Micromeet

SECURITY STANDARDS AND ARCHITECTURE

Micromeet AI-CRMS & AgentBrowser Security White Paper

Cloud Service and Client Security Architecture

STATUS
v1.0

LAST UPDATED
2026-06-05

OWNER
Micromeet

SECURITY STANDARDS AND ARCHITECTURE

Security Architecture Control Layers

Cloud capabilities, bounded client execution, and audit evidence are organized into one control framework so customers can understand the boundaries around data, credentials, and AI actions.

This document is for healthcare institutions, partners, and security review teams. It explains how Micromeet protects customer data, account credentials, AI workflows, and audit evidence across both cloud services and the Agent client that runs on customer computers.

Micromeet AI-CRMS and AgentBrowser are designed around security from the outset. They combine controlled cloud services with a bounded customer-side Agent client, creating a complete control framework across scalable cloud infrastructure, encrypted storage, automated backups, cloud monitoring, compliance capabilities, client isolation, credential protection, human confirmation, and audit traceability.

1. Security Architecture Overview

Micromeet AI-CRMS and AgentBrowser use a "controlled cloud service + bounded client Agent" architecture. The cloud side handles identity, policy, model orchestration, configuration release, logging, and operational services. The Agent client runs on customer computers and constrains AI behavior through local isolation, credential protection, network allowlists, human confirmation, and audit records.

The core security goals are:

- **Controlled data processing**: Task data enters Micromeet cloud services and authorized subprocessors according to authorized workflows. Vendor selection considers healthcare security posture and HIPAA-related compliance materials where relevant, and subprocessors are governed by purpose, region, access, and audit controls.
- **Verifiable boundaries**: Client capabilities come from centrally released, reviewed, and signed skill packs. Unauthorized capabilities cannot self-expand at runtime.
- **Human control**: Write, submit, delete, and other irreversible actions require user confirmation before execution.
- **Traceable evidence**: Key steps, operators, timestamps, inputs, outputs, confirmations, and version changes are auditable.
- **Cloud resilience**: Cloud services provide scalability, performance, encrypted storage, high availability, monitoring, and backups.

2. Cloud Service Security

Micromeet cloud services use managed cloud infrastructure to host business services, object storage, CDN, model orchestration, and operational monitoring. Cloud security controls cover growth and scale, reliability, secure storage, high availability, automated backups, cloud monitoring, physical security, and compliance offerings. Growth and Scale, Reliability and Performance, Secure Cloud Storage, High Availability, Automated Data Backups, Cloud Monitoring, and Compliance Offerings are included in Micromeet's cloud security capabilities. Physical Security is supported by the underlying cloud provider's data center security and compliance materials.

Growth and Scale

The cloud platform scales with customer growth and supports high-concurrency tasks, large audio/text workloads, and multi-institution usage. Capacity strategy covers compute, storage, network, and model invocation peaks.

Reliability and Performance

Managed services, health checks, capacity monitoring, and automated deployment help maintain responsiveness and service stability. Critical services are paired with alert thresholds, rollback procedures, and operational monitoring.

Secure Cloud Storage

Customer data is encrypted when stored in the cloud and protected in transit with TLS. Object storage, databases, and log stores are accessed by least privilege, and environment isolation reduces lateral access risk.

High Availability

Production services use multi-instance, multi-availability-zone, or cross-region replication strategies to reduce single points of failure. Core data has backup and recovery paths, with recovery targets available in customer review materials.

Automated Data Backups

Production data enters an encrypted backup environment and is backed up automatically, with support for recovery validation. Backup frequency, retention period, and RPO/RTO can be disclosed in customer review materials.

Cloud Monitoring

Cloud monitoring, security alerts, application logs, and access logs track system health, abnormal access, resource capacity, and failed tasks. Cloud monitoring is part of the operational and security response process.

Physical Security

The underlying data centers are protected by the cloud provider's physical access controls, video monitoring, environmental protections, and personnel controls, supported by the cloud provider's compliance materials.

Compliance Offerings

Compliance capabilities meet requirements, including ISO/IEC 27001, ISO/IEC 20000-1 and related certificate materials, plus HIPAA / PDP / PDPA alignment statements. Specific certificate scope and wording follow attachments.

2.1 Data Encryption and Storage Isolation

Cloud data is protected in transit with TLS and protected at rest through cloud platform encryption for databases, object storage, and backup environments. Access control follows least privilege: service accounts receive only the permissions required to complete their tasks, and production data access is constrained by roles, audit trails, and approval.

Key controls include:

- Databases, object storage, logs, and backup environments are protected by cloud platform encryption capabilities.
- Data transmission uses TLS to reduce man-in-the-middle and transport eavesdropping risks.
- Customer data is isolated by tenant, environment, and permission boundary; production data access enters audit records.
- Service accounts, operations accounts, and automated tasks are configured with least privilege.

2.2 Availability, Backups, and Recovery

Cloud services reduce interruption risk through multi-instance deployment, health checks, automatic recovery, automated backups, and recovery mechanisms. For healthcare workflows, Micromeet supports service restoration and business continuity through alerting, recovery procedures, data replay, and human review.

Customer security review materials may further provide:

- Production database backup frequency, object storage versioning, or backup strategy.
- RPO/RTO indicators and the recovery targets applicable by deployment mode or customer tier.

2.3 Cloud Monitoring and Incident Response

Micromeet continuously monitors application availability, error rates, resource capacity, authentication anomalies, key API calls, model invocation failures, and security alerts. Cloud logs are used for troubleshooting, audit support, and incident response triggers. Production data access logs include the user, timestamp, accessed object, action, and reason.

Cloud monitoring covers:

- Application health, error rate, latency, capacity, and failed tasks.
- Authentication anomalies, abnormal access, key API calls, and security alerts.
- Data access logs, operation logs, and audit summaries.
- Records of subprocessor, cloud resource, and runtime configuration changes.

3. Client Security

The AgentBrowser client runs on customer computers. Its security model does not depend on AI "never making a mistake." Instead, even if the agent encounters incorrect input, malicious webpages, or prompt injection, it cannot cross its boundaries to perform unauthorized actions. Client–side controls include signed skill packs, domain allowlists, process isolation, local encryption, OS credential stores, human confirmation, and complete audit trails. In customer–authorized tasks, AgentBrowser opens customer operational–system websites (business system pages) inside its built–in browser environment, and reads and parses the current page's visible data, view state, and interaction results to assist with reading, organizing, prefilling, and submitting. Related page data is used only within authorized workflows and agreed processing purposes, and is protected by domain allowlists, isolated browser contexts, local encryption, access controls, and audit records. AgentBrowser's execution boundary is limited to its built–in client browser environment: it can operate only on authorized webpages or business system pages opened inside AgentBrowser. It cannot control other local applications on the customer's computer, read other application windows, or inject commands into other applications. AgentBrowser also isolates and constrains internally opened webpages, reducing the risk that external local applications, unauthorized pages, or malicious scripts can manipulate business pages.

Bounded Agent Governance

Agent capabilities come from centrally authored, reviewed, and signed skill packs. Signatures are verified before loading, and the agent cannot self–evolve, invent new capabilities, or expand permissions at runtime.

Allowlisted Network Access

The client can open and access only explicitly approved webpage domains, APIs, and model endpoints. Navigation, requests, and potential data exfiltration to destinations outside the allowlist are blocked.

Sandboxed Isolation

AgentBrowser runs as a sandboxed desktop application. The agent can perceive page data, view state, and interaction results only within authorized webpages opened inside AgentBrowser. It cannot control other local applications, read across application windows, or inject commands into other applications. Internal webpages are isolated from other applications on the customer computer, and external local applications cannot use AgentBrowser to extract or manipulate business page data.

Encrypted Local Storage

Local data is stored in an encrypted database whose key is protected by the operating system credential store. Copying the database file does not make its contents directly readable.

Credential Protection

Customer system account credentials remain on the client in OS Keychain / DPAPI / Secret Service. They are not uploaded to Micromeet backend systems or model providers.

Human Approval for Writes

Write, submit, delete, and other irreversible actions require user confirmation before execution. AI proposes structured actions but cannot bypass the confirmation process.

Replayable Audit Trail

Agent steps, key inputs and outputs, confirmation actions, operators, timestamps, and version changes are recorded for troubleshooting, review, and compliance audit.

Prompt Injection Containment

Security does not rely on the model never being tricked. Even if malicious content influences the model, skill boundaries, domain allowlists, and human confirmation still constrain behavior.

3.1 Customer Credentials and Controlled Task Data Processing

AgentBrowser separates customer system login credentials from medical task data. Customer system credentials stored locally on the client are protected by operating-system secure storage. Business task data enters Micromeet cloud services and authorized subprocessors according to authorized workflows, for model invocation, record generation, logging, and operational support. Vendor review considers healthcare security posture and HIPAA-related compliance materials where relevant.

Related controls include:

- Locally stored client credentials are protected by operating-system secure storage.
- The application uses customer credentials only within user-authorized workflows to access customer-approved systems.
- Medical task data enters Micromeet cloud services and approved subprocessors according to authorized workflows and documented vendor review.
- Subprocessors are governed by purpose, region, access permissions, security obligations, and audit controls.
- Device retirement, offboarding account recovery, and credential clearing can be executed through the customer's existing IT process.
- Customers can choose interactive login or local credential persistence according to their security policy.

3.2 Write Actions Require Human Confirmation

AgentBrowser can assist with reading, organizing, filling, and submitting, but final write actions are triggered by user confirmation. For healthcare workflows, AI output is clinician-in-the-loop assistance: a physician or authorized user reviews before release, and the system retains raw AI output, edits, reviewer identity, release timestamp, and version history.

Actions are divided into three categories:

- **Read / analyze**: Allowed within the defined task scope and recorded with source and result.
- **Draft / prefill**: May be generated by AI but is presented as pending user confirmation.
- **Write / submit / delete**: Must be explicitly confirmed by the user and must generate an audit record.

3.3 Client Baseline and Customer Responsibility

Client security is jointly maintained by the customer and Micromeet. Micromeet is responsible for application isolation, signed updates, network allowlists, local encryption, and audit. Customers are responsible for device ownership, operating system patches, disk encryption, anti-malware protection, account lifecycle, and physical access control.

Responsibility Area	Micromeet	Customer
AgentBrowser application signing and updates	Responsible	Install approved version
Client operating environment OS patches and disk encryption	Provide security guidance	Responsible
Customer business system accounts	Does not host credentials	Create, authorize, revoke
Local audit records	Generate and protect	Retain or export per policy
Lost device / offboarding handling	Support clearing and revocation	Execute process

4. Data Privacy, Access Control, and Audit

Micromeet privacy controls are built around authorized processing, transparency, and traceability. AI workflows process customer data according to business task needs, and use Micromeet cloud services and authorized subprocessors for model calls, storage, logs, and operational support. Vendor review considers healthcare security posture and HIPAA-related compliance materials where relevant. AgentBrowser's reading of page data and view state from customer operational-system websites is limited to authorized task purposes such as reading, organizing, prefilling, submitting, and audit. Related data is protected through browser context isolation, access control, approved subprocessors, and audit records. Model calls and third-party subprocessors record purpose, region, data category, and security obligations. Employee or operations access to production data is constrained by least privilege, approval, audit, and training processes.

User Authentication

Supports customer identity systems, SSO, or minimized user authentication workflows. Administrators and high-risk actions use stronger authentication policies.

Least Privileged Access

Employees, service accounts, operations tooling, and customer accounts are configured with least privilege. Normal duties do not require direct access to customer data.

Immutable / Durable Logs

Production data access, client key actions, AI drafts, and human confirmations enter traceable logs. Retention periods can be described in customer contracts or security review materials.

Vendor Management

Subprocessors have defined purpose, region, data category, security obligations, contract/DPA status where applicable, change notification, and vendor-review evidence. Current vendor review includes HIPAA-related compliance materials published by Alibaba Cloud and OpenAI; Micromeet does not claim a vendor BAA unless separately executed.

5. Security Engineering and Lifecycle

Security does not begin after release. Micromeet implements code review, automated testing, dependency and vulnerability scanning, infrastructure as code, configuration review, security training, and change management throughout the software development lifecycle.

SDLC controls include:

- Code changes are reviewed and pass automated tests or release gates.
- Infrastructure configuration is managed in a reviewable and rollback-capable declarative form.

- Dependencies, images, cloud configuration, and public endpoints are scanned regularly and remediated by severity.
- High-risk systems undergo regular third-party security assessments or penetration testing, with latest status provided through the trust center or on customer request.
- Engineers receive secure development training covering authentication, authorization, input validation, data leakage, supply chain, and OWASP Top 10 risks.

6. Security Control Summary

Control Domain	Micromeet Security Capabilities
Cloud services	Scalability, performance, high availability, automated backups, cloud monitoring, encrypted storage, physical security, and compliance capabilities
Client	Signed skill packs, domain allowlists, sandbox isolation, local encryption, OS credential store, and human confirmation
Data privacy	Authorized data processing, approved subprocessors with vendor-review evidence, least privilege, and customer data access audit
Audit and traceability	Records of key operations, AI drafts, human confirmations, operators, timestamps, and version history
Security engineering	Code review, automated testing, vulnerability scanning, infrastructure as code, security training, and change management