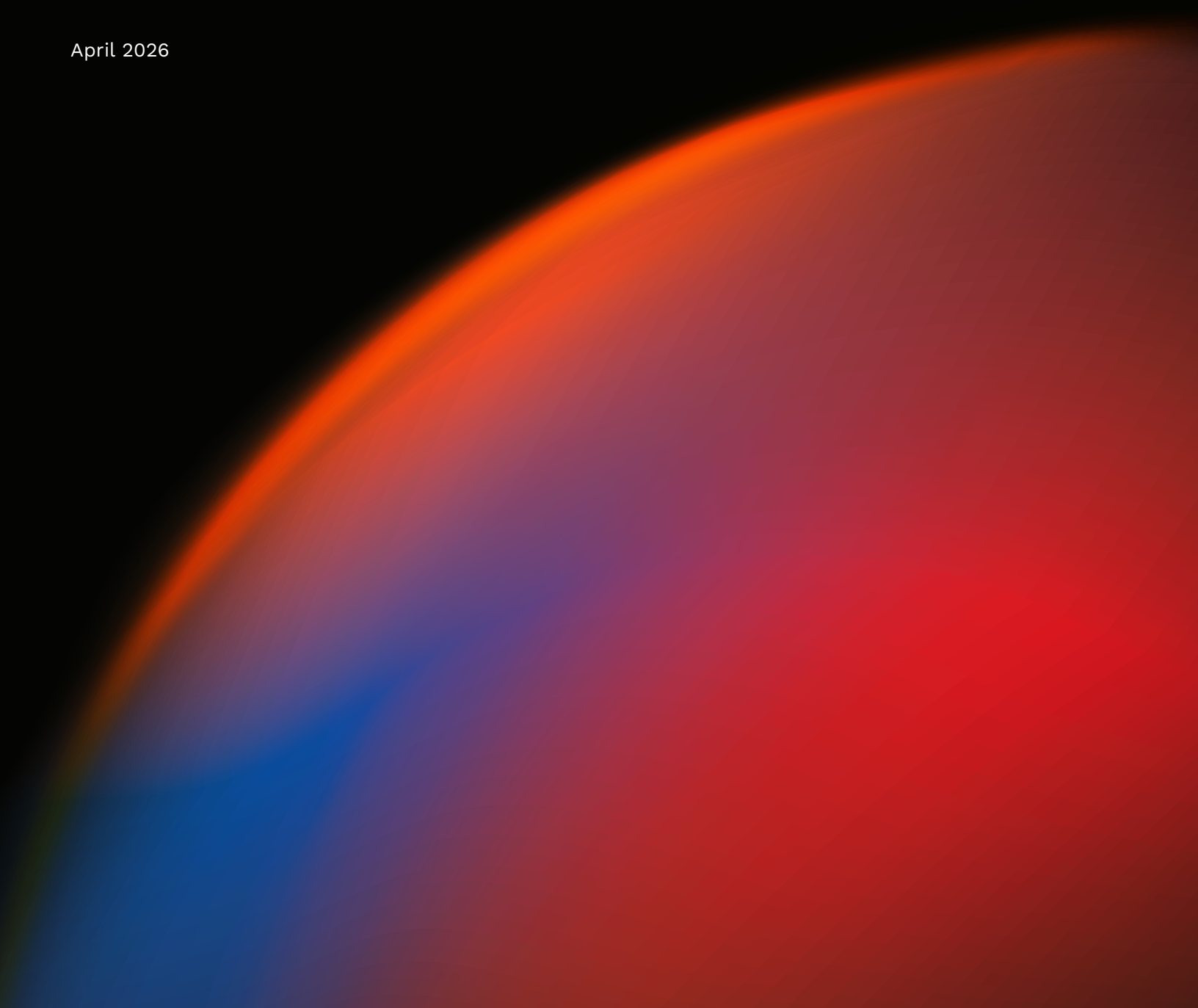


Transparency Report

April 2026

A large, abstract, curved graphic element in the bottom right corner, transitioning from a bright orange-red at the top to a deep red and then a dark blue at the bottom, set against a black background.

Contents

01	GOVERN (GV)	4
	Organizational Context (GV.OC).....	4
	Risk Management Strategy (GV.RM)	6
	Roles, Responsibilities, and Authorities (GV.RR)	6
	Policy (GV.PO)	7
	Oversight (GV.OV)	7
	Cybersecurity Supply Chain Risk Management (GV.SC).....	7
02	IDENTIFY (ID)	8
	Asset Management (ID.AM)	8
	Risk Assessment (ID.RA)	10
	Improvement (ID.IM)	10
03	PROTECT (PR)	11
	Identity Management, Authentication, and Access Control (PR.AA).....	11
	Awareness and Training (PR.AT).....	12
	Data Security (PR.DS).....	12
	Platform Security (PR.PS).....	13
	Technology Infrastructure Resilience (PR.IR).....	13
04	DETECT (DE)	14
	Continuous Monitoring (DE.CM).....	14
	Adverse Event Analysis (DE.AE)	16
05	RESPOND (RS)	17
	Incident Management (RS.MA)	17
	Incident Analysis (RS.AN)	18
	Incident Response Reporting and Communication (RS.CO)	19
	Incident Mitigation (RS.MI).....	19
06	RECOVER (RC)	20
	Incident Recovery Plan Execution (RC.RP)	20
	Incident Recovery Communication (RC.CO)	21

Introduction

The Transparency Report is a document that describes TrendAI™, the enterprise business unit of Trend Micro, and our security posture, which is aligned with NIST CSF 2.0. CSF 2.0 is a cybersecurity framework developed by the National Institute of Standards and Technology (NIST) that provides guidelines to systematically enhance an organization's cybersecurity risk management.

For more details, please refer to the following URL.

<https://www.nist.gov/cyberframework>

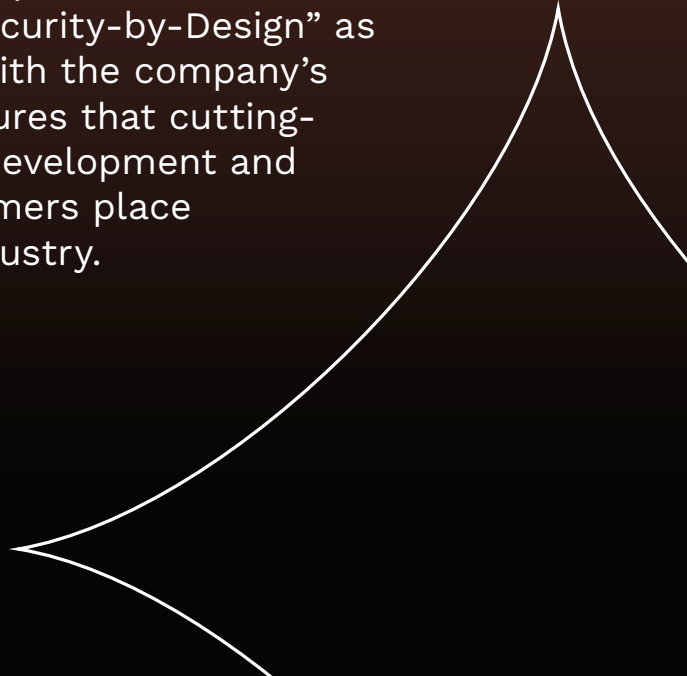
GOVERN (GV)

Organizational Context (GV.OC)

Business Strategy

TrendAI continues to grow under the unchanging corporate vision of making the world safe for exchanging digital information. This vision not only drives the development of TrendAI's AI-powered cybersecurity platform and services but also significantly influences our approach to security and risk management. Our platform and services, used by a diverse global customer base including enterprises, government agencies, critical infrastructure companies, and consumers, require absolute trust in our cybersecurity capabilities. As such, TrendAI consistently communicates our strategy and risk management practices clearly and effectively through our internal and external communication channels.

Furthermore, in product development, we balance our delivery capability between cloud-based and on-premise, addressing the diverse and ever-changing needs of our customers, particularly around compliance and data privacy requirements. This approach is implemented under the guidance of our global CISO, incorporating "Security-by-Design" as a default development process and aligning with the company's overall risk management framework. This ensures that cutting-edge security measures are applied at every development and delivery phase, enhancing the trust our customers place in us and our overall reputation within the industry.



Changing Organization

TrendAI has established a global compliance team that gathers, shares, reviews, and implements requirements from stakeholders worldwide, enhancing our overall level of security. Similarly, our global legal team fully collaborates and takes swift action on legal and regulatory compliance requirements, including privacy protection, data sovereignty, and security certifications. Through these efforts, TrendAI adapts quickly to changing regulatory requirements while maintaining our competitiveness in the international business environment.

To address the constantly evolving cyber threat landscape and business environment, TrendAI has transformed the company from a traditional function-based hierarchical model to an “objective-based non-hierarchical model” known internally as the “radial web.” This model moves away from a top-down decision-making structure, enabling employees across departments to proactively collaborate and swiftly implement necessary actions. This transformation in organizational structure allows TrendAI to rapidly adapt to changes, achieving sustainable growth and ensuring we are able to address our customers’ needs over the long term.

3 Pillars that Support Cybersecurity

TrendAI is a global cybersecurity leader with an advanced platform for detecting and protecting customers from threats while streamlining security operations. Completely aligned with the company’s corporate vision, TrendAI’s security and risk-management strategy is built on three fundamental pillars: people, process, and technology.

People: TrendAI declared our commitment to being a “threat defense expert” over 3 decades ago. This long-standing commitment supports our corporate vision and has resulted in a high level of security literacy among our employees, naturally elevating our overall security posture, and is reinforced with a strong education program for all employees.

Process: the organizational changes mentioned above greatly help in embedding our strategy and cyber risk management approach into the DNA of all teams and members.

Technology: In addition to highly effective traditional security capabilities, TrendAI has also been leveraging the power of artificial intelligence (AI) since 2006, well before the recent boom in generative AI. With an AI-powered platform that enables organizations to protect their ever-expanding attack surface – including AI –the technology enhances both our ability to detect and respond to threats for our customers – including our backend security processes and big data analysis from our millions of sensors spread across the globe. This improves the accuracy and operational excellence of our platform and service offerings, including TrendAI’s own security operations, and helps identify potential risks from threats and cyber attacks.

As a company that develops and deploys AI technologies, TrendAI recognizes our responsibility to ensure that these technologies are developed and used in ways that are ethical, transparent, and accountable.

Risk Management Strategy (GV.RM)

The purpose of risk management is to identify, evaluate, and address potential security threats and vulnerabilities before they can harm systems, data, or operations. By systematically assessing risks and implementing appropriate controls, it helps maintain compliance, protect nonpublic information, and information systems.

To effectively analyze, evaluate, categorize, and prioritize cybersecurity risks, TrendAI maintains a comprehensive risk management program aligned with international cybersecurity standards such as FedRAMP, PCI DSS, ISO 27001, ISO 27034-1, ISO 27014, and ISO 27017. A full list of our Compliance Program can be found on our Trust Center [https://www.trendmicro.com/en_us/about/trust-center/compliance.html]. We conduct periodic risk assessments, updating them as necessary to account for changes in information systems, nonpublic information, or business operations. These assessments thoroughly evaluate our assets and operating environment, allowing us to adapt controls in response to emerging threats and evolving technology.

We handle confidential information related to security threats from our customers, identifying such information as “Classified” and protecting it with advanced security measures designed to maintain data confidentiality and customer privacy. Additionally, to prevent any compromise to the Integrity and Availability of the service infrastructure that protects our customers, we have implemented and run comprehensive recovery measures (business continuity management).

TrendAI documents all essential information for each service in the Business Impact Analysis (BIA) Report, determining Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) and Recovery Point Objective (RPO) levels according to the service’s criticality. Business Continuity Plans (BCP) are reviewed and updated annually or whenever a major change occurs.

Roles, Responsibilities, and Authorities (GV.RR)

Cybersecurity risk management is carried out under the company’s internal security team, with each relevant department responsible for execution.

In TrendAI, global security governance is divided into two departments: the RDSec Team, which oversees the security of our platform and services, and the InfoSec Team, which oversees the security of information assets and systems.

RDSec Team

- Practicing Secure by Design
- Guiding Secure Coding
- Guiding Security Testing
- Providing Security Solutions
- Guiding DevSecOps Practices¹

InfoSec Team

- Security Risk Management
- Maintaining and Managing Security Certifications
- Developing and Operating Security Policies and Procedures
- Conducting Awareness, Education, and Training
- Implementing and Operating Security Management Measures
- Vulnerability Management
- Conducting Security Audits
- Security Monitoring and Incident Response

Cybersecurity risk management also includes HR practices.

New employees are required to complete a background check in accordance with local laws or regulations. Depending on the role or level, a criminal background check, education verification, and employment verification may also be conducted.

All employees must sign confidentiality / non-disclosure and invention assignment agreements as part of their initial employment terms and conditions. Additionally, they must receive security awareness training upon hire and renew it annually.

Policy (GV.PO)

TrendAI's information security policies are meticulously developed based on the Information Security Management System (ISMS) framework. These policies are implemented by each department and clearly communicated to all stakeholders.

To ensure continuous improvement and maintain a high level of organizational effectiveness, TrendAI conducts regular management reviews. These reviews help us identify areas for enhancement and ensure that our security measures remain robust and up-to-date. By adhering to these policies, we not only protect sensitive information but also foster a culture of security awareness across the organization.

In addition to our ISMS-based policies, TrendAI has established an AI Policy to guide the responsible development and use of artificial intelligence. This AI Policy is shaped by industry best practices and global standards, ensuring our approach is both ethical and effective. TrendAI ensures that our AI innovations are aligned with our longstanding commitment to security, privacy, and ethical responsibility.

Responsible Use of Artificial Intelligence - Trust Center

[\[https://www.trendmicro.com/en_us/about/trust-center/privacy.html?modal=s3c-btn-learn-more-3fe492\]](https://www.trendmicro.com/en_us/about/trust-center/privacy.html?modal=s3c-btn-learn-more-3fe492)

Oversight (GV.OV)

TrendAI's FedRAMP, ISO 27001, ISO 27034-1, ISO 27014, and ISO 27017 certificates include multiple elements of cybersecurity risk management. The resulting reports from audits are analyzed and leveraged to refine, improve, and adjust our risk management strategy—ensuring it remains aligned with evolving threats, business objectives, and industry best practices.

TrendAI follows those guidelines to ensure resources—whether financial, technological, or human—are strategically allocated for effective cybersecurity risk management. By aligning resource distribution with identified risks and business objectives, we maintain a resilient security posture across our platform, services, and operations.

Cybersecurity Supply Chain Risk Management (GV.SC)

TrendAI's Information Security Policy includes an Outsourcing Policy and Cloud Security Policy, which addresses supply chain risk management to ensure that controls are implemented to maintain the security of information when it is processed by another organization.

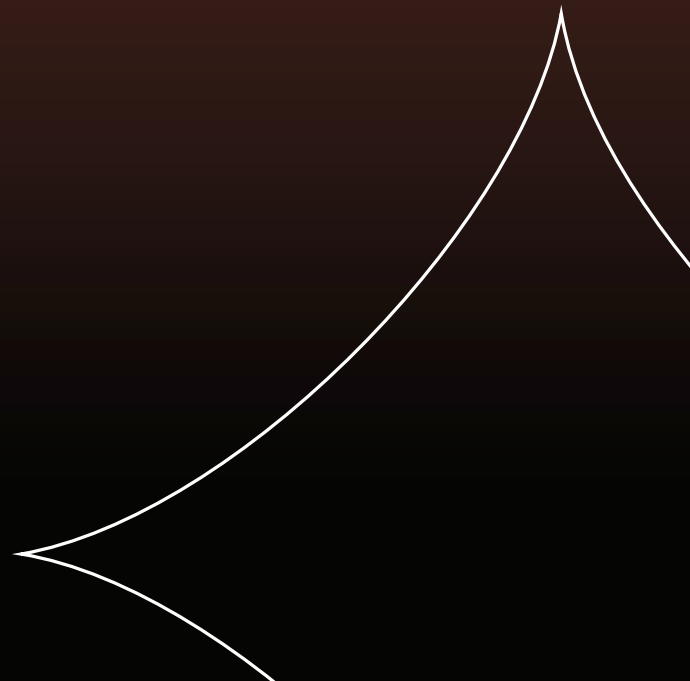
TrendAI maintains an Incident Management Policy, which is part of our corporate information security policy. Our Incident Management Policy has been defined as: Incident Monitoring and Response, Reporting Security Incidents, Reporting Security Weaknesses, Reporting Software Malfunctions, and Learning from Incidents. The responsibilities and handoff points for all relevant parties are included in the Incident Management Procedures, including suppliers.

The TrendAI security team has a vetting process to maintain the relationship with our supply chain partners via security reviews and risk assessment evaluations designed to meet the requirements.

IDENTIFY (ID)

Asset Management (ID.AM)

TrendAI identifies and inventories all critical assets—including hardware, software, and data—throughout their lifecycle. Our policies set clear standards for asset classification and handling, aligned with our Code of Conduct and employee agreements. By managing assets based on their sensitivity and importance, we ensure security and proper use from acquisition to decommissioning.



Data Classification and Prioritization

TrendAI maintains a detailed and current inventory of all critical assets, including physical devices, software, and data—regardless of whether they are owned internally or sourced from external partners. Each asset is carefully classified and prioritized according to its business value and risk profile, allowing us to provide targeted protection and ensure efficient allocation of resources.

To further enhance security and transparency, we map and monitor all authorized data flows and network structures. This proactive approach enables us to quickly detect and respond to any unauthorized activity, safeguarding our operations and our clients' trust.

Data at TrendAI is classified in accordance with our internal policies into four categories: Top Secret, Confidential, Internal Use Only, and Public. We conduct an annual review of our major information assets to ensure the accuracy of our inventory. Additionally, copies of all critical information assets are securely stored onsite to support business continuity and data integrity.

Asset Lifecycle and Supply Chain Management

At TrendAI, we take a comprehensive approach to asset management, covering the entire lifecycle of our devices and systems—from acquisition and deployment to ongoing maintenance and secure decommissioning. Each stage is governed by clear roles and procedures to ensure that assets are consistently protected and accurately tracked.

We maintain a detailed inventory of all devices, recording key information such as machine name, unique ID, purpose, asset owner, operating system, physical location, department, and environment (e.g., production, development, or testing). Department managers are responsible for helping keep this register up to date and reporting any changes promptly.

Recognizing that information sensitivity can change as our business evolves, we regularly review and update information classifications. Any changes or new classifications are approved by our Service Owners to ensure appropriate handling. Outdated classified documents are securely destroyed using advanced shredding technology, while obsolete electronic data is deleted, overwritten, and storage media reformatted to prevent unauthorized access.

TrendAI places a strong emphasis on supply chain security. All suppliers are carefully assessed based on potential outsourcing risks to business continuity and information security. High-risk suppliers undergo cross-functional reviews to ensure risks remain controlled, with corrective actions taken as needed. For cloud service providers, a mandatory security assessment is conducted in collaboration with the vendor, using compliance checklists and relevant criteria to ensure robust protection.

Through comprehensive asset management, rigorous information classification, and robust supply chain oversight, we demonstrate our ongoing commitment to transparency and information security for our customers, partners, and stakeholders.

Risk Assessment (ID.RA)

TrendAI considers cybersecurity risks as one of the most critical issues in our operations. Cyber risks are threats related to cyberspace and digital technologies. These risks arise from threats exploiting vulnerabilities, leading to real-world consequences that negatively impact the organization. Some specific risks include:

- > Information Leakage: Information being stolen or leaked.
- > Business Disruption: Interruption of operations due to DoS attacks, data tampering, or destruction.
- > Financial Theft: Money being stolen or extorted.
- > Reputational Damage: Damage to reputation due to direct or indirect impacts.

We strive to properly assess these risks by analyzing threats and vulnerabilities and working towards improvements.

Vulnerability Management Initiatives

TrendAI monitors vulnerabilities in third-party components and our proprietary code, responding quickly based on risk scores. Vulnerabilities are tracked through our change management system and managed through regular reviews. Additionally, we responsibly disclose vulnerability information and release patches in a timely manner based on their importance.

We also continuously review and update factors that could lead to vulnerabilities, anticipating risks. Specific measures include conducting penetration tests and red team exercises by third parties. These tests identify organizational weaknesses from an attacker's perspective and help us implement countermeasures.

In red team exercises, we test our systems' vulnerabilities from an attacker's viewpoint to improve our defense techniques and response processes. For example, in a 2023 scenario combining "watering hole attacks" and "human-operated ransomware," the effectiveness of our defenses was confirmed when devices were isolated before the attack was detected. Based on the results of these exercises, our blue team improves defense techniques and reviews incident response processes, implementing specific measures such as transitioning from on-premises to cloud versions and enhancing network micro-segmentation. Furthermore, we use the insights gained from these exercises to improve our security product detection logic and add new features, thereby enhancing security quality.

*Cyber Attack Exercises Practiced by TrendAI (Part 1) ~ Thoroughly Uncovering Organizational Pain Points from the Perspective of Cyber Attackers (Japanese) :

https://www.trendmicro.com/ja_jp/jp-security/23/g/expertview-20230710-01.html

Commitment to Risk Assessment

Through these risk assessment initiatives, TrendAI aims to protect information and ensure business continuity, providing an environment where our services can be used with confidence.

Improvement (ID.IM)

At TrendAI, we integrate cybersecurity risks—such as information leaks and business disruptions—into our comprehensive corporate risk management process. We continuously reassess our assets, evaluating their importance and the likelihood of potential threats, while proactively identifying emerging cybersecurity risks.

We believe in learning from every incident to minimize the chance of recurrence and reduce potential impact. Each incident is thoroughly analyzed to identify root causes and implement effective mitigating controls. To ensure our preparedness, our incident management process is tested, practiced, or reviewed at least once a year.

Our commitment to continuous improvement spans all key areas of cybersecurity: Governance, Identification, Protection, Detection, Response, and Recovery. Through these ongoing efforts, we strengthen our resilience and safeguard our customers, partners, and stakeholders.

PROTECT (PR)

Identity Management, Authentication, and Access Control (PR.AA)

TrendAI centralizes its identity system by syncing to a Single Identify provider (IdP). All user, service, and hardware credentials are managed from a unified platform. This ensures a single source of truth—credentials are issued and revoked in one system, reducing human error and simplifying audits.

When a new employee joins, HR validates their identity, and IT binds that proofed identity to formal credentials.

Every access—whether to on-prem servers, cloud apps, APIs, or hardware—is authenticated through credentials plus a second factor. This meets strong authentication standards and further lowers risk.

Identity assertions between systems are carried via secure protocols like SAML and TLS encryption. This ensures integrity and prevents tampering during cross system authentication

Access permissions are defined through roles and group policies. Profiles are assigned using the principle of least privilege (PoLP) and sensitive roles in leverage Privileged Identity Management for just-in-time elevation. Periodic reviews flag stale or excessive entitlements.

TrendAI enforces physical security controls for its on-prem data centers: badge access, surveillance, locked server racks, and audit logs—all risk-adjusted and monitored—complemented by cloud-only hardware managed under data center compliance mechanisms.

Awareness and Training (PR.AT)

As a cybersecurity company, TrendAI recognizes that people are the first line of defense against cyber threats. Our approach to awareness and training is designed to equip all personnel—including employees and contractors—with the knowledge and skills necessary to protect our clients and operations.

General Awareness and Continuous Learning

All users of our internal resources receive foundational cybersecurity training, covering topics such as social engineering, safe password practices, and the importance of reporting suspicious activity. We emphasize the consequences of policy violations and require annual refresher courses to reinforce best practices. Regular assessments ensure that basic cyber hygiene is understood and followed throughout the organization.

Role-Based Training for Specialized Functions

For specialized roles such as IT, finance, and executive leadership, we provide tailored, role-based training that addresses the unique risks these positions face. These programs are also mandated for relevant contractors. Individuals in these roles participate in periodic evaluations and annual updates to ensure their knowledge remains current and effective against evolving threats.

Data Security (PR.DS)

TrendAI believes that protecting the three key elements of data security—Confidentiality, Integrity, and Availability—is crucial.

For example, TrendAI implement the following measures:

Acceptable usage of portable devices (such as PDA's, mobile telephones, mobile messaging devices and USB memory sticks) must be defined and include guidelines. Conducting offline and offsite backups to avoid data loss in case of incidents. Ensuring the confidentiality and integrity of data, we determine encryption requirements for storage and transmission based on applicable legal and regulatory obligations, utilizing industry-standard technologies such as AES for data storage and TLS for data transmission. Messaging applications are allowed, but shall not be used to discuss company confidential information. Our cybersecurity platform is designed with built-in security measures from the initial development phase. TrendAI's platform undergoes regular evaluations and audits (ex: ISO27001, SOC2), and we follow strict guidelines for customer data protection to ensure comprehensive data security.

Platform Security (PR.PS)

Platform Security Management

At TrendAI, we rigorously manage platform configurations, conducting regular reviews and updates to ensure optimal security and performance. We also pay similar attention to hardware maintenance, replacing or disposing of equipment based on risk and lifecycle status. Through detailed log generation and continuous monitoring across all systems, we enable real-time incident detection and response, maintaining system integrity and availability. Additionally, we implement strict controls to prevent the installation and execution of unauthorized software to counteract the risks of malware and malicious software.

For example, in hardware asset management, customer and employee data must be destroyed or disposed of when no longer needed. Disposal must follow internal procedures for secure data destruction. For platform vulnerability management, users are required to apply the latest OS/software security patches to their computers, adhering to IT department requirements and guidelines. Users must apply vendor-provided security patches within the appropriate timeframe: critical security patches within 30 days and other severity patches within a maximum of 3 months.

Establishing Secure Software Development Practices

At TrendAI, we integrate security into the software development process from the initial stages and monitor its effectiveness throughout the lifecycle. Software is regularly updated based on risk, and we review industry vulnerability feeds related to third-party components to respond promptly. Secure development practices are integrated from the design phase, ensuring security throughout the development process. This approach protects applications from potential threats and enables us to deliver highly reliable software.

To achieve early detection and remediation of vulnerabilities, we undertake various initiatives. As part of our vulnerability management efforts, we leverage our world-leading Zero Day Initiative (ZDI) network and expertise to run bug bounty programs and maintain an internal security research team for vulnerability investigations. When vulnerabilities are found in our products, we strive to disclose information appropriately.

Technology Infrastructure Resilience (PR.IR)

TrendAI has designed our network as a series of segmented trust zones—strictly isolating development, testing, production, administrative, guest, and IoT environments. Only the bare minimum of necessary network paths are opened between them. Similarly, external connections (such as VPNs or cloud links) are tightly controlled: only expressly permitted traffic is allowed into and out of each zone based on defined access needs. This helps to limit impact in case of compromise and prevents attackers from easily pivoting or moving laterally across systems.

To reinforce that segmentation, a zero-trust network strategy is applied—where every access request to a resource, even internal ones, is continuously authenticated and authorized. This dynamic checking ensures only devices and users with verified security posture (e.g. endpoint health, strong authentication) can reach sensitive systems.

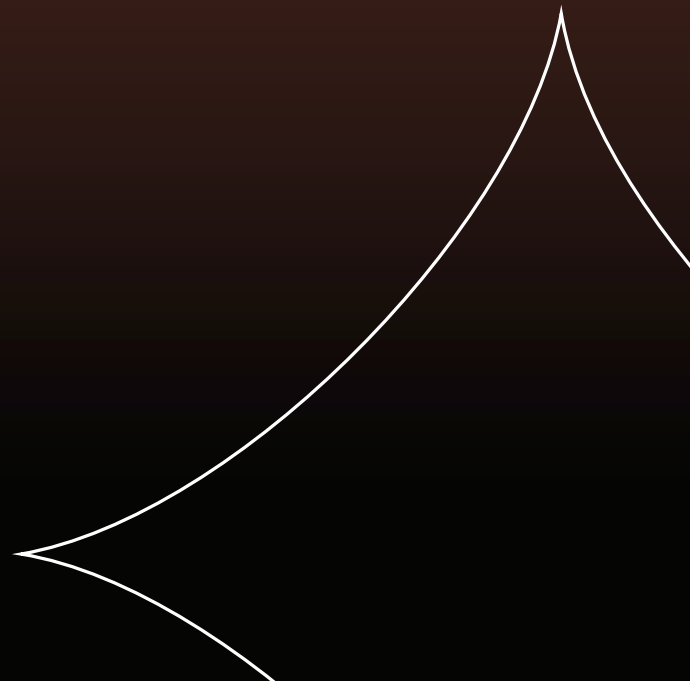
Additionally, pre-connect endpoint validation—such as device health checks before granting access—ensures that unmanaged, outdated, or compromised devices cannot penetrate secure environments.

Behind the scenes, a hardened boundary of firewalls, access control, intrusion detection/prevention systems (IDS/IPS) constantly enforce these segmentation policies and continuously monitor for attempts to bypass them. All traffic is logged and anomalous behaviors trigger alerts, enabling rapid incident detection and response.

DETECT (DE)

Continuous Monitoring (DE.CM)

Continuous monitoring is a cornerstone of TrendAI's cybersecurity strategy. We recognize that early detection of anomalies and potential threats is essential for protecting our assets and maintaining trust with customers and partners. Our monitoring framework covers networks, physical environments, personnel activity, external service providers, and critical computing resources, ensuring a comprehensive and proactive security posture.



Network, Physical, and Personnel Monitoring

Our networks and network services are continuously monitored to detect unusual activities and potential threats. This includes identifying unauthorized devices on both wired and wireless networks, and comparing network activity against established baselines to quickly spot deviations. We also monitor facilities for rogue wireless networks and changes in network security postures to support a zero-trust environment.

In addition to network vigilance, we maintain robust physical security monitoring. Access control systems such as badge readers, ID cards, and visitor logs are regularly reviewed for unusual access patterns or failed attempts. Physical security measures, including alarms and surveillance cameras, help us detect and respond swiftly to any signs of tampering or unauthorized entry.

Personnel activity and technology usage are monitored using advanced analytics. We employ behavior analytics software (ex. TrendAI Vision One) to identify anomalous user actions that may indicate insider threats. System logs are regularly reviewed to uncover unusual access patterns, and detection technologies are in place to promptly identify potential security incidents.

Monitoring of External Providers and Critical Assets

We extend our monitoring practices to all external service providers, including those offering remote or onsite support. Activities from cloud-based services and internet service providers are closely observed for deviations from expected behavior, ensuring third-party activities do not introduce new risks.

Our monitoring also covers all critical computing hardware and software. We continuously scan for malware, phishing attempts, data leaks, and configuration changes that could impact security. Authentication attempts are monitored to detect credential attacks, while endpoint technologies help us identify and isolate compromised devices before they can access sensitive resources. By maintaining this vigilant and layered monitoring approach, we ensure rapid detection and response to any adverse events, upholding the high standards of security for our organization and stakeholders.

Adverse Event Analysis (DE.AE)

TrendAI places strong emphasis on the timely and accurate analysis of anomalies and potential threats. Our approach combines advanced automation with expert review to ensure that potentially adverse events are rapidly identified, thoroughly analyzed, and appropriately escalated. By leveraging both technology and human expertise, we continuously refine our detection and incident response capabilities to protect our organization and our customers.

Event Correlation and Contextualization

Our security operations center relies on a centralized SIEM platform and log analysis tool (ex. TrendAI Vision One) to continuously monitor and analyze security events across our global infrastructure. We aggregate log data from a wide range of sources, including network devices, endpoints, cloud services, and physical access controls. Automated event correlation allows us to connect seemingly isolated events, providing a clearer understanding of threat actors, their methods, and potential indicators of compromise. We further enhance our analysis by integrating up-to-date cyber threat intelligence feeds and asset inventory data, enabling us to rapidly contextualize events and assess their relevance to our environment.

For technologies or environments that cannot be fully monitored with automation, our security experts regularly conduct manual log reviews. This combination of automated and manual analysis ensures that even subtle or emerging threats are not overlooked. When adverse events are detected, we estimate their potential impact and scope using both automated tools and expert assessment, allowing us to prioritize response actions effectively.

Communication and Incident Declaration

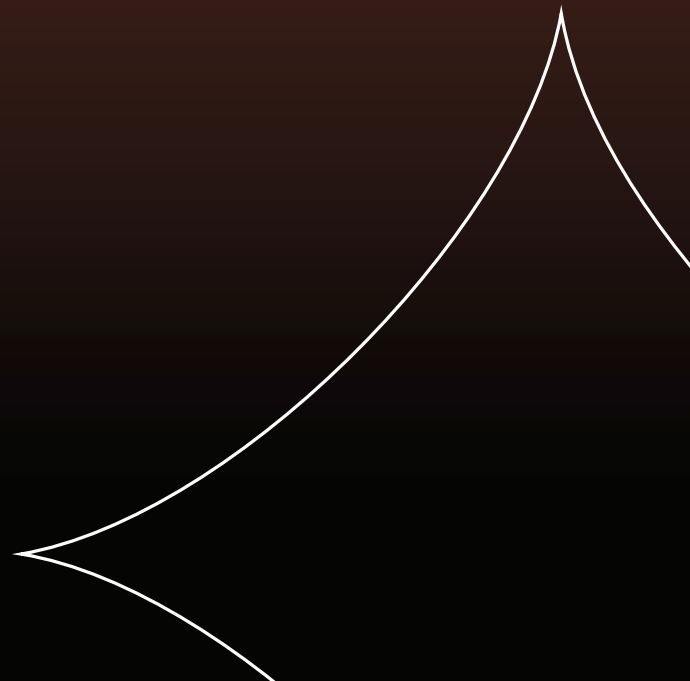
Clear and timely communication is a critical component of our adverse event analysis process. Alerts generated by our monitoring systems are immediately provided to authorized personnel, including our security operations center and incident response teams. Findings are shared through secure channels and, when necessary, tickets are automatically or manually created in our incident management system to ensure appropriate follow-up. We maintain strict access controls to ensure that only authorized staff can access sensitive analysis results and incident data.

Our criteria for declaring security incidents are clearly defined and aligned with standards such as ISO 27001 and SOC 2. When adverse events meet these criteria, incidents are formally declared and escalated according to our response procedures. We continuously review and refine our incident declaration process, taking into account lessons learned and the evolving threat landscape to ensure that our response remains both swift and effective.

RESPOND (RS)

Incident Management (RS.MA)

TrendAI recognizes that robust and transparent incident management is fundamental to maintaining trust and resilience. Our incident response framework is designed to ensure that every detected cybersecurity incident is managed systematically and in close coordination with relevant stakeholders. This section outlines our approach to incident management, emphasizing our commitment to timely detection, effective coordination, and continuous improvement.



Incident Detection and Response Coordination

Upon identification of a cybersecurity incident, our detection technologies automatically generate alerts and reports, ensuring rapid awareness and response. Each incident is promptly assigned to a designated incident lead, who coordinates actions across internal teams and, where appropriate, with third-party partners. We maintain established procedures for engaging external incident response specialists when necessary, ensuring that expertise and resources are mobilized without delay. Our response plan is closely aligned with business continuity and disaster recovery strategies, allowing for a seamless transition to recovery processes when required. Throughout the response, we maintain clear communication with stakeholders to ensure transparency and accountability.

Incident Assessment, Categorization, and Escalation

Every incident report undergoes an initial triage to confirm its relevance to cybersecurity and to determine the appropriate response activities. We apply predefined criteria to estimate the severity and potential impact of each incident, enabling us to prioritize effectively. Incidents are further categorized based on their nature, such as data breaches, ransomware, or service disruptions, and prioritized according to scope, urgency, and potential business impact. Our escalation protocols ensure that incidents are elevated to the appropriate level of management. The status of ongoing incidents is continuously tracked, and escalation decisions are made in consultation with designated stakeholders to maintain oversight and drive timely resolution.

Recovery Criteria

The decision to initiate recovery processes is guided by clear criteria that consider both the characteristics of the incident and the potential operational impact of recovery activities. We balance the need for swift restoration of services with the importance of preserving evidence and conducting thorough investigations. Lessons learned from each incident are systematically reviewed and integrated into our incident response plan, supporting ongoing refinement of our processes. The incident management process must be tested, practiced or reviewed at least annually.

Incident Analysis (RS.AN)

Effective incident analysis is a cornerstone of our cybersecurity operations. As a global leader in cybersecurity, we are committed to conducting thorough investigations for every cybersecurity incident, ensuring that our response is both timely and evidence-based. Our approach is designed not only to support immediate response and recovery but also to facilitate forensic investigations and continuous improvement of our security posture.

Investigation Process and Evidence Integrity

When an incident occurs, we initiate a structured investigation process that emphasizes both accuracy and transparency. All personnel involved in incident response, including responders, system administrators, and cybersecurity engineers, are required to meticulously document their actions throughout the investigation. These records are maintained in a secure format, ensuring that every step taken can be traced and verified. The incident lead is responsible for compiling a comprehensive record of the incident, safeguarding the integrity and authenticity of all documentation and information sources. This disciplined approach ensures that the provenance of all actions and evidence is preserved, supporting both internal reviews and potential external audits.

Data Collection, Magnitude Estimation, and Validation

A critical part of our analysis involves the systematic collection and preservation of incident data and metadata. We follow strict chain-of-custody procedures to maintain the integrity of all evidence, including details such as data source and timestamps. This practice ensures that all information remains reliable for forensic analysis and potential legal proceedings. To accurately assess the scope and magnitude of each incident, we review affected systems and investigate other potential targets for signs of compromise or persistent threats. Automated tools are employed to efficiently search for indicators of compromise across relevant assets. This comprehensive review allows us to validate the true impact of the incident and inform our response and recovery strategies.

Incident Response Reporting and Communication (RS.CO)

Transparent and timely communication is essential to effective incident response. As a global leader in cybersecurity, we understand that how we report and communicate during incidents not only affects our clients and partners but also demonstrates our commitment to regulatory compliance and industry best practices. Our approach is built to ensure that all relevant stakeholders are kept informed throughout every phase of an incident, supporting coordinated response and building trust.

Stakeholder Notification and Communication

When InfoSec confirms that customer and/or PII data records are impacted as result of a security incident, we take action to inform affected clients, business partners, and other stakeholders in accordance with contractual obligations and applicable regulations. Our procedures include notifying regulatory authorities and law enforcement agencies when required, ensuring that all legal responsibilities are met. We recognize the importance of clear and accurate communication, especially when sensitive data or critical business operations are involved. Notifications are tailored to the needs of each stakeholder group, providing them with timely, relevant information to support their own response actions.

Information Sharing and Coordination

Beyond initial notifications, we are committed to ongoing information sharing throughout the incident lifecycle. Internal teams and senior leadership are regularly updated on incident status, ensuring that decision-makers have the information they need to coordinate response efforts. When incidents involve third-party suppliers or partners, we follow established information sharing protocols defined in contracts and agreements, maintaining secure channels for exchanging sensitive information. We also participate in industry information sharing initiatives, such as contributing anonymized threat intelligence to critical industry sharing programs, such as the Microsoft MAPP program. (https://www.trendmicro.com/en_us/research/21/g/new-collaboration-with-adobe-and-mapp.html) This collaborative approach not only enhances our own response capabilities but also strengthens the broader cybersecurity community.

Incident Mitigation (RS.MI)

Incident mitigation is a critical part of our cybersecurity response strategy. As a global leader in cybersecurity, our priority is to act swiftly and decisively to prevent the spread of security events and reduce their impact. We combine advanced automated technologies (including new agentic AI capabilities) with expert human intervention to ensure that incidents are both contained and eradicated as efficiently as possible.

Containment and Eradication Process

Upon detection of a security incident, our first objective is to contain the threat and prevent further damage. We utilize a combination of cybersecurity technologies, such as threat detection technologies and advanced network security which can detect issues as well as initiate containment measures. At the same time, our incident response team has the authority to independently assess the situation and apply manual containment actions when necessary, ensuring flexibility and precision in our response.

Once the incident is contained, the focus shifts to eradication. Tools are employed to remove malicious elements from affected systems and restore normal operations. Our experts also conduct manual eradication procedures when required, particularly in complex scenarios where tailored actions are needed. Throughout the process, we maintain detailed records and continuously monitor the environment to confirm that the threat has been fully eliminated.

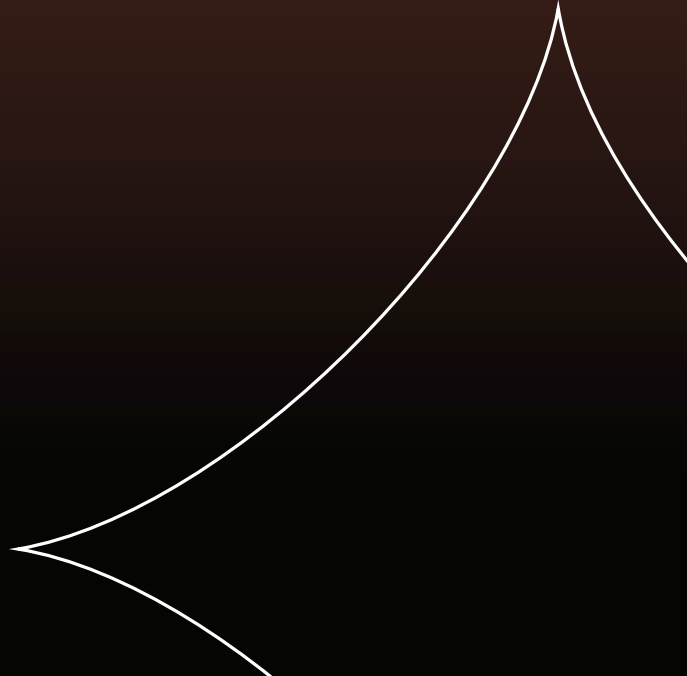
Ongoing Commitment

We are committed to regularly reviewing and updating our mitigation procedures to adapt to evolving threats and technologies. By combining automation with skilled human oversight, we ensure a robust and effective response to every incident. This approach not only limits the immediate impact of security events but also strengthens our overall resilience, reinforcing trust with our clients and partners.

RECOVER (RC)

Incident Recovery Plan Execution (RC.RP)

Ensuring swift and reliable recovery after a cybersecurity incident is essential for maintaining business continuity and client trust. As a global leader in cybersecurity, we are committed to executing structured recovery plans that restore affected systems and services while minimizing disruption. Our recovery process is designed to be thorough, transparent, and adaptable to each incident's unique context.



Recovery Plan Implementation and Integrity Assurance

Once an incident response process triggers the need for recovery, our team initiates the recovery portion of our incident response plan. All responsible personnel are briefed on their roles and the necessary authorizations to carry out recovery tasks. Recovery actions are selected and prioritized based on the impact to critical business functions, available resources, and ongoing assessments of organizational needs. Before any restoration begins, we verify the integrity of backups and other restoration assets, checking for signs of compromise or corruption. This step ensures only clean and reliable data is used to restore operations, safeguarding against reinfection or further disruption.

Restoration, Validation, and Post-Incident Review

Restoration efforts focus on bringing essential systems and services back online in the correct order, guided by business impact analyses and service delivery objectives. We work closely with system owners to confirm successful restoration and monitor performance to validate the adequacy of recovery actions. Before restored assets are returned to production, their integrity is verified, and root causes of the incident are addressed. Once normal operations are confirmed and all criteria are met, we formally declare the end of the recovery phase. An after-action report is prepared to document the incident, the steps taken, and lessons learned, it also supports continuous improvement to minimize the risk of recurrence of the same incident.

Incident Recovery Communication (RC.CO)

Effective communication during incident recovery is fundamental to maintaining trust and ensuring coordinated action among all stakeholders. As a global leader in cybersecurity, we prioritize transparency and clarity in sharing recovery progress across relevant teams.

Throughout the recovery process, we provide timely updates to designated stakeholders, including senior leadership, affected clients, and critical suppliers. Information about restoration activities is securely shared according to established response plans and contractual agreements. We ensure that all communications are consistent and comply with information sharing protocols, enabling informed decision-making and collaboration.

For incidents that require public disclosure, we follow approved messaging and notification procedures. Our updates clearly outline the recovery steps underway and the measures being implemented to prevent future occurrences. By maintaining open and structured communication, we reinforce our commitment to accountability and support a swift return to normal operations.

About TrendAI™

TrendAI™, the global AI security leader and enterprise business unit of Trend Micro, empowers organizations with full AI visibility and consolidated security that inspires confidence, drives innovation, and eliminates risk. Trusted by the largest enterprises and governments across 185 countries, TrendAI™ secures the entire organization, from identities to infrastructure to data. AI Fearlessly. [trendaisecurity.com](https://trendmicro.com/privacy)