CONVO SECURITY WHITEPAPER

Comprehensive Security Architecture for Conversation Intelligence

Version: 1.0
Date: September 1st, 2025
Classification: Public
Contact: markus@itsconvo.com

EXECUTIVE SUMMARY

Convo, Inc. provides enterprise-grade conversation intelligence with security and privacy built into every layer of our platform. This whitepaper details our comprehensive security architecture, demonstrating how we protect sensitive conversation data through defense-in-depth strategies, zero-trust principles, and continuous monitoring.

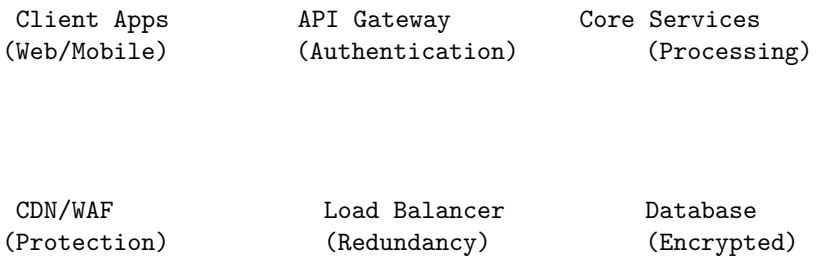
Key Security Highlights:

- **AES-256 encryption** for all data at rest and TLS 1.3 for data in transit
- **Zero-trust architecture** with multi-factor authentication and role-based access
- **SOC 2 Type I certified** with Type II in progress
- **GDPR and CCPA compliant** with comprehensive privacy controls
- **24/7 security monitoring** with automated threat detection
- **Sub-15 minute** incident detection with 72-hour breach notification

---

1. PLATFORM ARCHITECTURE OVERVIEW

1.1 High-Level Architecture



1.2 Security Zones

Our architecture implements multiple security zones with strictly controlled access:

- **DMZ (Demilitarized Zone):** Public-facing components with minimal privileges
- **Application Zone:** Core business logic with authenticated access only
- **Data Zone:** Encrypted storage with enhanced monitoring and access controls
- **Management Zone:** Administrative functions with privileged access requirements

1.3 Technology Stack Security

- **Cloud Provider:** AWS with enterprise security controls
- **Container Security:** Docker with security scanning and runtime protection
- **Orchestration:** Kubernetes with RBAC and network policies
- **Database:** PostgreSQL with transparent data encryption (TDE)
- **Cache:** Redis with encryption and authentication
- **Message Queue:** RabbitMQ with TLS and access controls

---

2. DATA SECURITY

2.1 Encryption Standards

Data at Rest

- **Algorithm:** AES-256-GCM with authenticated encryption
- **Key Management:** AWS KMS with HSM-backed key storage
- **Key Rotation:** Automatic 365-day rotation with backwards compatibility
- **Database:** Transparent Data Encryption (TDE) for all sensitive data
- **File Storage:** S3 server-side encryption with customer-managed keys
- **Backups:** Full encryption with separate key hierarchy

Data in Transit

- **Protocol:** TLS 1.3 with perfect forward secrecy
- **Cipher Suites:** ChaCha20-Poly1305, AES-256-GCM only
- **Certificate Management:** Automated renewal with 90-day certificates
- **Internal Communication:** mTLS for all service-to-service communication
- **API Security:** HTTPS enforcement with HSTS headers

2.2 Data Classification and Handling

Classification	Examples	Encryption	Access Controls	Retention
Highly Sensitive	Audio recordings, transcripts	AES-256 + Field-level	MFA + Approval	Customer configurable
Sensitive	User emails, metadata	AES-256	MFA + RBAC	30 days default
Internal	System logs, metrics	AES-256	RBAC	90 days
Public	Marketing content	Optional	Standard	Indefinite

2.3 Data Loss Prevention (DLP)

- **Content Inspection:** Real-time scanning for sensitive data patterns
- **Data Masking:** Automatic PII masking in logs and non-production environments
- **Egress Monitoring:** Automated detection of unusual data access patterns
- **USB/Device Controls:** Endpoint protection preventing unauthorized data export

---

3. ACCESS CONTROLS AND IDENTITY MANAGEMENT

3.1 Zero-Trust Architecture

Our zero-trust model verifies every access request regardless of location or previous authentication:

Principles:

- **Never Trust, Always Verify:** Every request authenticated and authorized
- **Least Privilege Access:** Minimum necessary permissions granted
- **Continuous Verification:** Real-time monitoring of access patterns
- **Microsegmentation:** Network and application-level isolation

3.2 Multi-Factor Authentication (MFA)

Required for all users:

- **TOTP (Time-based One-Time Password):** Google Authenticator, Authy
- **Hardware Security Keys:** FIDO2/WebAuthn support
- **SMS Backup:** Available but discouraged for security
- **Biometric Options:** For mobile applications

Administrative Access:

- **Hardware Keys Mandatory:** For all privileged operations
- **Conditional Access:** Location, device, and risk-based policies
- **Just-in-Time Access:** Temporary privilege elevation with approval

3.3 Role-Based Access Control (RBAC)

Standard User Roles

Role	Permissions	MFA Required	Data Access
Viewer	Read-only dashboard	Yes	Own team data
Analyst	Analytics, reports	Yes	Assigned accounts
Manager	Team management	Yes	Team data
Admin	Full customer account	Yes + Hardware Key	All customer data

System Roles

Role	Permissions	Additional Controls
Platform Admin	Cross-customer access	Background check, approval workflow
Security Team	Incident response	Privileged access management (PAM)
DevOps	Infrastructure	Bastion hosts, session recording

3.4 Privileged Access Management (PAM)

- **Just-in-Time Access:** Temporary privilege elevation for specific tasks
- **Session Recording:** All privileged sessions recorded and monitored
- **Approval Workflows:** Multi-person approval for sensitive operations
- **Emergency Access:** Break-glass procedures with full audit trail

---

4. NETWORK SECURITY

4.1 Network Architecture

```
Internet    WAF    Load Balancer    Application Servers

           CDN

                                        Private Subnets
                                        (Database, Cache)
```

4.2 Web Application Firewall (WAF)

AWS WAF with custom rules:

- **OWASP Top 10 Protection:** Automated blocking of common attacks
- **Rate Limiting:** API and page request throttling
- **Geo-blocking:** Restriction of access from high-risk countries
- **IP Reputation:** Real-time blocking of malicious IP addresses
- **Custom Rules:** Application-specific attack pattern detection

4.3 Network Segmentation

- **Public Subnets:** Only load balancers and bastion hosts
- **Private Subnets:** All application and database servers
- **Isolated Networks:** Separate VPCs for different environments
- **Microsegmentation:** Application-level network policies

4.4 DDoS Protection

- **AWS Shield Advanced:** Dedicated DDoS response team
- **CloudFlare Integration:** Global distributed traffic absorption
- **Rate Limiting:** Intelligent request throttling
- **Automatic Scaling:** Dynamic capacity to handle traffic spikes

---

5. APPLICATION SECURITY

5.1 Secure Development Lifecycle (SDLC)

Development Phase

- **Security Training:** Annual secure coding training for all developers
- **Code Reviews:** Peer review required for all code changes
- **Static Analysis:** Automated SAST scanning in CI/CD pipeline
- **Dependency Scanning:** Daily scans for vulnerable libraries
- **Secrets Management:** No hardcoded credentials, HashiCorp Vault integration

Testing Phase

- **Dynamic Analysis (DAST):** Automated web application scanning
- **Interactive Analysis (IAST):** Runtime application security testing
- **Penetration Testing:** Annual third-party security assessment
- **Bug Bounty Program:** Continuous external security testing

Deployment Phase

- **Container Scanning:** Security analysis of all container images
- **Infrastructure as Code:** Version-controlled, secure infrastructure templates
- **Zero-Downtime Deployments:** Blue-green deployments with rollback capabilities
- **Deployment Automation:** Consistent, repeatable deployment processes

5.2 API Security

- **OAuth 2.0 + PKCE:** Secure authorization for all API access
- **JWT Tokens:** Short-lived tokens with automatic rotation
- **Rate Limiting:** Per-user and per-endpoint request limits
- **Input Validation:** Strict validation of all API inputs
- **Output Encoding:** Prevention of injection attacks
- **API Gateway:** Centralized authentication and authorization

5.3 Session Management

- **Secure Cookies:** HttpOnly, Secure, SameSite attributes
- **Session Timeout:** Automatic timeout after 8 hours of inactivity
- **Concurrent Session Limits:** Maximum 3 active sessions per user
- **Session Invalidation:** Logout invalidates all user sessions
- **Session Binding:** IP and user-agent validation

---

6. INFRASTRUCTURE SECURITY

6.1 Cloud Security (AWS)

Account Security

- **AWS Organizations:** Centralized multi-account management
- **CloudTrail:** Comprehensive API logging across all accounts
- **Config:** Continuous compliance monitoring and remediation
- **GuardDuty:** Threat detection and incident response
- **Security Hub:** Centralized security findings management

Compute Security

- **EC2 Hardening:** CIS benchmarks applied to all instances
- **Systems Manager:** Patch management and configuration compliance
- **Inspector:** Vulnerability assessments for EC2 instances
- **Nitro Enclaves:** Hardware-isolated compute environments for sensitive processing

Storage Security

- **S3 Security:** Block public access, bucket policies, access logging
- **EBS Encryption:** All volumes encrypted with customer-managed keys
- **Snapshot Encryption:** Automated encrypted backups
- **Cross-Region Replication:** Encrypted replication for disaster recovery

6.2 Container Security

- **Base Image Security:** Minimal, regularly updated base images
- **Vulnerability Scanning:** Automated scanning with Trivy and Clair
- **Runtime Protection:** Falco for runtime security monitoring
- **Resource Limits:** CPU, memory, and I/O constraints
- **Network Policies:** Kubernetes network policies for microsegmentation

6.3 Monitoring and Logging

Security Information and Event Management (SIEM)

- **Centralized Logging:** All security events aggregated in Elasticsearch
- **Real-time Analysis:** Automated correlation and alerting
- **Threat Intelligence:** Integration with external threat feeds
- **Machine Learning:** Anomaly detection for unusual patterns

Monitoring Coverage

- **Application Performance:** New Relic for application monitoring
- **Infrastructure Monitoring:** CloudWatch and Prometheus
- **Security Monitoring:** Custom SIEM with automated response
- **User Activity Monitoring:** All user actions logged and analyzed

---

7. INCIDENT RESPONSE AND BUSINESS CONTINUITY

7.1 Incident Response Process

Detection (Target: <15 minutes)

- **Automated Monitoring:** SIEM alerts with ML-based anomaly detection
- **24/7 SOC:** Security operations center monitoring
- **Customer Reports:** Dedicated security reporting channels
- **Threat Intelligence:** External threat feed integration

Response (Target: <1 hour)

- **Incident Commander:** Designated response leader activation
- **Response Team:** Security, engineering, and management coordination
- **Communication Plan:** Internal and external stakeholder notification
- **Evidence Preservation:** Forensic data collection and chain of custody

Recovery (Target: <24 hours)

- **Containment:** Immediate isolation of affected systems
- **Eradication:** Threat removal and vulnerability patching
- **Recovery:** Service restoration with enhanced monitoring
- **Post-Incident Review:** Lessons learned and process improvement

7.2 Business Continuity and Disaster Recovery

High Availability Architecture

- **Multi-AZ Deployment:** Services distributed across availability zones
- **Load Balancing:** Automatic traffic distribution and failover
- **Database Clustering:** PostgreSQL with read replicas
- **Auto-scaling:** Dynamic capacity based on demand

Backup and Recovery

- **Recovery Time Objective (RTO):** 4 hours maximum
- **Recovery Point Objective (RPO):** 15 minutes maximum
- **Automated Backups:** Daily encrypted backups with 30-day retention
- **Cross-Region Replication:** Disaster recovery in separate AWS region
- **Backup Testing:** Monthly restore testing and validation

7.3 Communication and Notification

- **Customer Notification:** Email and dashboard notifications within 4 hours
- **Status Page:** Real-time service status at status.itsconvo.com
- **Regulatory Notification:** GDPR and other regulatory compliance within 72 hours
- **Public Communication:** Coordinated external communications when necessary

---

8. COMPLIANCE AND GOVERNANCE

8.1 Regulatory Compliance

GDPR (General Data Protection Regulation)

- **Data Processing Agreements:** Standard DPAs for all customers
- **Privacy by Design:** Privacy controls built into all features
- **Data Subject Rights:** Automated fulfillment of access, deletion, and portability requests
- **Cross-Border Transfers:** Standard Contractual Clauses for international transfers
- **Breach Notification:** 72-hour regulatory notification process

CCPA (California Consumer Privacy Act)

- **Consumer Rights:** Access, deletion, and opt-out mechanisms
- **Data Disclosure:** Clear privacy policy and data collection practices
- **Third-Party Sharing:** Transparent data sharing disclosures
- **Vendor Management:** Due diligence for all data processors

8.2 Security Certifications

SOC 2 (Service Organization Control 2)

- **Type I:** Point-in-time assessment of security controls (Completed)
- **Type II:** 12-month operational effectiveness assessment (Q2 2025)
- **Trust Service Criteria:** Security, availability, processing integrity, confidentiality
- **Independent Auditor:** Certified public accounting firm audit

ISO 27001 (Information Security Management System)

- **Implementation Timeline:** Q3 2025 certification target
- **Risk Assessment:** Comprehensive information security risk analysis
- **Management System:** Documented ISMS with continuous improvement
- **External Audit:** Third-party certification body assessment

8.3 Internal Governance

Security Governance Committee

- **Executive Sponsor:** CEO as security champion
- **Security Officer:** Dedicated security leadership role
- **Cross-Functional Team:** Engineering, legal, and operations representation
- **Regular Meetings:** Monthly security governance reviews

Policy Management

- **Annual Policy Review:** Comprehensive review of all security policies
- **Change Management:** Formal approval process for policy updates
- **Training and Awareness:** Regular security training for all employees
- **Compliance Monitoring:** Continuous monitoring of policy adherence

---

9. VENDOR AND THIRD-PARTY SECURITY

9.1 Vendor Risk Management

Vendor Assessment Process

1. **Security Questionnaire:** Comprehensive security assessment
2. **Due Diligence Review:** Evaluation of security practices and certifications
3. **Contract Terms:** Security requirements and liability allocation
4. **Ongoing Monitoring:** Regular security posture reviews
5. **Incident Coordination:** Joint incident response procedures

Key Vendor Categories

Vendor Type	Security Requirements	Monitoring
Cloud Infrastructure	SOC 2, ISO 27001, regular audits	Continuous
SaaS Applications	Security assessments, access reviews	Quarterly
Data Processors	DPAs, encryption, audit rights	Monthly
Professional Services	Background checks, NDAs	Project-based

9.2 Current Key Vendors

- **Amazon Web Services (AWS):** Primary cloud infrastructure provider
- **OpenAI:** AI processing for transcription and analysis
- **Cloudflare:** CDN and DDoS protection services
- **New Relic:** Application performance monitoring

9.3 Supply Chain Security

- **Software Bill of Materials (SBOM):** Comprehensive inventory of software components
- **Dependency Scanning:** Automated vulnerability scanning of third-party libraries
- **License Compliance:** Tracking and compliance with software licenses

- **Update Management:** Systematic approach to security updates

---

10. PRIVACY AND DATA PROTECTION

10.1 Privacy by Design Principles

Proactive Not Reactive

- Security and privacy measures implemented before data processing begins
- Anticipatory approach to privacy risks and threats
- Prevention-focused rather than remediation-focused

Privacy as the Default Setting

- Maximum privacy protection without user action required
- Opt-in consent for all non-essential data processing
- Minimal data collection by default

Data Minimization

- Collection limited to necessary data for service delivery
- Regular review and deletion of unnecessary data
- Purpose limitation for all data processing activities

10.2 Consent Management

- **Granular Consent:** Separate consent for different processing purposes
- **Easy Withdrawal:** Simple mechanisms for consent withdrawal
- **Consent Records:** Comprehensive logging of all consent interactions
- **Multi-Party Scenarios:** Consent management for conversation participants

10.3 Data Subject Rights

- **Right of Access:** Comprehensive data export in machine-readable format
- **Right to Rectification:** Data correction mechanisms
- **Right to Erasure:** Complete data deletion within 30 days
- **Right to Portability:** Data transfer to other service providers
- **Right to Restriction:** Processing limitation controls

---

11. SECURITY TESTING AND VALIDATION

11.1 Continuous Security Testing

Automated Testing

- **SAST (Static Application Security Testing):** Daily code analysis
- **DAST (Dynamic Application Security Testing):** Weekly application scanning
- **IAST (Interactive Application Security Testing):** Runtime security analysis
- **Container Scanning:** Every container build analyzed for vulnerabilities
- **Infrastructure Scanning:** Daily vulnerability assessment of all systems

Manual Testing

- **Code Reviews:** Security-focused peer review for all changes
- **Architecture Reviews:** Security assessment of design changes
- **Configuration Reviews:** Regular audit of security configurations
- **Access Reviews:** Quarterly review of user access and permissions

11.2 Penetration Testing

- **Annual External Testing:** Independent third-party security assessment
- **Quarterly Internal Testing:** Internal team security testing
- **Red Team Exercises:** Advanced persistent threat simulation
- **Bug Bounty Program:** Continuous external security research

11.3 Vulnerability Management

- **Asset Inventory:** Complete inventory of all systems and applications
- **Vulnerability Scanning:** Daily automated vulnerability assessments
- **Risk Assessment:** CVSS-based prioritization of security issues
- **Patch Management:** Systematic approach to security updates
- **Exception Management:** Risk-based approach to patching delays

---

12. TRAINING AND AWARENESS

12.1 Security Training Program

All Employees

- **Security Awareness:** Annual comprehensive security training
- **Phishing Simulation:** Monthly simulated phishing attacks
- **Incident Reporting:** Training on security incident identification and reporting
- **Data Handling:** Proper handling of sensitive customer data

Engineering Team

- **Secure Coding:** Annual secure development practices training
- **OWASP Top 10:** Current web application security risks

- **Threat Modeling:** Design-phase security risk assessment
- **Security Testing:** Integration of security testing into development

Management Team

- **Security Governance:** Leadership role in security program
- **Risk Management:** Understanding and managing security risks
- **Incident Response:** Management responsibilities during security incidents
- **Regulatory Compliance:** Understanding of compliance requirements

12.2 Security Culture

- **Security Champions:** Designated security advocates in each team
- **Continuous Learning:** Regular security knowledge sharing sessions
- **Industry Engagement:** Participation in security conferences and training
- **Security Metrics:** Regular reporting on security posture and improvements

---

13. CONTACT INFORMATION

13.1 Security Team Contacts

- **General Security Inquiries:** markus@itsconvo.com
- **Security Incidents:** markus@itsconvo.com (24/7 monitoring)
- **Vulnerability Reports:** markus@itsconvo.com
- **Compliance Questions:** markus@itsconvo.com

13.2 Emergency Contacts

- **Executive Escalation:** [Coming Soon]

13.3 External Resources

- **Bug Bounty Program:** [Coming Soon]
- **Security Documentation:** [Coming Soon]
- **Status Page:** https://www.itsconvo.com
- **Trust Center:** [Coming Soon]

CONCLUSION

Convo, Inc.'s comprehensive security program demonstrates our commitment to protecting customer data and maintaining the trust placed in our conversation

intelligence platform. Through defense-in-depth strategies, continuous monitoring, and adherence to industry best practices, we provide enterprise-grade security without compromising functionality or user experience.

Our security program continues to evolve with emerging threats and regulatory requirements. We welcome feedback and questions from customers, security researchers, and industry professionals as we work together to maintain the highest standards of information security.

For the most current version of this whitepaper and additional security documentation, please visit our Trust Center or contact our security team directly.

Document Information:

- **Version:** 1.0
- **Last Updated:** January 2025
- **Next Review:** July 2025
- **Classification:** Public
- **Distribution:** Available to customers and prospects upon request

---

This whitepaper provides an overview of Convo, Inc.'s security architecture and practices. For detailed technical implementations or specific security questions, please contact our security team at markus@itsconvo.com.