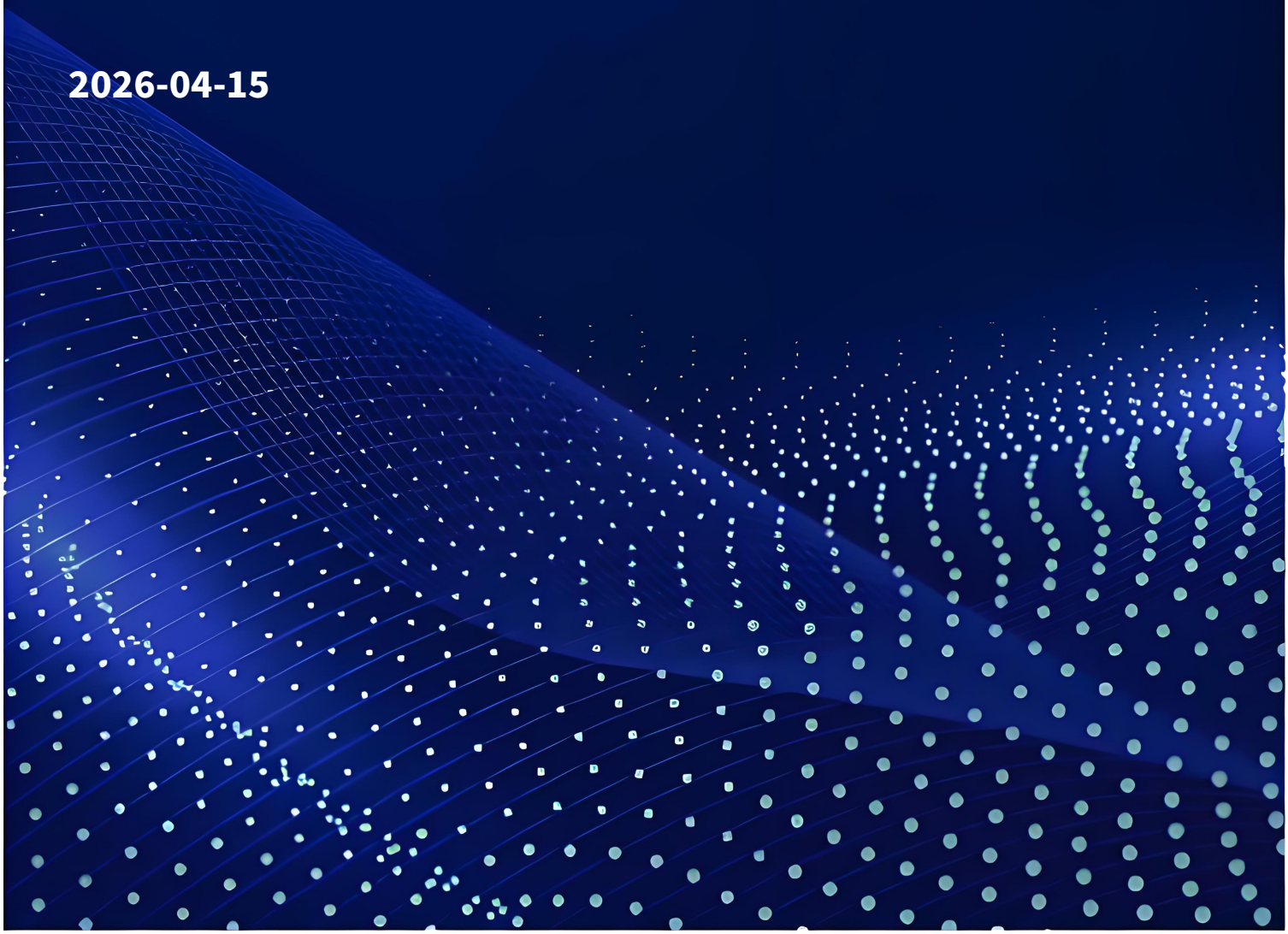
AuroraPrime

HIPAA Compliance White Paper

Accelerate drug development using AI

2026-04-15



Contents

OVERVIEW **4**
HIPAA Compliance Overview . . . 5

SECURITY GOVERNANCE **6**
HIPAA Administrative Safeguards . . . 6
Security Management Process . . . 6
Assigned Security Responsibility . . . 6
Workforce Security . . . 6
Information Access Management . . . 7
Security Awareness and Training . . . 7
Security Incident Procedures . . . 7
Contingency Plan . . . 8
Evaluation . . . 8
Third-Party Audits and Certifications . . . 8
Business Associates Contracts and Other Arrangements . . . 8
HIPAA Physical Safeguards . . . 9
Facility Access Controls . . . 9
Workstation Use & Workstation Security . . . 9
Device and Media Controls . . . 9
HIPAA Technical Safeguards . . . 10
Access Control . . . 10
Audit Controls and Integrity . . . 10
Person or Entity Authentication . . . 10
Transmission . . . 11
HIPAA Organizational Requirements . . . 11
Policies & Procedures and Documentation . . . 11

SECURITY SOLUTIONS **12**
Cloud Infrastructure . . . 12
Web Application Firewall(WAF) . . . 12
Server Load Balancer - SLB . . . 12
SSL Certificates . . . 12
Container-based Architecture . . . 13
Core Services . . . 13
Auth Hub - Authentication & Authorization . . . 13
Audit Trail - Audit Controls . . . 13

Monitor & Log Services 14
Performance & Business Monitor Service 14
Log Service 14

Appendix A –HIPAA SAFEGUARD AND SOLUTION MAPPING **15**

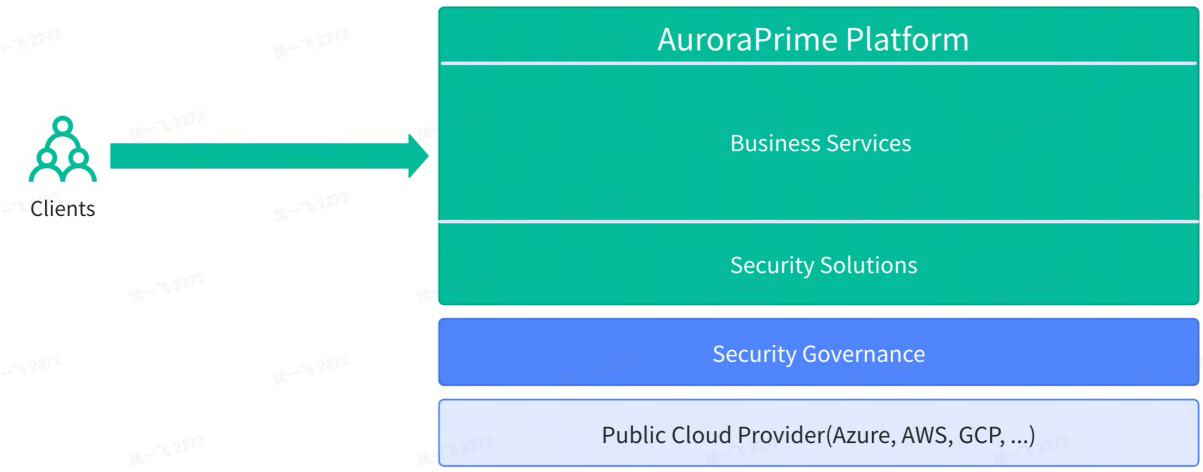
OVERVIEW

AuroraPrime, as a business platform of ALPHALIFE SCIENCES SGP PTE. LIMITED (hereafter abbreviated as AlphaLife), is a generative AI-powered platform designed specifically for content authoring and documentation in the life sciences. The platform automates the end-to-end creation of complex documents such as Clinical Study Reports (CSRs), protocols, and safety narratives. Built on a modular AI and LLM framework, AuroraPrime integrates flexibly with existing enterprise systems to streamline the product development lifecycle. The platform architecture follows a comprehensive software as a service (SaaS) model, combining self-developed services, open source middleware, and infrastructure from public cloud providers.

This paper describes AlphaLife's HIPAA Compliance approach, with respect to the Security Rule, for implementing safeguards to protect confidentiality, integrity, and availability of electronic Protected Health Information (ePHI). Protection of ePHI and compliance with the security rule is AlphaLife's responsibility. This paper allows our customers to understand how the products and services offered by AlphaLife address HIPAA security rules.

Achieving and maintaining HIPAA compliance includes administrative, physical, and technical safeguards. The elements for consideration of an integrated security approach include:

- AlphaLife Security Governance: General information technology controls performed by AlphaLife as part of normal business operations.
- AlphaLife Security Solutions: Products and services that implement specific security measures to address HIPAA security rule requirements.



This paper is structured to provide detailed information regarding the security provisions of each of the following:

- AlphaLife Security Governance

- AlphaLife Security Solutions

HIPAA Compliance Overview

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information. To fulfill this requirement, HHS published what are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule. The Privacy Rule, or Standards for Privacy of Individually Identifiable Health Information, establishes national standards for the protection of certain health information. The Privacy Rule calls this information "protected health information" (PHI). The Security Rule for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities" must put in place to secure individuals' "electronic protected health information" (ePHI). Within HHS, the Office for Civil Rights (OCR) has responsibility for enforcing the Privacy and Security Rules with voluntary compliance activities and civil money penalties.

HHS published a final Privacy Rule in December 2000, which was later modified in August 2002. This Rule sets national standards for the protection of individually identifiable health information by three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically. Compliance with the Privacy Rule was required as of April 14, 2003 (April 14, 2004, for small health plans).

HHS published a final Security Rule in February 2003. This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. Compliance with the Security Rule was required as of April 20, 2005 (April 20, 2006 for small health plans).

The Enforcement Rule provides standards for the enforcement of all the Administrative Simplification Rules.

HHS enacted a final Omnibus rule that implements a number of provisions of the HITECH Act to strengthen the privacy and security protections for health information established under HIPAA, finalizing the Breach Notification Rule.

SECURITY GOVERNANCE

HIPAA Administrative Safeguards

An important step in securing electronic Protected Health Information (ePHI) is to implement reasonable and appropriate administrative safeguards that establish the foundation for a covered entity's security program, as addressed by §164.308 of the HIPAA Security Rule. In compliance with HIPAA administrative safeguards, AlphaLife has implemented administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures. These measures protect ePHI and govern workforce conduct in relation to information protection.

Security Management Process

AlphaLife has a defined security management process to regulate overall strategies for information security and management procedures for the suite of products. This includes defining the responsibilities of members and business units within AlphaLife's information security structure. AlphaLife has established policies and procedures for governance and risk management, information security management, IT operations, and risk identification and assessment. To effectively govern the people elements of the business, AlphaLife provides learning and awareness training for all employees on company culture, vision, security, and privacy. Professional training on data protection is offered by internal and external experts and is available to all employees.

Assigned Security Responsibility

The AlphaLife Information Security Strategy directs the strategies for information security and management procedures for the information security program. Based on this strategy, AlphaLife has established guidelines to define the responsibilities and roles of members within the organization's information security structure. These responsibilities include monitoring information security incidents, coordinating security awareness training exercises, and providing resources to support internal audits and risk assessments.

Workforce Security

AlphaLife has policies and procedures in place addressing workforce access to ePHI with regard to the clearance of employees, appropriate employee authorizations, and termination processes. Background checks on prospective employees, depending on role and position, are documented

in the human resources management system. Employees are required to sign a confidentiality agreement and acknowledge the employee code of conduct. Vendors are required to sign a contract and confidentiality agreement as well as a business associate agreement, if deemed to be a covered entity.

Information Access Management

AlphaLife has policies and procedures in place surrounding logical access management. These include basic rules for segregation of duties per user role or responsibility, and appropriate controls over the enterprise user access management system. All access requests (provisioning and modification) for normal and privileged accounts are logged within the access management system. Access is only authorized after proper review and approval by management, based on risk level and minimum access necessary. Separated employees are removed via an automated process triggered when individuals are disabled within the human resources management system. This ensures that only authorized users have access to ePHI and related systems as well as configuration settings.

Security Awareness and Training

AlphaLife has established a security team responsible for developing the Security Awareness Training (SAT) program. This program promotes information security awareness among employees and ensures that policies regarding business conduct are known throughout the organization. All relevant policies and procedures are available on internal platforms and are easily accessible to employees.

To mitigate the possibility that malicious software compromises information systems housing ePHI, AlphaLife only authorizes specific channels to download software onto PCs and pushes antivirus software to physical servers and workstations as a means of protection from malware attacks and other potential cybersecurity threats.

Security Incident Procedures

AlphaLife has a robust security incident response plan in place to identify, address, and remediate information security incidents. Security incidents include attempted or successful unauthorized access, use, disclosure, modification, or destruction of information, or interference with system operations in an information system with access to covered information. In the event of an incident, AlphaLife uses multiple communication channels including text messages, emails, and online bulletin board posts to relay appropriate information to responsible parties. The procedures address

classification of security incidents, establish definitions for timely response, and detail corresponding solutions according to incident level.

Contingency Plan

To ensure AlphaLife is prepared for any event that could result in data being compromised, a variety of plans have been developed to demonstrate readiness. AlphaLife performs business continuity drills at least once per year, with business continuity reports issued accordingly. Additionally, AlphaLife has established targeted emergency response plans for identified technical failures of products and services. These plans are designed to reduce the impact on end users in the event of an emergency or incident.

Evaluation

AlphaLife has several policies and procedures in place to govern change management processes and ensure that all environmental and operational changes that would affect the security of ePHI are reviewed by information security management and other executive management on a periodic and ad-hoc basis.

Third-Party Audits and Certifications

AlphaLife maintains ISO 27001 certification and undergoes annual SOC 2 Type II audits conducted by Sensiba, demonstrating our commitment to industry-standard security practices and independent validation of our security controls. These third-party assessments provide additional assurance to our customers that AlphaLife's security measures meet rigorous external standards and are regularly evaluated by qualified independent auditors. The audit reports are available to customers upon request under appropriate confidentiality agreements.

Business Associates Contracts and Other Arrangements

AlphaLife requires vendors to sign contracts and confidentiality agreements; rights and obligations, scope of services, compliance requirements, and service levels are detailed within vendor service contracts. The customer and vendor contracting process is centralized and all customers and vendors are assessed to determine whether they are covered entities and therefore whether they require a business associate agreement.

HIPAA Physical Safeguards

An important step in protecting electronic Protected Health Information (ePHI) is to implement reasonable and appropriate physical safeguards for information systems and related equipment and facilities, as addressed by §164.310 of the HIPAA Security Rule. In compliance with HIPAA physical safeguards, AlphaLife has implemented physical measures, policies, and procedures to protect electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Facility Access Controls

AlphaLife has policies and procedures in place that specify the processes for accessing archive storage rooms. Employees who need to access archives must sign an archive access acknowledgement form and obtain permission from the executive management team. Additionally, AlphaLife has established a dedicated IT room managed by authorized IT personnel. Any personnel other than designated IT staff must receive approval from executive team members before entering the IT room.

Workstation Use & Workstation Security

AlphaLife has policies and procedures in place that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of enterprise workstations that can access ePHI or sensitive customer data. Employees are required to sign acknowledgement of AlphaLife acceptable server use and the enterprise code-of-conduct. Servers that have access to, transmit, store, or otherwise process ePHI are physically protected from unauthorized use, including, in particular, those housed in public cloud providers.

Device and Media Controls

AlphaLife has policies and procedures in place surrounding the management of devices and media that access, store, or transmit ePHI. This includes policies indicating that storage media that is discarded must be physically destroyed on the premises, thereby mitigating risk of that media being accessed by unauthorized individuals or entities. Hardware destruction and disposal of media containing sensitive information is recorded and maintained. IT asset identification and classification are included as part of the annual information security risk assessment process and is kept up-to-date on an ongoing basis.

HIPAA Technical Safeguards

An important step in protecting electronic Protected Health Information (ePHI) is to implement reasonable and appropriate technical safeguards for information systems that represent best business practices for technology use and configuration as well as associated technical policies and procedures. In compliance with HIPAA technical safeguards, AlphaLife has implemented several security measures and technical solutions that allow it to reasonably and appropriately implement the standards and implementation specifications.

Access Control

AlphaLife has policies and procedures in place governing logical access controls. These include basic rules for segregation of duties by varying roles and functions based on company structure and product teams, as well as processes for the centralized access management system. All access requests for normal and administrator accounts require authorization and management review to determine feasibility based on associated risk levels. Additionally, AlphaLife has established General Access Control strategies that require production and non-production environments to be segregated into different network security domains.

Audit Controls and Integrity

AlphaLife has a log management platform in place to monitor and record user operations at the network level and for the AlphaLife product suite. Log retention is configured within the system. Additionally, AlphaLife performs integrity checks to compare presently stored data to previous states. This ensures that unauthorized changes have not occurred and that data has not been altered or manipulated in a malicious way.

Person or Entity Authentication

AlphaLife has policies and procedures in place to ensure that user and entity accounts go through proper authentication measures. Customer access to AlphaLife product suites requires authentication using a provisioned global unique ID (“UID”) to validate legitimacy. When authentication fails, users are redirected to the login console and denied access to the product. Additionally, AuroraPrime supports two-factor authentication based on password and one-time password (OTP) for user authentication.

Transmission

AuroraPrime has established transmission security management policies and procedures that specify security requirements and measures to ensure data is transmitted securely. The data encryption services used by AuroraPrime (provided by public cloud providers) meet the requirements of the State Cryptography Administration and are certified accordingly. AuroraPrime supports secure communication channels with cryptographic protocols such as HTTPS. For applicable products, data at rest encryption is also implemented, leveraging solutions provided by public cloud providers.

HIPAA Organizational Requirements

An important step in protecting electronic Protected Health Information (ePHI) is to implement reasonable and appropriate organizational safeguards for important information security governance and HIPAA-mapped policies and procedures.

Policies & Procedures and Documentation

In compliance with ISMS/ISO 27001 requirements, AlphaLife has policies and procedures in place that ensure the development and documentation of formal policies and procedures, along with their periodic review and maintenance. AlphaLife's policies detail retention periods for documentation that comply with HIPAA requirements (6-year minimum). Policies and procedures are reviewed and updated annually as required by ISO 27001 and HIPAA. All documented policies and procedures are made available to individuals responsible for implementation via AlphaLife's internal platforms.

SECURITY SOLUTIONS

AuroraPrime is hardened with a wealth of technical security measures addressing HIPAA technical safeguard requirements. AuroraPrime achieves this through:

- Building high availability applications
- Providing account authentication and authorization services with two-level account credentialing for segregation of duties, multi-factor authentication, group authorization policies, fine-grained access control, and tokening
- Providing security audit support and data encryption

The following solutions are part of the security architecture offered within AuroraPrime solutions and include an overview of the product, a description of the key security features available, and a reference to the related HIPAA security rule specification.

Cloud Infrastructure

Web Application Firewall(WAF)

Web Application Firewall (WAF) is a SaaS-based web application security service that detects illegal web requests through its built-in security strategy and protects website servers against intrusions. AuroraPrime leverages WAF provided by cloud providers to detect and block malicious traffic directed to our websites and applications. WAF secures core business data and prevents server malfunctions caused by malicious activities and attacks.

Server Load Balancer - SLB

SLB is a server load balancing service that is used to distribute incoming traffic among several cloud servers. SLB extends the external service capability of application systems by traffic distribution. It improves the availability of application systems by eliminating a single point of failure.

SSL Certificates

Leveraging SSL Certificates Service from public cloud providers, AuroraPrime is hardened as HTTPS-secured websites to encrypt communications between users and the websites, ensuring that traffic is adequately protected from hijacking, snooping, and tampering [§164.312(e)(2)(ii) Transmission Security – Encryption].

Container-based Architecture

AuroraPrime is based on microservice architecture with applications running within containers. The platform is built on enterprise-grade infrastructure provided by public cloud providers. Leveraging Virtual Private Cloud (VPC), AuroraPrime's production environment is isolated from other environments. AlphaLife has policies and procedures in place governing employee access to the production environment.

AuroraPrime products run on managed Kubernetes clusters (e.g., AWS EKS, Azure AKS, or Google GKE), which provide scalability and ensure high availability of the platform.

Core Services

Auth Hub - Authentication & Authorization

Auth Hub is the core service of the AuroraPrime platform, responsible for authentication and authorization management. The service provides the following security functions:

- Implements SAML 2, OAuth 2, OpenID Connect and other protocols as SP, which can be easily integrated with internal and external identity authentication systems.
- Implements basic user group management functions and allows group-based permissions control, such as who can access which applications.
- Implements basic organizational concepts and allows users to join multiple organizations. Organization administrators can manage users' organizational relationships. In other words, it allows autonomy within the organization and reduces the need for super administrators to intervene.

Audit Trail - Audit Controls

Audit Trail is the core service of the AuroraPrime platform, responsible for recording user operations. The Audit Trail service records user operations in the following format to maintain data integrity:

- User
- Timestamp
- Operation object
- Operation type
- Operation content

- Labels
- Source

Monitor & Log Services

Performance & Business Monitor Service

Monitor service collects monitoring metrics of AuroraPrime resources (CPU, MEM, DISK) as well as product-defined metrics. Monitor service enables AuroraPrime OPS team to view and fully understand the usage of AuroraPrime resources, and the status and health of platform business, so that AuroraPrime OPS team can act promptly to ensure the availability of your application when an alarm is triggered.

Alarms are configured to trigger based on preset rules set by the OPS team based on usage, performance, and operational state [§164.312(b) Audit Controls] [§164.308(a)(1)(ii)(D) Information System Activity Review].

Log Service

AuroraPrime has set up a self-hosted log service that provides complete real-time data logging. The Log Service supports collection, consumption, shipping, search, and analysis of logs, improving the capacity for processing and analyzing large amounts of log data.

The prominent security features of this service include high reliability and tampering prevention for stored log data. On an append-only basis, users can add to logs but cannot modify or alter previous logs, maintaining log integrity [§164.312(c)(1) Integrity]. Additionally, the log service complies with HIPAA security rules including [§164.308(a)(7)(ii)(A) Contingency Plan – Data Backup Plan] and [§164.312(a)(1) Access Control].

Appendix A –HIPAA SAFEGUARD AND SOLUTION MAPPING

		HIPAA Security Rule Safeguards Addressed									
		§164.308(a)(1)(ii)(D) Information System Activity Review	§164.308(a)(5)(ii)(B) Protection from Malicious Software	§164.308(a)(5)(ii)(c) Log-in monitoring	§164.308(a)(5)(ii)(D) Password Management	§164.308(a)(7)(ii)(A) Data Backup Plan	§164.312(a)(1) Access Control	§164.312(a)(2)(iv)Encryption and Decryption	§164.312(b) Audit Controls	§164.312(e)(2)(i) Transmission Security -- Integrity Controls	§164.312(e)(2)(ii) Transmission Security -- Encryption
Security Solutions	WAF		☑				☑				
	SLB						☑				
	Container-based Architecture	☑					☑			☑	☑
	SSL							☑		☑	☑
	Auth Service		☑		☑						☑
	Audit Service	☑									
	Monitor Service	☑	☑			☑			☑	☑	
	Log Service	☑		☑		☑			☑	☑	