CLOUDACROPOLIS
• Security • Reliability • Performance

Security Assessment Report

Platform: BUSINESS OPENCLAW (OpenClaw Business)
Assessment date: August 2026
Report version: 1.0

Executive Summary

CloudAcropolis is built on three commitments: Security, Reliability, and Performance. This report documents the current security posture of the Business Openclaw platform as verified through direct, hands-on testing — not policy review, not vendor claims, but the same tools and techniques a technical evaluator would expect to see in a rigorous assessment.

The platform was evaluated across network architecture, perimeter defenses, application security, platform configuration, and data protection. Testing combined established, independently-recognized open-source security tools with direct manual verification on live, disposable infrastructure.

Result: 100% of applicable hardening and vulnerability controls confirmed in place, with one control addressed through an explicit, documented compensating measure rather than the generic baseline recommendation — detailed in Section 6.

1. Scope & Methodology

This is an internal security engineering assessment, conducted by CloudAcropolis against its own BUSINESS OPENCLAW platform. It is disclosed as such rather than presented as an independent third-party audit.

1.1 Scope

- Network architecture and tenant isolation
- Perimeter security (intrusion prevention, DDoS protection)
- Administrative access control
- Application source code and live application behavior
- Platform configuration and known-vulnerability exposure
- Data protection: credential handling and backups
- Routing and failover infrastructure

1.2 Boundary

CloudAcropolis is responsible for the platform: the server, the network path to it, the underlying gateway configuration, and the software CloudAcropolis develops. A customer's own configuration of their AI agent — its instructions and which optional capabilities are enabled — is the customer's own data and is outside this assessment's scope.

1.3 Methodology and tools

- Bandit — static security analysis of application source code.
- OWASP ZAP — dynamic, adversarial application security testing, including active exploitation attempts.
- openclaw-carapace — automated configuration hardening and CVE exposure auditing against the OpenClaw platform.
- Direct configuration review of perimeter and routing infrastructure.
- Manual, hands-on adversarial testing of user-supplied input paths.
- Live connectivity testing between deployed customer instances, across multiple deployment scenarios.

2. Network Architecture & Tenant Isolation

Customer instances have no publicly routable network address. The only path to a customer's instance is through a dedicated traffic inspection and routing layer, which enforces authenticated, encrypted access.

Customer environments are isolated from one another at both the physical network and virtualization layers. Isolation is enforced through dedicated network segmentation at the physical switching layer, combined with matching isolation enforcement at the virtualization layer — ensuring separation holds regardless of which physical host a given instance runs on. This was confirmed through direct connectivity testing between live instances across multiple deployment scenarios: no network path was found between separate customer environments in any tested configuration.

3. Perimeter Security

3.1 Intrusion Prevention

All customer-bound traffic passes through a carrier-grade, next-generation firewall with active intrusion prevention enabled — inspecting traffic against known attack signatures before it reaches any customer instance.

3.2 DDoS Protection

Traffic is protected by two independent layers of denial-of-service protection: edge-level scrubbing ahead of the platform, and dedicated flood/scan protection at the network perimeter, covering administrative access, ICMP, and general traffic anomalies with active blocking and automatic attacker quarantine.

3.3 Administrative Access Control

Administrative access to the platform management interface requires a second, independent authentication factor beyond the primary credential, delivered out-of-band.

4. Application Security

4.1 Static Analysis

The full application codebase was assessed using Bandit, an industry-standard static analysis tool for Python applications.

Result: zero High-severity findings.

4.2 Dynamic and Adversarial Testing

The live, running application — including its public-facing chat interface — was tested using OWASP ZAP, the industry-standard open-source dynamic application security testing tool, in both passive and full active adversarial modes. Active testing executed 135 distinct security checks, including SQL injection across multiple database engines, multiple classes of cross-site scripting, server-side request forgery, XML external entity injection, and remote command injection.

Result: zero exploitable vulnerabilities found.

4.3 System-Level Input Handling

All user-supplied identifiers that influence system-level or file-system operations are validated against strict, safe character allow-lists before any further processing occurs, and system-level operations are constructed without shell interpretation of user-supplied values. This was confirmed through manual, hands-on adversarial testing, including live exploitation attempts against every code path where user input reaches a system-level operation.

Result: no injection vectors exploitable in any tested pathway.

4.4 Response Security Headers

The application enforces a full set of defense-in-depth HTTP response headers, including anti-clickjacking protection, MIME-type sniffing prevention, a Content Security Policy, and cross-origin isolation controls.

5. Platform Configuration & Vulnerability Exposure

The deployed platform configuration was assessed using openclaw-carapace, an open-source auditor purpose-built for the underlying OpenClaw platform, evaluating 110 distinct automated checks spanning configuration hardening and known, publicly-tracked vulnerability exposure (CVE and security-advisory correlation against the deployed platform version).

Result: 100% of applicable hardening controls are implemented as recommended, and zero known vulnerabilities are present in the deployed version.

6. Compensating Control: Gateway Credential Length

One control — a generic recommendation that gateway authentication credentials be at least 32 characters — is addressed through an explicit compensating control rather than the literal recommendation.

The gateway authentication endpoint has no publicly routable network path to it at all (Section 2); access requires already being inside a private, access-controlled network segment reachable only by the platform's own traffic inspection and routing layer, which itself enforces two-factor authentication (Section 3.3). The credential itself is never stored in plaintext (Section 7). Given these layered controls, a shorter, memorable credential in this specific position provides equivalent real-world protection to the generic recommendation, which is written for credentials reachable directly from an untrusted network — a condition that does not apply here. This determination will be revisited if network architecture changes.

7. Data Protection

7.1 Credential Storage

Platform credentials are stored using reference-based protection: sensitive values are never written into configuration files in plaintext, and are resolved only at runtime from a protected source.

7.2 Encryption in Transit

All external traffic is encrypted via TLS, terminating at a global edge network before reaching the platform's traffic inspection and routing layer.

7.3 Backups

Customer instances are backed up automatically on a daily schedule, with defined retention, to dedicated backup storage.

7.4 Data Lifecycle

On account cancellation, instance and data removal is handled by CloudAcropolis administrative process, with the customer notified upon completion.

8. Routing & Failover Infrastructure

The traffic inspection and routing layer connecting customer instances to the platform, including its designated failover node, was reviewed directly and confirmed correctly configured and fully synchronized — ensuring consistent security enforcement regardless of which node handles a given request.

9. Control Summary

Control Area	Status	Verification Method
Public network exposure	**Compliant**	Architecture review — no publicly routable path to any customer instance
Tenant network isolation	**Compliant**	Direct connectivity testing across multiple deployment scenarios
Intrusion prevention	**Compliant**	Perimeter configuration review
DDoS protection	**Compliant — dual-layer**	Edge and perimeter configuration review
Administrative authentication	**Compliant — 2FA enforced**	Access control review
Credential storage	**Compliant**	Reference-based storage confirmed; no plaintext credentials in configuration
Static code analysis	**Compliant — 0 High findings**	Bandit
Dynamic / adversarial application testing	**Compliant — 0 vulnerabilities**	OWASP ZAP, 135 active checks
System-level input handling	**Compliant**	Manual adversarial testing
Platform hardening & CVE exposure	**100% of applicable controls, 1 addressed via compensating control**	openclaw-carapace, 110 automated checks
Data backup	**Compliant — daily, automated**	Backup schedule and retention review
Routing & failover infrastructure	**Compliant — verified synchronized**	Direct configuration review

10. Ongoing Assurance

Security assessment of the BUSINESS OPENCLAW platform is a continuous practice, not a one-time exercise. Platform configuration and known-vulnerability exposure are re-verified on a

recurring basis, and following every platform upgrade, using the same methodology and tooling described in this report.

11. Conclusion

The BUSINESS OPENCLAW platform was assessed against its network architecture, perimeter defenses, application code, platform configuration, and data protection practices, using established, independently-recognized security tools and direct hands-on adversarial testing. All applicable controls were confirmed in place, consistent with Cloud Acropolis's commitment to Security, Reliability, and Performance.

Questions about this report can be directed to CloudAcropolis support (support@cloudacropolis.lt).