Trellix

Information Security Overview

2024

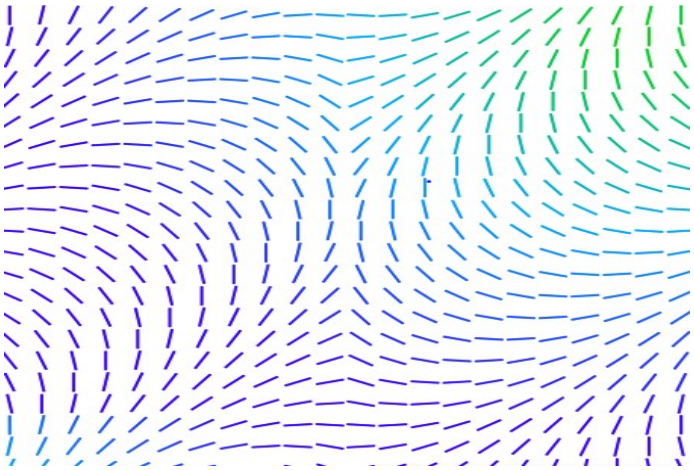


Table of Contents

Introduction

This document provides an overview of the Trellix Information Security Program.

Office of the Chief Information Security Officer (OCISO)

Information security is at the core of Trellix and has the full support and commitment from our CEO and top executives.

Trellix has implemented a centralized, global information security program led by the Office of the Chief Information Security Officer (OCISO). The OCISO organization is comprised of five main sub-organizations to support the confidentiality, integrity, and availability of Trellix information, assets, products, and services, and those that are entrusted to us. Those sub-organizations are:

- Governance, Risk, and Compliance
- Security Operations Center: US, Cork, Bangalore
- Product Security: Vulnerability Management, PSIRT, SDL, Security Architecture
- Federal Security Services
- OCISO Transformation: Customer Zero

The OCISO organization is customer zero at Trellix. We use our own Trellix products throughout the enterprise to prevent, detect, and respond to cyber threats that affect our business. By operating as customer zero, we can provide our product management teams valuable feedback which helps to ensure that the Trellix products we deliver to our customers are best in class.

With CEO and top executive commitment to information security and a global CISO-led security organization, Trellix engages, trains, and expects the entire workforce to exercise security in their daily role, as security is everyone's responsibility.

Information Security Management System

The Trellix Information Security Management System (Trellix ISMS) is at the core of the global information security program. It is designed to ensure that a risk-based approach is taken for the selection, implementation, and monitoring of appropriate security controls throughout the organization.

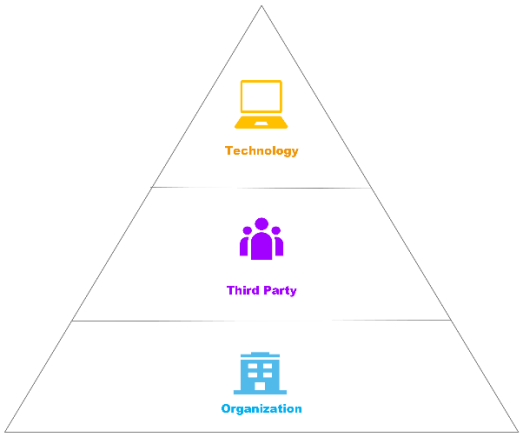
The baseline security controls that comprise the Trellix ISMS are based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 revision 5 and are further derived into management, operational, and technical categories. Industry standards, best practices, and additional security control frameworks may be

used for specific zones and products beyond the Trellix baseline, such as FedRAMP, ITGC/SOX, and others.

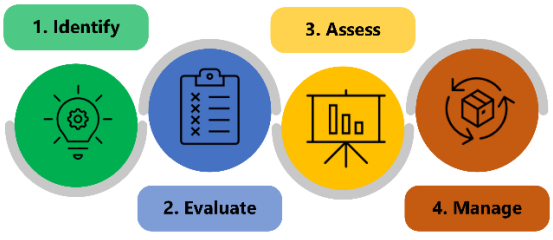
A set of internal policies and procedures govern the implementation, monitoring, and effectiveness of the security controls. Governance of the Trellix ISMS is maintained by management system reviews and operational reviews, focused on security operational control monitoring. The Trellix ISMS aligns and is certified to ISO/IEC 27001: 2013.

Information Security Risk Management

As part of the Trellix ISMS, Trellix Information Security Risk Management (Trellix ISRM) is critical for ongoing identification of threats, vulnerabilities, and risks to the enterprise. The Trellix ISRM consists of three tiers:



Each tier comprises of four phases to complete the Trellix ISRM process:



Each tier of the Trellix ISRM is built into existing business processes to provide continuous identification and management of risks. Information security risks are

captured into a risk register and reported. Trellix ISRM provides input into the Trellix ISMS baseline security controls.

Security Is Everyone's Responsibility

The high level of security at Trellix relies on a well-trained workforce. Where permitted under applicable law, Trellix employees are screened prior to hire, including undergoing, and passing background checks. Trellix personnel are required to acknowledge and consent to Trellix security and privacy policies once onboarded, including confidentiality obligations.

Once onboarded, Trellix personnel receive annual security awareness and data protection training as well as more detailed, role-based training where appropriate. In addition to training, ongoing security awareness activities based on identified risks and best practice are conducted throughout the year, such as the Trellix Immersive Phishing Program. As part of this program, Trellix personnel receive, at a minimum, one monthly simulated phishing email. Those who fall susceptible receive targeted training focused on identifying and reporting phishes.

Working on a Secure Network

The Trellix network is based on a segmented architecture, where certain zones are authorized for certain types of data processing, which then correspond to specific security controls.

Change management and security management enable Trellix to stay up to date on patches using centrally managed tools for deployment. Computer systems on the Trellix networks and computer systems used for Trellix business purposes have current, approved security, and malware protection measures in place. Trellix implements malware protection at a variety of locations, including, but not limited to the network, data centers, endpoints, servers, and email infrastructure. Logical access means are tested to determine their resistance to attacks and help to avoid any degradation or unwanted deletion.

Additionally, Trellix performs vulnerability scans against the internal infrastructure and externally to help ensure the latest content operating system and application-level updates are applied. Attack and penetration (A&P) testing are generally performed annually and performed more frequently in certain zones with critical data on existing services. New services are tested prior to production implementation. A&P testing is

conducted using a combination of internal Trellix resources and external service providers. Remediation of vulnerability scans and A&P is prioritized based on the severity of the vulnerability. Third parties are not granted access to internal Trellix systems without appropriate contractual agreements and security processes in place to appropriately protect Trellix data and assets.

Mobile devices connected to the Trellix network and information are required to be managed, helping to ensure that our mobile security controls are implemented and monitored. Additionally, mobile devices are not allowed to connect to our segmented production environments where customer data may be stored, processed, or transmitted. It is against company policy for Trellix information to be transferred or otherwise copied to a non-managed application or service.

Cloud Security

Trellix understands that cloud data security is critical. The security team works closely with our IT, engineering, and legal teams to understand and implement the required security controls for the relevant frameworks associated with cloud computing. Cloud management plane access is restricted following identity and access management (IAM) best practices, including utilizing multifactor authentication (MFA).

Asset discovery tools are implemented, and relevant data security technologies are used to protect Trellix information, including that of our customers, in Trellix controlled environments. Technologies implemented include data loss prevention (DLP) and encryption (client-side and server-side), as well as obfuscation, anonymization, tokenization, and masking. Continuous auditing occurs to highlight and help prevent possible data exposures. External-based perimeter assessments are performed at least weekly to significantly limit the attack vector and reduce the attack surface.

Data Protection

Data protection is a high priority for Trellix. Regardless of whether data is processed (collected, used, retained, disclosed, disposed, or otherwise acted on) on the Trellix network, or on a third-party vetted and approved cloud network, security controls are in place that are designed to ensure protection. Trellix requires the use of appropriate cryptographic controls to protect personal data—also known as personally identifiable information (PII) and personal information—in transit and at rest on removable media. This includes hard disk encryption on endpoints, including laptops.

Trellix data protection policies are designed so that access to all information assets is granted in a controlled manner based on the requester's "need-to-know," subject to the approval of the designated information asset owner and consistent with the "least privilege" principle.

Lawful Transfer of Personal Data

US Data Transfers

Our company is headquartered in the United States, and we have operations, entities, and service providers in the United States and throughout the world. As such, we and our service providers may transfer your Personal Data to, or store or access it in, jurisdictions that may not provide equivalent levels of data protection as your home jurisdiction. We will take steps to ensure that your Personal Data receives an adequate level of protection in the jurisdictions in which we process it.

EEA Data Transfers

We transfer Personal Data to countries outside of the EEA or Switzerland through a series of intercompany agreements based on the Standard Contractual Clauses in accordance with EU law and applicable EU regulations.

Residents of Japan, Argentina, and Canada Data

If you are a resident of Japan, Argentina, or Canada and you have an inquiry regarding your personal information we hold, including your personal information collected through your use of our products, you may request further information using the Individual Data Request Form.

Developing Secure Products

Trellix applications, whether purchased or developed internally, are subject to a release-to-production security review process. Trellix product software, IT applications, and cloud services are designed for security and privacy (using Security and Privacy by Design principles), while rigorous procedures are in place to find and remove security defects throughout the software lifecycle. These procedures define the Trellix Security Development Lifecycle (Trellix SDL), which consists of 32 technical, operational, and enterprise-level activities and reinforce our commitment to building secure software.

Please review the Trellix Product Security Practices document for more information. https://www.trellix.com/en-us/assets/docs/misc/ms-product-software-security-practices.pdf.

Maintaining Availability

Trellix recognizes that business continuity management and disaster recovery are holistic management processes and maintains a comprehensive corporate framework addressing continuity of operations that incudes emergency response, crisis management, business continuity, and disaster recovery. Trellix has business continuity plans with respect to significant business disruptions of critical operations. Such plans are structured to redirect and support Trellix and its customers in the event of an unexpected, harmful, or destructive incident. Core business services are replicated across Trellix offices and data centers. Should one site fail, services are redirected to other sites. Trellix leverages, among other practices, the following business continuity strategies:

- Relocating impacted businesses to designated recovery locations
- Using redundant processing capacity at other locations
- Rehearsing and testing recovery procedures

Trellix Security Operations Center

The Trellix Security Operations Center is where physical security and cybersecurity converge. Using the state-of-the-art technology, the Trellix Security Operations Center helps to ensure that all types of events, incidents, and cyberattacks are detected and responded to in a timely manner.

The Trellix Security Operations Center team identifies, hunts for, and react to threats. The tools used for these activities consist primarily of Trellix products supporting the customer zero concept. Trellix facilities utilize cameras and locks/key card/ badge access, which are monitored in its physical security practice. The Trellix Security Operations Center is physically and logically geo-redundant to maintain continuity.

Incident Response

Trellix maintains multiple information security incident response teams that follow established procedures for incident response training, testing, handling, monitoring,

reporting, and response assistance. These procedures help control and minimize the impact of an information security incident by defining the appropriate team and process by which to report and address an incident.

Reporting

The OCISO organization holds weekly operational reviews focused on security operations metrics, such as number of incidents, time to detect, and time to respond. This is part of overall Trellix ISMS governance.