TOKENCOD Cloud Security Whitepaper

Neutral - Professional - Secure - Trustworthy | TOKENCOD Security Team | July 2026

Note: This is an English translation of the original Chinese whitepaper. Embedded figures and diagrams (images) are retained only in the original document and are referenced by caption below; their contents are not translated in this text version.

Table of Contents

1. Preface

With the development and maturation of the cloud computing industry, more and more users are choosing to place their business on cloud platforms. While cloud platforms host a large number of users and massive amounts of business, they also shoulder greater responsibility. To ensure the continuous and sound operation of users' business and to protect the security and integrity of user data, the security of the cloud platform has always been TOKENCOD's top priority.

In recent years, security has become one of the competitive thresholds for cloud service providers. As the operational guarantee of TOKENCOD, network information security is a key activity that involves all employees and runs through the entire lifecycle of TOKENCOD's organization and products. From the establishment of infrastructure and product design to business continuity, and from the setup and operation of the organization, personnel recruitment and training to daily office work, network information security awareness has imperceptibly penetrated every person and every link of TOKENCOD. Security is the core of TOKENCOD's daily operations and disaster recovery work, and security has gradually become an important reason and basis for users to trust TOKENCOD.

2. Security Genes Build a Secure Platform

2.1 Professional Security Team

TOKENCOD's CEO and Chief Information Security Officer, Lai Qizhi, is a senior security expert in the Internet industry. Under his leadership, TOKENCOD has had deep-rooted security genes since its founding, and security has been an important factor in the cloud platform architecture design from the very beginning.

TOKENCOD has a dedicated security team that upholds the philosophy of being dedicated, professional, and focused, bringing together security experts and security professionals in various fields. The team consists of R&D, operations and maintenance, and operations personnel, covering infrastructure security, network security, host security, application security, and security management, and has dedicated teams responsible for the operation and handling of security vulnerabilities and security incidents. Every level and every link is controllable, trustworthy, and reliable.

2.2 Audit and Compliance Team

TOKENCOD has established a professional compliance team to complete internal security audits, ensure that the company, cloud platform, and cloud products comply with national and regional regulations, obtain international certification, and provide customers with compliance consulting services to help them complete regulation and certification more smoothly.

2.3 Employee Background Checks and Confidentiality Agreements

Before employees join, TOKENCOD, to the extent permitted by national and regional laws and regulations, uses a series of background check methods to ensure that new employees comply with the company's code of conduct, confidentiality regulations, business ethics, and information security policies. The level of detail of the background check depends on the requirements of the position and may involve criminal, professional history, and information security aspects. When

employees join, they sign security confidentiality agreements concurrently with their labor contracts.

2.4 Company-Wide Security Training

Every employee who joins TOKENCOD must first attend basic security training, including network information security, employee confidentiality responsibilities, office and Internet security, social engineering defense, security systems, and regulations. The security team also organizes targeted professional security training, including code security, process security, and security vulnerability analysis.

3. Foundational Security

3.1 Physical Security

1) Secure Physical Location

The data center facilities of TOKENCOD are located in accordance with relevant international standards and national and local security requirements. Both self-built and leased data centers are subject to strict requirements and control.

2) Infrastructure Security

TOKENCOD data center facilities use dual power supply, are equipped with diesel generators, and major equipment is connected to UPS power. Both the power system and the air-conditioning system adopt high-availability redundant configurations. All areas of the data center are connected to automatic fire detection devices and equipped with complete fire extinguishing equipment.

3) Data Center Security Management

TOKENCOD data center facilities are staffed by dedicated personnel 24/7. Visits require approval, registration, and accompaniment by dedicated personnel. Data center on-duty personnel conduct daily inspections to check the environmental status of the data center and the operating status of the equipment. Equipment vendors are arranged to conduct regular equipment inspections, maintenance, and upgrades. Data center staff must undergo thorough training and be familiar with the operation of data center equipment, data center monitoring status, data center management, and emergency response procedures. Emergency plans are formulated for fire protection, disaster recovery, and important systems, and data center personnel are arranged to conduct regular drills to become proficient in emergency response procedures.

3.2 Network Security

1) Network Security Isolation

As one of the earliest cloud computing vendors in China to use SDN (Software Defined Network) technology, TOKENCOD has made tenant isolation the first principle of cloud network design since its inception. TOKENCOD uses SDN technology to build an Overlay network to solve the problem of isolation between multiple tenants. Each user is assigned an independent network ID. Only data packets belonging to the same user and carrying the same network ID are allowed to access each other. Packets from different users are forcibly terminated at the SDN forwarder, thereby ensuring that user data cannot be sniffed by other users.

2) VPC Private Network

All availability-zone networks of TOKENCOD are designed according to the VPC (Virtual Private Cloud) architecture. Users can quickly build custom subnets, and each subnet is completely isolated from the others (based on Layer 2 of the network). The new-generation VPC 2.0 launched by TOKENCOD features the industry's most flexible custom network segment approach, and also provides the industry's first subnet cross-availability-zone capability. When hosts migrate between availability zones, the intranet address can remain unchanged, achieving stronger disaster recovery capability.

3) DDoS Protection

In recent years, the number and scale of DDoS (Distributed Denial of Service) attacks have shown a trend of rapid growth, and the scope of impact has expanded to multiple industries. Cloud platforms host the business of many customers and have also become a hard-hit area for DDoS attacks.

TOKENCOD has a professional DDoS network security protection team, and the cloud platform is connected to professional DDoS protection equipment, which can effectively defend against many common types of attacks such as SYN FLOOD, UDP FLOOD, and CC, ensuring the normal operation of cloud platform business.

To ensure that customer business is not affected by DDoS attacks, the DDoS network security protection team has translated 10 years of protection experience into the Anti-DDoS service UADS, providing customers with a professional advanced protection system with an attack protection capability of up to 600 Gbps domestically and 2 Tbps overseas. For details, see Section 6.3 Anti-DDoS Service.

4. Data Security

4.1 Secure Data Transmission to the Cloud

When public cloud users choose TOKENCOD and migrate and deploy their own business to the TOKENCOD public cloud, TOKENCOD provides users with corresponding tools and technical means, maintaining maximum compatibility with users' existing data formats, and supports encrypted data transmission (such as HTTPS, SSH, etc.).

Relying on the high-quality network links provided by partner operators, TOKENCOD provides users with dedicated line access services, connecting users' local business to TOKENCOD data centers via dedicated lines, featuring exclusive lines, security and privacy, low latency, and stable quality, to build a hybrid architecture that meets complex business scenarios such as legacy business transformation, remote disaster recovery, and multi-region business expansion.

4.2 Data Security Protection in the Cloud

Public cloud users share TOKENCOD's underlying hardware. Through secure architecture design, TOKENCOD ensures strict logical isolation between user data and business, ensures that user data in the same resource pool is invisible to each other, and cloud hosts are isolated by account. Through network isolation technology, hosts and data of different users are invisible to each other and cannot be accessed via the intranet.

TOKENCOD uses distributed storage. Files are divided into many data fragments that are stored separately on different devices, and each data fragment is stored in multiple copies. Data availability reaches 99.9999%. TOKENCOD cloud hosts can connect to the Data Ark, exclusively supporting continuous data protection, and supporting data recovery at any second within 12 hours, at any hour mark within 24 hours, and at any zero-hour mark within 3 days, protecting data to the greatest extent.

4.3 Secure Data Erasure When Leaving the Cloud

Before a customer requests data deletion or before equipment is discarded or resold, TOKENCOD will thoroughly delete all user data through advanced zeroing operations so that it cannot be recovered, and will degauss scrapped hard disks.

Scenarios for the thorough deletion of customer data do not include TOKENCOD retaining data for 7 days for users who fail to renew in time, to prevent important data from being deleted because users cannot renew in time for some reason.

4.4 Data Ownership and User Privacy Protection

As an independent cloud computing vendor, TOKENCOD promises that customers have absolute ownership of their data, and guarantees the privacy, integrity, and persistence of data.

TOKENCOD strictly complies with national laws and regulations and service agreements. Without the user's permission, it will not provide user data to third parties, will not store user data in overseas data centers or use it for overseas business or data analysis, and will not externally present private data such as user personal information.

5. Security Operations

5.1 Process Security

[Figure 5-1: Secure Development Process - see original document]

To ensure the security of users' use of the cloud platform and cloud products, TOKENCOD strictly controls the entire development lifecycle and embeds network information security into it. TOKENCOD's secure development lifecycle mainly includes the following processes:

1) Requirements analysis: conduct risk analysis of requirements and add security review of requirements.

2) Architecture design: conduct multi-level reviews of the system architecture based on security modeling methods.

3) Development and implementation: provide professional training on secure development, code security, etc. to R&D personnel, standardize R&D personnel's compliance with secure coding standards, and provide and use secure APIs.

4) Testing and acceptance: the quality department strictly controls quality, conducting functional testing, baseline testing, security vulnerability scanning, and penetration testing to promptly discover and fix security vulnerabilities.

5) Release and launch: use grayscale release, and conduct regular security vulnerability scanning after launch.

6) Security operations: apply monitoring and early warning systems, establish sound emergency response procedures, and complete the handling and tracking of problems.

5.2 Vulnerability Management

[Figure 5-2: Vulnerability Management Process - see original document]

TOKENCOD's Security Center has a dedicated team for vulnerability management and discovery. The main responsibility of the vulnerability management team is to discover, track, investigate, and fix security vulnerabilities. Through digital "vulnerability scoring" operations, each real vulnerability is classified, prioritized by severity, and tracked for remediation. TOKENCOD's Security Center maintains contact with members of various security research communities and accepts external vulnerability reports.

5.3 Cloud Platform Anti-Intrusion

Drawing on years of anti-intrusion experience, TOKENCOD's security team has brought together several anti-intrusion security defense experts to build a multi-layered, three-dimensional intrusion defense and detection system around security systems such as IDS (Intrusion Detection System), IPS (Intrusion Prevention System), HIDS (Host-based Intrusion Detection System), and vulnerability scanners, ensuring that platform security is not affected by intrusions.

Strict network isolation is implemented among all users on the TOKENCOD platform. After a user is compromised, the intrusion cannot penetrate and spread to other users through the cloud platform network.

5.4 Incident Management and Emergency Response

Customers who encounter any problems while using products can provide feedback to technical support. The TOKENCOD team provides 7x24-hour technical support with 90-second rapid response. TOKENCOD has established a sound security management system, classifies and grades security incidents, and responds to and handles them according to procedures. Incidents involving products are all defined as operational quality incidents, and clear incident handling mechanisms and reward and punishment systems are established to ensure rapid response, quick location, and professional resolution, protecting customer rights and interests.

TOKENCOD monitors industry security intelligence at all times. Upon discovering security incidents that may affect merchants or the platform (such as the discovery of high-risk vulnerabilities in the industry), it will immediately initiate emergency procedures to ensure the security of customers and the platform. TOKENCOD's service availability has been publicly disclosed on the Trusted Cloud website, and its level has always been in the first tier of the industry. TOKENCOD signed China's first batch of Trusted Cloud insurance, supporting compensation of up to 100 times.

6. Customer Cloud Security Solutions

6.1 Division of Security Responsibilities on the Cloud

When customer business goes to the cloud, while TOKENCOD provides customers with all-around security guarantees, it also reminds customers to pay attention to their own security

responsibilities.

[Figure 6-1: Division of Security Responsibilities on the Cloud - see original document]

When customers rent cloud services, TOKENCOD provides customers with a secure cloud platform and security product solutions, but the first responsible party for the security of customer business is still the customer themselves, for example, ensuring the availability of their own business, eliminating weak passwords, dividing internal account permissions, purchasing appropriate security products and protection, and cooperating with relevant national policies and regulations to ensure the security and compliance of their own business (for example, classified protection, etc.).

6.2 Security Product Solutions

Summarizing years of experience in the security industry and gathering a team of security experts, TOKENCOD has developed a set of cloud security products to provide customers with defense-in-depth security protection. The products cover network security, host security, application security, data security, operations security, security management, and security services, providing more than 10 security products and services to meet customers' various security needs.

[Figure 6-2: Full Map of TOKENCOD Cloud Security Products - see original document]

6.3 Solution Advantages

1) Flexible and tailorable solutions. Enterprises and organizations can choose security products that suit them according to their own security protection needs and cost budgets.

2) Support for private cloud and hybrid cloud architectures. All security products can be deployed separately on customers' managed machines.

3) Continuous optimization and improvement. Compared with traditional security solutions, they can remain advanced and not fall behind the development of the times.

4) Simple and convenient deployment. No impact on existing business, and no code changes required.

6.4 Core Products and Technologies of the Solution

1) Anti-DDoS Service UADS

Anti-DDoS (TOKENCOD Anti DDoS) provides DDoS attack protection for filed (ICP-filed) domain names or origin server IPs (including non-TOKENCOD elastic public IPs). When a user's domain name or origin server IP (including non-TOKENCOD elastic public IPs) is subjected to large-scale DDoS attacks, the Anti-DDoS IP can proxy the origin server IP to face users, hide the origin server IP, and divert attack traffic to the Anti-DDoS IP, ensuring the stable and normal operation of the origin server.

[Figure 6-3: Architecture Diagram of TOKENCOD Anti-DDoS Service - see original document]

2) Host Intrusion Detection UHIDS

Host Intrusion Detection is an Agent deployed on cloud hosts that integrates detection, remediation, and defense, supporting TOKENCOD cloud hosts as well as Alibaba Cloud hosts,

Tencent Cloud hosts, and servers hosted on private clouds. It can promptly discover hackers' intrusion behaviors, including remote logins, successful brute-force logins to servers, installation of backdoor trojans, and high-risk vulnerabilities on servers.

[Figure 6-4: Application Diagram of Host Intrusion Detection - see original document]

3) Web Application Firewall UWAF

Web Application Firewall (TOKENCOD Web Application Firewalls) is a web application firewall provided for enterprises, used to monitor and block common attacks targeting web sites. It supports the discovery of web attack behaviors such as SQL injection and XSS cross-site scripting. It can reduce the risks of downtime, tampering, and data theft for users, and hide the origin server to prevent direct attacks on the origin server.

[Figure 6-5: Comparison Before and After System Access to UWAF - see original document]

[Figure 6-7: Anti-DDoS Combined with UWAF - see original document]

4) Web Vulnerability Detection UWS

Web Vulnerability Scanning (TOKENCOD Web Scan) is a security service used to detect vulnerabilities in Web sites. It can accurately and comprehensively scan vulnerabilities in Web site programs to prevent vulnerabilities from being exploited by hackers and affecting website security. Compared with traditional or open-source vulnerability scanning products, it has advantages such as more comprehensive data crawling, lower false positive rate, timely vulnerability database updates, and no impact on business.

5) SSL Certificate Management USSL

SSL Certificate Management (TOKENCOD SSL) provides customers with a unified SSL certificate management service. Customers can conveniently complete certificate application, purchase, review, issuance, and other certificate processes on the cloud, and can also manage their existing certificates in a unified manner. TOKENCOD SSL Certificate Management supports a keyless security solution, meaning the private key certificate does not need to be uploaded and is verified by accessing the private key server, making it more secure.

6) Database Auditing UAuditDB

Database Auditing reviews audit and transaction logs to track various behaviors of operations on the database. General auditing mainly records operations on the database, changes to the database, the person who executed the operation, and other attributes. These databases are recorded on an independent platform with high accuracy and integrity. When conducting forensic inspection of database activities or states, auditing can accurately reflect various changes in the database and provide evidence for analyzing various normal, abnormal, and non-compliant operations on the database.

7) Bastion Host UHAS

The Bastion Host (TOKENCOD Host Audit System) provides users with a centralized operations and maintenance management solution. Operations personnel can remotely access cloud hosts (UHost) through the bastion host and record all operations on cloud hosts, facilitating scene reproduction and responsibility tracing when problems occur, and improving the level of internal operations risk control for enterprises.

[Figure 6-8: Application Diagram of TOKENCOD Bastion Host - see original document]

8) Situational Awareness USSA

Situational Awareness provides customers with a one-stop security monitoring platform. When users discover security problems, they can first log in to Situational Awareness to view the current overall security status on the cloud, and can conduct trend analysis of security incidents that have occurred in the past. Situational Awareness outputs the overall security status of the network, hosts, and applications, helping customers who lack a security defense system and security management system to establish a complete three-dimensional protection solution of pre-event prediction, in-event protection, and post-event forensic analysis.

9) Classified Protection Assessment Service UDBCP

The Classified Protection Assessment Service (UDBCP) aims to help customers complete the requirements of classified protection and obtain reports. The service includes two parts: consulting services and assessment services. The services that enterprises can obtain include:

(1) Classified Protection Consulting Service

Provide professional advice for enterprises' classified protection work, assist enterprises in system grading and filing, use technical means and interview investigation methods to discover the gap between the enterprise's current security status and national classified protection requirements, and then complete the design of classified protection construction rectification plans and assist in the preparation of security management system documents in accordance with relevant national classified protection standards.

(2) Classified Protection Assessment Service

State-certified assessors conduct network security classified protection assessment of the enterprise's system to be assessed according to the relevant assessment standards and specifications for national network security classified protection, and issue a classified protection assessment report stamped by an institution with national classified protection qualification.

10) SOS Emergency Response

TOKENCOD has established an SOS Emergency Response team composed of multiple security experts with rich security attack and defense experience, providing 7x24-hour security emergency response. It monitors industry security intelligence at all times, and upon discovering security incidents that may affect merchants or the platform (such as the emergence of high-risk vulnerabilities), it will immediately initiate emergency procedures to ensure the security of merchants or the platform.

7. Security Compliance and Auditing

While customers enjoy the convenience and improved efficiency of using cloud services, they also face challenges of data security and business compliance. TOKENCOD anticipates customers' needs and defends cloud platform security. Through industry-authoritative compliance certifications, TOKENCOD creates a secure space for customers, allowing them to deploy business on the secure and trustworthy TOKENCOD platform with peace of mind. TOKENCOD will, in accordance with national laws and regulations, user needs, and the development of the cloud computing industry, continue to pay attention to and complete more certifications,

demonstrating its strength to users.

7.1 Laws and Regulations

TOKENCOD strictly complies with national laws, regulations, and policy requirements, and follows the standards and specifications in the cloud computing industry and network information security. In particular, on June 1, 2017, when the country fully implemented the Cybersecurity Law, TOKENCOD placed even greater emphasis on user privacy protection, network information security, and intellectual property protection, executing in accordance with legal provisions and the requirements of public security authorities to ensure that the cloud platform and cloud products provided comply with national laws and regulations.

7.2 Cloud Computing Business Licenses

TOKENCOD and its partners, on the basis of possessing telecom business IDC licenses and ISP licenses, took the lead in obtaining the telecom business cloud computing license issued by the Ministry of Industry and Information Technology (MIIT), possessing formal cloud computing service business licenses. Customers can use TOKENCOD cloud services approved by the state with confidence.

7.3 Cloud Compliance Certification System

[Figure 7-1: Cloud Compliance Certifications of the TOKENCOD Supplier System - see original document]

July 2014: First batch to pass Trusted Cloud service certification, obtaining cloud host, cloud database, cloud cache, and cloud distribution service certifications.

August 2014: The cloud service platform passed the Level 3 Classified Protection assessment by the Ministry of Public Security with a high score.

August 2015: First batch to pass the big data product capability certification led by the Data Center Alliance.

July 2016: Obtained the latest version of ISO/IEC 27001:2013 Information Security Management System certification.

August 2016: Passed the CSA STAR international cloud security certification jointly launched by CSA and BSI.

September 2016: As one of the first domestic pilot units, took the lead in passing Trusted Cloud security certification, later renamed Trusted Cloud data security certification.

September 2016: Passed ISO/IEC 20000:2011 Information Technology Service Management System certification.

December 2016: Passed the first batch of ITSS cloud computing service capability assessment by MIIT, and obtained the highest level (Enhanced Level) certification.

April 2017: Obtained the highest level of "Five-Star+ and Five-Star" cloud host grading issued by Trusted Cloud.

December 2017: Passed ISO/IEC 9001:2015 Quality Management System certification.

7.4 Platform Compliance Certification Services

When customers need various compliance certifications (for example, customers need to complete classified protection assessment themselves), TOKENCOD can provide customers with certificates, reports, and other publicly available evidence obtained by the cloud platform, and give customers services and assistance as much as possible, helping customers complete certification more smoothly.