Security Foundations for Trend Micro Product Development & Service Offerings

Trend Micro's approach to security across the entire company, including our product & service development, is to leverage a solid security foundation centered on data protection by design and privacy by default. More information on trust and privacy can be found in our Trend Micro Trust Center: www.trendmicro.com/trustcenter.

Information Security Team

Trend Micro has a dedicated Information Security (InfoSec) department in charge of ensuring the security of the Trend Micro network, SaaS applications, code repositories and employee workstations. The InfoSec team works closely with the service operation teams and development organizations on various aspects of security controls and training.

Security Awareness, Employee Screening and Acceptable Use

All Trend Micro employees undergo a security awareness training course upon hire and on a yearly basis. All employees must adhere to Trend Micro's Internet, Computer, Remote Access and Mobile device acceptable use policies. Failure to adhere to these policies may result in disciplinary actions which could include termination. All new employees and contractors are required to complete a comprehensive background check.

Trend Micro software developers are enrolled in annual companywide secure coding training activities. The events include training sessions, quizzes and Capture the Flag (CTF) activities. Training topics are based on industry recognized common flaws and exposures such as SANS Top 25 and OWASP Top 10.

Security Certifications

In addition to rigorous internal standards for security, Trend Micro has undertaken external validation of our security practices. We have multiple ISO certifications, including ISO 27001, 27014, 27017, 27034 for our SaaS offerings today, as well as ISO 27000 certification for our support systems. You can see our full list of certifications on our web site:
https://www.trendmicro.com/en_us/about/legal/product-certifications.html

Passwords Policies and Standards

Trend Micro adheres to the following password polices and standards:

- Passwords must be changed at least on a bi-annual basis.
- Passwords must not be inserted into email messages or other forms of electronic communications.
- Passwords must not be shared or revealed to anyone.
- Passwords must be changed immediately if compromise is suspected.

- Passwords must be encrypted during transmission and stored hashed with a salt.
- Passwords must be at least eight alphanumeric characters long.
- Passwords must contain both upper and lower-case characters (e.g., a-z, A-Z).
- Password reuse prevention is enforced.
- Passwords must not be based on personal information, names of family, etc.

Remote Access and Authentication Policies and Standards

Remote access to Trend Micro's infrastructure is strictly controlled and monitored. All authentication methods used adhere to industry best practices/standards such as-certificate-based and/or multi-factor authentication. Where appropriate, single sign-on (SSO) leveraging the corporate directory is used.

Change Control and/or Change Management Plan

Trend Micro follows industry best practices for SaaS deployments, upgrades and changes. All software changes follow a rigorous validation and approval process through testing, staging and production system rollout. Changes are formally tracked and reviewed for complete traceability based on defined change management processes.

Physical Security Policy

All access to Trend Micro offices and networks is strictly controlled and limited to authorized or accompanied users only. Access is given through a key card system and an approval is required before entry is granted into sensitive areas. Our SaaS offerings or system components that are hosted externally are in secure Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) facilities.

Security Log Review

Security logs are reviewed for all systems on a daily basis by the service operations teams. Security event logs are also integrated with internal communication and alerting tools for real time oversight and event triage. If a security incident is suspected, it is immediately reported to the Trend Micro Infosec team, where a formal incident response plan is executed. In addition, InfoSec independently monitors Trend Micro services environment logs.

Incident Response Plan

If a security incident is discovered, the incident is prioritized based on severity. A dedicated team of technical experts is assigned to investigate, advise on containment procedures, perform forensics, and manage communication.

Following an incident, the team examines the root cause, and revises the response plan accordingly.

In the event of a breach involving personal data of a European citizen, Trend Micro will follow its obligations under GDPR. For more information, see https://www.trendmicro.com/en_us/about/trust-center/privacy/gdpr.html

In the event of a breach involving personal data of residents in regions outside the European Union, Trend Micro will follow its obligations under applicable laws.

Vulnerability Assessment and Penetration Testing

Our services undergo continuous security tests conducted by security experts to detect and rectify common security issues.

Trend Micro SaaS services are scanned with leading vulnerability scanning tools. When a vulnerability is found the account owners and the InfoSec team are notified automatically.

Business Continuity/Disaster Recovery

Upon the creation of any new service at Trend Micro, a team consisting of business and technical stakeholders is put together to create a business continuity plan containing backup, recovery and testing plans. These plans are approved by senior management and are tested at regular intervals.

Software Security

Trend Micro cultivates a development environment where products and services are built to be secure by design and various controls are enforced throughout the development lifecycle.

1. Static Code Analysis
   Trend Micro projects in active development are regularly scanned using a leading static analysis security tool, and a clean scan is a requirement for each product release.

2. Dynamic Analysis of Web Applications
   Trend Micro InfoSec conducts web application assessments of all products and services which utilize web interfaces. The assessments are conducted for any major release and at least annually using several leading dynamic analysis scanners.

3. Software Composition Analysis
   3rd Party Components included with Trend Micro products and services are inventoried and monitored continuously against NVD vulnerability feeds. Vulnerabilities (CVEs) are prioritized according to the associated CVSS score.

4. Vulnerability and Patch Management
   Vulnerabilities are continuously monitored and tracked via internal records. Each vulnerability is assigned a CVSS Score. Patching requirements enforce timelines of

addressing a vulnerability according to CVSS. In addition, vulnerabilities found and responsibly disclosed to Trend Micro via external researchers are addressed and assigned CVEs as required through Trend Micro's responsible disclosure program.

5. Safe Compilation
   All C/C++ projects are scanned continuously to ensure flags for ASLR, PIE, SSP are enforced. Compliance and adoption of safe compile flags is monitored as part of the release criteria.

6. Secure Design Process
   Engineers are required to review the application or service threat model for new features and significant product changes. Engineers must provide secure design documentation as part of the release criteria. Where appropriate, Trend Micro leverages FIPS certified cryptography and has also certified some products under the Common Criteria evaluation system. More information about our use of FIPS and Common Criteria can be found here:
   https://www.trendmicro.com/en_us/about/trust-center/compliance.html

7. Change Control
   All changes to code repositories are monitored and require detailed records, reviews and approvals. Industry leading tools are used for source control and change management.

8. Data Privacy
   Data privacy impact assessments are performed in accordance with Article 35 of the GDPR. All products and services are required to maintain a data collection inventory and update the corresponding data collection disclosure public document for new releases. A listing of Trend Micro data collection disclosure documents can be found on the following page: https://success.trendmicro.com/data-collection-disclosure.

   Data collected by Trend Micro products and services are governed by Trend Micro's privacy notice, which is available on the following page:
   https://www.trendmicro.com/en_us/about/trust-center/privacy.html