Tuya AI Security and Compliance White Paper

Practicing Responsible AI, Building a Trusted Intelligent Ecosystem

Version: V1.0
Release Date: 20251230

Content

Foreword

Opportunities and Responsibilities in the New Era of Intelligence

We are living in a new era of the AI-driven Internet of Everything. Intelligent voice assistants, AI-powered visual recognition, and personalized scene recommendations are integrating into the homes, workplaces, and daily lives of users worldwide with unprecedented depth and breadth. As a leading global AI cloud platform service provider, Tuya Smart is dedicated to empowering millions of devices with intelligence through technological innovation, connecting brands, manufacturers, developers, and end-users across the globe.

However, while AI technology enhances convenience and efficiency, it also introduces complex and unique challenges: **data privacy, algorithmic fairness, system reliability, and global compliance**. When AI can "hear" our voices, "see" our environments, and "predict" our behaviors, establishing and maintaining user trust is no longer an option—it is the cornerstone of our sustainable business development.

At the Crest of the Wave: Global AI Trends and Regulatory Landscape

The global race for AI technology has begun, accompanied by increasingly rigorous and complex regulatory frameworks. Understanding this macro background is fundamental to building trusted AI.

- Technological Development Trends:
  - **Convergence**: AI is deeply coupled with IoT, Edge Computing, and Big Data technologies, giving birth to intelligent entities capable of real-time perception, decision-making, and action (e.g., AI speakers, smart home robots).
  - **Democratization**: Generative AI and Large Language Model (LLM) technologies are rapidly cascading down to various terminal devices. While delivering ultimate personalized experiences, this also significantly expands the attack surface for data collection and model inference.
  - **Boundary Expansion**: AI is moving from the virtual world to the physical world. Its decisions are beginning to directly impact physical safety (e.g., smart security, elderly care) and critical infrastructure.
- Global Legislation and Regulatory Trends:
  - **EU AI Act**: Pioneering a "risk-based" regulatory approach, it classifies AI systems for control. It comprehensively bans AI applications deemed to have "unacceptable risks" (e.g., social scoring) and sets extremely strict obligations for high-risk AI systems (e.g., critical infrastructure, medical devices).
  - **China's AI Governance Framework**: China has promulgated regulations such as the Interim Measures for the Management of Generative Artificial Intelligence Services, emphasizing inclusive prudence and classified, graded supervision. It requires AI service providers to assume responsibility for network information security, data security, and personal information protection, and to establish content governance mechanisms.

- **US and Rest of World**: The US is driving AI safety standards through executive orders, emphasizing red-teaming and safety assessments for powerful AI models. Meanwhile, economies worldwide are accelerating the construction of local AI governance systems modeled after EU and Chinese regulations. The core consensus of legislation focuses on safety, transparency, fairness, and accountability.

In this context, compliance is not merely a legal requirement but a passport to global markets and a core competitive advantage.

Tuya Smart: Global AI Cloud Platform Service Provider

- **Tuya's AI Strategy**: To empower developers, accelerate Physical AI innovation, and amplify the enabling effect of the platform. Based on general engines like the TuyaOpen open-source development framework and the AI Agent development platform, we provide developers with convenient AI technology and ecosystem support. This significantly lowers the barrier to AI development, assists in creating various life Agents, accelerates the integration of AI technology with the physical world, and promotes the large-scale implementation of Physical AI.
- **Our Approach**: By building an AI system that is human-centric, compliant, transparent, risk-controlled, and responsible, Tuya provides AI empowerment for hardware products. We aim to continuously output differentiated value for developers and create a safer, more convenient, and smarter lifestyle for users.

Tuya Smart's Vision for AI Security and Compliance

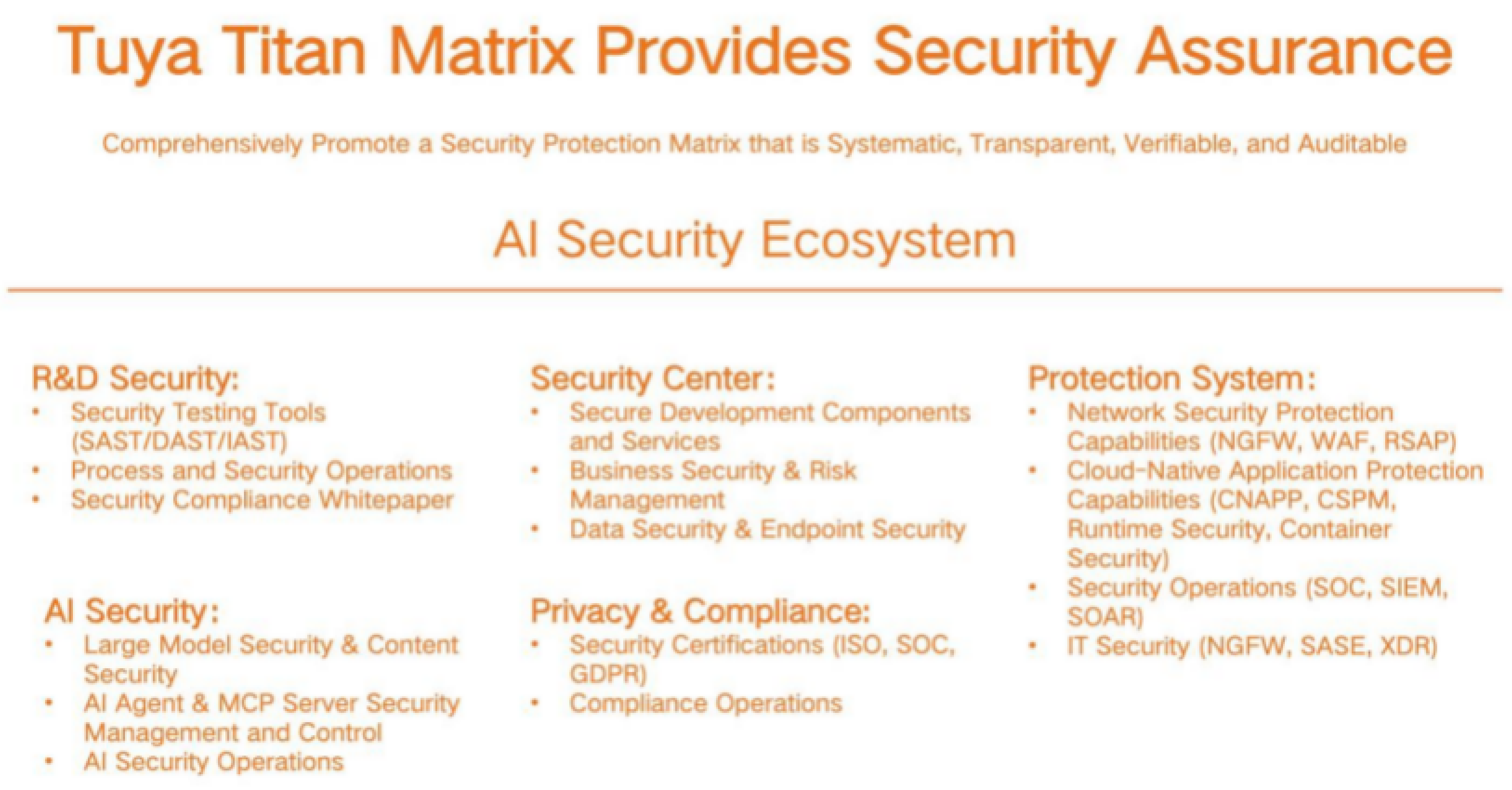
Tuya Smart's vision for AI Security and Compliance is to be a builder of a trusted intelligent ecosystem. We firmly believe that security and compliance are not constraints on innovation, but the prerequisites and core drivers of innovation. Our commitments are:

- **Responsible to Users**: Ensuring user data receives the highest level of protection, giving users full right to know and control their data and devices.

- **Responsible to Partners**: Providing our customers (OEMs/ODMs, brands) with secure, reliable, and compliant AI innovative products and technology platforms, helping them quickly enter global markets and maximize business risk avoidance.

- **Responsible to Society**: Guided by ethics, we develop and deploy AI technology responsibly, promoting tech for social good and preventing technology abuse.

To realize this vision, Tuya Smart has created the '**Titan Matrix**', an integrated intelligent security brand that spans the entire AI business lifecycle, providing a reliable security foundation for global developers and users.



Tuya Titan Matrix Provides Security Assurance

Comprehensively Promote a Security Protection Matrix that is Systematic, Transparent, Verifiable, and Auditable

AI Security Ecosystem

R&D Security:

- Security Testing Tools (SAST/DAST/IAST)
- Process and Security Operations
- Security Compliance Whitepaper

AI Security:

- Large Model Security & Content Security
- AI Agent & MCP Server Security Management and Control
- AI Security Operations

Security Center:

- Secure Development Components and Services
- Business Security & Risk Management
- Data Security & Endpoint Security

Privacy & Compliance:

- Security Certifications (ISO, SOC, GDPR)
- Compliance Operations

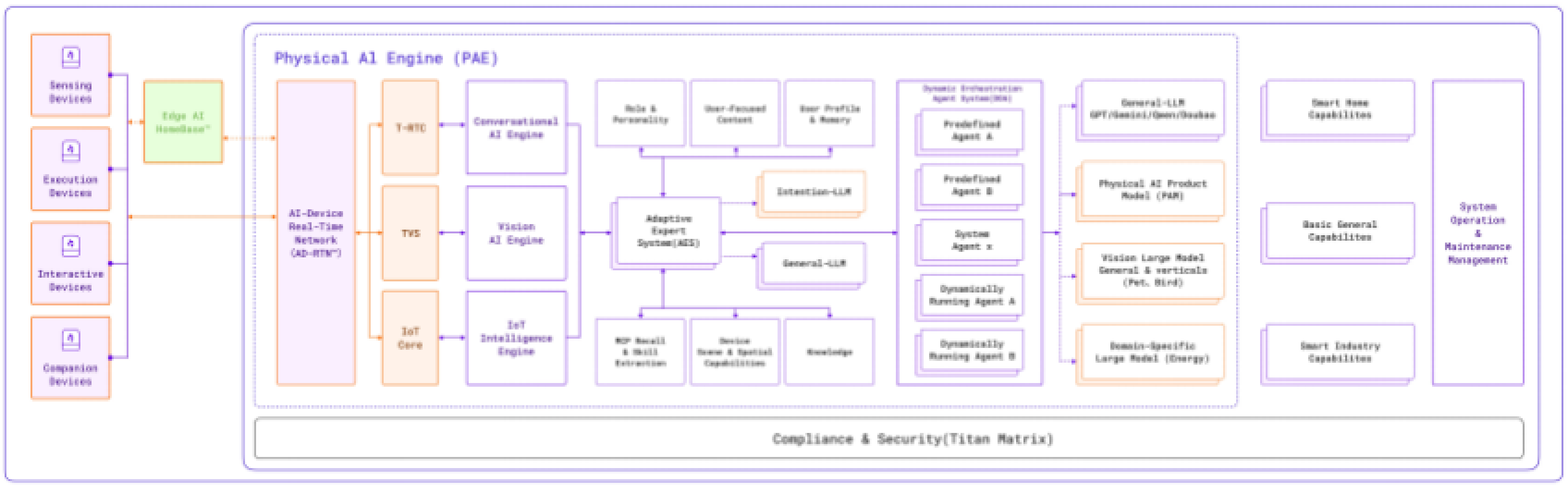
Protection System:

- Network Security Protection Capabilities (NGFW, WAF, RSAP)
- Cloud-Native Application Protection Capabilities (CNAPP, CSPM, Runtime Security, Container Security)
- Security Operations (SOC, SIEM, SOAR)
- IT Security (NGFW, SASE, XDR)

Chapter 1: Tuya Smart AI Panorama and Responsible AI Framework

1.1 Tuya AI Business Panorama

Leveraging Tuya Smart's deep capabilities in IoT and AI convergence, Tuya AI is dedicated to creating an intelligent ecosystem that seamlessly integrates into real life. Our core is ‘ **Your AI Life Assistant** ’—using **Hey Tuya** as a unified conversational entry point to break boundaries between devices and scenes, achieving "multi-terminal synergy, responsive at a call." It is not just a voice and text interaction interface, but a Super Agent with memory and understanding capabilities. It delves into core scenarios such as home security, energy saving, health, companionship, and efficiency, providing proactive services ranging from security guardianship and energy management to health advice and office efficiency enhancement.



Sensing Devices
Execution Devices
Interactive Devices
Companion Devices
Edge AI HomeBase™
Physical AI Engine (PAE)
AI-Device Real-Time Network (AD-RTN™)
T-RTC
TVS
IoT Core
Conversational AI Engine
Vision AI Engine
IoT Intelligence Engine
Role & Personality
User-Focused Content
User Profile & Memory
Adaptive Expert System(AES)
Intention-LLM
General-LLM
MCP Recall & Skill Extraction
Device Scene & Spatial Capabilities
Knowledge
Dynamic Orchestration Agent System(DOA)
Predefined Agent A
Predefined Agent B
System Agent x
Dynamically Running Agent A
Dynamically Running Agent B
General-LLM GPT/Gemini/Qwen/Doubao
Physical AI Product Model (PAM)
Vision Large Model General & verticals (Pet, Bird)
Domain-Specific Large Model (Energy)
Smart Home Capabilites
Basic General Capabilites
Smart Industry Capabilites
System Operation & Maintenance Management
Compliance & Security(Titan Matrix)

To achieve this vision, we have built a complete technology stack from hardware innovation to system services. For developers, we provide an **AI Hardware Innovation Development Platform**. Through the open TuyaOS and TuyaOpen, we empower global developers to quickly create innovative hardware such as AI headphones, AI learning machines, and AI robots. At the system layer, our proprietary **Physical AI Engine (PAE)** intelligent engine integrates device real-time networking, audio/video communication, IoT core connectivity, dialogue, and visual AI engines. Through an adaptive expert system and agent orchestration platform, it flexibly schedules industry large models and specialized skills, allowing AI to not only understand speech and vision but also proactively comprehend user intent and schedule appropriate services. We are moving from "conversational intelligence" to "scenario-based proactive service," striving to become the "Physical JARVIS" that truly understands you in every home, evolving intelligence from connecting to thinking, and from executing commands to anticipating needs.

Core Modules and Components:

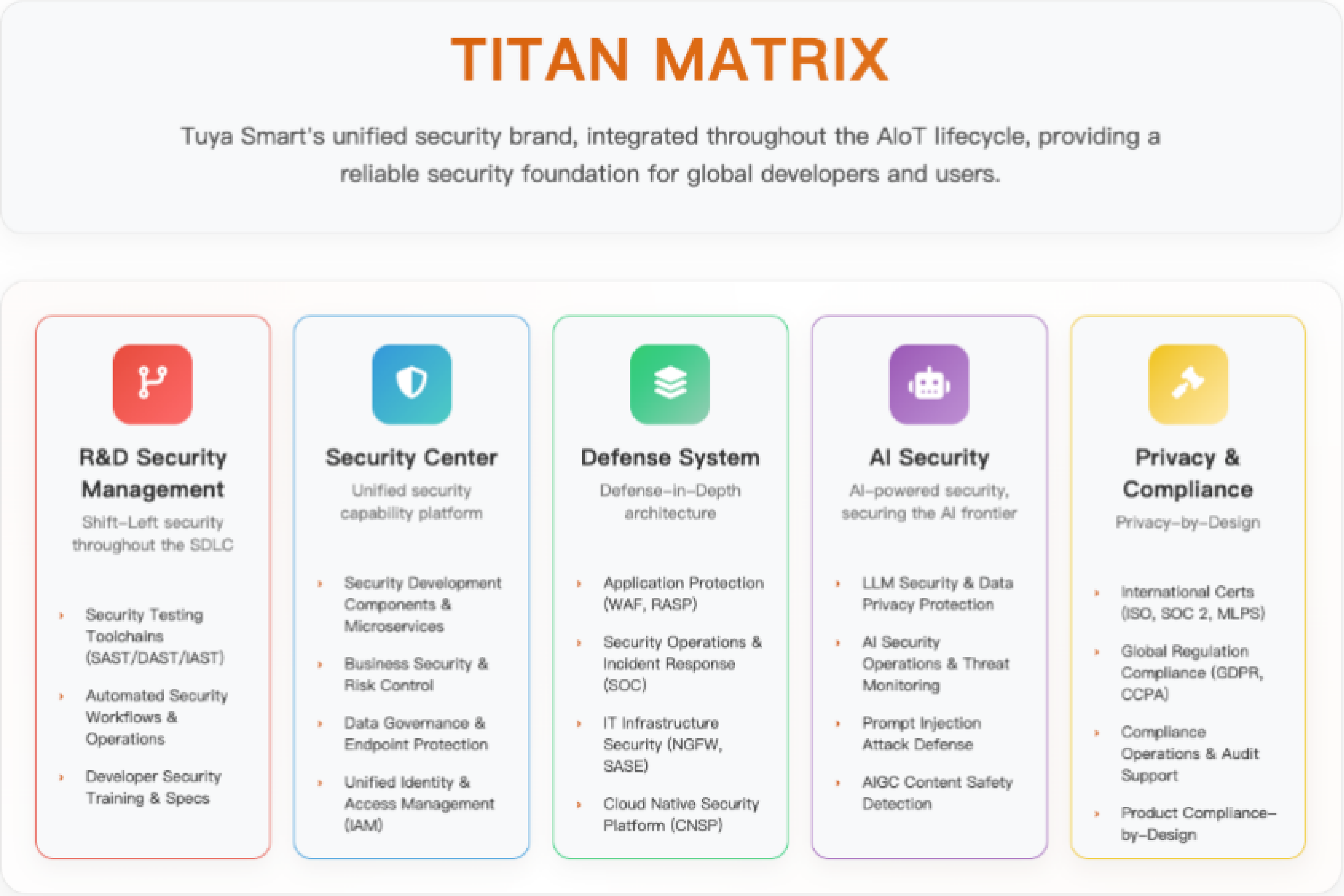
- **AI Foundation (including Conversational AI Engine、Vision AI Engine、AES、DOA)**: A low-latency, highly stable, and highly autonomous software-hardware integrated AI solution for developers. It provides unified model lifecycle management and basic Agent services, including terminal SDKs, streaming transmission services, cloud AI modules, and developer platforms.
- **AI Agent Development Platform**: Integrated with global mainstream large language models (LLMs), offering developers efficient and flexible agent management functions. Developers can

easily deploy and run agent-related applications through configuration and debugging.

- **TuyaOpen**: An advanced open-source AI and IoT development framework that helps you quickly build smart connected products. The framework supports multiple chip platforms and RTOS-like operating systems, easily integrating LLMs and multi-modal AI functions—including voice, vision, and sensor processing—injecting the power of next-generation AI into your hardware. Current AI intelligent terminals implemented based on TuyaOpen include AI toys, AI cameras, AI door locks, AI digital photo frames, AI learning machines, AI smart screens, and AI watches.
- **Hey Tuya (Tuya Super AI Assistant App)**: Hey Tuya is a super life AI assistant launched by Tuya Smart, built on Tuya's powerful IoT and AI convergence capabilities. It is a guardian of the family, a planner of life, and a partner in work. Hey Tuya brings natural, proactive, and intelligent companionship by talking to you, understanding your needs, remembering your habits, and working synergistically with various Physical AI devices.

1.2 Tuya Titan Matrix: Full Lifecycle Governance and Intelligent Defense System

Tuya Smart has built an integrated trusted architecture, '**Titan Matrix**', which fuses AI security, privacy protection, and compliance governance. This architecture ensures the safety, reliability, and compliance of AI systems through four pillars: "**Endogenous Security, Compliance-Driven, Intelligent Defense, and Continuous Improvement.**"



TITAN MATRIX

Tuya Smart's unified security brand, integrated throughout the AIoT lifecycle, providing a reliable security foundation for global developers and users.

R&D Security Management
Shift-Left security throughout the SDLC
- Security Testing Toolchains (SAST/DAST/IAST)
- Automated Security Workflows & Operations
- Developer Security Training & Specs

Security Center
Unified security capability platform
- Security Development Components & Microservices
- Business Security & Risk Control
- Data Governance & Endpoint Protection
- Unified Identity & Access Management (IAM)

Defense System
Defense-in-Depth architecture
- Application Protection (WAF, RASP)
- Security Operations & Incident Response (SOC)
- IT Infrastructure Security (NGFW, SASE)
- Cloud Native Security Platform (CNSP)

AI Security
AI-powered security, securing the AI frontier
- LLM Security & Data Privacy Protection
- AI Security Operations & Threat Monitoring
- Prompt Injection Attack Defense
- AIGC Content Safety Detection

Privacy & Compliance
Privacy-by-Design
- International Certs (ISO, SOC 2, MLPS)
- Global Regulation Compliance (GDPR, CCPA)
- Compliance Operations & Audit Support
- Product Compliance-by-Design

1.2.1 Endogenous Security: Product-Level Security and Privacy Protection

We deeply integrate security and privacy requirements into the AI product R&D process, implementing end-to-end protection covering data, algorithms, and systems:

- **Data Security**: Through data classification and grading, anonymization, and encryption during transmission and storage, we ensure control over training data and application data throughout the process.

- **Algorithmic Reliability**: Establishing model risk assessment, fairness testing, and adversarial example defense mechanisms to guarantee the explainability and robustness of AI decisions.

- **System Security**: Strengthening infrastructure security controls such as AI service interface authentication and inference environment isolation.

1.2.2 Compliance by Design: A Global Regulatory Framework

We have established an AI compliance governance framework guided by regulatory adherence, ensuring products and services meet target market requirements:

- **Regulation Mapping**: Systematically identifying and implementing key regulatory requirements such as the EU AI Act, GDPR, and China's Interim Measures for the Management of Generative AI Services.

- **Compliance Embedding**: Transforming compliance requirements (e.g., data subject rights protection, algorithm filing, high-risk AI system supervision) into executable product control points.

- **Audit Readiness**: Maintaining complete AI system documentation, data processing records, and audit trails to support internal/external audits and regulatory inquiries.

1.2.3 Intelligent Defense: AI-Empowered Security Operations

We innovatively use AI technology to enhance overall security defense capabilities, achieving an intelligent upgrade of security operations:

- **Intelligent Threat Detection**: Applying machine learning algorithms to analyze network traffic, user behavior, and system logs to identify Advanced Persistent Threats (APTs) and Zero-Day attacks in real-time.

- **Automated Response**: Building AI-based Security Orchestration, Automation, and Response (SOAR) workflows to achieve rapid judgment and disposal of security incidents.

- **Predictive Protection**: Predicting potential attack paths and implementing proactive defense strategies through big data analysis and threat intelligence mining.

1.2.4 Continuous Improvement: Trusted AI Governance Ecosystem

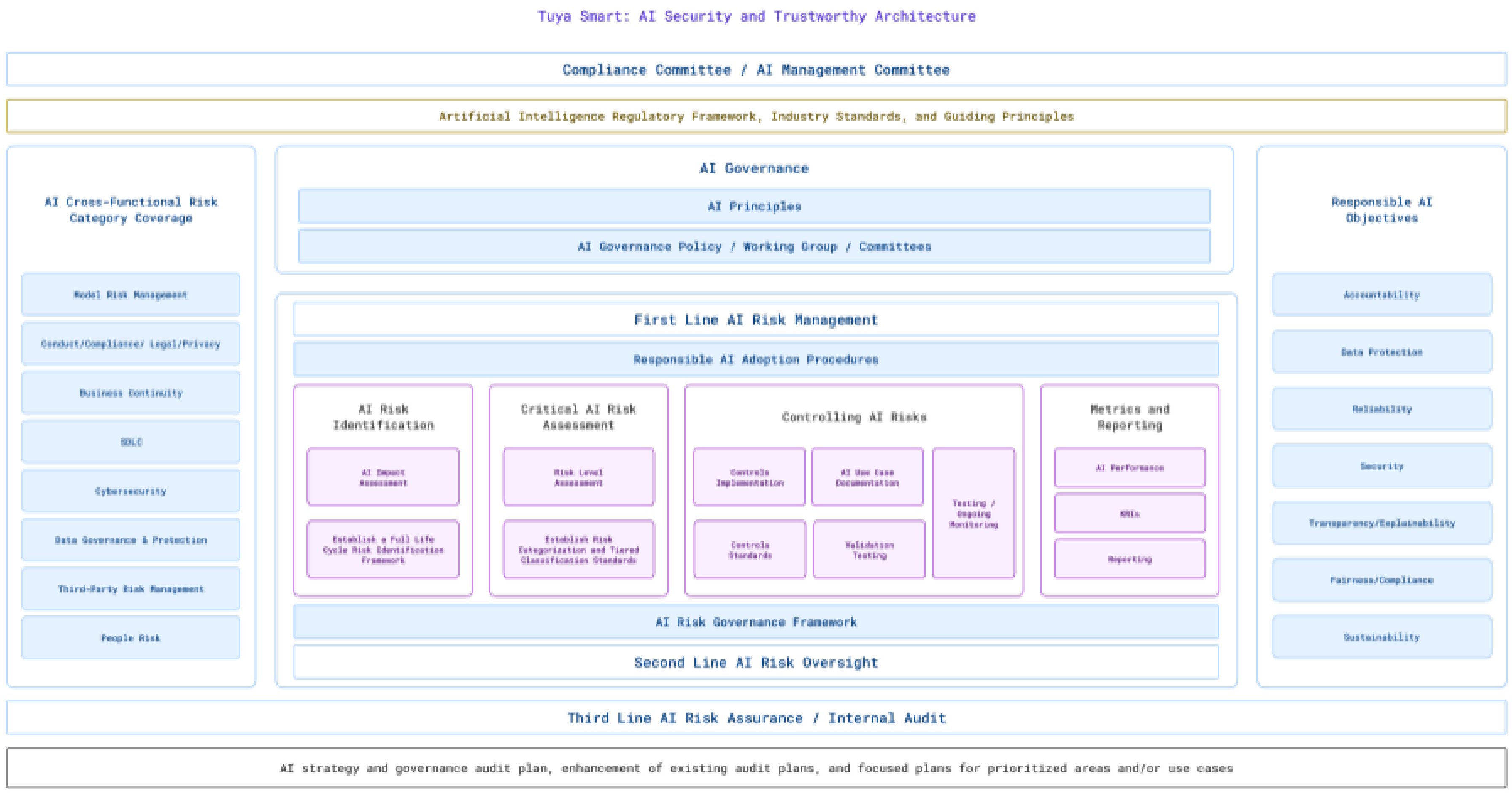
We have established a mechanism for the continuous improvement of AI security and trust:

- **Responsibility System**: Defining security responsibility boundaries for AI system owners, developers, and operators.

- **Risk Assessment Mechanism**: For high-risk AI applications, the Compliance Committee leads AI impact assessments and information security risk assessments to ensure potential risks are identified and controlled during the design and deployment phases.

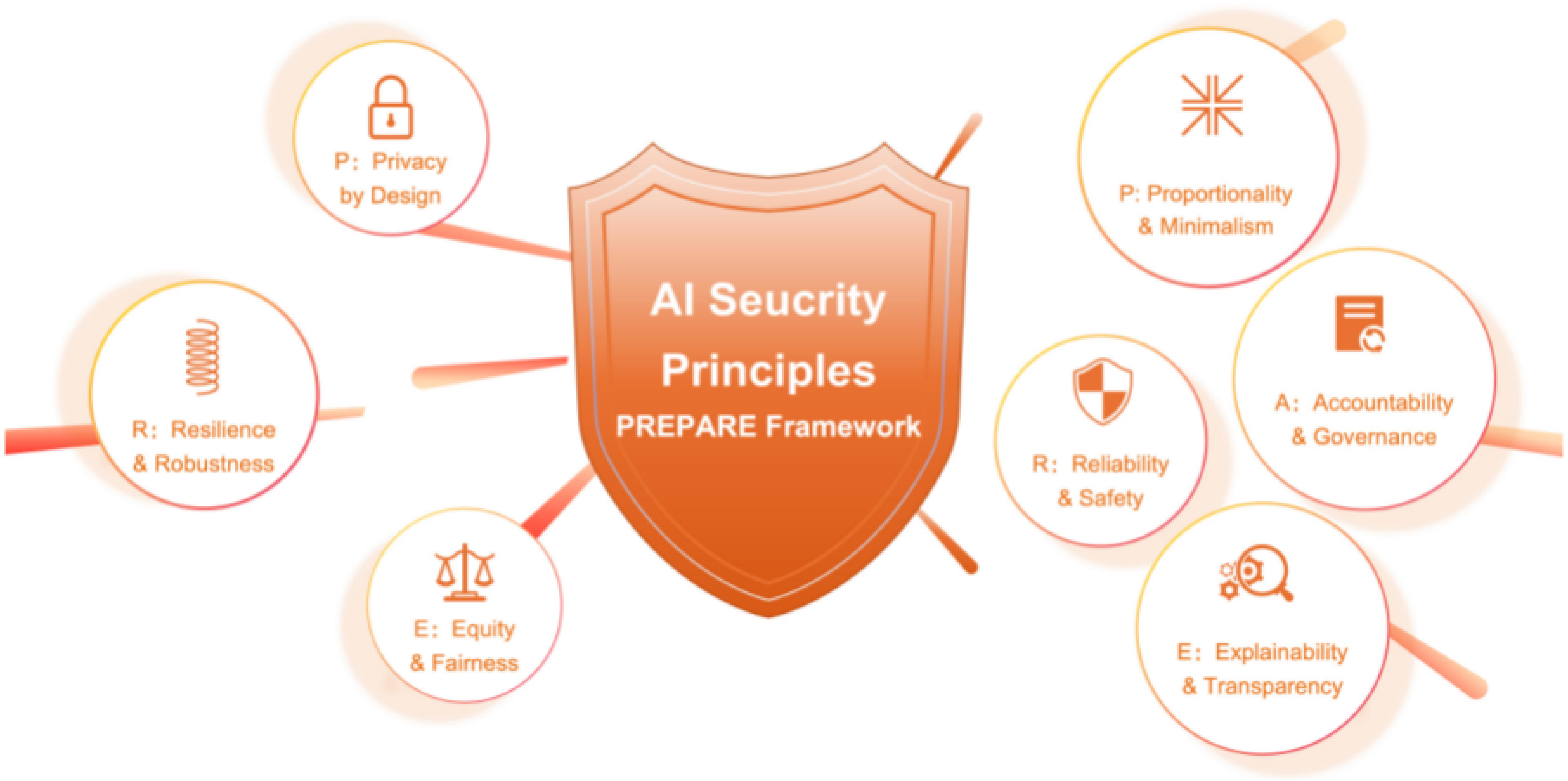
- **Transparency Construction**: Enhancing AI system transparency through model watermarking, full-link model log monitoring, AI white papers or reports, developer documentation, and user notifications.

This architecture forms a trusted AI system with "compliance as the baseline, security as the foundation, and intelligence as the engine." It meets current regulatory requirements while reserving secure scalability for future AI technology evolution, providing solid and trusted support for Tuya Smart's global AI business.


Tuya Smart: AI Security and Trustworthy Architecture
Compliance Committee / AI Management Committee
Artificial Intelligence Regulatory Framework, Industry Standards, and Guiding Principles
AI Cross-Functional Risk Category Coverage
Model Risk Management
Conduct/Compliance/ Legal/Privacy
Business Continuity
SDLC
Cybersecurity
Data Governance & Protection
Third-Party Risk Management
People Risk
AI Governance
AI Principles
AI Governance Policy / Working Group / Committees
First Line AI Risk Management
Responsible AI Adoption Procedures
AI Risk Identification
AI Impact Assessment
Establish a Full Life Cycle Risk Identification Framework
Critical AI Risk Assessment
Risk Level Assessment
Establish Risk Categorization and Tiered Classification Standards
Controlling AI Risks
Controls Implementation
AI Use Case Documentation
Controls Standards
Validation Testing
Testing / Ongoing Monitoring
Metrics and Reporting
AI Performance
KRIs
Reporting
AI Risk Governance Framework
Second Line AI Risk Oversight
Responsible AI Objectives
Accountability
Data Protection
Reliability
Security
Transparency/Explainability
Fairness/Compliance
Sustainability
Third Line AI Risk Assurance / Internal Audit
AI strategy and governance audit plan, enhancement of existing audit plans, and focused plans for prioritized areas and/or use cases

1.3 Our Core Principles for Responsible AI

Core Security Principles: The PREPARE Framework


AI Seucrity Principles
PREPARE Framework
P: Privacy by Design
R: Resilience & Robustness
E: Equity & Fairness
P: Proportionality & Minimalism
A: Accountability & Governance
R: Reliability & Safety
E: Explainability & Transparency

To realize this vision, Tuya Smart strictly follows the **PREPARE** core security principles throughout the AI product lifecycle:

- **P - Privacy by Design**: Privacy protection is embedded in every link of design and architecture from the inception of the product, rather than being a remedial afterthought.

- **R - Resilience & Robustness**: Ensuring AI systems can withstand threats such as adversarial attacks and data poisoning, and maintain the stability and reliability of core functions under abnormal conditions.

- **E - Equity & Fairness**: Committed to eliminating algorithmic bias through diverse datasets and continuous bias detection, ensuring fairness and justice in AI decisions.

- **P - Proportionality & Data Minimalism**: Strictly adhering to the "minimum necessary" principle for data collection, processing only the least amount of data required to achieve specific purposes.

- **A - Accountability & Governance**: Establishing a clear AI security responsibility system and governance structure to ensure all AI activities are traceable, auditable, and accountable.

- **R - Reliability & Safety**: Ensuring that AI functions, especially when controlling physical devices (such as electrical lighting, home appliances, etc.), do not cause personal or property risks due to errors or malicious commands.

- **E - Explainability & Transparency**: Within the scope of technical feasibility, striving to make the AI decision-making process transparent to users and providing clear, easy-to-understand user notifications.

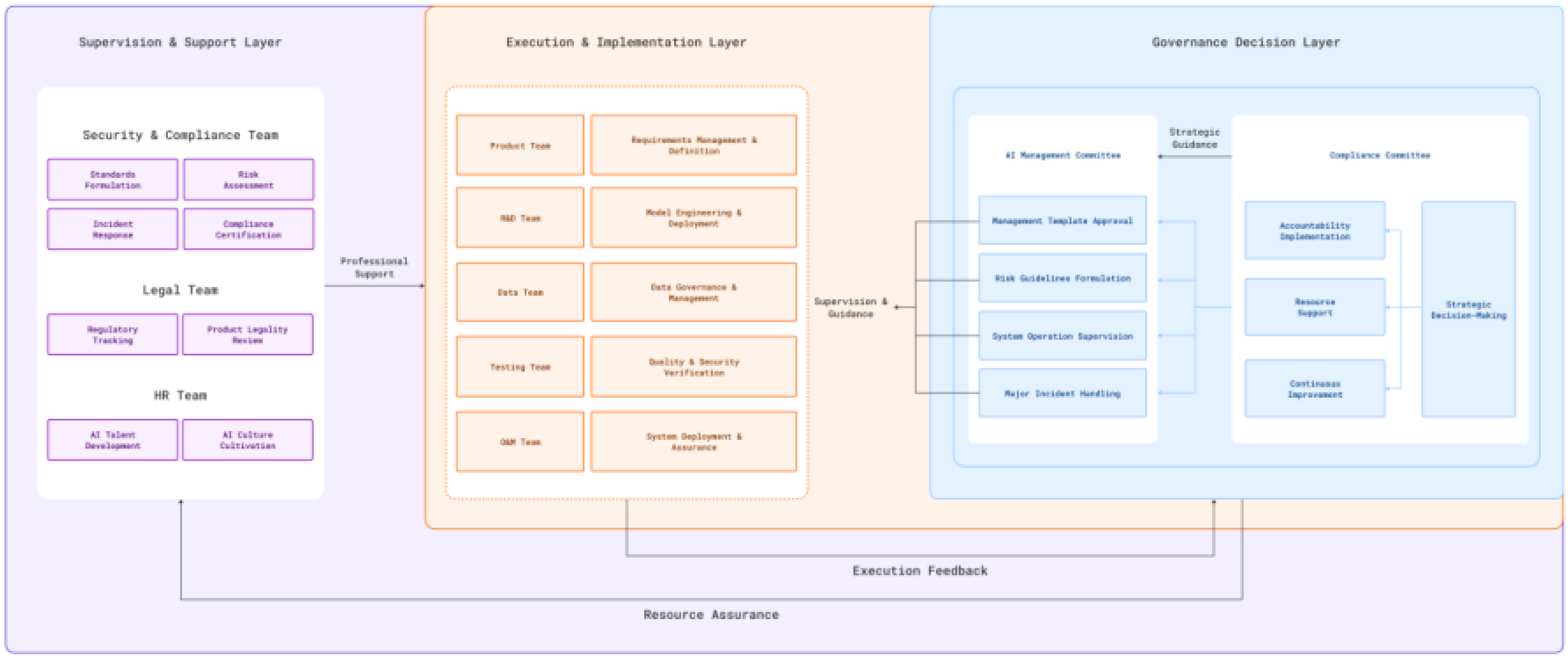
Chapter 2: Robust AI Governance and Organizational Assurance

Tuya's AI management system is established in accordance with the EU AI Act, relevant international AI standards, and Tuya’s strategic positioning in cloud computing and AIoT. Its fundamental purpose is to systematically manage AI-related opportunities and risks, ensuring that the development and application of AI technology adhere to the principle of "Innovation-Driven, Trustworthy AI Security; Lawful and Compliant AI Use, Guaranteeing Fairness, Transparency, and Explainability." This system provides strong support for the robust implementation of the Group's Physical AI strategy.

2.1 AI Risk Governance Architecture

Tuya Smart has established a clearly-defined AI risk governance architecture, supported by comprehensive policies and processes. This is bolstered by an efficient AI risk management system designed to ensure the safety, reliability, and compliance of our global AI products and services, thereby earning the trust of customers and end-users worldwide.

Tuya Smart - AI Governance Architecture



1. Governance and Decision-Making Layer: Strategic Leadership and Top-Level Oversight

This layer serves as the ultimate authority for AI governance, responsible for strategic decision-making and resource allocation.

- **Compliance Committee**: As the highest decision-making body, it ensures AI policies align with corporate strategy, approves major resource investments, and makes decisions on critical AI risks.
- **AI Management Committee**: As the cross-functional management core, it is responsible for approving AI management objectives and risk criteria, and supervising the effective operation of the entire AI risk management system.

Role	Responsibility Description
Compliance Committee	The Tuya Compliance Committee is the ultimate responsible body for AI governance. It demonstrates leadership and commitment to the AI

	management system by: ● **Ensuring Alignment**: Ensuring AI policies and strategic objectives remain consistent with the Group's AI strategic direction. ● **Implementing Integration**: Fully integrating AI management requirements into the Group's organizational structure, business processes, and technical practices. ● **Guaranteeing Resources**: Ensuring the provision of necessary funding, infrastructure, and human resources for establishing, implementing, maintaining, and continuously improving the AI management system. ● **Driving Improvement**: Hosting management reviews to drive continuous improvement in the effectiveness of the AI management system and making decisions on the treatment and acceptance of critical AI risks.
AI Management Committee	Tuya has established a cross-functional Security and Compliance Committee as the management and coordination organization for AI governance. Its main responsibilities include: ● Reviewing and approving supporting implementation rules and standards for these measures. ● Approving Group-level AI management objectives and risk acceptance criteria. ● Supervising the effectiveness of AI impact assessments and risk management activities. ● Coordinating the handling of major AI incidents and disputes.

2. Execution and Implementation Layer: Product R&D and Deployment

This layer consists of various business and technical departments responsible for pushing AI products from concept to market. They are the direct practitioners of AI governance requirements.

- Teams across Product, R&D, Data, Testing, and Operations perform their respective duties, forming a complete loop from demand proposal, model development, data management, and quality testing to system deployment and launch, collectively ensuring the technical reliability, security, and performance of AI systems.

3. Supervision and Support Layer: Compliance Assurance and System Construction

This layer provides professional support, supervision, and assurance for AI governance, ensuring corporate behavior complies with internal and external norms.

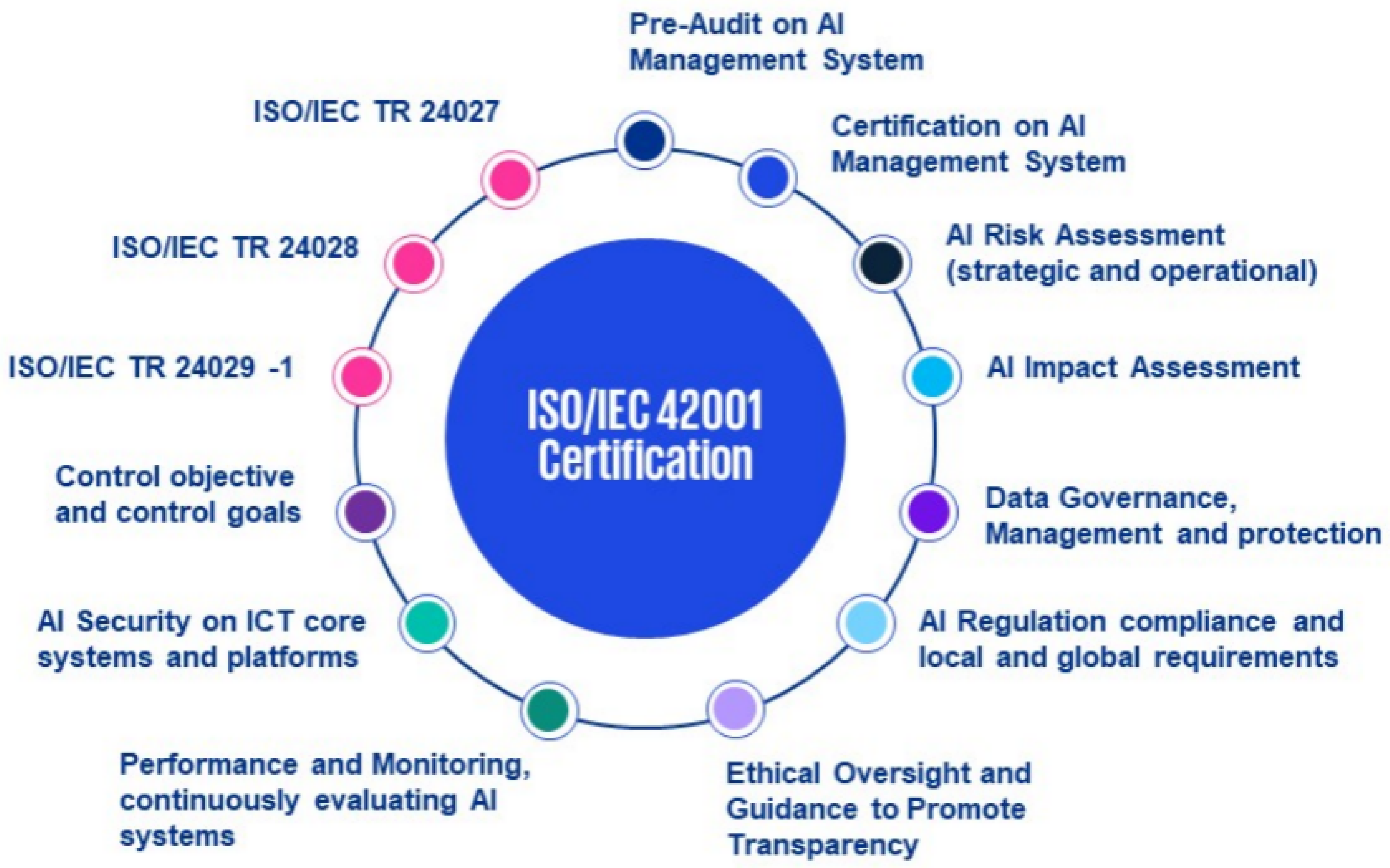
- **Security & Compliance Team**: The core supervisory force, responsible for formulating security standards, executing risk assessments and tests, and leading incident response and compliance certification.
- **Legal Team**: Responsible for tracking laws and regulations to ensure the legality of AI products.
- **HR Team**: Responsible for building the AI talent system and cultivating the company's AI culture to provide talent support for the governance architecture.

2.2 AI Management System Certification

Tuya Smart has been awarded the **ISO/IEC 42001:2023 Artificial Intelligence Management System Certification** by the international authoritative certification body DNV, becoming one of the first AI platform enterprises globally to receive this certificate. This certification signifies that Tuya Smart has established a systematic and standardized governance framework throughout the entire lifecycle of AI R&D, application, and management, laying a solid foundation for providing safer, more reliable, and trustworthy AI products and services to global customers.

ISO/IEC 42001, jointly developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), aims to help organizations establish effective management systems when developing, implementing, and maintaining AI technologies. It covers multiple aspects including AI system planning and strategy, project management, requirements and design, implementation and operation, and monitoring and evaluation.

During the certification process, Tuya Smart underwent a comprehensive assessment of its AI management system by the auditing body, covering the entire process from AI strategic planning and risk management to implementation and operation.


Pre-Audit on AI Management System
Certification on AI Management System
AI Risk Assessment (strategic and operational)
AI Impact Assessment
Data Governance, Management and protection
AI Regulation compliance and local and global requirements
Ethical Oversight and Guidance to Promote Transparency
Performance and Monitoring, continuously evaluating AI systems
AI Security on ICT core systems and platforms
Control objective and control goals
ISO/IEC TR 24029 -1
ISO/IEC TR 24028
ISO/IEC TR 24027
ISO/IEC 42001 Certification

The assessment showed Tuya Smart's excellence in multiple dimensions:

- **Governance Architecture**: Established a top-down AI governance architecture with clear rights and responsibilities.
- **Lifecycle Management**: Executed systematic management covering the full lifecycle of AI systems.
- **Data Security**: Strictly adhered to data minimization and anonymization principles.
- **Transparency**: Strived to make the AI decision-making process transparent to users within the scope of technical feasibility.

2.3 Institutionalization and Process Standardization

A sound management system is the cornerstone of sustainable AI development. Tuya has taken the lead in the industry to build a complete AI security and compliance management regulation system. Through strict control of regulations and processes, AI governance concepts are fully integrated into the organizational structure and business processes.

Building a Three-Tier Governance Structure with Clear Responsibilities

Tuya Smart has established a top-down, clearly accountable three-tier AI governance structure with "Tuya Artificial Intelligence Management Charter" as the top-level design. The governance decision-making level is responsible for strategic guidance and top-level oversight; the execution and implementation level focuses on product development and deployment; the supervision and support level provides compliance assurance and system building. This structure ensures effective implementation of AI governance requirements across the entire organization, achieving seamless connection from strategy to execution.

Establishing a Full Lifecycle Management System Throughout AI Products

According to the "AI System Full Lifecycle Strategy Specification," Tuya Smart embeds privacy protection, security, and ethical considerations into every stage from conceptual design to system retirement. We adhere to the principle of "security by design, compliance by design," conducting preliminary risk assessments during the planning phase to clarify the legality, legitimacy, and necessity of projects; strictly following secure coding standards during development; performing comprehensive impact assessments before deployment; implementing continuous monitoring during operations; and ensuring smooth and orderly decommissioning during retirement. This end-to-end management ensures full-cycle controllability of AI product quality and risks.

Implementing Tiered Risk Assessment for Precise AI Risk Control

The "AI System Assessment and Risk Assessment Management System" provides Tuya Smart with a systematic risk assessment framework. We require assessments at key stages of all AI systems, including new system introduction, major changes, and scenario expansion. By establishing risk level determination standards and implementing corresponding mitigation measures for different risk levels, we effectively identify and prevent AI bias, security, and personal information risks, ensuring optimal balance between technological innovation and risk prevention.

Strengthening Data Source Governance to Ensure Training Data Quality

Data is the "fuel" of AI; its quality directly determines model reliability and fairness. All businesses and services on the Tuya platform strictly prohibit using developer or user unauthorized data for training. Meanwhile, the "AI System Training Data Management Specification" establishes clear requirements for the entire process of data collection, cleaning, labeling, storage, usage, and destruction. We particularly emphasize the legality of data sources and the principle of minimal necessity, reducing data bias and security risks at the source through strict data quality management processes, providing high-quality "nutrition" for model training.

Improving Emergency Response Mechanisms to Enhance Security Incident Handling Capability

The "Artificial Intelligence System Security Incident Management Method" establishes a standardized, efficient AI security incident emergency response process. This system clearly defines security incident definitions, classification standards, reporting paths, and handling procedures, ensuring rapid response, minimal loss, and regulatory reporting compliance when incidents such as data breaches, model misuse, or system attacks occur. Through regular drills and continuous optimization, we continuously improve the organization's security incident response capabilities.

Optimizing Resource Management Efficiency for Sustainable Development

The "Artificial Intelligence System Resource Management Regulations" provides unified management of computing resources, model resources, and data resources relied upon throughout the AI system lifecycle. By standardizing cloud computing resource application, allocation, monitoring, and cost optimization, as well as model file version management and storage specifications, Tuya Smart ensures efficient operation of AI systems while avoiding resource waste, controlling operational costs, and achieving unity of economic and social benefits.

Strict Supplier Management to Build a Trusted AI Ecosystem

The "Artificial Intelligence Supplier Management Specification" extends AI risk management to the supply chain. We implement unified security and compliance requirements for all suppliers providing AI-related products, services, tools, models, or solutions, ensuring the credibility and security of the entire AI ecosystem. This system effectively controls externally introduced AI application risks, guaranteeing continuous stability of data security and service quality.

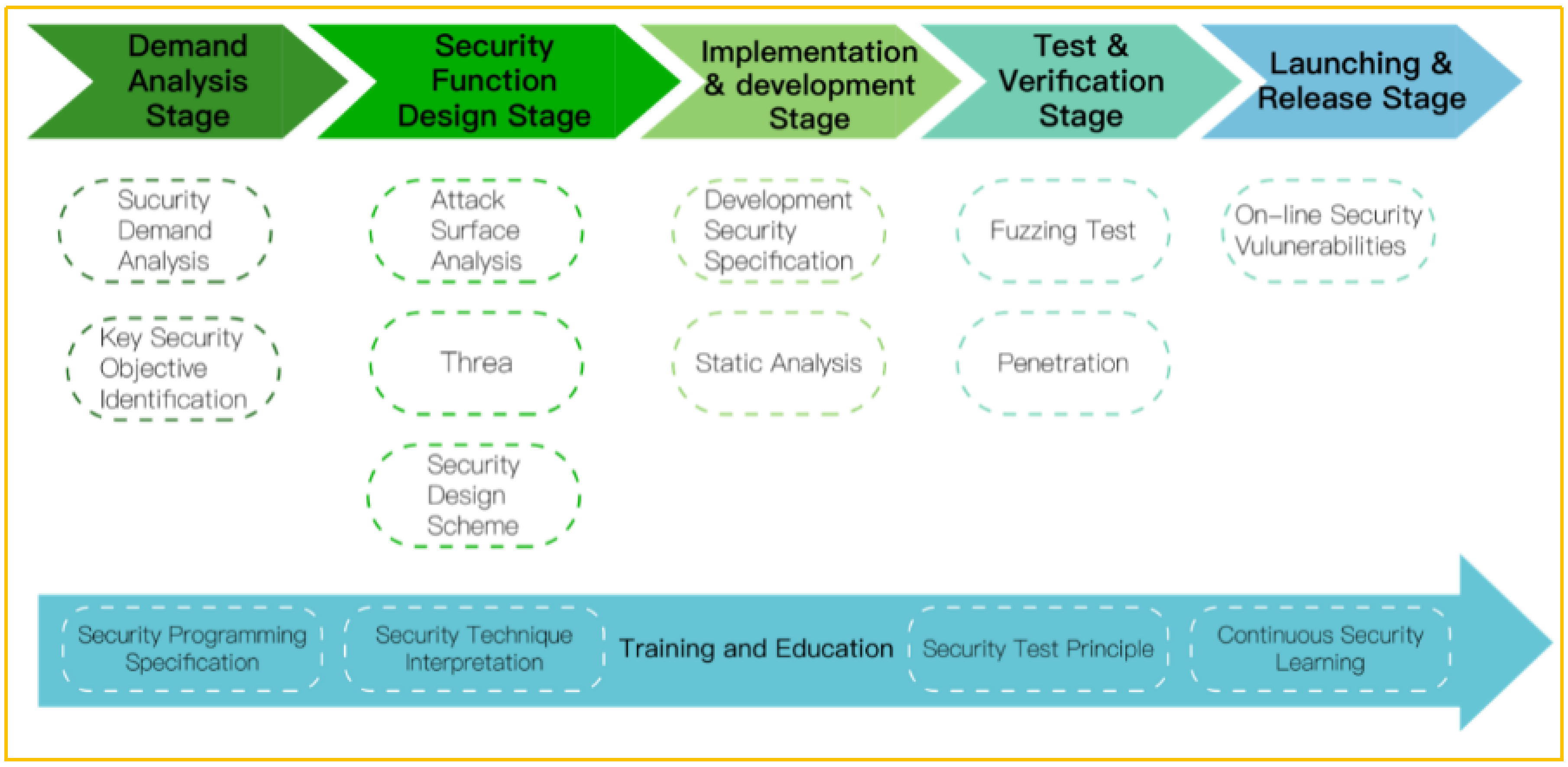
Through the collaborative operation of these seven systems, Tuya Smart has established a standardized, process-oriented, and institutionalized AI governance system. This system not only complies with ISO/IEC 42001 international standards but is also continuously optimized and improved in practice, providing solid institutional support for Tuya's global AI business operations.

In the future, Tuya Smart will continue to improve the AI governance framework, promote deep integration of institutional requirements and business practices, and safeguard AI technology innovation with systematic management capabilities, contributing Tuya's wisdom to the healthy and orderly development of the global artificial intelligence industry.

Chapter 3: The AI Security Development Life Cycle—Ingrained in Our DNA

Tuya implements systematic management covering the entire lifecycle of all artificial intelligence systems, ensuring every stage from requirements design to final retirement meets compliance, ethical, and security requirements.

Tuya's AI application development security lifecycle is the practical core of the '**Titan Matrix**' R&D security management pillar. It comprehensively covers all stages of the system development lifecycle and is uniformly monitored and managed through a security management platform, essentially achieving fully automated process tracking and security rating.


Demand Analysis Stage
Security Function Design Stage
Implementation & development Stage
Test & Verification Stage
Launching & Release Stage
Sucurity Demand Analysis
Key Security Objective Identification
Attack Surface Analysis
Threa
Security Design Scheme
Development Security Specification
Static Analysis
Fuzzing Test
Penetration
On-line Security Vulunerabilities
Security Programming Specification
Security Technique Interpretation
Training and Education
Security Test Principle
Continuous Security Learning

3.1 Planning and Design Phase

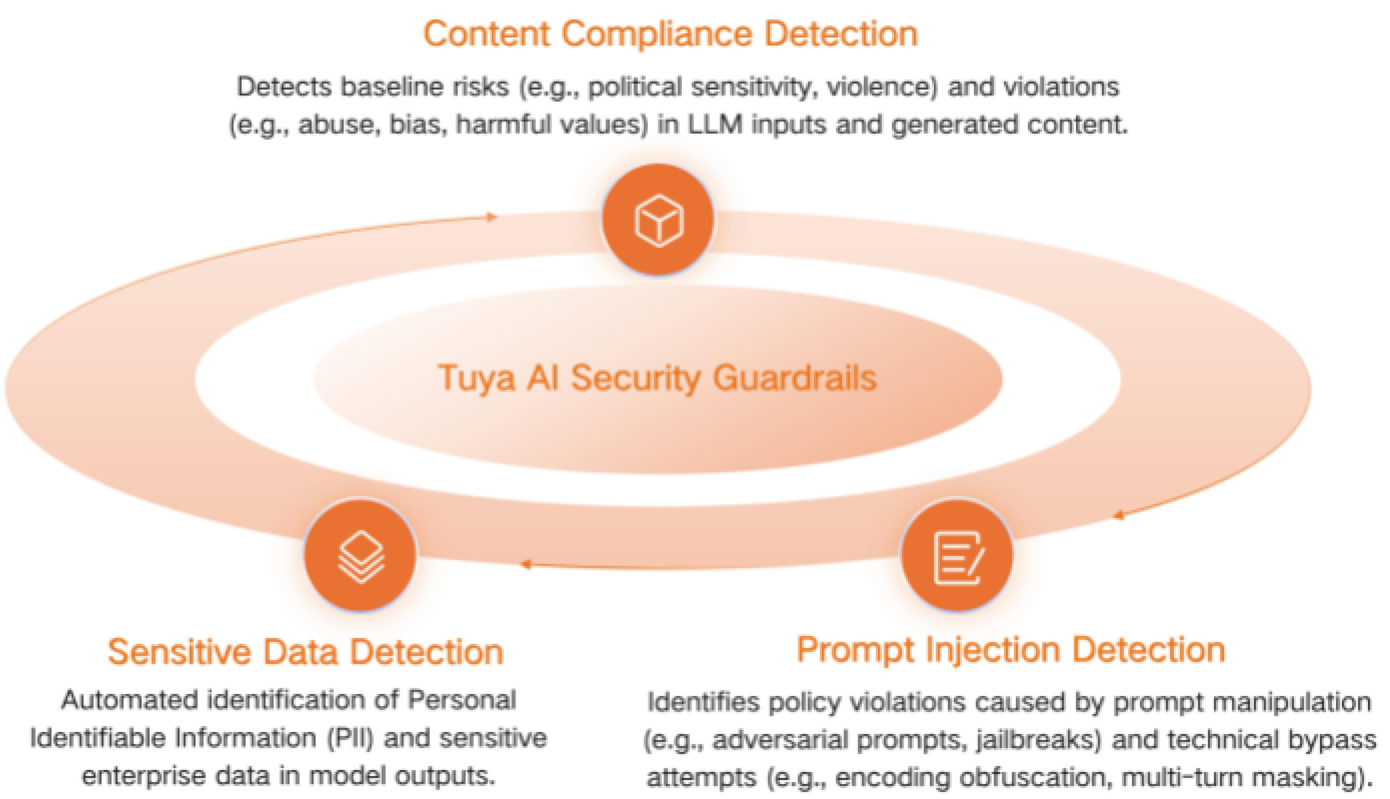
- **Requirement Definition and Boundary Control**: Clearly define business scope, system boundaries, and design operational domains in the PRD, detailing functional, performance, security, compliance, and ethical requirements. By clearly delineating applicable and non-applicable scenarios, control the operational boundaries of AI systems from the source to prevent scope creep and scenario misuse risks. Simultaneously specify technical selection, resource budget, and other constraint conditions to establish a clear framework for subsequent development.
- **Risk Assessment**: Conduct AI system impact assessments jointly with legal, compliance, security, and technical departments to systematically identify high-risk scenarios and perform risk rating. Focus on analyzing potential impacts on individual rights and social public interests in scenarios involving personal information processing, automated decision-making, generative AI applications, etc., ensuring compliance and ethical risks are identified and assessed for nature, probability, and severity during the requirements phase.
- **Technical Feasibility Assessment**: Perform technical feasibility analysis from four dimensions: data, models, engineering operations, and supply chain. Assess the accessibility, legality, and quality of training data; the rationality of algorithm selection and compliance implementation

paths; the technical complexity of system integration; and dependency risks on third-party components. Identify major technical risks through comprehensive assessment and propose mitigation strategies.

- **Platform Process Support**: Based on project application scenarios and legal foundations, provide semi-automated project security and privacy compliance assessments through internal security operations platforms and compliance management platforms, along with the security compliance department's continuous knowledge accumulation on large models and large model business risks, ensuring maximum risk identification during the planning and design phase.

3.2 Data Preparation and Model Development Phase

- **Data Management**: Follow the "Tuya AI System Training Data Management Specification" to ensure datasets used for training and testing comply with data security and privacy protection regulations during collection, labeling, storage, and processing, improving data quality, representativeness, and diversity, effectively identifying and mitigating data bias. In AI-related businesses involving personal data processing, strictly implement the principles of data minimization and anonymization.
- **Model Design and Training**: Adopt appropriate technologies and architectures to enhance model robustness, security, and explainability. Continuously evaluate and document model performance and potential biases during development
- **Supply Chain Security**: Conduct security assessments on used models and APIs according to the "Tuya Artificial Intelligence Supplier Management Specification."
- **Development Training**: To ensure developers fully understand and follow the "Tuya AI Secure Coding Specification," the Tuya security team provides comprehensive training and education courses covering basic concepts of secure coding, best practices, and how to apply this knowledge in specific projects.
- **Model Development**: R&D teams strictly adhere to the "Tuya AI Secure Coding Specification," implementing specialized security solutions provided by the security department based on risk scenarios. For example, in all input and output scenarios of models, developers must strictly integrate the AI security guardrail SDK provided by the security department for AI injection attack detection and content security compliance development components. Additionally, the security department provides various security vulnerability protection components and security capability components.



Content Compliance Detection

Detects baseline risks (e.g., political sensitivity, violence) and violations (e.g., abuse, bias, harmful values) in LLM inputs and generated content.

Tuya AI Security Guardrails

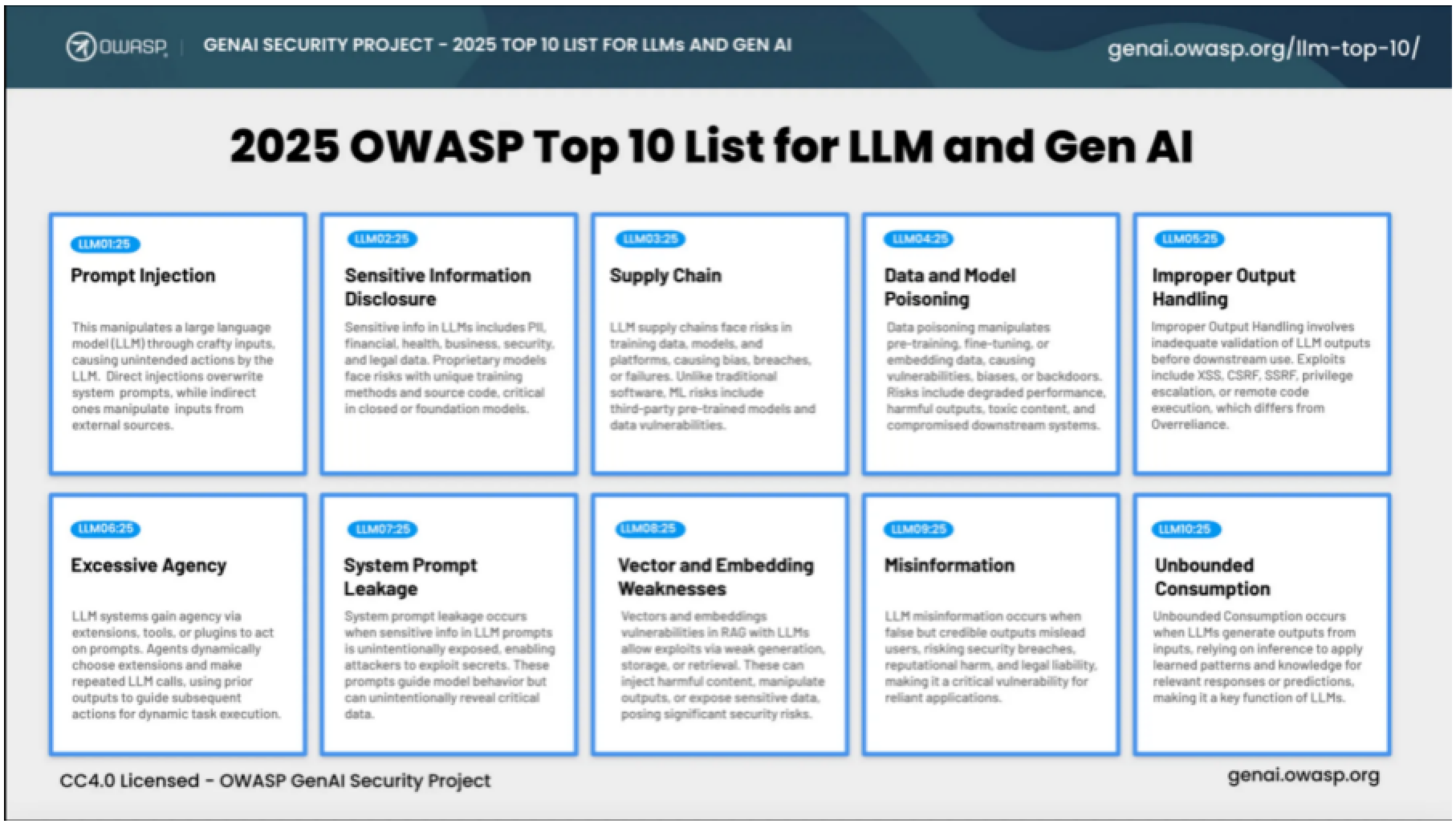
Sensitive Data Detection

Automated identification of Personal Identifiable Information (PII) and sensitive enterprise data in model outputs.

Prompt Injection Detection

Identifies policy violations caused by prompt manipulation (e.g., adversarial prompts, jailbreaks) and technical bypass attempts (e.g., encoding obfuscation, multi-turn masking).

- **Testing and Verification**: Conduct thorough testing in simulated and controlled real environments to verify performance in predefined and edge scenarios (such as unstable networks and abnormal data in IoT devices).
- **Adversarial Attack Protection**: R&D and testing teams must perform privilege escalation testing on AI services and related interfaces using tools and test cases provided by the security team. The security team conducts automated security scanning and auditing based on OWASP Top 10 for LLMs standards, continuously accumulating AI security test cases, including but not limited to supply chain security testing and code auditing, as well as expert manual security assessments to continuously verify large model security.



OWASP | GENAI SECURITY PROJECT - 2025 TOP 10 LIST FOR LLMs AND GEN AI

genai.owasp.org/llm-top-10/

2025 OWASP Top 10 List for LLM and Gen AI

LLM01:25
Prompt Injection
This manipulates a large language model (LLM) through crafty inputs, causing unintended actions by the LLM. Direct injections overwrite system prompts, while indirect ones manipulate inputs from external sources.

LLM02:25
Sensitive Information Disclosure
Sensitive info in LLMs includes PII, financial, health, business, security, and legal data. Proprietary models face risks with unique training methods and source code, critical in closed or foundation models.

LLM03:25
Supply Chain
LLM supply chains face risks in training data, models, and platforms, causing bias, breaches, or failures. Unlike traditional software, ML risks include third-party pre-trained models and data vulnerabilities.

LLM04:25
Data and Model Poisoning
Data poisoning manipulates pre-training, fine-tuning, or embedding data, causing vulnerabilities, biases, or backdoors. Risks include degraded performance, harmful outputs, toxic content, and compromised downstream systems.

LLM05:25
Improper Output Handling
Improper Output Handling involves inadequate validation of LLM outputs before downstream use. Exploits include XSS, CSRF, SSRF, privilege escalation, or remote code execution, which differs from Overreliance.

LLM06:25
Excessive Agency
LLM systems gain agency via extensions, tools, or plugins to act on prompts. Agents dynamically choose extensions and make repeated LLM calls, using prior outputs to guide subsequent actions for dynamic task execution.

LLM07:25
System Prompt Leakage
System prompt leakage occurs when sensitive info in LLM prompts is unintentionally exposed, enabling attackers to exploit secrets. These prompts guide model behavior but can unintentionally reveal critical data.

LLM08:25
Vector and Embedding Weaknesses
Vectors and embeddings vulnerabilities in RAG with LLMs allow exploits via weak generation, storage, or retrieval. These can inject harmful content, manipulate outputs, or expose sensitive data, posing significant security risks.

LLM09:25
Misinformation
LLM misinformation occurs when false but credible outputs mislead users, risking security breaches, reputational harm, and legal liability, making it a critical vulnerability for reliant applications.

LLM10:25
Unbounded Consumption
Unbounded Consumption occurs when LLMs generate outputs from inputs, relying on inference to apply learned patterns and knowledge for relevant responses or predictions, making it a key function of LLMs.

CC4.0 Licensed - OWASP GenAI Security Project

genai.owasp.org

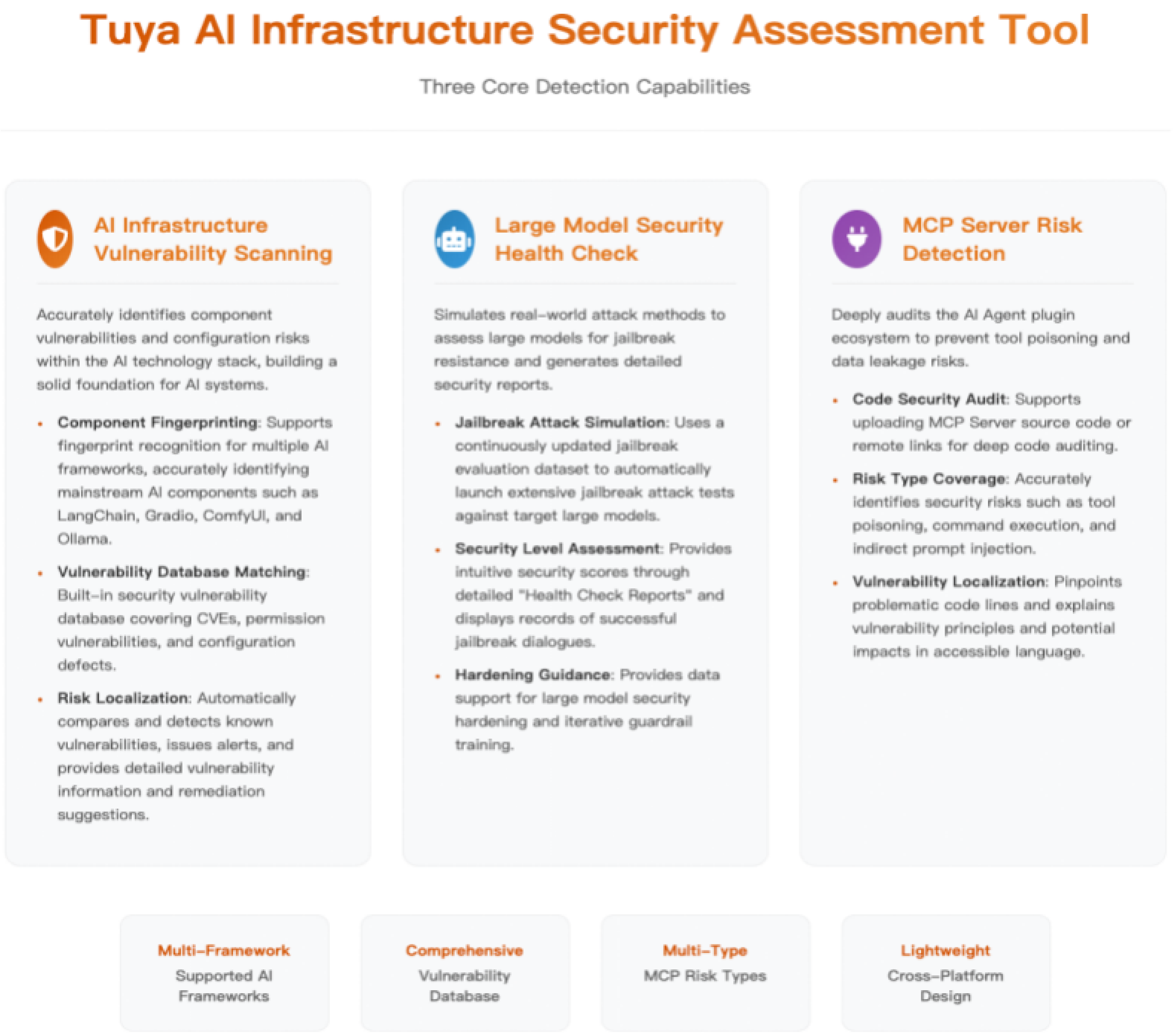
3.3 Deployment and Launch Phase

- **Before deployment**, conduct comprehensive impact assessments according to the "Tuya Artificial Intelligence System Impact Assessment and Risk Assessment Management System," systematically analyzing potential consequences for individuals, groups, society, and the environment, and documenting assessment results and risk handling measures.

- **The deployment environment** must undergo final security audit verification, including security verification of deployed hosts and images, as well as other baseline security checks such as configuration, version vulnerabilities, and compliance baselines to ensure the environment meets security baseline requirements for release.
- **Based on review and test report conclusions** from security and compliance platforms, make final decisions on project deployment and launch. Only after passing reviews and testing can the project be released and deployed.
- **After deployment**, dedicated human supervision roles and intervention mechanisms ensure humans can effectively override, interrupt, or correct AI outputs during critical decisions or system anomalies.

3.4 Operations and Monitoring Phase

- **Tuya's large model risk monitoring system** utilizes observable monitoring tools to monitor model prediction drift, performance degradation, and abnormal behaviors in real time.
- **Tuya has also deployed** large model security vulnerability scanning tools to perform 24/7 security scanning and assessment of large models, AI Agents, MCP services, and related infrastructure and interfaces.



Tuya AI Infrastructure Security Assessment Tool

Three Core Detection Capabilities

AI Infrastructure Vulnerability Scanning

Accurately identifies component vulnerabilities and configuration risks within the AI technology stack, building a solid foundation for AI systems.

- **Component Fingerprinting**: Supports fingerprint recognition for multiple AI frameworks, accurately identifying mainstream AI components such as LangChain, Gradio, ComfyUI, and Ollama.
- **Vulnerability Database Matching**: Built-in security vulnerability database covering CVEs, permission vulnerabilities, and configuration defects.
- **Risk Localization**: Automatically compares and detects known vulnerabilities, issues alerts, and provides detailed vulnerability information and remediation suggestions.

Large Model Security Health Check

Simulates real-world attack methods to assess large models for jailbreak resistance and generates detailed security reports.

- **Jailbreak Attack Simulation**: Uses a continuously updated jailbreak evaluation dataset to automatically launch extensive jailbreak attack tests against target large models.
- **Security Level Assessment**: Provides intuitive security scores through detailed "Health Check Reports" and displays records of successful jailbreak dialogues.
- **Hardening Guidance**: Provides data support for large model security hardening and iterative guardrail training.

MCP Server Risk Detection

Deeply audits the AI Agent plugin ecosystem to prevent tool poisoning and data leakage risks.

- **Code Security Audit**: Supports uploading MCP Server source code or remote links for deep code auditing.
- **Risk Type Coverage**: Accurately identifies security risks such as tool poisoning, command execution, and indirect prompt injection.
- **Vulnerability Localization**: Pinpoints problematic code lines and explains vulnerability principles and potential impacts in accessible language.

Multi-Framework
Supported AI Frameworks

Comprehensive
Vulnerability Database

Multi-Type
MCP Risk Types

Lightweight
Cross-Platform Design

- **Tuya maintains a comprehensive logging mechanism** that records key inputs, decision processes, and output results of AI systems in detail, ensuring auditability and traceability to meet troubleshooting, customer inquiries, and compliance review needs.
- **Through developing and practicing emergency response plans**, we can promptly respond to and handle AI system-related incidents.
- **Tuya's open security ecosystem** receives security and compliance risk reports from white hat hackers through the Security Response Center (SRC) and offers bounties. Regularly, third-party security companies perform security assessments of security services and capabilities, and the security department conducts internal offensive and defensive exercises against AI scenarios and businesses. To advance AI security ecosystem building, Tuya SRC offers double bounty rewards for AI-related services and applications.

Tuya Smart Security
Response Center (Tuya SRC)
Protecting the Global IOT Ecosytem
src.tuya.com
Submit Bugs, Earn Rewards

3.5 Decommissioning and Archiving Phase

- **Establish clear system retirement plans** to ensure services are decommissioned smoothly and orderly, notifying relevant users and customers.
- **According to data retention policies**, securely dispose of or archive models, data, and logs related to the system to prevent residual security and privacy risks.

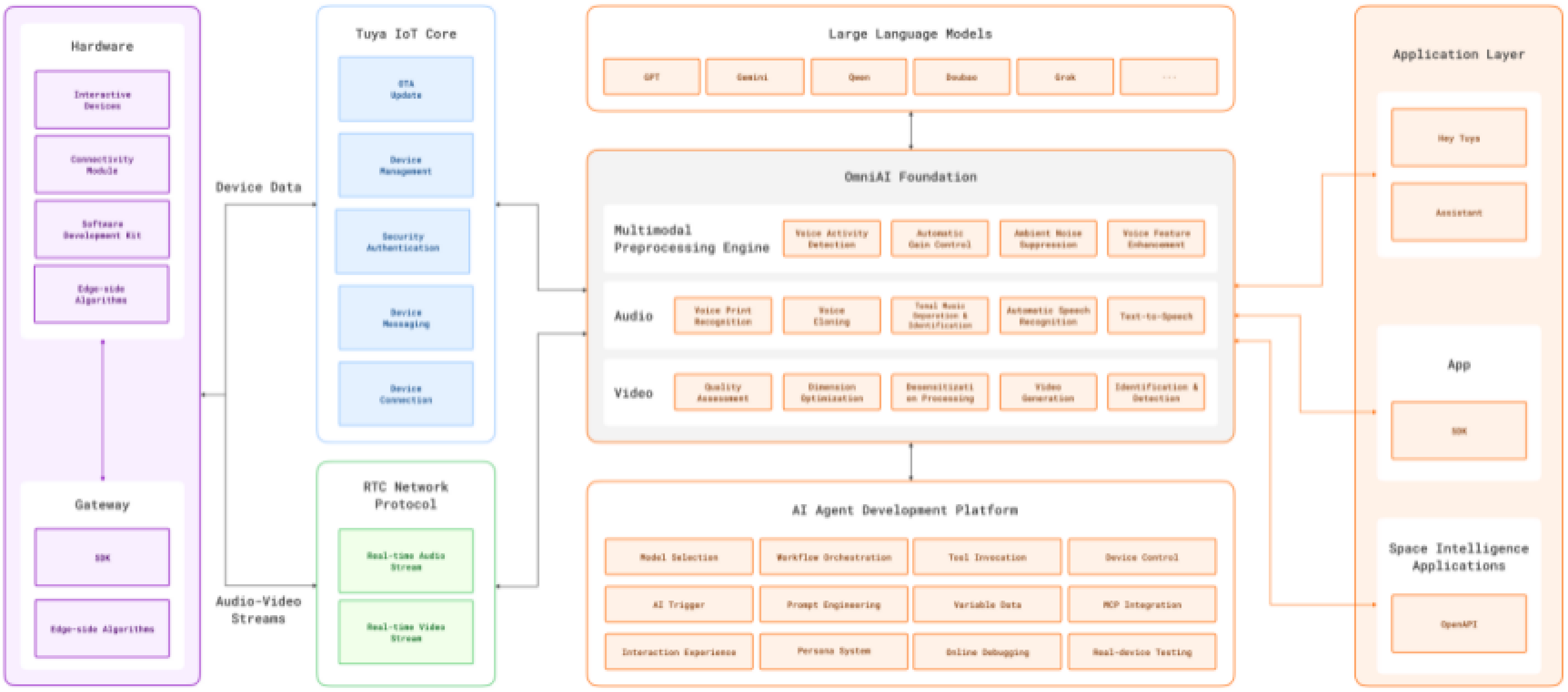
.

Chapter 4: AI Security Practices Focusing on Core Business Scenarios

4.1 AI Platform: A Secure, Open, and Neutral Ecosystem

Keywords: Prompt Injection, Content Safety, AI Agent Security Control, MCP Gateway & Data Permissions, LLM Attack & Defense

Tuya's AI platform is committed to building interoperable development standards, connecting brands, OEM manufacturers, developers, retailers, and intelligent needs across various industries. Based on global public cloud infrastructure, Tuya's developer platform enables interconnectivity of smart scenarios and intelligent devices, handling billions of device interaction requests daily. The platform services cover three aspects: hardware development tools, IoT cloud services, and smart industry development, creating a one-stop product intelligence and IoT application development experience, providing developers with comprehensive support from technology to marketing channels.



The current platform integrates multiple language models, providing users with efficient and flexible intelligent agent management capabilities. Users can easily deploy and run agent-related applications through configuration and debugging. Agents can connect to plugin functions allowing calls to various tools or APIs, such as device queries, device control, and scenario control. Plugins extend agent capabilities, enabling them to perform more diverse and complex tasks. At the same time, agents also support connecting to Tuya's official or customer-owned knowledge bases to better answer user questions or execute tasks.

Under the protection of the 'Titan Matrix' security brand, Tuya's AI platform has established the following security practices:

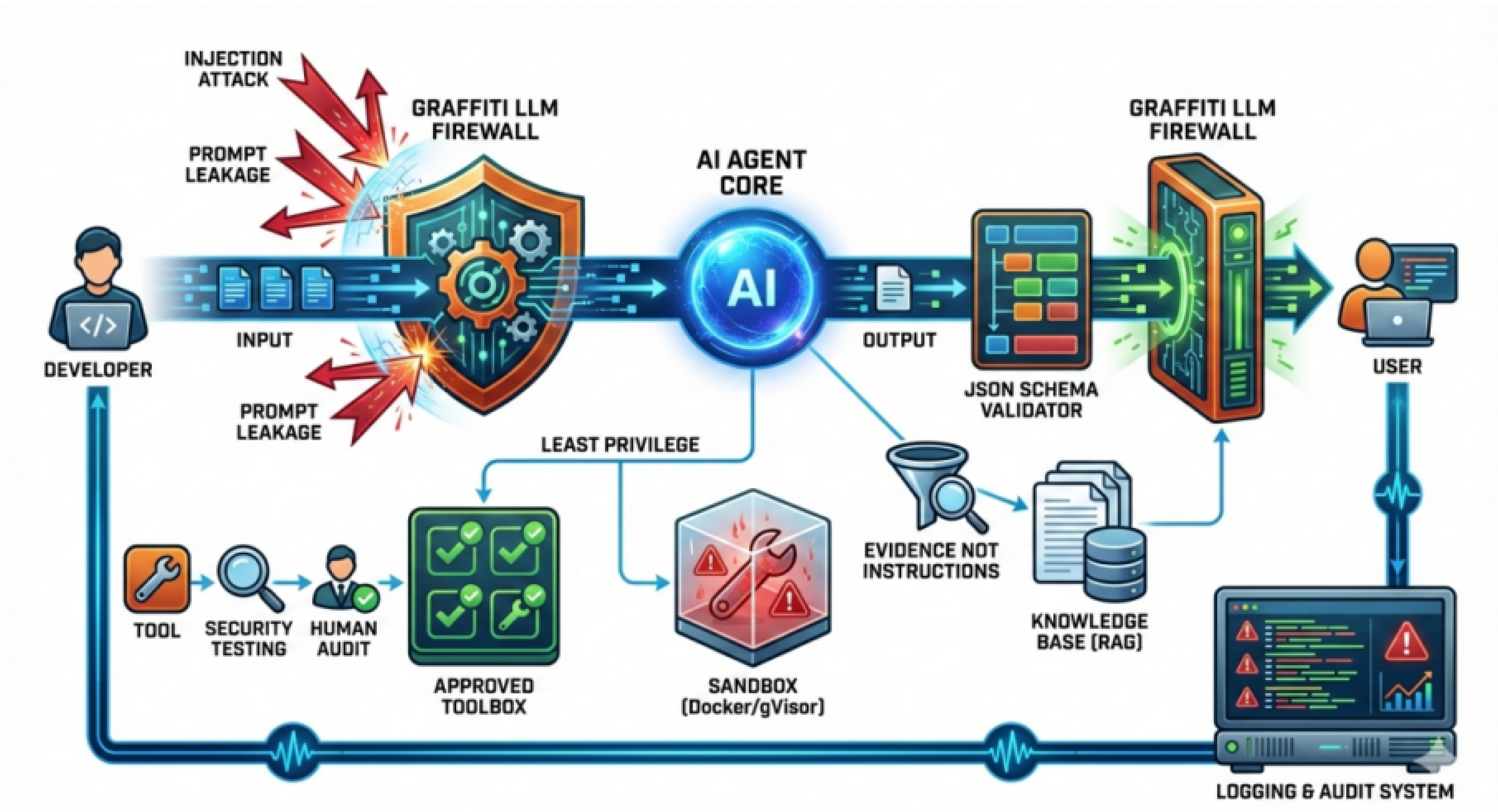
Prompt Attack Detection

The large model firewall is one of the core capabilities provided by the 'Titan Matrix' security center. Tuya's large model firewall specializes in defending against injection attacks targeting generative AI, accurately identifying adversarial attack behaviors such as jailbreak instructions, role-playing inducements, and system instruction tampering, building an "immune defense line" for AI systems. Currently, strict detection and interception are implemented in scenarios such as AI dialogue input/output and AI Agent instruction interaction input/output.

Content Security Detection

For content security compliance, relying on the capabilities of the 'Titan Matrix' security center, Tuya implements content compliance detection and sensitive content detection, conducting multi-dimensional compliance reviews of text content in generative AI input/output, covering risk categories such as politically sensitive content, pornography, bias and discrimination, and negative values, ensuring AI-generated content complies with laws, regulations, and platform standards. Simultaneously, deeply detecting potential privacy data and sensitive information that may be leaked during AI interactions, supporting identification of sensitive content involving personal privacy and enterprise privacy, preventing training data leakage and dialogue information overflow risks. Currently, detection is mandatorily enabled in all scenarios involving AI dialogue, intelligent customer service, knowledge base Q&A, etc.

AI Agent Configuration Audit



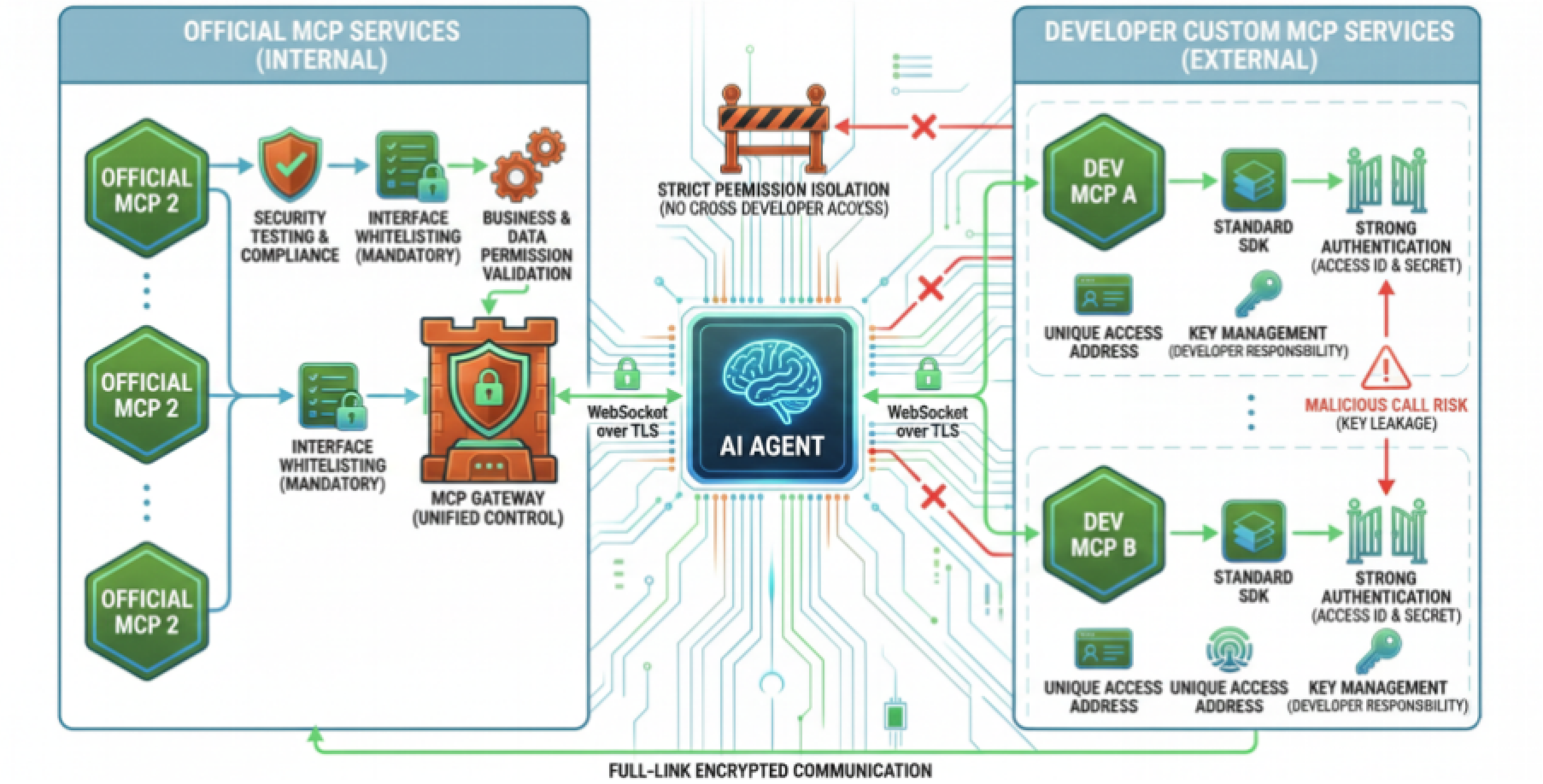
The input and output of AI Agents configured by developers are also connected to Tuya's large model firewall to prevent injection attacks, prompt leakage, and implement targeted content security filtering. At the same time, outputs are forced to conform to predefined JSON Schema to prevent output tampering or unexpected operations. For knowledge base RAG mounting, instruction removal is mandatory, explicitly informing the model that referenced documents are "evidence" rather than "instructions" to prevent indirect injection.

Additionally, all official tools launched on the platform must undergo strict security testing and risk assessment before release, requiring manual audit and confirmation by the security team. Ensure each Agent tool is assigned the minimum permissions necessary to complete its tasks. High-risk operations must run in isolated environments (such as Docker, gVisor).

Finally, Tuya's services and applications strictly record key Agent decisions, tool calls, and abnormal events for post-event tracing and analysis, ensuring continuous monitoring and auditing of third-party AI Agent risks.

MCP Service Audit

Tuya's MCP services are divided into official MCP and developer-customized MCP categories. For official MCP, we implement unified control through our self-developed MCP gateway. All internal MCP services must pass strict security testing and compliance assessments before launch, and mandatory interface call whitelisting is enforced—each interface must pass security review before configuration. Simultaneously, all services must integrate business permission and data permission verification to fundamentally prevent privilege escalation.


OFFICIAL MCP SERVICES (INTERNAL)
OFFICIAL MCP 2
SECURITY TESTING & COMPLIANCE
INTERFACE WHITELISTING (MANDATORY)
BUSINESS & DATA PERMISSION VALIDATION
OFFICIAL MCP 2
INTERFACE WHITELISTING (MANDATORY)
MCP GATEWAY (UNIFIED CONTROL)
OFFICIAL MCP 2
STRICT PEEMISSION ISOLATION (NO CROSS DEVELOPER ACOYSS)
WebSocket over TLS
AI AGENT
WebSocket over TLS
DEVELOPER CUSTOM MCP SERVICES (EXTERNAL)
DEV MCP A
STANDARD SDK
STRONG AUTHENTICATION (ACCESS ID & SECRET)
UNIQUE ACCESS ADDRESS
KEY MANAGEMENT (DEVELOPER RESPONSBILITY)
MALICIOUS CALL RISK (KEY LEAKAGE)
DEV MCP B
STANDARD SDK
STRONG AUTHENTICATION (ACCESS ID & SECRET)
UNIQUE ACCESS ADDRESS
UNIQUE ACCESS ADDRESS
KEY MANAGEMENT (DEVELOPER RESPONSBILITY)
FULL-LINK ENCRYPTED COMMUNICATION

For developer-customized MCP services, the platform provides standard SDKs for integration. Each service receives a unique access address, Access ID, and Access Secret generated by the platform, implementing strong authentication mechanisms—only authenticated requests can access the corresponding MCP service. Developers must properly safeguard keys to prevent malicious calls. The platform implements strict permission isolation policies—developers can only configure their own MCP services to their AI Agents, ensuring services between different developers do not interfere with each other, effectively preventing unauthorized configuration and malicious contamination.

All MCP service communications are based on WebSocket over TLS protocol, building a secure and reliable full-chain persistent connection, ensuring data confidentiality, integrity, and availability during transmission.

AI Service Data Permission Design

Tuya platform implements data classification (e.g., public, internal, confidential, personal sensitive information) for all business data. Different data levels correspond to different access policies, ensuring high-sensitivity data remains under the highest protection level.

Simultaneously, all AI services have no direct authority to call Tuya's internal underlying services such as IoT Core, databases, or big data services, preventing business and data privilege escalation.

Through a unified interface service gateway, the gateway strictly calls authentication services to verify applications and services, along with the corresponding business and data permissions of developers or end users. Permission logic, based on RBAC (Role-Based Access Control), introduces dynamic attributes such as environment and data sensitivity to implement effective authentication decisions.

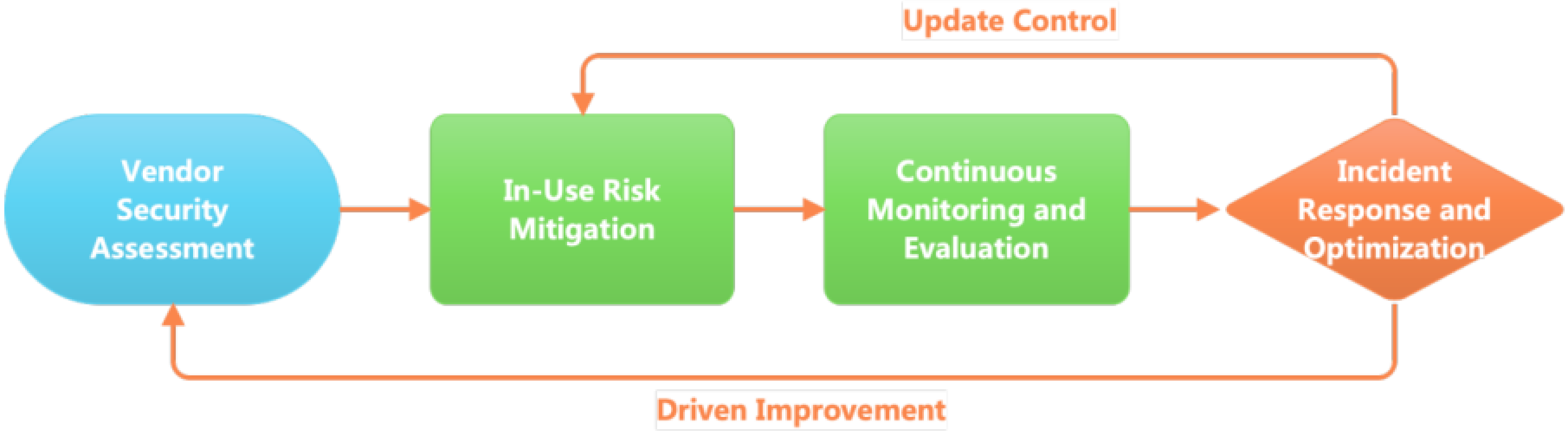
During AI interactions, when displaying data, automatic masking is applied to sensitive fields such as ID numbers and phone numbers. Static anonymization further protects user privacy.

LLM Security Audit

All third-party Large Language Models (LLMs) integrated into the Tuya platform undergo rigorous security assessments and compliance audits by the Tuya Security and Compliance Department. This process encompasses security management strategies covering the service's entire lifecycle.

1. **Prior to Procurement or Integration of Any Third-Party LLM:**

- **Security and Compliance Questionnaires**: We distribute detailed questionnaires to suppliers covering their data security and privacy protection policies (e.g., encryption methods for training data and user inputs, whether data is used for continuous training, and data retention periods), model security capabilities (built-in content filtering and protection against adversarial attacks), compliance certifications (such as SOC 2 Type II, ISO 27001, and MLPS assessments), and security incident response processes.
- **Contractual and Legal Constraints**: We explicitly define Data Processing Agreements (DPAs) within service contracts to ensure suppliers fulfill their legal obligations as data controllers or processors. Additionally, contract terms strictly stipulate requirements regarding data ownership, confidentiality, and prohibitions on using data for model training, while also defining penalty and accountability mechanisms for security violations.
- **LLM Security Testing**: The security team conducts manual, expert-level security testing on the models. If risks are identified, procurement and delivery can only proceed after remediation is completed and verified.


Update Control
Vendor Security Assessment
In-Use Risk Mitigation
Continuous Monitoring and Evaluation
Incident Response and Optimization
Driven Improvement

2. **Risk Mitigation and Control During Usage:**

- **Strict API Key Management**: We utilize a secure key management system for the storage and rotation of API keys, strictly avoiding any hardcoding within the codebase.
- **Secure Proxy Gateway**: We have developed an internal Unified LLM Security Gateway. All requests are forwarded through this gateway, which centrally implements content security filtering, rate limiting, quota management, and comprehensive audit logging.

3. **Continuous Monitoring and Periodic Assessment:**

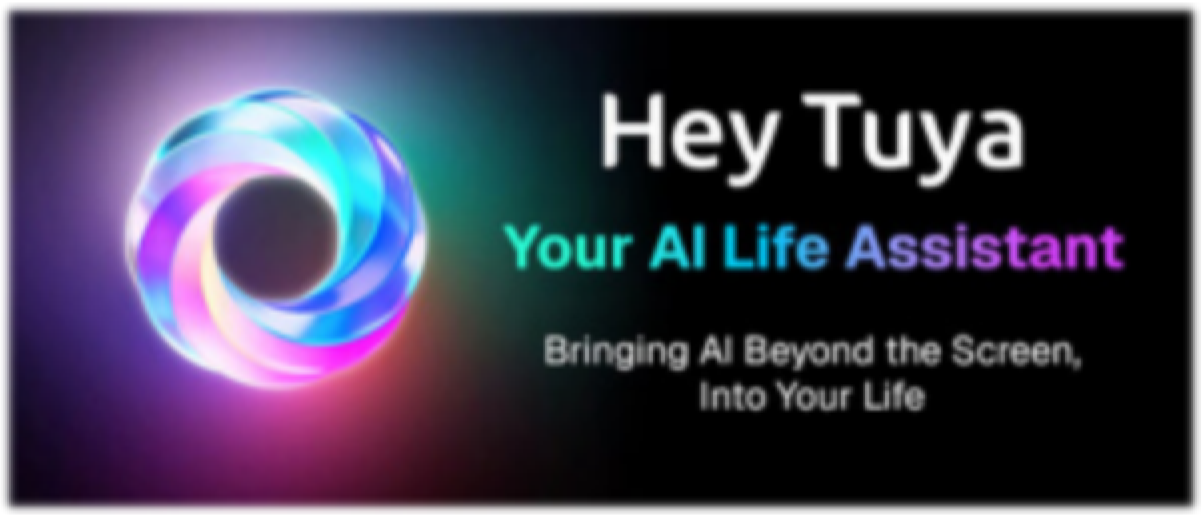
- **Periodic Security Re-evaluation**: We repeat the initial assessment process every six to twelve months to review the supplier's security status for any changes or new security incidents.

- **Red Teaming and Adversarial Testing**: We periodically organize internal security teams or engage third parties to conduct simulated attacks against the AI services in use.

4.2 Hey Tuya: A Secure and Reliable Smart Home Assistant

Keywords: Privacy Data Protection, Content Safety Filtering, Data Security Assurance, Mobile Application Security

Tuya is dedicated to creating "Your AI Life Assistant." As the core AI Agent, **Hey Tuya** supports multiple interaction modalities including text, voice, and video, and operates seamlessly across various terminals such as mobile phones, cenrtral control panels, and smart speakers. Centered on core daily life scenarios—security, energy conservation, efficiency, health, and companionship—Tuya has cultivated a matrix of AI Agent products. Through a collaborative multi-Agent architecture, we provide users with a comprehensive, intelligent living experience.



Privacy Protection Statement

Tuya's mobile applications strictly comply with international laws, regulations, and mainstream global information security and privacy protection standards. We maintain a comprehensive user personal information protection scheme, including but not limited to: public disclosure of collection and usage rules, robust process assurance, advanced Privacy by Design (PbD) standards, explicit statements regarding the purpose, method, and scope of personal information collection, complete user consent solutions, and detailed channels for complaints, reporting, and manual feedback handling to safeguard user privacy rights.

Furthermore, the privacy statement explicitly details the data collection and usage related to AI services, listing specific functions and potential data collected. It includes Tuya's commitments, such as strictly prohibiting the use of user-input content for model training. The application also transparently displays filing information for algorithms and models within China, outlining their basic principles, operating mechanisms, and application scenarios. Additionally, detailed lists of all third-party AI services used are provided, specifying the content collected and specific usage scenarios.

Content Safety Filtering

Tuya implements full-link compliance detection for the interactive content of Hey Tuya services, covering risk dimensions such as political sensitivity, pornography, discrimination, and values to ensure lawful and compliant outputs. Simultaneously, the platform deeply screens for and identifies potential leaks of personal and corporate privacy information during interactions, performing mandatory desensitization (masking) on all suspected sensitive data in AI outputs to fundamentally eliminate the risk of information leakage.

Data Security Assurance

The entire interaction process between the App and cloud-based AI services is based on the WebSocket over TLS protocol. This secure and reliable persistent connection guarantees the confidentiality, integrity, and availability of data during transmission. Furthermore, user-uploaded images and videos stored in the Tuya Cloud are mandatorily encrypted using AES-128.

Mobile Application Security

Tuya Smart's mobile applications undergo rigorous hardening, including but not limited to anti-tampering, code obfuscation, emulator detection, Root environment detection, anti-debugging, and interface hijacking protection, effectively securing client programs. For local data generated by the client, secure encryption methods are used for storage with strictly restricted read/write permissions. Specifically, critical information such as keys is securely stored using the mobile operating system's native key storage services (e.g., Keystore/Keychain).

4.3 AI Toys: Guardianship for Special Groups

Keywords: Children's Privacy Protection, Children's Content Safety, Terminal Communication Security, Smart Terminal Security

The Tuya Smart AI Toy Solution embeds Large Language Models (LLMs) into toys, achieving an intelligent upgrade. This solution enables low cost, high efficiency, rapid time-to-market, and a unified brand image.

Children's Privacy Protection

Tuya Smart meets the requirements of relevant laws regarding children's privacy protection in mainstream countries, including COPPA (Children's Online Privacy Protection Act). Measures include:

1. Age verification and parental authorization mechanisms.
2. Strict restrictions on children's data retention.
3. Data minimization and purpose limitation to ensure data security and compliance.

Currently, a dedicated privacy protection statement for children is provided within the App. Additionally, risk warnings for children are included on product packaging and in user manuals.

Content Safety Grading

We have implemented strict content safety grading for AI services related to children's toys. Specific filtering and handling schemes are in place for content involving legal red lines, psychological health impacts, and value formation.

In addition to using the Large Model Firewall to detect and intercept inputs and outputs, Tuya Smart continuously collects and organizes compliance test cases. We conduct routine verification and continuous adversarial testing on AI services to guarantee the safety and compliance of output content.

AI Service Point-to-Point Communication Security

- Signaling Communication Security: The first layer establishes a transmission channel based on the TLS 1.2 protocol, utilizing ECDHE key exchange to achieve forward secrecy and ensure the ephemeral nature of session keys. The second layer encrypts business data using the AES-128-GCM algorithm. This algorithm employs the NIST-certified AEAD mode to simultaneously protect data confidentiality and integrity. Keys are generated based on device and user identities, implementing dual-factor key derivation to ensure key uniqueness.

- Link End-to-End Authentication: Beyond relying on reliable signaling communication links, the end-to-end process mandates dual-sided verification of temporary usernames and passwords generated based on the device's unique key and permission information. Simultaneously, the terminal generates its own local authentication information. This constitutes a second layer of security authentication. Only after completing these two layers of end-to-end authentication can the TVS link be established.
- Link End-to-End Encryption: We adopt a dual protection mechanism consisting of a "One Device, One Secret" base key (EK) and a Temporary Session Key (TSK). For every session, the terminal generates a new random encryption key to secure communication; this key is derived end-to-end, meaning the cloud service cannot store or perceive it. Additionally, data transmission utilizes an HMAC-SHA256 message authentication mechanism to prevent Man-in-the-Middle (MITM) attacks.

Smart Terminal Security

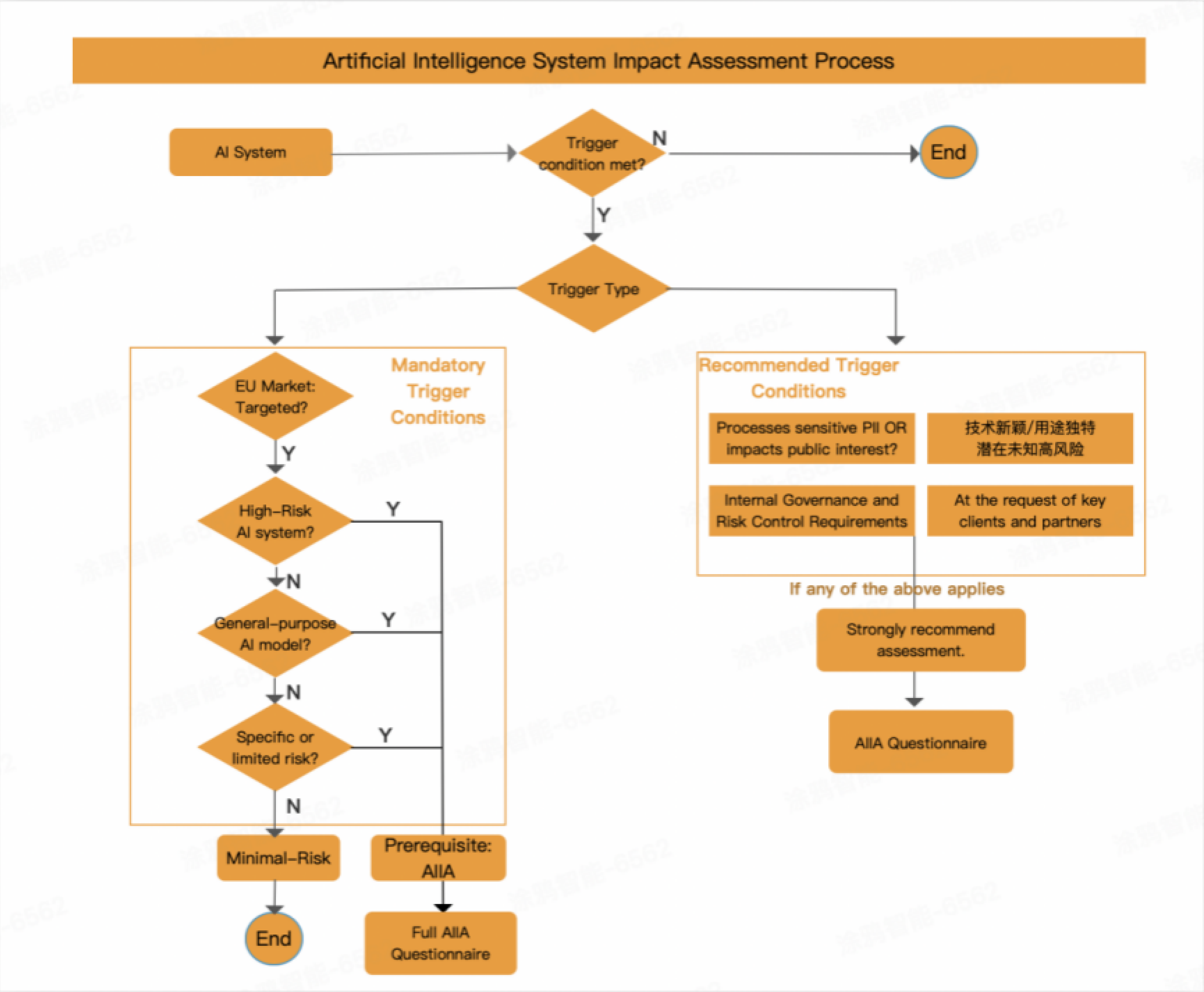
- **Device Authentication**: During production, Tuya Smart hardware solutions are provisioned with a pair of device authentication credentials. These credentials are unique to every device and bound to the module's environment (including Chip ID and MAC address). This information is signed into the data packet for every session request. Every communication must verify the accuracy of the module's environmental information and device authentication credentials to be considered valid.
- **OTA Security**: Tuya employs multiple protection measures for the firmware upgrade process:
  1. During firmware packaging, the tool generates firmware integrity verification information composed of multiple variables.
  2. When the client requests firmware, the server issues download information and firmware verification data. This verification data uses a secure HMAC signature algorithm signed with the device's unique identity key, ensuring the legitimacy and immutability of the firmware during transmission.
  3. After downloading, the client calculates the firmware verification data and compares it with the server's provision. During decompression, it validates the integrity verification information calculated by the packaging tool. The firmware is written only after passing this dual verification.
  4. If the write fails or the device cannot function normally after the update, it automatically rolls back to the previous firmware version.
- **Data Security**: To safeguard core data, critical information stored locally on the smart terminal is encrypted using AES. The encryption key is randomly generated during the chip's initialization and stored securely. It is used exclusively for local encryption and is never used for business processing or external interaction.

Chapter 5: Proactive Risk Monitoring and Defense System

Tuya Smart is committed to establishing a forward-looking, systematic AI risk management framework deeply integrated into the enterprise risk management system. This ensures that AI risks are identifiable, controllable, and manageable.

5.1 Risk Assessment Mechanism

Tuya has established and maintains the *AI System Impact Assessment and Risk Assessment Management Policy*, which defines standardized processes for risk identification, analysis, evaluation, and updates. Current assessments are categorized into periodic assessments and event-driven assessments.



Artificial Intelligence System Impact Assessment Process
AI System
Trigger condition met?
N
End
Y
Trigger Type
Mandatory Trigger Conditions
EU Market: Targeted?
Y
High–Risk AI system?
Y
N
General–purpose AI model?
Y
N
Specific or limited risk?
Y
N
Minimal–Risk
End
Prerequisite: AIIA
Full AIIA Questionnaire
Recommended Trigger Conditions
Processes sensitive PII OR impacts public interest?
技术新颖/用途独特
潜在未知高风险
Internal Governance and Risk Control Requirements
At the request of key clients and partners
If any of the above applies
Strongly recommend assessment.
AIIA Questionnaire

- **Periodic Assessments**: Comprehensive AI-specific risk assessments are conducted at least annually, covering all deployed and high-risk AI systems currently under development.
- **Event-Driven Assessments**: Targeted risk assessments must be initiated immediately upon the occurrence of major technological changes, business model adjustments, regulatory updates, or security incidents.

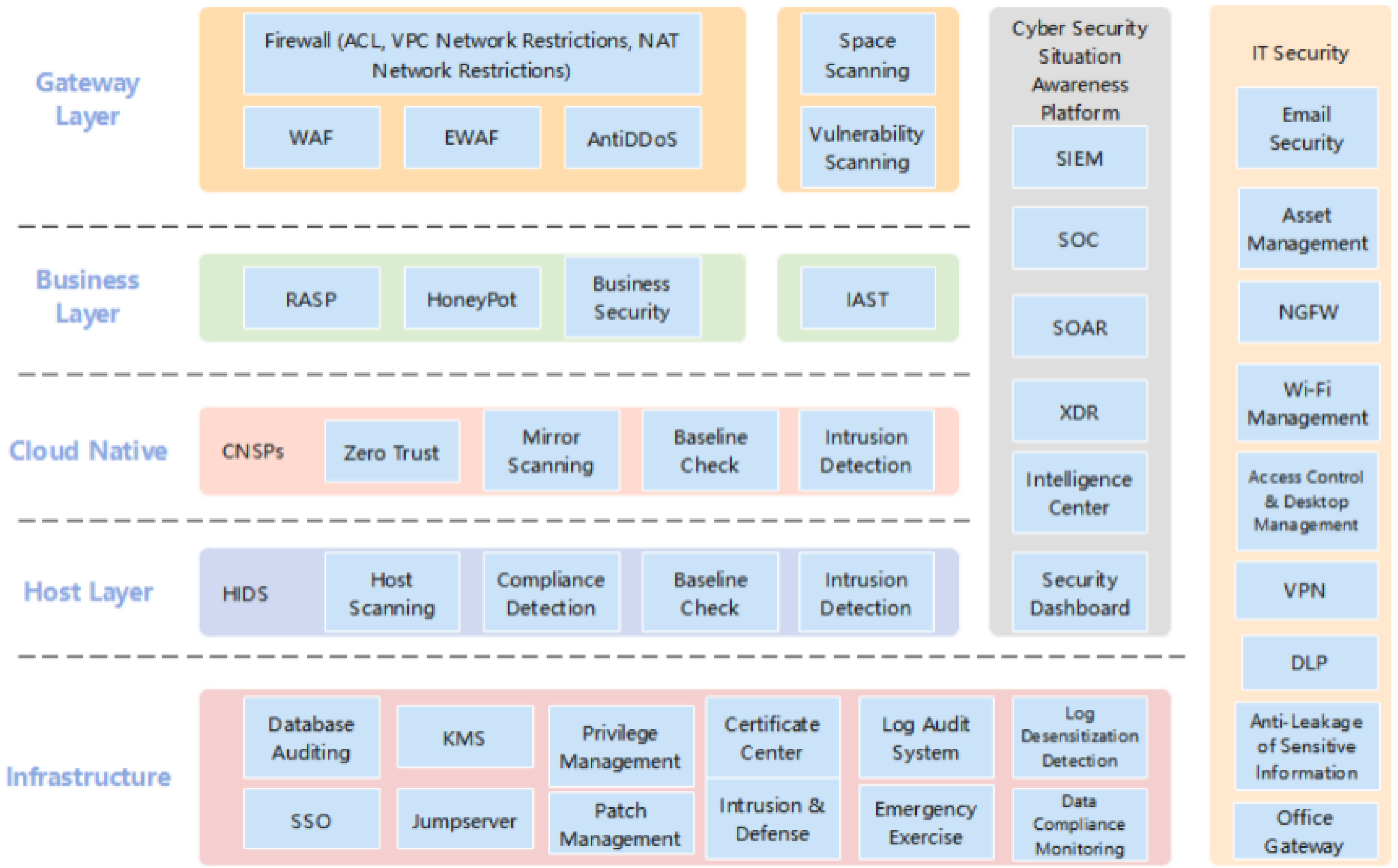
5.2 Risk Treatment and Acceptance

- **Incident Response**: Execute the AI security incident emergency response process in accordance with the AI System Security Incident Management Measures.
- **Risk Mitigation**: Formulate and execute risk treatment plans based on assessment results, prioritizing technical and managerial measures to reduce risk.
- **Residual Risk Management**: Residual risks that cannot be economically or effectively eliminated or reduced must be clearly documented and submitted to the Compliance Committee for approval, based on the Group's established risk acceptance criteria.

5.3 Compliance Assurance

- All AI activities must strictly adhere to applicable laws, regulations, and industry requirements regarding artificial intelligence, data security, and personal information protection in the jurisdictions where operations occur.
- Tuya's Legal and Compliance Department dynamically tracks legislative trends and organizes regular compliance reviews to ensure proactive compliance for the Group's AI business.
- For AI systems operating in regions with strict AI regulations (such as the European Union), Tuya enforces a mandatory compliance review by the Legal and Compliance Department prior to deployment, requiring written approval before proceeding.

5.4 Security Assurance



Gateway Layer: Firewall (ACL, VPC Network Restrictions, NAT Network Restrictions) · WAF · EWAF · AntiDDoS · Space Scanning · Vulnerability Scanning

Business Layer: RASP · HoneyPot · Business Security · IAST

Cloud Native: CNSPs · Zero Trust · Mirror Scanning · Baseline Check · Intrusion Detection

Host Layer: HIDS · Host Scanning · Compliance Detection · Baseline Check · Intrusion Detection

Infrastructure: Database Auditing · KMS · Privilege Management · Certificate Center · Log Audit System · Log Desensitization Detection · SSO · Jumpserver · Patch Management · Intrusion & Defense · Emergency Exercise · Data Compliance Monitoring

Cyber Security Situation Awareness Platform: SIEM · SOC · SOAR · XDR · Intelligence Center · Security Dashboard

IT Security: Email Security · Asset Management · NGFW · Wi-Fi Management · Access Control & Desktop Management · VPN · DLP · Anti-Leakage of Sensitive Information · Office Gateway

Leveraging the robust 'Titan Matrix' protection system, Tuya has built a mature, defense-in-depth architecture. This system encompasses comprehensive, granular protection spanning network, server, application, and code levels. Relevant security capabilities include Web Application Firewalls (WAF), Runtime Application Self-Protection (RASP), Cloud-Native Security Platforms (CNSPs), Host-based Intrusion Detection Systems (HIDS), HoneyPots, and Security Information and Event Management (SIEM) platforms, alongside numerous business security applications and components. This multi-layered mechanism identifies and responds to various Internet threats across technical architectures.

Currently, AI attack and defense capabilities are fully integrated into Tuya's defense-in-depth network security architecture. This includes AI Large Model Firewalls, AI HoneyPots, and AI business log security auditing:

- **LLM Firewall**: Implements content security, content compliance, and interception of prompt injection attacks.
- **AI HoneyPots**: Beyond simulating conventional business services, these cover specific large model infrastructures, including Model Context Protocol (MCP) honeypots.
- **AI Business Log Auditing**: Based on application log streams fully integrated into Tuya's SIEM, this function detects and assesses risks regarding potential attacks and coordinates with SOAR and other security systems to block risks.

5.5 Continuous Monitoring and Reporting

Tuya utilizes a unified observability platform to correlate, store, and analyze AI system logs, metrics, traces, and proprietary security event data. This data fusion breaks down data silos, enabling rapid drill-down from anomalous metrics to relevant error logs and specific request traces during troubleshooting, significantly shortening the time required for root cause analysis.

Tuya has also introduced advanced intelligent analysis technologies to achieve deep perception and proactive warning of AI system risks. Risk events identified during monitoring are graded in real-time (e.g., Basic, Watch, Control). By constructing a "Technology-Application-Business" risk correlation graph, Tuya transforms isolated alerts into a systematic perception of risk posture. For example, if model inference anomalies, surges in associated data source access, and abnormal network traffic are detected simultaneously, the system automatically correlates these events and elevates the overall risk level.

Regarding automated risk response and closed-loop processing, Tuya has established automated response capabilities deeply linked with the monitoring system, upgrading risk handling from "manual response" to "system self-healing."

1. **Automated Playbooks Deeply Integrated with SOAR**: The Security Orchestration, Automation, and Response (SOAR) platform is deeply integrated into the AI risk monitoring system. Automated playbooks are pre-configured for defined AI risk scenarios (e.g., prompt injection attacks, policy-violating model outputs, resource abuse). Once the monitoring system triggers an alert, the SOAR playbook automatically executes a series of actions, such as isolating the compromised model instance, invoking the firewall API to block the source IP, or temporarily taking high-risk model services offline for review while automatically generating an incident ticket.
2. **Continuous Monitoring of Assets and Supply Chain**: Specialized tools are used to continuously scan and monitor internal AI assets (including unauthorized "shadow" model services) and the AI supply chain (e.g., third-party models, datasets, open-source components). This system automatically identifies known vulnerabilities in components (such as unauthorized access

vulnerabilities in specific frameworks) and licensing compliance issues, comparing them in real-time against vulnerability databases and threat intelligence to achieve proactive risk discovery and management.

Finally, through a regular risk reporting mechanism, the status of AI risk management is incorporated into the Group's overall risk reporting system and reported to the Compliance Committee.

Chapter 6: Compliance Practices Following Global Regulations

6.1 International Standards System

In the global practice of the 'Titan Matrix' Privacy and Compliance pillar, Tuya has obtained a matrix of ISO certifications, including ISO/IEC 42001 (Artificial Intelligence Management System), ISO/IEC 27001 (Information Security Management System), ISO/IEC 27701 (Privacy Information Management System), and ISO/IEC 27017 (Code of Practice for Information Security Controls for Cloud Services). These certifications demonstrate that Tuya's AI capabilities possess globally leading security and compliance assurance at both the product and service levels.

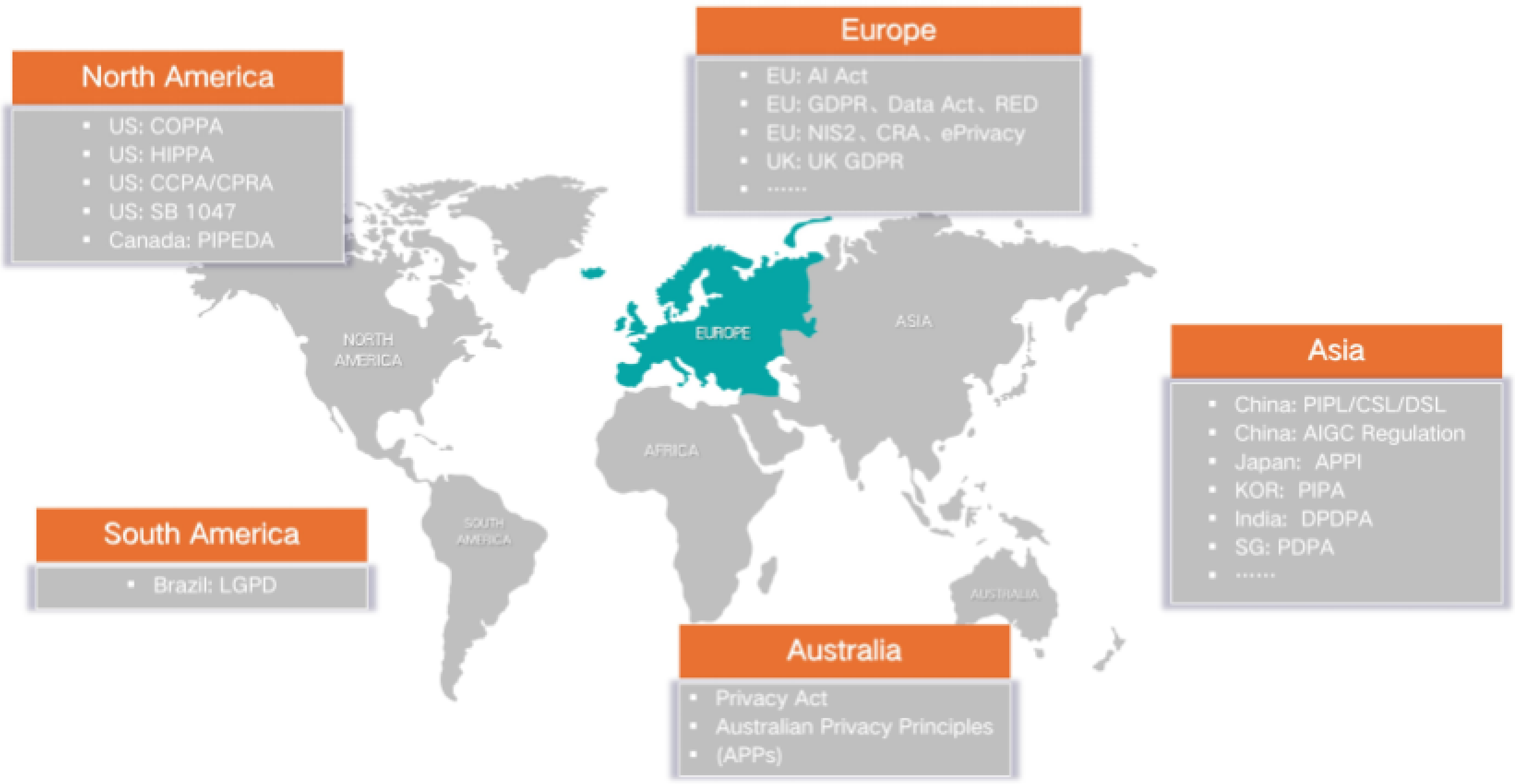
Simultaneously, Tuya holds authoritative third-party SOC 2 & SOC 3 audit reports, as well as regulatory audit reports covering GDPR, CCPA, PIPEDA, and other national regulations. We also conduct red teaming exercises and security assessment reports tailored to Tuya's products and services. These audits serve as authoritative validation of the 'Titan Matrix' capabilities, proving that Tuya steadfastly and continuously executes its commitment to advanced security and compliance.

bsi ISO/IEC 27701 Privacy Information Management CERTIFIED
bsi CSA STAR Cloud Security CERTIFIED
bsi ISO/IEC 27001 Information Security Management CERTIFIED
bsi ISO/IEC 27017 Cloud Security Management CERTIFIED
AICPA SOC
AICPA SOC2 Type II Audit
CQC
ISO9001 Quality Management System CERTIFIED
DNV
ISO/IEC 42001 AI Management System CERTIFIED
EU GDPR
EU GDPR
CCPA
CCPA
PIPEDA Québec Bill64
TÜV SÜD
DPDPA
TRUSTe Certified Privacy Powered by TrustArc
DEKRA
RED DA
TÜV SÜD
ETSI 303645
TÜV SÜD
NISTIR 8259
TÜV SÜD
PSTI
psacertified
PSA Level 1
ioXt
ioXt IoT Security Certification
paloalto UNIT 42
Palo Alto Network Unit42 Penetration Testing Report
UnderDefense
Under Defense Penetration Testing Report
RAPID7
Rapid7 Penetration Testing Report
AsiaInfo
AsiaInfo Cybersecurity Red Team/Blue Team Exercise Report
Chaitin Cybersecurity Red Team/Blue Team Exercise Report

6.2 Global Regulatory Mapping

Tuya closely monitors global AI regulatory trends and continuously aligns its practices with major international regulatory frameworks. Throughout the design, development, testing, deployment, and operation of our AI lifecycle, we strictly adhere to the laws and regulatory requirements of various jurisdictions, ensuring the safety, transparency, and compliance of our products and services. Based on a governance strategy of "Global Unified Baseline + Regional Adaptation," Tuya has constructed a global regulatory mapping matrix covering AI, security, privacy, and data.

Global AI & Data Act



North America
- US: COPPA
- US: HIPPA
- US: CCPA/CPRA
- US: SB 1047
- Canada: PIPEDA

Europe
- EU: AI Act
- EU: GDPR、Data Act、RED
- EU: NIS2、CRA、ePrivacy
- UK: UK GDPR
- ......

Asia
- China: PIPL/CSL/DSL
- China: AIGC Regulation
- Japan: APPI
- KOR: PIPA
- India: DPDPA
- SG: PDPA
- ......

South America
- Brazil: LGPD

Australia
- Privacy Act
- Australian Privacy Principles
- (APPs)

1. European Union: Risk Classification and Compliance Practices under the EU AI Act

The EU AI Act, which will come into full effect in August 2026, is the world's first comprehensive regulation covering the entire AI lifecycle. It classifies AI systems into Unacceptable Risk, High Risk, Limited Risk, and Low Risk categories. Tuya implements this through both institutional policies and practical applications:

(1) Prohibition of Unacceptable and High-Risk Categories

- Tuya commits not to develop, provide, or sell systems explicitly classified as Unacceptable Risk under the EU AI Act.
- In principle, Tuya does not involve itself in High-Risk AI systems. If an exception is required, it must undergo high-level risk control approval and complete technical documentation.

(2) Institutionalization of Internal Risk Classification

Tuya has formulated the AIoT Device Control Risk Classification Model and Management Specification. Based on the principle of "Foreseeable Risk — Severity — Probability," this specification classifies AI-controllable devices and commands. It clarifies AI control requirements and human confirmation requirements to safeguard user and device safety, ensuring that the AI decision-making chain is secure, controllable, and auditable.

(3) Transparency, Explainability, and User Right to Know

For Limited Risk and Low Risk scenarios, Tuya:

- Clearly identifies the AI identity within the interaction interface.
- Discloses algorithmic logic, data usage purposes, and potential impacts in privacy policies and documentation.
- Provides explainable descriptions to users.
- Offers human-machine collaboration mechanisms.

These requirements align with the transparency obligations under Article 52 of the EU AI Act.

(4) Supply Chain Responsibility and Model Governance

Tuya has also established a compliance review process for third-party models, plugins, and suppliers, including:

- Compliance assessment of model sources and training data.
- AI system risk assessment and impact assessment.

- Output quality and security compliance testing.
- Supply chain security compliance questionnaire review.

2. China: Regulation of Generative AI and Deep Synthesis

China has formed a systematic regulatory framework for AIGC (Artificial Intelligence Generated Content) and algorithm governance. Tuya implements these requirements synchronously across three dimensions: institutional policies, product capabilities, and operational processes.

Following the Measures for the Labeling of Artificially Generated or Synthesized Content, effective September 2024, Tuya conducted in-depth interpretation and full-staff compliance training, implementing both explicit and implicit labeling as required. Simultaneously, Tuya comprehensively strengthens management in content safety, algorithm security, and data compliance by adhering to regulations such as the Provisions on the Administration of Deep Synthesis Internet Information Services, the Interim Measures for the Management of Generative Artificial Intelligence Services, and the Provisions on the Administration of Algorithmic Recommendations for Internet Information Services.

3. Global AI and Data Protection Regulations Tracked by Tuya

Tuya has built a continuously updated global regulatory library to guide product design, algorithm governance, security assessment, and privacy compliance.

(1) European Union

EU AI Act, EU Data Act, GDPR, RED (Radio Equipment Directive), NIS 2, Cyber Resilience Act, ePrivacy Directive.

(2) United States

California SB 1047, CCPA/CPRA, COPPA, HIPAA.

(3) China

AIGC Labeling Measures, Deep Synthesis Provisions, Generative AI Measures, Algorithm Recommendation Provisions, Provisions on Necessary Personal Information for Apps, Cybersecurity Law, Data Security Law, Personal Information Protection Law (PIPL).

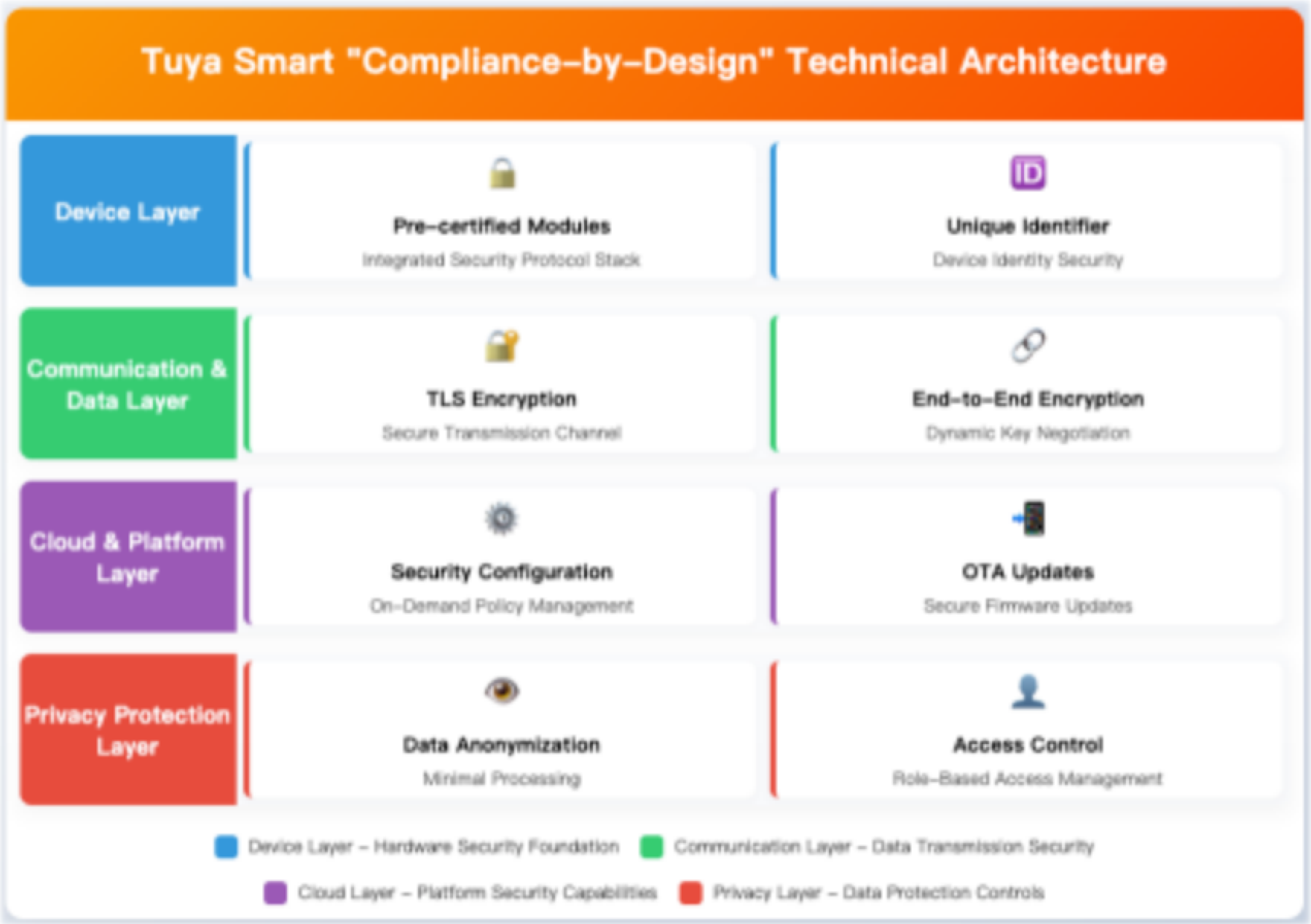
(4) Other Key Jurisdictions

- **India**: DPDP + DPDP Rules (2025)
- **South Korea**: PIPA, AI Basic Law (Draft)
- **Brazil**: LGPD, Brazilian AI Act (Draft)
- **Singapore**: PDPA
- **Canada**: PIPEDA, Quebec Law 25
- **United Kingdom**: UK GDPR, PSTI (Product Security and Telecommunications Infrastructure Act)
- **Australia**: Privacy Act 1988
- **Vietnam**: Law on Cybersecurity
- **Saudi Arabia**: PDPL

Tuya will continue to track global AI and data protection regulations, constantly refining our compliance system to safeguard global user rights and assist clients in operating securely and compliantly across all markets.

6.3 Product Compliance-by-Design

Within Tuya Smart's technical ecosystem, "Compliance-by-Design" is not an isolated step but a systematic technical architecture integrated throughout product hardware, software, communications, and the cloud. By transforming core security and compliance requirements into executable, verifiable technical specifications and automated tools, we ensure compliance is embedded from the very inception of the product.



Tuya Smart "Compliance-by-Design" Technical Architecture

Device Layer	**Pre-certified Modules** Integrated Security Protocol Stack	**Unique Identifier** Device Identity Security
Communication & Data Layer	**TLS Encryption** Secure Transmission Channel	**End-to-End Encryption** Dynamic Key Negotiation
Cloud & Platform Layer	**Security Configuration** On-Demand Policy Management	**OTA Updates** Secure Firmware Updates
Privacy Protection Layer	**Data Anonymization** Minimal Processing	**Access Control** Role-Based Access Management

🟦 Device Layer - Hardware Security Foundation 🟩 Communication Layer - Data Transmission Security

🟪 Cloud Layer - Platform Security Capabilities 🟥 Privacy Layer - Data Protection Controls

- **Device Side**: We are dedicated to establishing an immutable security foundation at the physical level. Our pre-certified hardware modules offer technical value by deeply integrating security protocol stacks within their internal firmware that comply with target market regulations. For example, to meet cybersecurity requirements in major markets like the EU (RED) and the UK (PSTI), module firmware defaults to enabling and correctly configuring essential security functions, such as wireless communication encryption strength, unique device identifiers, and secure software update mechanisms.
- **Communication & Data Layer**: All data transmission is conducted via high-strength TLS 1.2/1.3 encrypted channels. Additionally, content employs an extra layer of AES security encryption to ensure data confidentiality and integrity during transmission. For highly sensitive business operations, end-to-end encryption is implemented, where keys are dynamically negotiated and generated end-to-end, ensuring decryption can only be performed by the user and the user's terminal.
- **Cloud & Platform Layer**: We provide native security capabilities, allowing developers to configure security for apps and terminal devices on-demand based on their needs, while supporting secure OTA (Over-The-Air) upgrade mechanisms.
- **Privacy Protection**: We translate privacy design principles into concrete technical control measures. This includes Data Minimization and Anonymization: In the data reporting link, the platform supports field-level desensitization (masking) and anonymization of device logs and operational data, ensuring unnecessary personal identifiers are not uploaded or stored without affecting business functions. It also includes Granular Access Control: The platform implements a Role-Based Access Control (RBAC) model. Developers can define fine-grained data and device operation permissions for their application users, ensuring users can only access devices and data within their authorized scope, technically enforcing the principle of separation of privileges.

Chapter 7: Transparent Communication and Future Outlook

7.1 Our Commitment: Continuous Transparency and Improvement

We firmly believe that transparency is the cornerstone of trust. We commit to:

1. **Proactive Disclosure**: Regularly publishing AI security and governance transparency reports, disclosing key security metrics, compliance progress, and summaries of ethical reviews.
2. **Open Participation**: Inviting customers, developers, and academic institutions to participate in security standard discussions and threat intelligence sharing through the **'Titan Matrix Security Ecosystem Alliance.'**
3. **Responsive Feedback**: Maintaining open communication channels and providing timely, responsible responses to every security inquiry or suggestion from users, partners, or researchers.

We will continue to iterate and improve, ensuring our actions remain synchronized with the world's most advanced responsible AI practices.

7.2 The Path Ahead: From Security and Compliance Practitioner to Trusted Intelligent Ecosystem Architect

Looking forward, Tuya Smart will leverage the integrated security foundation of '**Titan Matrix**' to lead the secure and trusted development of Physical AI (AI integrated with physical systems and IoT):

Defining Next-Generation AI-Native Security

We will continue to invest in cutting-edge security research and development, focusing on:

- **Edge Intelligence Security**: Developing lightweight, high-reliability on-device AI security modules to provide local, real-time privacy computing and threat defense for massive IoT devices, reducing latency and reliance on cloud synergy.
- **Deepfake and Multimodal Attack Defense**: Building specialized detection and traceability systems against AI-generated forged audio/video and cross-modal (combined image-text, voice command) attacks to safeguard the authenticity of the digital world.
- **Self-Evolving Security Intelligence**: Deepening the application of AI in security operations (AISecOps) to create an "adaptive immune system" capable of autonomous learning from attacks and dynamic adjustment of defense strategies.

Ecosystem Win-Win: Transforming Enterprise-Grade Security into Developer Confidence

We believe that the ultimate form of security is one where developers do not need to be distracted by it. Therefore, we do not deliver security as an optional extra or a complex standalone API. Instead, we are committed to deeply embedding the enterprise-grade security capabilities of "Titan Matrix" into every piece of Tuya's infrastructure and services.

- **Native Integration, Seamless Protection**: When a developer uses Tuya's AI Agent development platform to configure an agent, prompt injection detection and content safety filtering are already active by default. When a device control interface is called, rigorous permission verification and behavioral risk control are already operating at the underlying layer. Security is no longer an external module requiring separate integration; it is a fundamental capability, just like the computing and storage provided by the platform.
- **Unified Foundation, Consistent Experience**: From the TuyaOpen open-source framework to cloud API services, we have pre-configured a unified security foundation for all development paths. This means that regardless of the entry point used to build AIoT applications, developers automatically receive security and privacy-by-design that meets global mainstream regulatory requirements, significantly lowering compliance barriers and potential risks.

By doing so, we empower global developers to create innovative products with top-tier security DNA without needing to be security experts. Tuya's goal is to enable every developer to focus on creating business value while enjoying a solid, reliable sense of security provided by the platform layer.

Our Determination: Tuya Smart's objective is not only to be the most secure AI platform but also to become a foundational architect of a trusted intelligent ecosystem. With "Titan Matrix" as our engine and transparency and openness as our guiding principles, we will join hands with global partners to embrace a secure, reliable, and human-centric future of the Intelligence of Everything.

Appendix

A. Glossary

- **Titan Matrix**: Tuya Smart's integrated intelligent security brand. It encompasses five key pillars: R&D Security Management, Security Center, Multi-dimensional Defense System, AI Security, and Privacy & Compliance. It provides full-stack, lifecycle security capabilities for the Tuya AIoT ecosystem and developers.
- **PREPARE Framework**: The core principles of Responsible AI followed by Tuya Smart. The acronym stands for **P**rivacy-by-Design, **R**esilience, **E**quity, **P**roportionality, **A**ccountability, **R**eliability, and **E**xplainability.
- **AI Lifecycle Management**: The systematic and integrated security management and compliance control of an AI system throughout its entire process, from planning, design, development, and deployment to operation, decommissioning, and archiving.
- **Algorithm Filing**: A compliance obligation based on Chinese regulations, such as the Provisions on the Administration of Algorithmic Recommendations for Internet Information Services, requiring algorithm providers to submit basic algorithmic information through official channels to enhance transparency.
- **Residual Risk**: The remaining risk that exists after all reasonable and feasible risk treatment measures have been implemented, which must be actively managed and formally accepted.
- **Defense-in-Depth Architecture**: A cybersecurity design philosophy that deploys overlapping security protections across multiple layers—including network, host, application, and data—to mitigate the risk of a single point of failure in the defense line.
- **AI Agent**: An intelligent entity capable of perceiving its environment, making decisions, and executing actions to achieve specific goals. In this context, it often refers to intelligent applications based on Large Language Models (LLMs) that can invoke tools (e.g., controlling hardware devices).
- **MCP (Model Context Protocol)**: An open protocol that allows LLMs to access external data sources and tools in a secure and standardized manner. The Tuya platform provides an official MCP Gateway for the secure management of related services.
- **Observability**: The ability to gain deep insights into the internal state and performance of a system by collecting and analyzing three types of data: logs, metrics, and traces. It serves as the technical foundation for continuous monitoring.
- **SOAR (Security Orchestration, Automation, and Response)**: A technology that enables organizations to streamline security operations by connecting security tools and predefining playbooks to automate and standardize incident response workflows.
- **WAF (Web Application Firewall)**: A security solution used to monitor, filter, and block HTTP traffic to and from a web application, defending against common web-based attacks.
- **SIEM (Security Information and Event Management)**: A platform responsible for centralized collection and correlation analysis of various security logs and events for threat detection and

investigation.

- **Prompt Injection Attack**: A security attack targeting LLMs where an attacker uses specially crafted inputs (prompts) to induce the model to bypass original security constraints or instructions and perform unintended actions.
- **Adversarial Exmaples**: Specially constructed input data designed to cause a machine learning model to make incorrect predictions or classifications. Defending against such attacks is a critical component of model robustness.
- **Data Poisoning**: An attack occurring during the model training phase, where malicious samples are injected into the training data to influence the learning process, ultimately compromising the model's performance or behavior.
- **LLM Firewall**: A security system specifically deployed for LLM applications. Core functions typically include prompt injection detection and security filtering of input/output content.
- **Red Teaming**: A proactive security assessment methodology that tests the effectiveness of a system's defenses by simulating the tactics, techniques, and procedures (TTPs) of real-world attackers.
- **Physical AI**: Artificial Intelligence that deeply interacts with the physical world through IoT devices and can produce real-world impacts. This is a core strategic direction for Tuya's AI vision.

B. List of Tuya's Core AI Management Policies

- *Tuya AI Management Charter*
- *Management Measures for AI System Security Incidents*
- *Regulations for AI System Resource Management*
- *Management Policy for AI System Impact and Risk Assessments*
- *Strategic Specification for AI System Lifecycle*
- *Management Specification for AI System Training Data*
- *Management Specification for AI Suppliers*

C. List of Obtained Security & Privacy Certifications and Audits

Global

- **ISO/IEC 42001:2023**: AI Management System Certification
- **ISO/IEC 27001:2022**: Information Security Management System Certification
- **ISO/IEC 27017:2015**: Code of Practice for Information Security Controls for Cloud Services
- **ISO/IEC 27701:2019**: Privacy Information Management System Certification
- **CSA STAR**: Cloud Security Alliance STAR Certification
- **SOC 2 Type II**: AICPA SOC 2 Audit Report (evaluating controls related to security, availability, processing integrity, confidentiality, and privacy)
- **SOC 3**: AICPA SOC 3 Audit Report

- **Enterprise Privacy Certification (EPC)**
- **CMMI 3.0**: Capability Maturity Model Integration Level 3
- **ISO 9001:2015**: Quality Management System Certification
- **PSA Certified Level 1**: IoT Device Security Evaluation and Certification
- **ioXt Manufacturer Certified**: IoT Security Certification

Regional

- **[EU] GDPR**: Verification Report
- **[EU] RED DA**: EU Radio Equipment Directive Compliance
- **[EU] ETSI EN 303 645**: EU Cybersecurity Standard for Consumer IoT
- **[EU] CE Marking**: EU Safety, Health, and Environmental Protection Requirements
- **[EU] RoHS**: Restriction of Hazardous Substances Directive
- **[EU] REACH**: Registration, Evaluation, Authorisation and Restriction of Chemicals
- **[US] CCPA**: Verification Report
- **[US] NISTIR 8259**: NIST IoT Cybersecurity Baseline Compliance
- **[US] FCC**: Federal Communications Commission EMC Standards
- **[China] MLPS 2.0 Level 3**: Multi-Level Protection Scheme (3.0) Registration
- **[China] CQC**: China Quality Certification
- **[China] CCC**: China Compulsory Certificate
- **[UK] PSTI**: Product Security and Telecommunications Infrastructure Act
- **[Canada] PIPEDA & Quebec Law 25**: Privacy Protection Assessment Reports
- **[Canada] IC**: Industry Canada EMC Requirements
- **[India] DPDPA**: Compliance Assessment Report for the Digital Personal Data Protection Act

D. Contact Us

Tuya Vulnerability Bounty Platform: https://src.tuya.com

Titan Matrix Security & Compliance Support: sec@tuya.com