Micromeet

SECURITY STANDARDS AND ARCHITECTURE

Buku Putih Keamanan Micromeet AI-CRMS & AgentBrowser

Arsitektur Keamanan Layanan Cloud dan Klien

VERSI
v1.0

DIPERBARUI
2026-06-05

PEMILIK
Micromeet

SECURITY STANDARDS AND ARCHITECTURE

Lapisan kontrol arsitektur keamanan

Kemampuan cloud, eksekusi klien yang dibatasi, dan bukti audit disusun dalam satu kerangka kontrol agar batas data, kredensial, dan tindakan AI terlihat jelas.

Dokumen ini ditujukan untuk institusi layanan kesehatan, mitra, dan tim peninjau keamanan. Dokumen ini menjelaskan bagaimana Micromeet melindungi data pelanggan, kredensial akun, alur kerja AI, dan bukti audit di sisi layanan cloud maupun klien Agent yang berjalan di komputer pelanggan.

Micromeet AI-CRMS dan AgentBrowser dirancang dengan keamanan sebagai dasar. Keduanya menggabungkan layanan cloud yang terkendali dengan klien Agent di sisi pelanggan yang dibatasi, sehingga membentuk kerangka kontrol lengkap yang mencakup infrastruktur cloud yang dapat diskalakan, penyimpanan terenkripsi, pencadangan otomatis, pemantauan cloud, kemampuan kepatuhan, isolasi klien, perlindungan kredensial, konfirmasi manusia, dan jejak audit.

1. Gambaran Umum Arsitektur Keamanan

Micromeet AI–CRMS dan AgentBrowser menggunakan arsitektur "layanan cloud terkendali + Agent klien yang dibatasi". Sisi cloud menangani identitas, kebijakan, orkestrasi model, rilis konfigurasi, log, dan layanan operasional. Klien Agent berjalan di komputer pelanggan dan membatasi perilaku AI melalui isolasi lokal, perlindungan kredensial, allowlist jaringan, konfirmasi manusia, dan catatan audit.

Tujuan keamanan utama adalah:

- **Pemrosesan data terkendali**: Data tugas masuk ke layanan cloud Micromeet dan subprosesor resmi sesuai alur kerja yang diotorisasi. Subprosesor yang terlibat dalam pemrosesan data kesehatan memenuhi persyaratan kepatuhan HIPAA dan dikendalikan berdasarkan tujuan, wilayah, akses, dan audit.
- **Batas yang dapat diverifikasi**: Kemampuan klien berasal dari skill pack yang dirilis, ditinjau, dan ditandatangani secara terpusat. Kemampuan yang tidak diotorisasi tidak dapat memperluas diri pada saat runtime.
- **Kontrol manusia**: Tindakan tulis, kirim, hapus, dan tindakan lain yang tidak dapat dibatalkan memerlukan konfirmasi pengguna sebelum dieksekusi.
- **Bukti yang dapat ditelusuri**: Langkah penting, operator, waktu, input, output, konfirmasi, dan perubahan versi dapat diaudit.
- **Ketahanan cloud**: Layanan cloud menyediakan skalabilitas, performa, penyimpanan terenkripsi, ketersediaan tinggi, pemantauan, dan pencadangan.

2. Keamanan Layanan Cloud

Layanan cloud Micromeet menggunakan infrastruktur cloud terkelola untuk menjalankan layanan bisnis, penyimpanan objek, CDN, orkestrasi model, dan pemantauan operasional. Kontrol keamanan cloud mencakup growth and scale, reliability, secure storage, high availability, automated backups, cloud monitoring, physical security, dan compliance offerings. Growth and Scale, Reliability and Performance, Secure Cloud Storage, High Availability, Automated Data Backups, Cloud Monitoring, dan Compliance Offerings telah menjadi bagian dari kemampuan keamanan cloud Micromeet. Physical Security didukung oleh keamanan pusat data dan materi kepatuhan dari penyedia cloud dasar.

Growth and Scale

Platform cloud dapat berkembang mengikuti pertumbuhan pelanggan dan mendukung tugas berkonkurensi tinggi, beban kerja audio/teks berskala besar, serta penggunaan oleh banyak institusi. Strategi kapasitas mencakup puncak komputasi, penyimpanan, jaringan, dan pemanggilan model.

Reliability and Performance

Layanan terkelola, health check, pemantauan kapasitas, dan deployment otomatis membantu menjaga respons dan stabilitas layanan. Layanan penting dilengkapi ambang peringatan, prosedur rollback, dan pemantauan operasional.

Secure Cloud Storage

Data pelanggan dienkripsi saat disimpan di cloud dan dilindungi dalam transit menggunakan TLS. Penyimpanan objek, basis data, dan log store diakses dengan prinsip least privilege, sementara isolasi lingkungan mengurangi risiko akses lateral.

High Availability

Layanan produksi menggunakan strategi multi–instance, multi–availability–zone, atau replikasi lintas wilayah untuk mengurangi single point of failure. Data inti memiliki jalur pencadangan dan pemulihan, dengan target pemulihan yang dapat diberikan dalam materi peninjauan pelanggan.

Automated Data Backups

Data produksi masuk ke lingkungan backup terenkripsi dan dicadangkan otomatis, dengan dukungan validasi pemulihan. Frekuensi backup, periode retensi, dan RPO/RTO dapat diungkapkan dalam materi peninjauan pelanggan.

Cloud Monitoring

Pemantauan cloud, peringatan keamanan, log aplikasi, dan log akses melacak kesehatan sistem, akses abnormal, kapasitas sumber daya, dan tugas gagal. Pemantauan cloud menjadi bagian dari proses respons operasional dan keamanan.

Physical Security

Pusat data dasar dilindungi oleh kontrol akses fisik, pemantauan video, perlindungan lingkungan, dan kontrol personel dari penyedia cloud, dengan dukungan materi kepatuhan penyedia cloud.

Compliance Offerings

Kemampuan kepatuhan memenuhi kebutuhan, termasuk materi sertifikat ISO/IEC 27001, ISO/IEC 20000–1, serta pernyataan keselarasan HIPAA / PDP / PDPA. Cakupan sertifikat dan formulasi sertifikasi mengikuti lampiran.

2.1 Enkripsi Data dan Isolasi Penyimpanan

Data cloud dilindungi dalam transit dengan TLS dan dilindungi saat disimpan melalui kemampuan enkripsi platform cloud untuk basis data, penyimpanan objek, dan lingkungan backup. Kontrol akses mengikuti prinsip least privilege: akun layanan hanya mendapat izin yang diperlukan untuk menyelesaikan tugas, dan akses ke data produksi dibatasi oleh peran, jejak audit, dan persetujuan.

Kontrol utama meliputi:

- Basis data, penyimpanan objek, log, dan lingkungan backup dilindungi oleh kemampuan enkripsi platform cloud.
- Transmisi data menggunakan TLS untuk mengurangi risiko man–in–the–middle dan penyadapan transport.
- Data pelanggan diisolasi berdasarkan tenant, lingkungan, dan batas izin; akses data produksi masuk ke catatan audit.
- Akun layanan, akun operasional, dan tugas otomatis dikonfigurasi dengan least privilege.

2.2 Ketersediaan, Backup, dan Pemulihan

Layanan cloud mengurangi risiko gangguan melalui deployment multi-instance, health check, pemulihan otomatis, backup otomatis, dan mekanisme pemulihan. Untuk alur kerja layanan kesehatan, Micromeet mendukung pemulihan layanan dan kontinuitas bisnis melalui peringatan, prosedur pemulihan, replay data, dan tinjauan manusia.

Materi peninjauan keamanan pelanggan dapat menambahkan:

- Frekuensi backup basis data produksi, versioning penyimpanan objek, atau strategi backup.
- Indikator RPO/RTO serta target pemulihan yang berlaku berdasarkan mode deployment atau tingkat pelanggan.

2.3 Pemantauan Cloud dan Respons Insiden

Micromeet memantau ketersediaan aplikasi, tingkat kesalahan, kapasitas sumber daya, anomali autentikasi, panggilan API penting, kegagalan pemanggilan model, dan peringatan keamanan secara berkelanjutan. Log cloud digunakan untuk troubleshooting, dukungan audit, dan pemicu respons insiden. Log akses data produksi mencakup pengguna, waktu, objek yang diakses, tindakan, dan alasan.

Pemantauan cloud mencakup:

- Status aplikasi, tingkat kesalahan, latensi, kapasitas, dan tugas gagal.
- Anomali autentikasi, akses abnormal, panggilan API penting, dan peringatan keamanan.
- Log akses data, log operasi, dan ringkasan audit.
- Catatan perubahan subprosesor, sumber daya cloud, dan konfigurasi runtime.

3. Keamanan Klien

Klien AgentBrowser berjalan di komputer pelanggan. Model keamanannya tidak bergantung pada asumsi bahwa AI "tidak akan pernah salah". Sebaliknya, bahkan jika Agent menemukan input yang salah, halaman web berbahaya, atau prompt injection, Agent tidak dapat melewati batasnya untuk melakukan tindakan yang tidak diotorisasi. Kontrol sisi klien mencakup skill pack bertanda tangan, allowlist domain, isolasi proses, enkripsi lokal, penyimpanan kredensial OS, konfirmasi manusia, dan jejak audit lengkap. Dalam tugas yang diotorisasi pelanggan, AgentBrowser membuka situs sistem operasional pelanggan (halaman sistem bisnis) di lingkungan browser bawaannya, lalu membaca dan mengurai data yang terlihat pada halaman saat ini, status tampilan, dan hasil interaksi untuk membantu membaca, menyusun, mengisi awal, dan mengirimkan. Data halaman terkait hanya digunakan dalam alur kerja yang diotorisasi dan tujuan pemrosesan yang disepakati, serta dilindungi oleh allowlist domain, konteks browser terisolasi, enkripsi lokal, kontrol akses, dan catatan audit. Batas eksekusi AgentBrowser terbatas pada lingkungan browser bawaan di dalam klien: Agent hanya dapat mengoperasikan halaman web atau halaman sistem bisnis yang diotorisasi dan dibuka di dalam AgentBrowser. Agent tidak memiliki kemampuan untuk mengendalikan aplikasi lokal lain di komputer pelanggan, membaca jendela aplikasi lain, atau menyuntikkan perintah ke aplikasi lain. AgentBrowser juga mengisolasi dan membatasi halaman yang dibuka di dalamnya, sehingga mengurangi risiko aplikasi lokal eksternal, halaman yang tidak diotorisasi, atau skrip berbahaya memanipulasi halaman bisnis.

Bounded Agent Governance

Kemampuan Agent berasal dari skill pack yang ditulis, ditinjau, dan ditandatangani secara terpusat. Tanda tangan diverifikasi sebelum dimuat, dan Agent tidak dapat berevolusi sendiri, menciptakan kemampuan baru, atau memperluas izin saat runtime.

Allowlisted Network Access

Klien hanya dapat membuka dan mengakses domain halaman web, API, dan endpoint model yang disetujui secara eksplisit. Navigasi, permintaan, dan potensi eksfiltrasi data ke tujuan di luar allowlist akan diblokir.

Sandboxed Isolation

AgentBrowser berjalan sebagai aplikasi desktop yang disandbox. Agent hanya dapat merasakan data halaman, status tampilan, dan hasil interaksi di dalam halaman web yang diotorisasi dan dibuka di AgentBrowser. Agent tidak dapat mengendalikan aplikasi lokal lain, membaca lintas jendela aplikasi, atau menyuntikkan perintah ke aplikasi lain. Halaman internal diisolasi dari aplikasi lain pada komputer pelanggan, dan aplikasi lokal eksternal tidak dapat menggunakan AgentBrowser untuk mengekstrak atau memanipulasi data halaman bisnis.

Encrypted Local Storage

Data lokal disimpan dalam basis data terenkripsi, dengan kunci yang dilindungi oleh penyimpanan kredensial sistem operasi. Menyalin file basis data tidak membuat isinya dapat dibaca secara langsung.

Credential Protection

Kredensial akun sistem pelanggan tetap berada pada klien di OS Keychain / DPAPI / Secret Service. Kredensial tersebut tidak diunggah ke backend Micromeet atau penyedia model.

Human Approval for Writes

Tindakan tulis, kirim, hapus, dan tindakan lain yang tidak dapat dibatalkan memerlukan konfirmasi pengguna sebelum dieksekusi. AI hanya mengusulkan tindakan terstruktur dan tidak dapat melewati proses konfirmasi.

Replayable Audit Trail

Langkah Agent, input dan output penting, tindakan konfirmasi, operator, timestamp, dan perubahan versi dicatat untuk troubleshooting, peninjauan, dan audit kepatuhan.

Prompt Injection Containment

Keamanan tidak bergantung pada model yang tidak pernah tertipu. Bahkan jika konten berbahaya memengaruhi model, batas skill, allowlist domain, dan konfirmasi manusia tetap membatasi perilakunya.

3.1 Kredensial Pelanggan dan Pemrosesan Data Tugas Terkendali

AgentBrowser memisahkan kredensial login sistem pelanggan dari data tugas medis. Kredensial sistem pelanggan yang disimpan secara lokal pada klien dilindungi oleh penyimpanan aman sistem operasi. Data tugas bisnis masuk ke layanan cloud Micromeet dan subprosesor resmi sesuai alur kerja yang diotorisasi, untuk pemanggilan model, pembuatan catatan, log, dan dukungan operasional. Subprosesor yang terlibat dalam pemrosesan data kesehatan memenuhi persyaratan kepatuhan HIPAA.

Kontrol terkait meliputi:

- Kredensial yang disimpan secara lokal pada klien dilindungi oleh penyimpanan aman sistem operasi.
- Aplikasi hanya menggunakan kredensial pelanggan dalam alur kerja yang diotorisasi pengguna untuk mengakses sistem yang disetujui pelanggan.
- Data tugas medis masuk ke layanan cloud Micromeet dan subprosesor yang patuh HIPAA sesuai alur kerja yang diotorisasi.
- Subprosesor dikendalikan berdasarkan tujuan, wilayah, izin akses, kewajiban keamanan, dan audit.
- Pensiun perangkat, pemulihan akun saat offboarding, dan penghapusan kredensial dapat dijalankan melalui proses IT pelanggan yang sudah ada.
- Pelanggan dapat memilih login interaktif atau penyimpanan kredensial lokal sesuai kebijakan keamanan mereka.

3.2 Tindakan Tulis Memerlukan Konfirmasi Manusia

AgentBrowser dapat membantu membaca, menyusun, mengisi, dan mengirimkan, tetapi tindakan tulis final dipicu oleh konfirmasi pengguna. Untuk alur kerja layanan kesehatan, output AI diperlakukan sebagai bantuan clinician-in-the-loop: dokter atau pengguna yang berwenang meninjau sebelum dirilis, dan sistem menyimpan output AI asli, pengeditan, identitas peninjau, waktu rilis, dan riwayat versi.

Tindakan dibagi menjadi tiga kategori:

- **Baca / analisis**: Diizinkan dalam cakupan tugas yang ditentukan dan dicatat dengan sumber serta hasil.
- **Draf / pengisian awal**: Dapat dibuat oleh AI, tetapi disajikan dalam status menunggu konfirmasi pengguna.
- **Tulis / kirim / hapus**: Harus dikonfirmasi secara eksplisit oleh pengguna dan harus menghasilkan catatan audit.

3.3 Baseline Klien dan Tanggung Jawab Pelanggan

Keamanan klien dijaga bersama oleh pelanggan dan Micromeet. Micromeet bertanggung jawab atas isolasi aplikasi, update bertanda tangan, allowlist jaringan, enkripsi lokal, dan audit. Pelanggan bertanggung jawab atas kepemilikan perangkat, patch sistem operasi, enkripsi disk, perlindungan anti-malware, siklus hidup akun, dan kontrol akses fisik.

Area Tanggung Jawab	Micromeet	Pelanggan
Penandatanganan dan update aplikasi AgentBrowser	Bertanggung jawab	Menginstal versi yang disetujui
Patch OS dan enkripsi disk lingkungan operasi klien	Memberikan panduan keamanan	Bertanggung jawab
Akun sistem bisnis pelanggan	Tidak menyimpan kredensial	Membuat, mengotorisasi, mencabut
Catatan audit lokal	Membuat dan melindungi	Menyimpan atau mengekspor sesuai kebijakan

Area Tanggung Jawab	Micromeet	Pelanggan
Perangkat hilang / offboarding	Mendukung penghapusan dan pencabutan	Menjalankan proses

4. Privasi Data, Kontrol Akses, dan Audit

Kontrol privasi Micromeet dibangun di sekitar pemrosesan yang diotorisasi, transparansi, dan keterlacakan. Alur kerja AI memproses data pelanggan sesuai kebutuhan tugas bisnis, dan menggunakan layanan cloud Micromeet serta subprosesor resmi untuk panggilan model, penyimpanan, log, dan dukungan operasional. Subprosesor yang terlibat dalam pemrosesan data kesehatan memenuhi persyaratan kepatuhan HIPAA. Pembacaan AgentBrowser atas data halaman dan status tampilan dari situs sistem operasional pelanggan dibatasi untuk tujuan tugas yang diotorisasi seperti membaca, menyusun, mengisi awal, mengirimkan, dan audit. Data terkait dilindungi melalui isolasi konteks browser, kontrol akses, subprosesor yang patuh HIPAA, dan catatan audit. Panggilan model dan subprosesor pihak ketiga mencatat tujuan, wilayah, kategori data, dan kewajiban keamanan. Akses karyawan atau operasional ke data produksi dibatasi oleh least privilege, persetujuan, audit, dan pelatihan.

User Authentication

Mendukung sistem identitas pelanggan, SSO, atau alur autentikasi pengguna yang diminimalkan. Administrator dan tindakan berisiko tinggi menggunakan kebijakan autentikasi yang lebih kuat.

Least Privileged Access

Karyawan, akun layanan, tooling operasional, dan akun pelanggan dikonfigurasi dengan least privilege. Tugas normal tidak memerlukan akses langsung ke data pelanggan.

Immutable / Durable Logs

Akses data produksi, tindakan penting klien, draf AI, dan konfirmasi manusia masuk ke log yang dapat ditelusuri. Periode retensi dapat dijelaskan dalam kontrak pelanggan atau materi peninjauan keamanan.

Vendor Management

Subprosesor memiliki tujuan, wilayah, kategori data, kewajiban keamanan, dan pemberitahuan perubahan yang jelas. Subprosesor yang terlibat dalam pemrosesan data kesehatan memenuhi persyaratan kepatuhan HIPAA, dengan daftar publik mengikuti trust center atau lampiran kontrak.

5. Rekayasa Keamanan dan Siklus Hidup

Keamanan tidak hanya dimulai setelah rilis. Micromeet menerapkan peninjauan kode, pengujian otomatis, pemindaian dependensi dan kerentanan, infrastructure as code, peninjauan konfigurasi, pelatihan keamanan, dan manajemen perubahan di sepanjang siklus hidup pengembangan perangkat lunak.

Kontrol SDLC meliputi:

- Perubahan kode ditinjau dan lulus pengujian otomatis atau release gate.
- Konfigurasi infrastruktur dikelola dalam bentuk deklaratif yang dapat ditinjau dan di–rollback.

- Dependensi, image, konfigurasi cloud, dan endpoint publik dipindai secara berkala dan diperbaiki berdasarkan tingkat keparahan.
- Sistem berisiko tinggi menjalani penilaian keamanan pihak ketiga atau penetration testing secara berkala, dengan status terbaru tersedia melalui trust center atau berdasarkan permintaan pelanggan.
- Engineer menerima pelatihan secure development yang mencakup autentikasi, otorisasi, validasi input, kebocoran data, supply chain, dan risiko OWASP Top 10.

6. Ringkasan Kontrol Keamanan

Domain Kontrol	Kemampuan Keamanan Micromeet
Layanan cloud	Skalabilitas, performa, ketersediaan tinggi, backup otomatis, pemantauan cloud, penyimpanan terenkripsi, keamanan fisik, dan kemampuan kepatuhan
Klien	Skill pack bertanda tangan, allowlist domain, isolasi sandbox, enkripsi lokal, penyimpanan kredensial OS, dan konfirmasi manusia
Privasi data	Pemrosesan data yang diotorisasi, subprosesor patuh HIPAA, least privilege, dan audit akses data pelanggan
Audit dan keterlacakan	Catatan operasi penting, draf AI, konfirmasi manusia, operator, timestamp, dan riwayat versi
Rekayasa keamanan	Peninjauan kode, pengujian otomatis, pemindaian kerentanan, infrastructure as code, pelatihan keamanan, dan manajemen perubahan