ALTNETIX LLC
VitaAI Platform

HOST HARDENING DOCUMENTATION

Infrastructure Security Baseline and Hardening Standards

Control Reference	INFRA-8
Document Version	1.0
Effective Date	June 1, 2026
Next Review	June 1, 2027
Classification	Confidential – Internal & Customer Use
Maintained by	Altnetix LLC Security & Compliance Team
Contact	compliance@altnetix.com

1. Purpose and Scope

This document describes the security hardening measures applied to Altnetix LLC's Azure App Service infrastructure, network controls, and supporting services. Hardening is aligned with the CIS Microsoft Azure Foundations Benchmark v1.5 and HIPAA §164.312 technical safeguard requirements.

2. TLS and Transport Security

Cipher Suite Configuration

All CBC-mode and static-RSA cipher suites have been disabled following a Qualys SSL Labs assessment (score: A). The following TLS 1.2 suites are enabled:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC02F) — forward secret, AEAD
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC030) — forward secret, AEAD

TLS 1.3 is enabled with TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, and TLS_CHACHA20_POLY1305_SHA256.

HSTS Configuration

HTTP Strict Transport Security is configured with max-age=31536000 (1 year), includeSubDomains, and preload. This is enforced at both the application layer (ASP.NET Core middleware) and the IIS layer (URL Rewrite outbound rule) to prevent platform-level override.

Protocol Controls

TLS 1.0 and 1.1 are disabled at the Azure App Service platform level. Minimum TLS version is set to 1.2 in App Service configuration. HTTPS-only mode is enforced.

3. Security Response Headers

All API responses include the following security headers:

Header	Value	Purpose
Strict-Transport-Security	max-age=31536000; includeSubDomains; preload	Force HTTPS for 1 year
X-Content-Type-Options	nosniff	Prevent MIME sniffing
X-Frame-Options	DENY	Block iframe embedding (clickjacking)
X-XSS-Protection	0	Disable legacy XSS auditor (CSP preferred)
Referrer-Policy	no-referrer	Prevent referrer header leakage
Content-Security-Policy	default-src 'self'; object-src 'none'	XSS amplification defence
Permissions-Policy	geolocation=(), camera=(), payment=()	Restrict browser features
Cross-Origin-Opener-Policy	same-origin	Spectre side-channel isolation

4. Network Security

- Azure App Service is configured with IP restrictions to deny direct public access to management ports

- Database connectivity uses private endpoints — no public internet access to Azure SQL
- Azure Key Vault access is restricted to the App Service managed identity via RBAC
- Outbound network traffic is filtered through Azure firewall policies
- DDoS Protection Standard is enabled at the virtual network level

5. Access Control

- All production systems require MFA for administrative access
- Just-in-time (JIT) VM access is enabled where applicable
- Service accounts use managed identities — no credential rotation required
- Azure RBAC is used with least-privilege roles for all service and user access
- Privileged access is audited via Azure Monitor and reviewed quarterly

6. Monitoring and Patch Management

- Microsoft Defender for Cloud monitors security posture and compliance
- Application Insights provides APM, error tracking, and anomaly detection
- Azure App Service automatically applies OS-level patches (managed platform)
- Application dependencies are scanned weekly; high-severity CVEs patched within 7 days
- Security alerts trigger automated incident tickets within 5 minutes