Verdict & Executive Summary

GO_WITH_EXCEPTIONS

Common server risks reduced. Remaining decisions made visible.

Point-in-time server hardening, validation, and evidence review with identifying details removed.

EVIDENCE WINDOW

Closeout snapshot · 2026-06-30
Primary closeout snapshot

Private operator access addendum · 2026-07-11
Separate access addendum

PRODUCTION VPS · IDENTIFIERS REMOVED
Public identifiers removed

WHAT THIS REPORT DOES NOT CLAIM

Scope boundary: baseline server hardening, validation, and evidence. No penetration test, forensic investigation, malware clearance, compliance certification, or always-on response service is claimed.

This is a baseline hardening delivery report. It is not a penetration test, forensic conclusion, malware-clearance statement, compliance certification, or promise that compromise is impossible.

COMPLETED CONTROLS

- SSH now accepts approved keys only. Direct root login, passwords, and keyboard-interactive login were disabled.
- Administrator users, privileges, and SSH keys were reviewed. An unnecessary root-equivalent group membership and an active stale sudoers backup were removed from use.
- Fail2Ban was installed for SSH and checked while running. Security-only automatic updates were configured without automatic reboot.
- Available security logs were reviewed across a 14-day window. Telegram alert delivery and scheduled checks were verified at closeout.

REMAINING OWNER DECISIONS

HIGH	Persistent firewall policy was incomplete at closeout.
HIGH	Some application and administrator entry points remained public by owner decision.
MEDIUM	A recovery path and database dump existed, but an actual restore was not performed.
MEDIUM	Package and reboot maintenance still required an approved maintenance window.

Before → After

The After column is not an all-clear. It shows verified improvements beside the decisions and risks that still belong to the owner.

AREA	BEFORE	AFTER · CONTROL PLUS EXPLICIT EXCEPTION
SSH	public access needed stronger login controls.	approved keys only; direct root, password, and keyboard-interactive login disabled. Public SSH still remained reachable at closeout.
Administrator access	users, privileges, groups, and keys required review.	retained access paths were reviewed and an unnecessary root-equivalent group membership was removed.
Fail2Ban	no established SSH protection baseline.	an SSH-only jail was installed, activated, and checked while running.
Updates	automatic updates covered broader sources and maintenance was pending.	security-only updates were configured and automatic reboot was disabled; maintenance remained pending.
Logging	local security logs were available but had not yet been reviewed across the 14-day closeout window.	the available 14-day history was reviewed and summarized with its limits.
Alerts	alert delivery and the current-state baseline had not yet been validated for this case.	the baseline was initialized without replaying old noise; Telegram delivery and scheduled checks were verified at closeout.

WHAT REMAINED VISIBLE Persistent firewall work was incomplete; some public application and administrator exposure remained; restore was not performed; package and reboot maintenance was still pending.

Private Admin Access & Recovery

AT CLOSEOUT · 2026-06-30

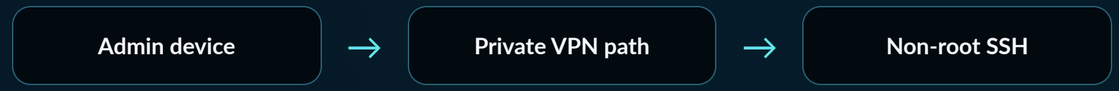
- AT CLOSEOUT · SSH accepted approved keys only, but the SSH entry point still remained public for administrator and recovery access.
- AT CLOSEOUT · The owner confirmed provider console or rescue access and a provider restore path. Those recovery paths were not exercised during this engagement.
- AT CLOSEOUT · An application database dump was created and its catalog could be read. No restore was performed.

RECOVERY BOUNDARY

LIMIT · The later VPN result did not change public SSH and did not prove that administrator access was private-only.

SEPARATE POST-CLOSEOUT ACCESS ADDENDUM

POST-CLOSEOUT ACCESS ADDENDUM · 2026-07-11 · Later evidence, kept separate from the 2026-06-30 closeout.



- A named private operator VPN path completed a real handshake and transport check.
- The expected non-root administrator connected through that private path using the assigned access profile.
- The validated private session did not change the operator workstation's normal host routes.
- When the validated session ended, its temporary network runtime closed without remaining namespace or runtime residue.

STILL PENDING

PENDING OWNER DECISION · Removal of the later operator VPN peer was not authorized or evidenced.

The private operator access validation dated 2026-07-11 happened after closeout and must remain separate from the 2026-06-30 result.

Firewall & Approved Service Exposure

A port number alone does not tell you what is using it.

A port number is only the doorway. To understand the risk, we also record which program is behind it, which system account runs that program, who can reach it, why it is needed, and what the owner approved.

EVERY APPROVED EXPOSURE NEEDS A CONTRACT

- Protocol + port
- Bind scope
- Service / process
- System user
- Allowed source
- Business purpose
- Owner decision

WHY CHANGES MATTER

Why same-port drift matters: HTTPS can stay on TCP port 443 while a different program takes over, runs as a more powerful system user, or becomes reachable from more places. The port number still looks normal, but the security meaning has changed. A new listener, a new allow rule, or any of these identity or source changes deserves review.

A runtime firewall rule blocked traffic to one discovery service, but the program still listened on the server. A listening program and a traffic rule are different facts.

The persistent firewall baseline was still incomplete at the 2026-06-30 closeout.

OBSERVED EXPOSURE DECISIONS

		BIND	SYSTEM USER	ALLOWED SOURCE	BUSINESS PURPOSE
TCP · 80	nginx web redirect	public IPv4/IPv6	withheld from public artifact	public	redirect web traffic
TCP · 443	nginx HTTPS	public IPv4/IPv6	withheld from public artifact	public	serve encrypted web traffic
TCP · 22	sshd	public IPv4/IPv6	withheld from public artifact	public at closeout	key-only administrator and recovery access
TCP · port withheld	application backend; identifier withheld	not evidenced	not evidenced	public	application traffic
TCP · port withheld	administrator surface; identifier withheld	not evidenced	not evidenced	public	service administration
Protocol and port: withheld	discovery service; identifier withheld	public listener verified	not evidenced	blocked at the host by a runtime rule	service discovery
UDP · port withheld	VPN data path; identifier withheld	not evidenced	not evidenced	not evidenced	encrypted remote access

TCP · 80	APPROVED
TCP · 443	APPROVED
TCP · 22	ACCEPTED AT CLOSEOUT
TCP · port withheld	ACCEPTED RISK
TCP · port withheld	PRIVATE-ACCESS CANDIDATE; RESIDUAL RISK
Protocol and port: withheld	RUNTIME RESTRICTION APPROVED; PERSISTENCE PENDING
UDP · port withheld	APPROVED WHEN REQUIRED

A listener list alone cannot prove every provider, container, address-family, or network path. This report does not present the firewall as universal.

Alerts, Logging & 14-Day Snapshot

BOUNDED EVIDENCE WINDOW

Historical snapshot · Available local logs across the 14 days ending at closeout.

530,700 available authentication events reviewed	**181,448** failed or invalid SSH attempts observed	**0** successful root SSH logins found in the available window
0 successful SSH password logins found in the available window	**156** Fail2Ban ban events recorded	**VERIFIED** Telegram alert delivery for the main case was verified at closeout. Scheduled alert checks were active at closeout.

WHAT BECOMES VISIBLE

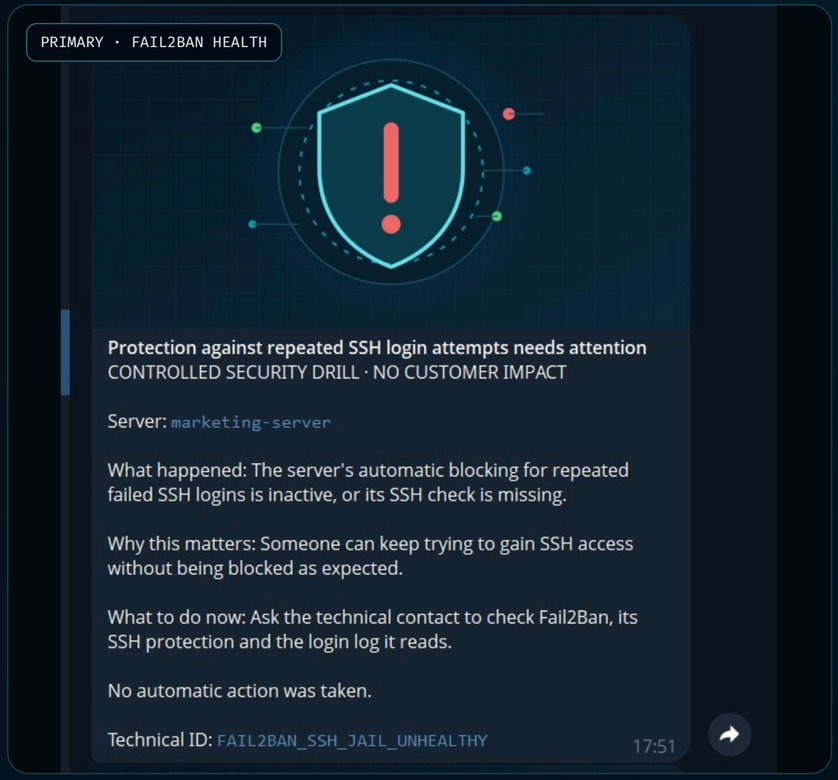
What became visible from the available history: heavy public SSH noise, whether successful root or password logins appeared, and how often Fail2Ban ban events were recorded.

The 14-day snapshot describes available history. Separately, the alert baseline was initialized from the approved current state without replaying old brute-force noise into Telegram.

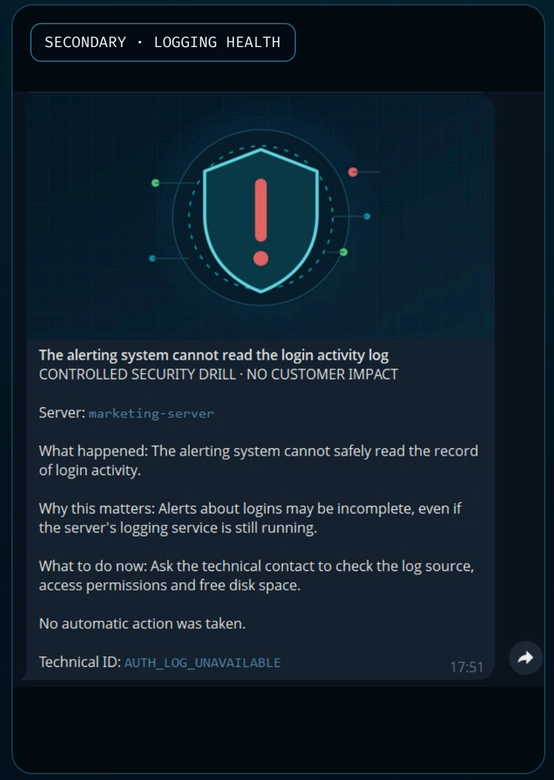
This was a surface review of available local logs, not forensics. Missing or rotated logs limit the view, and zero observed successes do not prove that an earlier compromise never occurred.

Alerts make important changes visible for review. The base engagement did not include an always-on investigation team, ongoing triage, or incident response.

PRIMARY · FAIL2BAN HEALTH



SECONDARY · LOGGING HEALTH



SEPARATE CONTROLLED VALIDATION · MARKETING-SERVER

PRIMARY PROOF · Fail2Ban component-health alert in native Telegram dark mode. SECONDARY PROOF · Authentication-log readability alert. Separate controlled validation · marketing-server · No customer impact. These screenshots confirm current alert presentation and delivery only; they are not evidence from the anonymized production case.

An alert or a change from the approved baseline is a reason to review evidence, not proof of an attack.

Safe Update & Reboot Plan

SECURITY-ONLY POLICY CONFIGURED

Updates are safest when every change has a recovery gate and a measurable stop condition.

CURRENT POLICY

POLICY CONFIGURED · Security-only automatic updates were configured and automatic reboot was disabled.

MAINTENANCE STILL REQUIRED

MAINTENANCE STILL REQUIRED · A reboot was required at closeout. Package and reboot work was not completed during the base pass.

Maintenance window · Not scheduled in this case.

SAFE MAINTENANCE SEQUENCE

1. **Recovery gate**
   Confirm who can recover access, what backup or rollback artifact exists, and who can approve a stop before changing the server.
2. **Health baseline**
   Record how the application, data path, dependencies, ports, and outside health checks behave before maintenance.
3. **One reversible stage**
   Change one package, service, container, database step, or reboot stage inside the approved window.
4. **Validate or stop**
   Recheck administrator access, workload health, public exposure, data paths, and alerts. Roll back the stage if measurable health becomes worse.

NOT CLAIMED

CLOSEOUT LIMIT · The reboot was not completed and a fully patched post-reboot state was not confirmed.

This sequence reduces maintenance risk; it cannot remove every failure mode or promise a successful recovery.

Residual Risks & Recommended Next Steps

WHAT STILL NEEDS A DECISION

HIGH	Persistent firewall rules were incomplete, so the long-term exposure policy still required a separate owner-approved change.
HIGH	Some application and administrator entry points remained directly public by owner decision.
MEDIUM	A recovery path and database dump existed, but recovery was not proven through an actual restore.
MEDIUM	One discovery-service restriction existed only in the running firewall state at closeout, not as a finished persistent policy.
MEDIUM	Ongoing alert review and response were outside this engagement.
MEDIUM	Package and reboot maintenance remained separate work requiring a maintenance window.

RECOMMENDED NEXT STEPS

- RECOMMENDED · Build and validate the persistent firewall policy around the approved exposure register.
- RECOMMENDED · Review container-published ports and create a Docker exposure cleanup plan where containers bypass the expected host view.
- RECOMMENDED · Run a controlled backup restore drill and record the recovery time, dependencies, and result.
- RECOMMENDED · Schedule the staged package and reboot maintenance plan with owner-approved stop conditions.
- RECOMMENDED · Define who reviews alerts, how quickly important changes are checked, and when an incident specialist is needed.
- RECOMMENDED · Use a 30-day exposure watch to review new listeners, service identity changes, wider allowed sources, and new firewall allow rules.

RECOMMENDATION BOUNDARY

These are recommended next decisions, not controls already delivered. Commercial scope and price are deliberately separate from this report.

Handoff & Operator Offboarding

The owner keeps control of the server and the evidence.

DOCUMENTS AND OWNERSHIP RETAINED

- The owner retains control of administrator access and recovery decisions.
- The alert recipient and delivery boundary were documented. Ongoing investigation, triage, and incident response were not included.
- Before → After, exposure, change, validation, and residual-risk records were assembled for handoff.
- Credentials, private keys, raw logs, and identifying network or access details are omitted from this public artifact.

SUPPORT BOUNDARY

During the agreed support window, support covers regressions caused by the implemented base controls. New services or ports, application incidents, provider problems, and ongoing alert review require separate scope.

EXACT OFFBOARDING STATE

PENDING OWNER DECISION

POST-CLOSEOUT OPERATOR VPN PEER REMOVAL · PENDING OWNER DECISION. Removal was not authorized or evidenced.

WHAT OPERATOR OFFBOARDING MEANS

Engagement-specific operator access is the only access in scope for operator offboarding.

Any client-owned employee VPN peers remain under the owner's control. Offboarding applies only to engagement-specific operator access.

A pending item remains visible until the owner authorizes it and completion evidence exists.

CLOSEOUT PRINCIPLE

Access, evidence, residual risk, and next decisions should remain understandable without relying on the operator.