Development Platform

Security Whitepaper

Milesight Technology Co., Ltd.

Contents

Introduction

About Milesight Development Platform

The Milesight Development Platform (hereafter referred to as "the Platform") is a powerful middleware platform to connect and manage Milesight devices, simplify custom integration and accelerate application development.

As an ethical industry player aiming to leverage technological advancements for social good, Milesight places paramount importance on information security, legal compliance, and data privacy. Our commitment ensures that developers can confidently leverage the Platform.

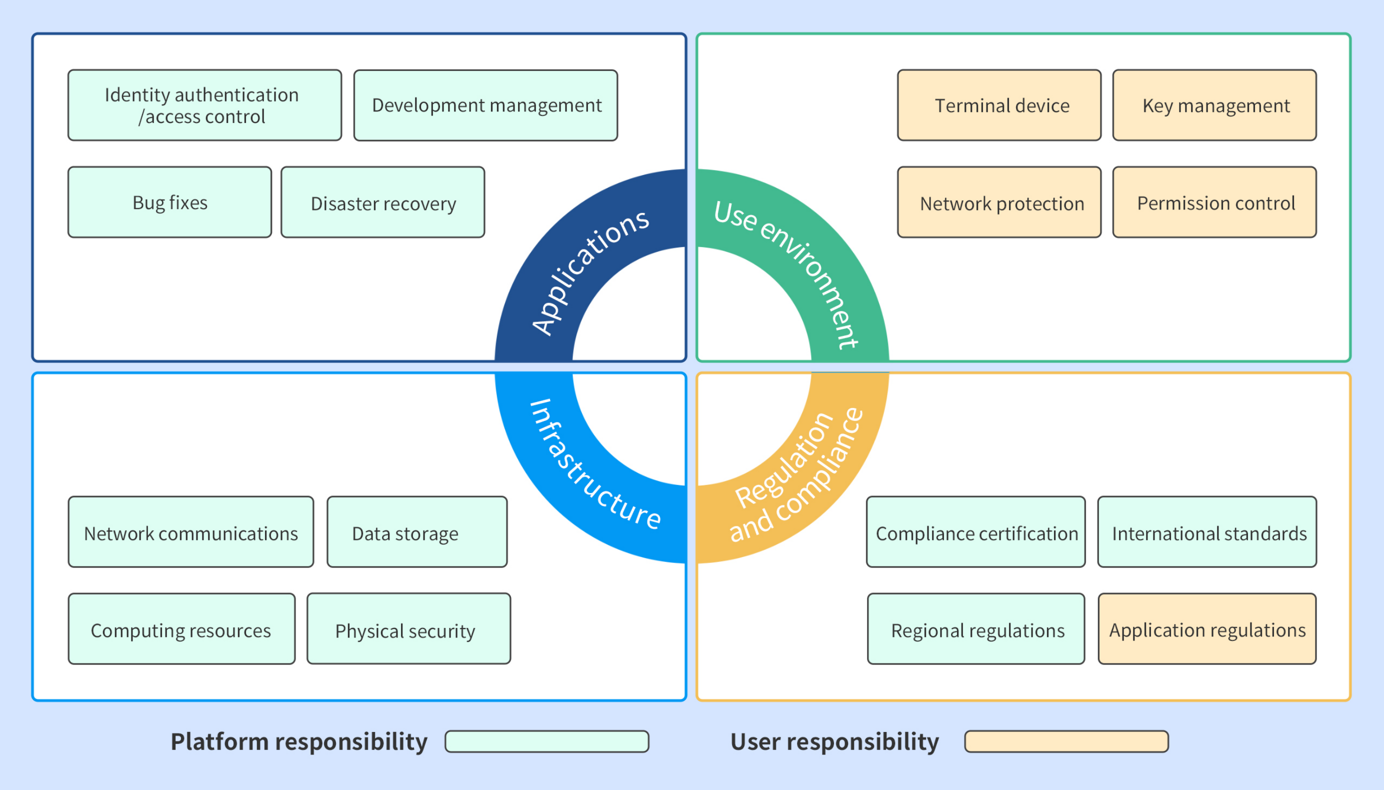
Platform Security Strategy Overview

The Platform's information security strategy encompasses a multi-layered defense, procedural, and punitive approach. Besides general corporate-level security investment, there are policies and resources specifically dedicated to the Platform. Additionally, fostering a culture of security awareness through continuous training and education empowers employees to recognize and respond to cyber threats effectively.

This document is written to systematically introduce the attributes of the Platform and its approach towards security, compliance, privacy, and data processing.

1.0 Shared Security Responsibility

When implemented in collective efforts, security practices will have the maximal impact. This is why besides ensuring the company's internal information security rigorosity, we also actively engage with our platform users and stakeholders to foster information security awareness. To facilitate developers' understanding of security responsibilities within different use scenarios, we've developed the following responsibility sharing model:



At Milesight, we are committed to ensuring the stability and security of our infrastructure and services. Meanwhile, customers should also take necessary measures to maximize information security.

We strongly recommend that customers do the following:

- Set strong passwords and implement permission control.
- Enable the application IP whitelist function.
- Enable TLS 1.3 for all HTTP and MQTT communications and verify server certificates.
- Manage account credentials and application keys carefully to prevent leaks. If a key is compromised, regenerate it immediately.
- Enhance Webhook security by enabling HTTPS, regularly updating certificates, verifying request signatures, and taking other reasonable measures to protect your servers and stored data.
- Strengthen local device network protection by enabling firewalls and replacing weak SSH passwords for LoRa gateways.

2.0 Security Compliance and Privacy Protection

2.1 Security Compliance and Standards Adherence

Milesight has established and implemented a robust information security system and obtained relevant certifications, including:

ISO 9001

ISO 27001

The two certifications are summarized as follow:

Certification	What the Certification Means
ISO/27001 Information Security Management System	Milesight has put in place a system to manage risks related to the security of data it owns or handles, and this system respects all the best practices and principles enshrined in this International Standard.
ISO 9001 Quality Management System	Milesight has put in place effective processes and trained staff to deliver flawless products or services time after time.

2.2 Privacy Protection

Privacy protection is one of the top priorities of the Platform. We adhere to privacy by design (PbD) principles. From product inception to deployment, we integrate privacy considerations, minimizing risks and enhancing user trust.

The Platform adheres to international privacy regulations, including the EU's General Data Protection Regulation (GDPR). For details of Milesight Development Privacy Policy, please visit https://www.milesight.com/legal/development-platform/privacy-policy

3.0 Security Culture

3.1 Cyber Security Group

Milesight has a dedicated Cyber Security Group under the Department of Information. The group oversees cyber security issues and privacy protection policies within the company, including the Platform, promptly addressing any security concerns, and more importantly, taking actions in precautions to prevent possible security breaches.

3.2 Milesight Development Platform Security Team

Besides the corporate-level Cyber Security Group, we also established a dedicated Cyber Security Team specifically for the Platform, comprised of personnel spanning across product, research and development, maintenance, and testing. The team is responsible for the security of the Platform's design, service development, operational services, and vulnerability remediation.

3.3 Security in Human Resources Management

Employees play a pivotal role in shaping our products, culture, and overall success. As an integral part of our security efforts, we've incorporated security and ethics into every stage of the employee lifecycle—from recruitment to resignation.

Recruitment

- Candidates undergo rigorous vetting by a professional background check organization before joining Milesight.
- Our checks cover education, employment history, external references, and criminal records, adhering to local labor laws and regulations.

Onboarding

- New employees receive comprehensive onboarding that emphasizes Milesight's Employee Code of Conduct and information security requirements.
- All employees need to sign confidentiality agreements upon job entry. Those handling critical data or consumer information sign the highest level of confidentiality agreement and/or non-competition agreement as needed and undergo a series of dedicated trainings to fully understanding their security responsibilities.

On-the-Job Practices

- Ongoing online security and privacy awareness training is mandatory for all employees.
- Trainings cover topics including security principles, best practices and standards such as GDPR.
- Exams are held regularly to test and refresh employees' command of related knowledge.

Resignation

- The resignation process involves work handover and access permissions cleanup.
- Upon resignation, employees must hand over their physical and logical access rights as per our established process.
- Milesight audits compliance with the confidentiality period specified in the signed agreement.

3.4 Security Education

For Technical Staff

Regular technical training sessions are conducted by the network security and R&D teams. Technical personnel are required to be periodically trained and tested on the following topics:

Information Security

1.General information security
2.Cryptography
3.Network security protocols
4.Host security
5.Service security

Network Security

1.Computer network security
2.Wlan security
3.Spoofing attack principle and application
4.Denial of service attack principle and application
5.Firewall principle and application
6.VPN overview and application
7.Security audit overview and application
8.WAF principle and application
9.Intrusion detection system overview and application

Web Common Vulnerability

1.Web fundamentals
2.Malicious code
3.Web common vulnerabilities
4.Web vulnerability analysis
5.Web vulnerability exploitation technology
6.Network security hardening

Emergency Response Processes

1.Emergency response
2.Emergency drill

General Employee Training

We regularly organize general security knowledge-sharing sessions company-wide. These sessions encourage employees to adhere to common cyber security best practices and the latest threat awareness, fostering a culture of vigilance and responsible cybersecurity practices. Topics covered include:

- Phishing awareness
- Ransomware preparedness
- Password hygiene
- Safe Internet practices
- Mobile security

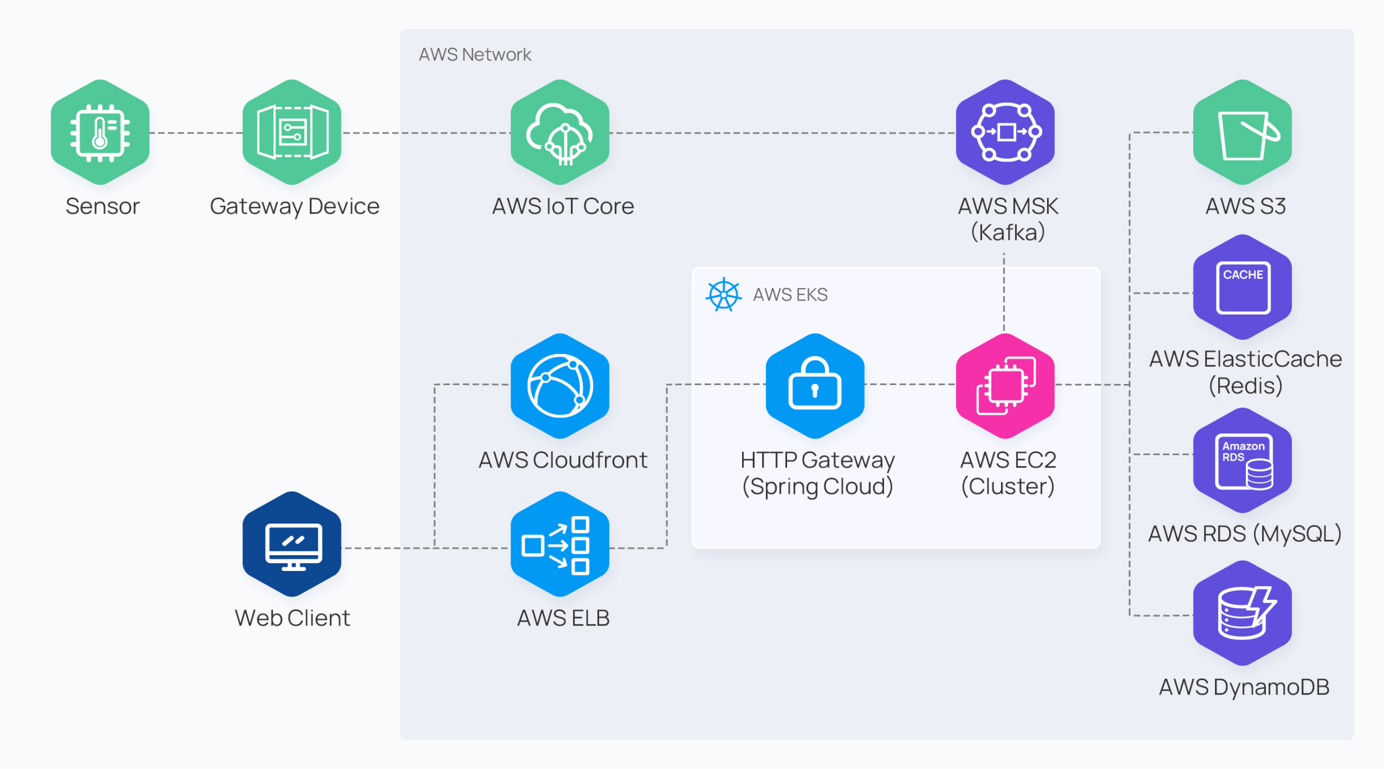
3.5 Security Violation Accountability

Milesight enforces accountability measures for security violations. Every Milesight employee is held accountable for their actions and outcomes at work, not only concerning technologies and services but also in terms of legal responsibility. If there is a violation, its nature and severity are assessed based on the consequences, regardless of the violator's intent, and disciplinary actions will be taken accordingly. If legal violations are involved, cases are handed over to law enforcement. If there is a security breach, both direct and indirect management are also held responsible for any negligence or complicity.

4.0 Services and Network Security

4.1 Cloud Services Security

The infrastructure of our platform is provided by the AWS cloud platform, utilizing a global multi-region service node architecture to leverage the reliable and secure services offered by AWS. The services the Platform uses include EKS, RDS, Amazon Managed Streaming for Apache Kafka, ElastiCache, DynamoDB, IoT Core, S3, CloudFront, EC2, VPC, NAT Gateway, and NLB. All servers operate within the AWS internal network which contains reliable fundamental network isolation and security measures.



AWS Network: Provides fundamental network isolation and security.
AWS EKS: Used for running and managing containerized applications.
AWS ELB: Distributes traffic to ensure high availability and load balancing.
AWS CloudFront: Accelerates content delivery.
AWS IoT Core: Connects and manages Internet of Things (IoT) devices.
AWS MSK: Handles and streams large-scale data.
AWS EC2: Offers compute resources to support various applications and services.
AWS S3: Used for storing and managing massive amounts of data.
AWS ElastiCache: Enhances caching performance.
AWS RDS: Manages relational databases.
AWS DynamoDB: Provides high-performance NoSQL database services.

Through the collaborative efforts of these components, the architecture achieves a high-performance, scalable, and secure cloud environment that meets the needs of various application scenarios.

4.2 Network Isolation

In our network architecture, we implement network isolation using security components. By utilizing Virtual Private Cloud (VPC), we ensure secure network segmentation. The Elastic Load Balancer (AWS ELB) serves as the traffic entry point, guaranteeing high availability and load balancing. The NAT Gateway (SNAT) acts as the outbound access point, allowing EC2 instances to securely access the internet without needing a public IP, thereby achieving isolation from the public network. This setup ensures network security and efficient resource utilization.

4.3 Network Protection

We continuously monitor network traffic for signs of malicious activity or policy violations. System administrators and cyber security will be promptly alerted to suspicious events and swiftly intervene to prevent potential breaches.

4.4 Application Isolation

We use containerization to achieve application isolation. Containerization is a software deployment process that bundles an application’s code with all the files and libraries it needs to run on any infrastructure. It provides process-level isolation, separating applications and their dependencies. This reduces the impact of one application on another, enhancing the overall security and stability of the system.

5.0 Platform Security

5.1 Intrusion Detection

To safeguard our APIs, Milesight employs Web Application Firewall (WAF) solutions. These WAFs act as a critical security layer, filtering and monitoring HTTP requests to detect and block malicious traffic. This proactive approach ensures that our APIs remain secure and reliable, providing robust protection against potential vulnerabilities and unauthorized access.

5.2 Encrypted Transmission

Our server's RESTful API enforces HTTPS protocol, supporting TLS 1.3 encryption. We use ECDSA signatures on digital certificates to prevent content interception or tampering, ensuring secure network communication.

5.3 Identity Authentication

Most RESTful APIs utilize JWT (JSON Web Tokens) as authentication credentials. We support token revocation through password modification or application key updates, preventing identity forgery and credential leaks.

5.4 API Rate Limiting

Requests are rate-limited based on IP, device, and account characteristics. This effectively blocks malicious requests, ensuring quality service for legitimate users.

5.5 Protection Against SQL Injection and Remote Code Execution

All inbound data undergoes validation checks on the server side. Both front-end and back-end components escape and filter potentially executable data, defending against common attack vectors.

5.6 HTTP Security Headers

We employ common HTTP security response headers such as X-Frame-Options, X-Xss-Protection, CORS, CSP, HSTS to ensure browser access security.

6.0 Data Security

6.1 Data Collection

Minimal Data Collection Principle

We adhere to the principle of minimal data collection, only gathering necessary information for conducting business. Additionally, we collect data fields that are authorized and agreed upon by the customer. User data, including login credentials and payment information, is solely managed by Platform users themselves and is not stored on the Platform.

User Consent of Data Collection

Before collecting and using the information, we will inform you clearly and seek your explicit consent. At the same time, we will ensure the legitimacy of the information sources before collection, and understand the scope of authorization and consent obtained by the personal information provider, including the purpose of use, authorized transfer, sharing, and public disclosure. If our processing activities of personal information exceed the scope of authorization and consent, we will obtain your explicit consent within a reasonable period after obtaining the personal information or prior to processing it.

6.2 Data Masking

To safeguard data privacy, we exhibit only desensitized corporate and personal information within the Platform. This approach extends internally across the entire platform, including log printing, monitoring alarms and more.

6.3 Data Encryption

We use TLS to encrypt data for secure transmission.

6.4 Data Storage Security

In our system, data storage is encrypted using AWS services, with key management handled by AWS Key Management Service (KMS). This ensures that sensitive information remains secure at rest. For confidential data, such as passwords, we employ salted hash encryption. By using strong hash algorithms (e.g., SHA-256) and random salts during key transmissions, and Bcrypt during key storage, we protect against rainbow table attacks and enhance security. Storing only the hashed values of passwords, rather than the plaintext, further mitigates risks.

6.5 Data Isolation and Storage

In the Platform, we strictly segregate data across different environments: development, testing, staging, and production. Formal data is never used in any other environment. Additionally, we operate four global data centers, with all data stored locally. To enhance isolation, data is bound to user IDs, ensuring separation between accounts.

6.6 Data Deletion and Destruction

Our platform provides users with the ability to delete connected devices. When a device is deleted, its associated data is thoroughly cleaned. Similarly, users can delete applications, rendering requests using the associated ClientID ineffective for authentication. Additionally, account holders have the option to log out, which results in the removal of all personal information.

7.0 Development and Secure Operations

7.1 Personnel and Operational Security

All Platform operations personnel must undergo IAM authentication before performing any tasks. Daily operational activities are logged and retained on AWS for auditing purposes and can be assessed by relevant auditing personnel. Network firewalls are tightly controlled, with only project leads and department heads having permission to modify critical services accessible within the company intranet.

7.2 Secure Software Development

Program Design

All Platform operations personnel must undergo IAM authentication before performing any tasks. Daily operational activities are logged and retained on AWS for auditing purposes and can be assessed by relevant auditing personnel. Network firewalls are tightly controlled, with only project leads and department heads having permission to modify critical services accessible within the company intranet.

Program Development

Our CI/CD pipeline incorporates tools like SonarQube for code scanning. At various stages (code writing, merging, and deployment), we analyze code for security issues such as SQL injection, cross-site scripting (XSS), buffer overflows, and overall code quality. During the development phase, all code submissions undergo SonarQube checks, unit testing, and review by at least one security lead before being approved for merging into the code repository. Subsequently, the quality assurance team conducts three or more rounds of testing to ensure compliance with release standards.

Change Initiation and Review

After development, project managers initiate change requests. The change team promptly reviews each request, assessing implementation personnel, specifics, steps, impact, risk assessment, and rollback plans.

7.3 Cloud Service Availability Monitoring

Our platform maintains efficient 24/7 monitoring mechanisms for service availability and system operation. Unified monitoring tools track key metrics across infrastructure, applications, middleware, databases, and network devices. Automated alerts trigger notifications to relevant operations teams based on predefined thresholds, allowing early containment of anomalies and ensuring service recovery. This approach ensures high availability, performance, and robust security, meeting diverse application requirements.
Specific monitoring metrics include:

- **Service Availability:** Monitoring cloud services' online status and response times to ensure timely availability. Unhealthy instances are automatically removed from load balancers.
- **Performance Metrics:** Monitoring CPU usage, memory utilization, disk I/O, and network bandwidth to maintain resource efficiency and stability.
- **Error Rates:** Detecting system errors and failure rates promptly for timely resolution and reduced service downtime.
- **User Experience:** Evaluating response times and success rates for user interactions to optimize service quality.

Additionally, centralized dashboards provide quantified insights into core service metrics, enabling informed decisions regarding resource scaling.

7.4 Log Management

Effective log management is integral to system security and compliance. Our strategies and measures include:

Log Collection and Storage

We centrally collect and store real-time logs from system components, applications, networks, and audits. Log types include system logs, application logs, network logs, and audit logs, ensuring comprehensive coverage. Logs are stored securely in redundant storage systems, ensuring persistence and availability.

Log Protection

Access control: Strict IAM policies govern access to log data, allowing only authorized users and services.
Retention policies: We define log retention based on compliance requirements and business needs, ensuring availability within specified timeframes and secure deletion after expiration.

Log Monitoring and Analysis

Our services support log analysis, generating valuable security insights and operational reports. Automated alerts are configured to notify relevant personnel immediately upon detecting suspicious activities or anomalies.

Log Auditing and Compliance

We maintain audit logs for all API calls and user activities, ensuring traceability and transparency.

Best Practices for Log Management

We adhere to best practices for log management, including:

- Standardized log formats and structures facilitate collection, storage, and analysis.
- Regular log data backups ensure rapid recovery in case of data loss or corruption.
- Employee training enhances awareness and responsiveness to log management and security incidents.

7.5 High Availability of Data Services

In our high availability (HA) architecture for business services within the EKS (Amazon Elastic Kubernetes Service) environment, we prioritize robustness and resilience. Here are the key components of our HA approach:

1.API Traffic Ingress with NLB (Network Load Balancer): To ensure high availability, we use an NLB as the entry point for API traffic into the EKS cluster. This architecture allows business services to consume traffic reliably.

2.Deployment Strategy: Business services are deployed using multiple replicas and anti-affinity rules for pods. By distributing replicas across different nodes, we minimize the risk of service disruption due to node failures.

3.Multi-AZ Node Groups: Our EKS node groups are distributed across multiple availability zones (AZs) within the same data center. Each AZ has an elastic scaling service to maintain multiple servers running simultaneously. In case of a node failure, automatic isolation occurs to prevent service degradation.

4.Autoscaling for Node Availability: We utilize Autoscaling to dynamically adjust the number of nodes based on demand. This ensures that sufficient capacity is available to handle workload spikes while maintaining high availability.

7.6 Disaster Recovery and Redundancy

We perform daily backups, retaining data for seven days. This practice ensures data availability and resilience against loss or corruption. We have defined RTO (Recovery Time Objective), RPO (Recovery Point Objective), and SLA (Service Level Agreement) and set disaster recovery strategy accordingly.

At the system access layer, we ensure high availability by leveraging public gateway services provided by our foundational service provider. For the backend, we adopt a multi-instance approach to guarantee service reliability. Additionally, we closely monitor both traffic and failures. In cases of sudden traffic spikes or failures, we implement a graceful degradation mode to safeguard business availability. Our Platform defines specific metrics for maximum tolerable downtime, recovery time objectives, and minimum service levels. We tailor response strategies based on different business interruption scenarios.

7.7 Vulnerability Management

1.Our operations team actively monitors publicly disclosed vulnerabilities.

2.The development team performs daily checks on the vulnerability database, assessing newly discovered vulnerabilities in software dependencies. Based on threat severity, they prioritize updates, ensuring timely fixes.

3.After addressing vulnerabilities, we roll out upgrades gradually during service deployment to minimize downtime and service interruptions.

4.Rigorous regression testing follows each update to ensure that new versions do not introduce additional issues or regressions.

7.8 Security Feedback

We welcome any security-related vulnerability reports or suggestions via email at iot.support@milesight.com.

Summary

In today’s intricate technological landscape, where new threats arise constantly, selecting a platform that guarantees security and privacy for your organization and users is crucial. Milesight remains vigilant and committed to maintaining reliable Platform services while safeguarding information integrity and privacy of all end users. We will continue to improve the Platform's security features and drive innovation, collaboration, and value for our stakeholders.

Make Sensing Matter

Milesight

☎ +86-592-5085280

🌐 www.milesight.com

✉ iot.support@milesight.com

📍 Building C09, Software Park Phase III, Xiamen 361024, Fujian, China