose the data center location based on data sovereignty or geographic or other considerations. High availability is achieved as each product is designed to use multiple availability zones within each region.

Customer Engagement – Client Services

Trend Micro provides different levels of support to customers using their products including:

- Corporate Support – Business Success Portal, technical support email, and phone support are provided, with direct support options are provided on a 5x8 basis.
- Premium Support – In addition to corporate support options, 7x24 access to a dedicated Customer Service Manager is provided. Additionally, onsite support options are available based on geographic availability.
- Online Help – Case management for security incident management, AI-based Trend Companion (in Trend Vision One), and online help options integrated into each product.

Products provide a set of reports relevant to the product offering, and reports are available on-demand within each product. Options exist in some products to customize the reports, with Trend Vision One providing the most capabilities in this regard. Additional support options are available based on the product and service offering.

Customer Engagement – Offboarding

To satisfy privacy requirements, public documentation is maintained that describes the data collected and the retention periods. To facilitate customers' requests to disengage, utilities are provided to perform mass uninstallation of Trend Micro products from customer endpoints and other devices.

Trend Micro Apex One as a Service

Trend Micro Apex One as a Service is an optional offering provided by Trend Micro to host the required Apex One management infrastructure on behalf of the customer. While customers can always build and manage the Apex One management server and agent communication server(s), Trend Micro provides the ability to host these on the customer's behalf.

Trend Micro Apex One as a Service is hosted in Azure as one Windows virtual machine for the management server and at least one Windows virtual machine for the agent communication server. Each hosted environment is completely isolated from all other hosted environments using Azure cloud-native isolation technologies.

Trend Micro Apex One as a Service also provides the backend infrastructure for the Vision One Standard Endpoint Protection service. An additional shared system component is used to provide integration between the Trend Vision One console and the Apex on a Service infrastructure for all command-and-control functions.

Customer Engagement – Onboarding

For new Trend Micro Apex One as a Service activations, the customer is directed to the Trend Micro License Activation Service to complete their service activation. During this step, a Trend Micro account is created if one does not exist. When the product registration is complete, the customer is directed to the Trend Micro Apex One as a Service Intermedia Portal (iPortal) to provide technical details needed to create the hosting environment, including the time zone, Azure region, and language. Once these details have been provided, the customer's hosted environment is automatically created within the Trend Micro Apex One as a Service platform. The linked Trend Micro account is used to provision the administrator account for the Apex One management server interface.

To install agents on the customer's endpoint, the administrator connects to the Apex One management server to download a pre-configured agent installation package for use on all of their endpoints.

Customer Engagement – Client Services

Trend Micro Apex One as a Service customers will use the management console in the same way as if it were locally hosted. Customers are responsible for configuring agent settings, logging, authentication, reporting, and all other aspects of Trend Micro Apex One as a Service.

Trend Micro Apex One as a Service customers have the option of creating additional user accounts for administering Trend Micro Apex One as a Service, including using the Trend Micro SSO service, local Trend Micro Apex One as a Service user accounts, or through identity provider integrations such as Microsoft Entra ID and SAML. Pre-defined RBAC roles include the following:

- Administrator
- Administrator_and_DLP_Compliance_Officer
- DLP_Compliance_Officer
- DLP_lncident_Reviewer
- Operator
- Power_User
- Read-only_User
- Threat_lnvestigator

Customers can also create custom roles to suit their individual needs.

Customer Engagement – Offboarding

When a customer's license has expired, Trend Micro Apex One as Service retains the customer's hosted environment for 30 days. Once the grace period has expired, the virtual machines are placed into sleep mode for an additional 30 days. At the end of

the sleep period, the virtual machines, databases, and all other assets are automatically deleted by Azure without possibility of retrieval.

Trend Micro Cloud App Security

Trend Micro Cloud App Security integrates with and provides protection for cloud storage services, including Microsoft 365 services, Box, Dropbox, and Google Workspace. The Trend Micro Cloud App Security platform protects against ransomware, phishing, business email compromise, zero-day and hidden malware, and unauthorized transmission of sensitive data via cloud-to-cloud integration. The core capabilities within the platform consists of two primary modes: application programming interface (API) mode and online mode.

The API mode uses Microsoft or Google API for access to customer-provisioned mailboxes. When an email is sent, it is retrieved via API and scanned via the Trend Micro Cloud App Security backend to detect viruses, phishing attempts, and web reputation-associated threats. The online mode uses root access to customer email inboxes, where emails are transmitted to Trend Micro Cloud App Security via Simple Mail Transfer Protocol (SMTP). Via Trend Micro Cloud App Security, files are scanned for sensitive data and security issues.

A dashboard feature provides statistics to clients regarding customer protection, risk users, and other potential threats. Email policies can be configured to protect against advanced threats and data loss. Audit and API integration logs are available via the Trend Micro Cloud App Security console. Policy can be configured to quarantine risky emails, and the quarantined messages can be reviewed via the Trend Micro Cloud App Security console.

The Trend Micro Cloud App Security console can be used to generate reports on threats, organized by organization and associated services. Reports can be scheduled or run on-demand. Large entities can manage multiple tenants via the Trend Micro Cloud App Security console. Administrative features enable management of service accounts and associated access tokens, automation and integration APIs, Outlook quarantining, email reporting, and role and group assignments.

Customer Engagement – Onboarding

The onboarding process is shared with other services. Please see the Customer Engagement – Onboarding section under Trend Micro Services Overview for more information.

Customer Engagement – Client Services

The client services processes are shared with other services. Please see the Customer Engagement – Client Services section under Trend Micro Services Overview for more information.

Customer Engagement – Offboarding

When a client contract nears expiry, the client is notified that their license is due to expire. If the client chooses not to continue services, the client is responsible for deprovisioning processes on their end. An automatic deprovisioning flow is in place

upon license expiry. Clients can additionally make on-demand deprovisioning requests through the Trend Micro ticketing system.

Logs and quarantined emails generated by customer traffic are not immediately removed. Clients can choose to release or access quarantined emails or files prior to deprovisioning. A 10-day grace period is used to allow clients to renew their services, after which data is automatically purged.

Trend Cloud One

Trend Cloud One is a Cloud-Native Application Protection Platform (CNAPP) solution providing security protections for technologies, including servers (physical, virtual, or cloud workloads), networks, applications, containers, cloud storage, and infrastructure and helps to protect sensitive data in a customer's cloud environments through a wide range of security controls. Central management consoles provide the ability to easily drill down for details and allow for administrators to implement policies and manage security events.

Trend Cloud One provides the following services to its customers:

- Cloud One Network Security provides network traffic inspection using a Tipping Point TPS deployed as a virtual machine in a customer's AWS or Azure cloud environment.
- Network-Based Virtual Patching is used to block known suspicious traffic related to common vulnerabilities and exposures (CVEs).
- Option for customers to deploy in their own environment or for Trend Micro to host the virtual appliance on the customer's behalf.

Trend Cloud One – Endpoint & Workload Security is based on Trend Micro's Deep Security Agent and provides an extensive set of security protections for server-based workloads, including:

- Intrusion Detection and Prevention
- Anti-Malware
- Bidirectional Firewall
- Web Reputation
- Integrity Monitoring
- Log Inspection
- Events and Reports
- Application Control

Trend Cloud One - File Storage Security provides anti-malware scanning for files in cloud storage, such as AWS S3 buckets or Azure Storage Accounts.

Trend Cloud One - Cloud Sentry uses agentless technology to perform daily scans of AWS EC2-, ECR-, and Lambda-based resources for malware and AWS EC2 EBS volumes for changes to critical files.

Trend Cloud One – Conformity provides cloud security posture management (CSPM) monitoring of cloud infrastructure configurations for adherence to various industry standards such as Center for Internet Security benchmarks, National Institute of

Standards and Technology (NIST), Health Insurance Portability and Accountability Act (HIPAA), and International Organization for Standardization (ISO) 27000.

By design, the services do not send the content of sensitive data files to the Cloud One management environment. For instance, only file hashes are sent from File Security to the backend when identifying if the file contains suspicious payloads. Additionally, the Deep Security Agent used in Cloud One Workload Security sends only security events and agent operational information to the Trend Cloud One Console and none of this data contains customer sensitive data.

Trend Cloud One is entirely hosted within AWS using a combination of EC2, Docker containers with ECS, Lambda, Relational Database Service (RDS), DynamoDB, and S3. All administrative connections to the Trend Cloud One environment are only through AWS Systems Manager (SSM Agent) allowed only for privileged users.

Customer Engagement – Onboarding

For Trend Cloud One onboarding, customers can sign up for free 30-day trial directly at https://cloudone.trendmicro.com or through the AWS Marketplace. Customers are also onboarded using Trend Micro's standard process. Please see the Customer Engagement – Onboarding section under Trend Micro Services Overview for more information.

Customer Engagement – Client Services

The client services processes are shared with other services. Please see the Customer Engagement – Client Services section under Trend Micro Services Overview for more information.

Customer Engagement – Offboarding

Upon license expiration, Trend Cloud One retains all information in the system and allow continued use for 30 days ("grace period") to facilitate license renewal. After 30 days, the system will be unusable but the data will remain for an additional 60 days (90 days total). After 90 days, the data is marked for deletion and purged from the system after 30 days (120 days total).

Trend Micro Email Security

Trend Micro Email Security is an enterprise-level cloud email gateway that provides protection against phishing, ransomware, business email compromise, spam, and other email-related threats. The solution integrates with Microsoft Exchange Server, Office 365, Gmail, and other cloud-based or on-prem email solutions. Core capabilities within the platform include the following:

- The platform uses domain name system (DNS) records, SMTP protocol, and email scanning and filtering to determine whether to quarantine or delete email in accordance with client configuration.
- A dashboard within the Trend Micro console provides email scan and statistics data. Client-configured domains can be established with inbound and outbound servers to direct where delivery should be performed and allow relay of email to Trend Micro Email Security services.

- Available inbound protection features that can be configured include connection filtering based on sender, recipient, IP reputation, and reverse DNS validation; domain-based authentication including sender IP match, sender policy framework, and domain-based message authentication, reporting, and conformance; virus scanning and file password analysis, spam filtering, correlated intelligence, content filtering, and data loss prevention. Available outbound protections include Transport Layer Security (TLS) peer connection filtering, spam filtering, and virus scanning.
- Logs and reports can be configured to detail information such as email traffic summaries, threat detections, virtual analyzer detections and trends, and DMARC compliance.
- Administrative functionality within the Trend Micro console allows configuration of policy objects, account and end user management, and management of email continuity (allowing access to quarantined email in the event of a network interruption), service integration, director management, and logon access control, including login restrictions based on IP.
- A migration tool is in place to allow clients to migrate data from InterScan Messaging Security Suite or InterScan Messaging Security Virtual Appliance (IMSS/IMSVA) to the Trend Micro Email Security platform.
- An email recovery function allows emails marked for deletion to be restored for a 14-day period.

Customer Engagement – Onboarding

The onboarding process is shared with other services. Please see the Customer Engagement – Onboarding section under Trend Micro Services Overview for more information.

Customer Engagement – Client Services

The client services processes are shared with other services. Please see the Customer Engagement – Client Services section under Trend Micro Services Overview for more information.

Customer Engagement – Offboarding

When a client contract nears expiry, the client is notified that their license will expire soon. If the client chooses not to continue services, the client is responsible for deprovisioning processes on their end. An automatic deprovisioning flow is in place upon license expiry. Clients can additionally make on-demand deprovisioning requests through the Trend Micro ticketing system.

Logs and quarantined emails generated by customer traffic are not immediately removed. Clients can choose to release or access quarantined emails prior to deprovisioning. A 30-day grace period is used to allow clients to renew their services, after which data is automatically purged.

Trend Micro ID Protection

Trend Micro ID Protection is an identity monitoring and protection service which helps consumers manage their online identities. The identity monitoring services includes

monitoring the dark web for email addresses, mobile phone numbers, credit cards, driver's license, passport, bank account, national identifiers, and other regional-specific identity data for indicators of misuse. The product also includes an identity vault for managing login credentials and a privacy monitoring service. The vault feature ensures secure storage for online identities, such as social media and banking credentials. Trend Micro ID Protection also includes privacy monitoring as a Chrome-based browser extension, monitoring outbound browser activity for data being sent to known, black-listed destinations. When such communication is identified, the extension blocks the outbound traffic.

Trend Micro ID Protection is sold through mobile phone app stores for Android and IOS devices as well as directly through the Trend Micro website.

Customer Engagement – Onboarding

Upon downloading the application from the mobile device online store, Trend Micro ID Protection is enabled for a seven-day trial. Users can either purchase a subscription through the mobile device-provided mechanism or through the Trend Micro website.

Data Management – Identity Monitoring

All collected personal information supported by the service is hashed using SHA-256 in the end user's device, with the hash sent to the Trend Micro ID Protection backend. Consumer personally identifiable information (PII) is never stored directly in the backend, only hashed equivalents. The service relies on the Trend Micro Dark Web Monitoring service to detect potentially compromised identifiers. When such an identifier is detected, the system performs a hash of the data and compares it to the hashed versions in its database.

Data Management – Vault

Upon initial installation, a client key is generated locally on the device. The key is used to perform all password encryption and decryption operations locally and is never transferred to the backend for any purpose. When installing the service on another device, a mechanism is provided to transfer the key from the first device such that both devices can now be used. The key is generated using a device-specific encryption library to create a random 128-bit value.

Data Management – Privacy

The privacy extension does not use sensitive information as it explicitly blocks all traffic destined to known suspicious destinations.

Customer Engagement – Client Services

The Trend Micro ID Protection portal generates weekly reports for privacy events and generates emails upon detection for any suspicious identity monitoring events.

Customer Engagement – Offboarding

Consumer data is retained indefinitely until a request is made by the user to remove their data. To satisfy privacy requirements, public documentation is maintained that describes the data collected.

Trend Micro Managed XDR

Trend Micro Managed XDR is an optional Security Operations Center (SOC) service provided by Trend Micro for customers who do not have internal expertise to work with incidents and observed attack techniques and other indicators of potentially suspicious activity. When engaged by Trend Micro customers, Trend Micro SOC analysts receive and respond to alerts, working with customer-supplied contacts throughout the process.

Trend Micro Managed XDR services use a follow-the-sun model to provide 24x7 coverage with locations in:

- Dallas, TX
- Cork, Ireland
- Manilla, Philippines
- Singapore
- Tokyo, Japan

Customer Engagement – Onboarding

When customers choose one of the Service One support packages, the Trend Micro Managed XDR services Service Delivery Manager (SDM) engages with the customer to perform additional onboarding activities. The activities include meetings with the customer to understand the customer's needs, to help the customer to understand how the Trend Micro Managed XDR services service works, and to capture these discussions as part of the Trend Micro Managed XDR team customer documentation.

Customers are provided instructions with how to use the Trend Vision One Managed XDR portal UI, which includes the following:

- Managing contacts for alerts and reports
- Managing response pre-approval for various actions that can be taken by the Managed XDR analyst
- Managing critical assets such printers, wireless routers, or other critical assets to provide additional context to SOC analysts
- Configuring integrations with other Trend Vision One and external applications such as synchronizing Trend Vision One Workbench cases with the customer's Service Now tenant

Customer Engagement – Client Services

Monthly reports are generated by the Trend Micro Managed XDR Vision One service and automatically distributed to customers. The Trend Micro Managed XDR team is available to review these reports with the customer as requested. Additionally, a quarterly service review meeting is scheduled with each customer, unless the customer opts out, to discuss the previous quarter's results such as service-level objective (SLO) performance and issues experienced during the period. During this meeting, Trend Micro also solicits feedback about the customer's service and experience and reviews the report with the customer to address any concerns.

Customer Engagement – Case Management

When Trend Vision One notifies the Trend Micro Managed XDR analyst of a potential incident, the analyst creates a case in the Trend Micro Managed XDR customer relationship management (CRM) tool PS1, based on Microsoft Dynamics365. The case will be worked in PS1 until resolved, including all customer email-based interactions. Other tools used by Trend Micro Managed XDR analysts include Microsoft Sentinel and Trend Vision One Response Actions.

Customer Engagement – Offboarding

Trend Micro Managed XDR follows the Trend Vision One data retention and destruction schedule.

Trend Vision One

Trend Vision One platform is an integrated set of cybersecurity tools developed to provide organizations with a unified framework and UI for threat intelligence, detection, and mitigation. At its core, Trend Vision One uses a distributed architecture comprising endpoint agents, network sensors, and cloud-based analytics engines.

Core capabilities within the Trend Vision One platform include:

- Network Security
  - Employs IPS inspects network traffic for malicious activity
  - Blocks network-based attacks and block access to malicious websites
  - SSL/TLS inspection to decrypt and inspect encrypted network traffic for threats and policy violations
  - Utilizes deep packet inspection (DPI) to analyze packet payloads for malware and exploit attempts
- Email Security
  - Analyzes email headers, sender reputation, and content to identify and quarantine unsolicited emails and phishing attempts
  - Performs inline scanning of email attachments and embedded links to detect and quarantine malicious files and URLs
  - Utilizes signature-based detection, behavior analysis, and sandboxing
  - Implements URL categorization and reputation scoring to block access to malicious websites and phishing landing pages
  - Enforces policy-based content inspection and filtering to prevent unauthorized disclosure of sensitive information via email
  - Supports predefined and custom DLP policies for identifying and blocking emails containing confidential data, such as personally identifiable information (PII) or intellectual property
  - Integrates with encryption and data masking technologies to automatically encrypt or redact sensitive content based on policy rules
  - Implements email authentication protocols such as SPF, DKIM, and DMARC to verify the authenticity of incoming emails and prevent spoofing and impersonation attacks
- Cyber Risk Exposure Management
  - Provides a detailed report of potential vulnerabilities and exposures by using active and passive scanning techniques to identify and enumerate

all assets within the organization's network, including servers, endpoints, applications, and cloud resources
    - Maintains accurate inventory of system components and assets
    - Prioritizes vulnerabilities based on severity and exploitability
    - Secure configuration management and minimizes attack surface
    - Supports incident response workflow and automated remediation actions quickly
    - Generates evidence of vulnerability assessment, risk management activities, and security controls implementation
    - Provides continuous monitoring
    - Cyber Governance Risk and Compliance Management
        - Uses pre-defined compliance policies for common security frameworks, such as Payment Card Industry Data Security Standard (Payment Card Industry Data Security Standard) and HIPAA to continuously evaluate endpoint compliance status
    - Cyber Attack Prediction
        - Simulates possible attack vectors based on overall risks identified by the platform
- XDR
    - Uses lightweight agents, network sensors, and cloud connectors to collect security telemetry data from endpoints, servers, network devices, email gateways, cloud workloads, and applications
    - Enables centralized log management, protection, and retention
    - Has encryption capabilities for data in transit and at rest
    - Supports log aggregation, search and analysis for investigation and compliance monitoring
    - Provides vulnerability management for scanning, patching, and risk mitigation
- Endpoint
    - Uses lightweight agents deployed across endpoints to monitor system activities, detect malware, and enforce security policies
    - Leverages behavior-based detection algorithms and signature-based scanning to identify and quarantine malicious files and processes
    - Identifies and responds to anomalous endpoint behavior
    - Blocks access to malicious websites and web-based threats
    - Data loss prevention to monitor and prevent unauthorized transmission of sensitive data
    - Prevents data breaches and unauthorized data exfiltration
    - Manages device control to restrict access to removable storage devices, such as USB

Customer Engagement – Onboarding

The onboarding process is shared with other services. Please see the Customer Engagement – Onboarding section under Trend Micro Services Overview for more information.

Customer Engagement – Client Services

The client services processes are shared with other services. Please see the Customer Engagement – Client Services section under Trend Micro Services Overview for more information.

Customer Engagement – Offboarding

Upon license expiration, Trend Vision One retains all information in the system for 30 days ("grace period") to facilitate license renewal. After 30 days, the data is purged.

Worry-Free Service

Worry-Free Services is an endpoint detection solution targeted at small businesses based significantly on the Apex One endpoint agent, but with many options further simplified for ease of management. Provided as a software as a service (SaaS) platform, customers can work with a local Trend Micro partner to activate, configure, and use the product or they can manage the service directly.

Customer Engagement – Onboarding

Two customer onboarding scenarios are supported: self-managed and partner managed. Self-managed customers are directly responsible for activating, configuring, and using Worry-Free Services. For partner-managed customers, partners pre-configure a Worry-Free Services tenant on behalf of their customers and manage the product on behalf of their customers. Only the self-managed scenario is directly addressed by this audit.

When the customer places the order, the Order Management (OM) team triggers an activation link to the end user. Similar to other products, the customer follows the link to activate the product and create a root user in the Foundation IAM service shared by all Trend Micro products and services.

Worry Free has 2 data centers: NABU and EMEA. These data centers are in AWS US-West-2 and EU-Central-1 regions. Global customers are assigned a region directly by Trend Micro. For example, Japanese and South American customers use the US deployment. Customers can direct the assignment by choosing a license in a specific region at the time of placing the order.

Customer Engagement – Client Services

Worry-Free Services provide different levels of support to customers using their products including:

- Business Success Portal (https://success.trendmicro.com)
- Phone-based technical support email and phone support are provided on a 5x8 basis.
- Online Help – Online help options integrated into the portal
- Partner support – Self-managed customers can engage with a Trend Micro partner at any time

Worry-Free Services provide a reporting interface to create one-time and scheduled (weekly or monthly) reports. Report content can include multiple event sources,

including virus and malware, spyware and grayware, web reputation, URL filtering, behavior monitoring, device control, and network virus.

Customer Engagement – Authentication and Access Control

Customer accounts are created and managed in the Trend Micro-managed Poseidon SSO service. As Worry-Free Services are intended for small business use, SAML or other forms of external single-sign on are not supported. Customers are able to create other user accounts within the portal. Different roles exist in the Worry-Free Services portal, including Administrator, Auditor, and Support Administrator.

Customer Engagement - Offboarding

Upon license expiration, the customer's tenant will enter a 30-day grace period during which the product remains fully functional. After that, the tenant will enter a 30-day lockout period during which time the customer cannot login or use the product, but the data remain intact. At the end of the lockout period, all data is automatically purged. Customers can also request to have their data purged at any time.

To satisfy privacy requirements, public documentation is maintained that describes the data collected and the retention periods.

Infrastructure

The organization maintains network diagrams that illustrate the network architecture, internal connectivity, and connectivity to external resources.

Software

Trend Micro business units maintain software inventories. Each business unit maintains documentation of the software and the packages used to build their respective applications. Vulnerability scanning tools are used to create automatically updated software bill of materials (SBOMs), including custom, bespoke, and third-party software components.

People

Trend Micro’s Information Security Organization operates under the Chief Information Officer (CIO) and includes specialized teams responsible for governance, operations, monitoring, secure development, and cross-functional coordination. Roles and responsibilities are clearly defined to ensure accountability, policy enforcement, and effective risk management. The CIO and executive leadership team set the strategic direction for information security, regularly communicating the importance of cybersecurity through internal briefings, strategic reviews, and company-wide town halls, reinforcing a security-first culture. The CIO and leads the InfoSec function, which is organized into key sub-functions: GRC, Security Operations, Security Monitoring, and Security Development. The Governance, Risk, and Compliance (GRC) team and broader InfoSec function design and implement security policies, monitor compliance, and manage audits and risk assessments, and a Board of Directors has been established that provides company oversight.

Data

Trend Micro has established a policy that defines the requirements for handling customer and employee data, including how it is used, stored, and destroyed. Storage, usage, export, replication, archival, and destruction restrictions are defined for customer and employee data. Business units maintain their own inventories of data, and the data within the inventories is classified in accordance with classification policies defined in the Trend Micro Global Information Security Policy. Information is classified as top secret, confidential, internal use only, or public, and data is handled, labeled, and disposed of in accordance with the data classification.

The organization has established a policy that governs how long data is retained based on data type, business need, and regulatory and contractual regulations. Data is required to be retained in accordance with applicable laws and with the Trend Micro formal retention schedule. Retention periods are defined for all data categories, including employee data, customer data, and corporate records, with the schedule documenting additional details for each data type such as where records are held. The schedule defines retention periods for both global and European data, along with details on where records are held. Data related to security incidents is required to be retained for three years, until closure of the case, or as required by applicable laws.

Each product team ensures that encryption best practices are used to secure data in transit and at rest. The encryption methods in place include the following:

- Trend Micro Apex One as a Service – The SOPS command line is used for encryption and decryption. Data is protected via AES-256 encryption at rest and that access is restricted to authorized personnel via Jenkins and GitHub Actions.
- Trend Micro Cloud App Security - Customer configuration is stored via Azure SQL database and encrypted with AES 256 at rest and TLS in transit.
- Trend Cloud One – TLS 1.2 is used where possible for data transmission, and data is encrypted at rest. TLS 1.2 and HTTP are used for CloudFront security. A minimum protocol of TLS 1.2 is in place for load balancer security profiles, and an RSA 2048 key is in place with SHA-256 with RSA signature algorithm.
- Trend Micro Email Security – TLS 1.2 and 1.3 are used, and an RSA 3072 key is in place with a SHA-256 signature algorithm. Data is stored via AWS RDS, S3, and EBS, all of which are protected via AWS Key Management Service (KMS) keys. AWS KMS keys are used for data encryption. AWS KMS keys are used and rotated annually to encrypt user settings and customer information.
- Trend Micro ID Protection – AWS KMS is used to encrypt sensitive data at rest, and data transmissions are protected via TLS 1.2 or higher. HTTPS via TLS 1.2 is used to encrypt client facing traffic, and encryption at rest with AWS KMS key is used to protect the vault service database. DynamoDB and DocumentDB are used to securely store and restrict access to sensitive information.
- Trend Micro Managed XDR – SSL/TLS is used to secure connections to the database cluster, and Aurora MySQL databases are encrypted via AWS KMS. HTTPS with a minimum protocol of TLS 1.2 is in place, and AWS KMS keys are used to protect information within databases. AWS Secret Manager is used to securely store, automatically rotate, and restrict access to sensitive data elements.

- Trend Vision One – TLS 1.2 is used where possible for data transmission, and data is encrypted at rest. TLS 1.2 is used with supported ciphers include TLS RSA with AES-128 and AES-256, as well as TLS ECDHE RSA with AES-128 and AES-256.
- Worry-Free Services – AWS encryption is used to protect databases. AWS KMS keys are used to protect database backups. Sensitive information is stored via AWS and distribution lists are used to restrict access to such information.

The organization has a process for managing encryption keys. Azure and AWS are used across the organization to maintain encryption keys and certificates. Key length and encryption requirements must be chosen based on legal requirements and the organization's risk assessment. The key management system's asset owner is responsible for defining key protection policies. Keys are required to be regularly rotated and securely stored. Access control restrictions implemented for keys are required to be reviewed semi-annually.

Data traffic of cloud customers in jointly used network environments is segregated on network level. In-scope applications employ a multi-tenant model with customers accessing shared compute and network resources and data persistence provided by shared database infrastructure. Customer traffic is co-mingled using load balancers, API gateways and similar services and is separated from other customers at the application layer. To ensure the confidentiality and integrity of all application data, all customer requests are encrypted with TLS 1.2 using strong cipher suites.

Processes and Procedures

Management has developed and communicated procedures to guide the provision of the organization’s services. Changes to procedures are performed annually and authorized by management. These procedures cover the following key security life cycle areas:

- Data classification
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, user functionality, master passwords, powerful utilities, and security devices

Section B: Principal Service Commitments and System Requirements

Regulatory Commitments

The organization bases its policies, processes, and procedures based on industry regulations, including ISO, SOC 2, Payment Card Industry Data Security Standard (PCI DSS), General Data Protection Regulation (GDPR), and California Consumer Privacy Act (CCPA). The Trend Micro website includes a data collection notice, data processing addendum, a list of sub-processors, and other content relevant to applicable global privacy laws and has a list international compliance industry and governmental certifications.

Contractual Commitments

Trend Micro maintains contractual materials and a company website that communicates the scope of services to customers as well as the responsibilities of respective parties. The Global Products Agreement applies to all Trend Micro products and services, including cloud-based services. The agreement addresses specific security-related requirements and commitments, including customer responsibilities for configuration and suitability of use. The agreement addresses protection of personal information, HIPAA Business Associate Agreement (BAA), and a mutual non-disclosure agreement (NDA) and includes the following topics:

- Scope of Agreement
- Grant of Rights
- Company Responsibilities
- Company Data
- Maintenance and Support
- Confidentiality
- Warranty and Exclusions
- Liability
- Term and Termination
- Intellectual Property Indemnity
- General Provisions
- Contracting Entity and Governing Law

System Design

Trend Micro products are designed to meet regulatory and contractual commitments. These commitments are based on the services that Trend Micro provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that Trend Micro has established for its services. Trend Micro establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in Trend Micro's system policies and procedures, system design documentation, and contracts with clients.