Executive Security Report

Period: 11/30/2025 - 11/30/2025

Executive Summary

8	1	7
Total Findings	Critical Issues	Action Required

Security Findings

Infrastructure Security Controls

CRITICAL

Category: Security Architecture | Provider: Infrastructure Team

Enterprise-grade security infrastructure: Multi-region deployment with automatic failover (99.9% uptime SLA). TLS 1.3 encryption for all data in transit. AES-256 encryption for data at rest. DDoS protection with rate limiting and WAF. Network segmentation with zero-trust architecture. Kubernetes-based infrastructure with automated security patching. Regular penetration testing (quarterly) by third-party security firms.

Compliance Certifications & Standards

HIGH

Category: Compliance | Provider: Compliance Team

Current compliance framework: SOC 2 Type II (in progress, expected Q1 2026). GDPR compliant data processing and privacy controls. ISO 27001 information security management practices. NIST Cybersecurity Framework alignment. OWASP Top 10 security controls implemented. Regular third-party security audits and assessments. Documented incident response and business continuity plans.

Data Protection & Privacy

HIGH

Category: Data Privacy | Provider: Privacy Team

Comprehensive data protection measures: Customer data isolated by tenant (multi-tenant with strict separation). PII encrypted with field-level encryption where applicable. Data retention policies: 90 days for operational data, 7 years for compliance. Right to erasure (DSAR) requests processed within 30 days. Data Processing Agreements (DPA) available upon request. No selling or sharing customer data with third parties. Regular privacy impact assessments (PIAs) conducted.

Access Control & Authentication

HIGH

Category: Identity & Access | Provider: Security Team

Robust access control mechanisms: Multi-factor authentication (MFA) required for all admin accounts. Role-based access control (RBAC) with principle of least privilege. Single Sign-On (SSO) support via SAML 2.0 and OAuth 2.0. Session management with automatic timeout (30 minutes inactivity). API authentication using secure token-based auth (JWT). Regular access reviews and account audits. Password policies: 12+ characters, complexity requirements, 90-day rotation.

Incident Response & Business Continuity

MEDIUM

Category: Operations | Provider: Operations Team

Prepared for incidents with documented procedures: 24/7 security monitoring and alerting. Incident response plan with defined escalation procedures. RTO (Recovery Time Objective): 4 hours for critical systems. RPO (Recovery Point Objective): 15 minutes data loss maximum. Daily automated backups with 30-day retention. Disaster recovery testing conducted quarterly. Security incident notification within 72 hours (GDPR requirement). Forensic investigation capabilities for serious incidents.

Vendor & Supply Chain Security

MEDIUM

Category: Third-Party Risk | Provider: Procurement Team

Third-party risk management: All vendors undergo security assessment before onboarding. Subprocessor agreements for any data processing partners. Regular vendor security reviews (annually minimum). Cloud providers: Vercel (hosting), MongoDB (database), Redis Labs (cache). Email services: SocketLabs/SendGrid with DKIM/SPF/DMARC. External APIs: HIBP, AbuseIPDB, Shodan, VirusTotal (read-only access). Vendor breach notification requirements in all contracts.

Security Monitoring & Logging

MEDIUM

Category: Monitoring | Provider: Security Team

Comprehensive security monitoring: Centralized logging with 90-day retention minimum. Security Information and Event Management (SIEM) integration. Automated anomaly detection and alerting. Failed authentication attempt monitoring (lockout after 5 attempts). API rate limiting to prevent abuse (1000 req/hour). Audit logs for all administrative actions. Database query monitoring and access logging. Regular log review and security analytics.

Development & DevSecOps

LOW

Category: Secure Development | Provider: Engineering Team

Security-first development practices: Secure SDLC with security requirements in planning phase. Code review required for all production changes. Dependency scanning for vulnerable packages (daily). Static Application Security Testing (SAST) in CI/CD pipeline. Container image scanning before deployment. Secrets management via environment variables (never in code). Automated security testing as part of deployment process. Version control with branch protection and audit trails.