Security Assessment Report

Platform: N8N FOR 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 n8n for Business 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, platform and third-party software vulnerability exposure, platform configuration, and data protection. Testing combined established, independently-recognized open-source security tools with direct manual verification on live 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 N8N FOR BUSINESS 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, TLS configuration)
- Administrative access control
- Third-party platform vulnerability exposure and live exploit verification
- Platform configuration and provisioning consistency
- 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 provisioning process CloudAcropolis develops and maintains. n8n itself is third-party, open-source software; a customer's own workflow configurations — what they build and which credentials they connect — are the customer's own data and are outside this assessment's scope.

1.3 Methodology and tools

- Nuclei — automated exploit verification against every publicly disclosed n8n CVE with an available template, including a fully authenticated exploitation attempt for the most severe disclosed vulnerability.
- OWASP ZAP — dynamic, adversarial application security testing in both API-scan and AJAX-spider modes, including active exploitation attempts.

- Direct, five-layer manual infrastructure audit (operating system, network, administrative access, container runtime, application configuration), conducted against live instances.
- Direct configuration review of perimeter, routing, and provisioning infrastructure.
- Provisioning-pipeline verification: fixes traced to their root cause and confirmed applied automatically on an independently-provisioned test instance.

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.

Each customer instance runs on its own dedicated virtual machine, isolated on a private network segment that is unreachable not only from the internet but from other internal servers outside its permitted access list. Container-published network ports are explicitly restricted at the firewall's forwarding layer to only the specific internal hosts each service requires — confirmed through direct, layer-by-layer configuration review.

3. Perimeter Security

3.1 Intrusion Prevention

All customer-bound traffic passes through a global edge network before reaching a carrier-grade, next-generation firewall pairing — configured in an active-active high-availability pair — inspecting traffic 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 perimeter-level protection with automated rate-limiting.

3.3 Administrative Access Control

Administrative (SSH) access to each instance is restricted at the firewall level to a defined set of internal management subnets only — never reachable from the customer-facing network path. Repeated failed authentication attempts are automatically rate-limited and temporarily blocked. Customer-facing administrative terminal access is a fully separate mechanism, gated by one-time-passcode authentication.

3.4 Transport Security

All external traffic is encrypted via TLS, with HTTP Strict Transport Security enforced at the perimeter to prevent downgrade to an unencrypted connection on any subsequent visit.

4. Third-Party Platform Vulnerability Exposure

4.1 CVE Exploit Verification

n8n is third-party, open-source software; CloudAcropolis does not maintain or modify its source code. The applicable equivalent of source-code analysis for third-party software is direct, live verification against every disclosed vulnerability affecting the platform. Every CVE publicly disclosed against n8n through the assessment date, with an available automated verification template, was tested directly against a live instance — including a full, authenticated exploitation attempt (genuine credentials, live session, crafted exploit payload) against CVE-2025-68613, a CISA Known Exploited Vulnerability rated critical.

Result: zero exploitable vulnerabilities confirmed across all tested CVEs. Deployed platform version confirmed current against every publicly disclosed n8n vulnerability as of the assessment date.

4.2 Dynamic and Adversarial Testing

The live, running application — including its editor interface and REST API — was tested using OWASP ZAP, the industry-standard open-source dynamic application security testing tool, combining API-focused scanning with AJAX-spider crawling suited to n8n's single-page application architecture. Testing covered SQL injection across multiple database engines, multiple classes of cross-site scripting, remote code execution classes including Log4Shell and Spring4Shell, server-side template injection, XML external entity injection, and path traversal, among a combined 170 or more distinct security checks.

Result: zero exploitable vulnerabilities found.

4.3 Webhook and Endpoint Exposure

n8n's webhook-triggered workflow endpoints, and their available authentication mechanisms, were reviewed directly against the platform's own documented configuration options. Production webhook and administrative interface access were confirmed to sit behind the same network-isolation and TLS controls described in Section 2 and Section 3.

5. Platform Configuration & Provisioning Consistency

The deployed platform configuration — operating system patch level, container runtime, network firewall enforcement, and application-level settings — was assessed through direct manual review across five layers, then traced to its root cause in the automated provisioning process and corrected there rather than on individual instances. The corrected provisioning process was independently validated by provisioning a new instance and confirming every control applied automatically, with no manual intervention required.

Result: 100% of applicable hardening controls confirmed in place, verified reproducible through the provisioning pipeline itself.

6. Compensating Control: Administrative SSH Credential Policy

One control — a generic recommendation that direct administrative SSH access disable password authentication and direct root login in favor of key-based access only — is addressed through an explicit compensating control rather than the literal recommendation.

The administrative SSH interface has no network path reachable from the customer-facing side of the platform at all (Section 3.3); access requires already being inside a defined internal management subnet. Repeated failed authentication attempts are automatically rate-limited and temporarily blocked. Customer administrative access uses a fully separate, one-time-passcode-gated mechanism that never touches this interface. Given these layered controls, the current administrative SSH credential policy 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 and workflow credentials are encrypted at rest using an explicitly configured, instance-specific encryption key, never left to an implicit default.

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 & Patching

Customer instances are backed up and patched on a defined monthly cadence. Operating-system security updates, and the container runtime, are additionally refreshed from CloudAcropolis's own internally-maintained package cache on a daily schedule, ensuring new instances provision from current, not stale, software — verified during this assessment by confirming a freshly-provisioned instance carried only a single pending update.

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 high-availability failover pairing, was reviewed directly and confirmed correctly configured and synchronized across both nodes — 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 configuration review, container-level firewall enforcement
Intrusion prevention	Compliant	Perimeter configuration review
DDoS protection	Compliant — dual-layer	Edge and perimeter configuration review
Administrative authentication	Compliant — network-isolated, rate-limited	Access control review
Transport security	Compliant — HSTS enforced	Live HTTP response verification
CVE exploit verification	Compliant — 0 exploitable	Nuclei, every disclosed CVE with available template
Dynamic / adversarial application testing	Compliant — 0 vulnerabilities	OWASP ZAP, 170+ checks
Platform hardening & provisioning consistency	Compliant — verified reproducible	5-layer manual audit; validated on fresh instance
Credential storage	Compliant	Instance-specific encryption key confirmed explicit
Data backup & patching	Compliant — monthly instance cadence, daily package cache	Backup/patch schedule review

Routing & failover infrastructure	Compliant — verified synchronized	Direct configuration review, both HA nodes

10. Ongoing Assurance

Security assessment of the N8N FOR BUSINESS 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 provisioning change, using the same methodology and tooling described in this report.

11. Conclusion

The N8N FOR BUSINESS platform was assessed against its network architecture, perimeter defenses, third-party software vulnerability exposure, 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 CloudAcropolis's commitment to Security, Reliability, and Performance.

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