

ISSUE OF OCTOBER 31, 2026 · WEEK OF OCT 25-31

MAG212 CYBER

WEEKLY INTELLIGENCE



UNDERSTAND THE THREAT. BUILD THE DEFENSE.

CYBERSECURITY / NETWORKING / AI & TECHNOLOGY

EL MOSTAFA OUCHEN
cyber.mag212.com

EDITOR'S BRIEFING · OCTOBER 25–31, 2026

This week, trust was the attack surface.

This was a week about borrowed trust. In the stories that mattered most, attackers did not break the strongest control. They stood where that control already trusted them. A signing service signed because an internal caller asked. A firewall obeyed its own management plane. An editor extension arrived, likely by auto-update, under a familiar publisher ID. A sign-in page was genuine and the MFA prompt was real, but the session belonged to someone else. The common defect is not a missing product. It is a boundary that checks who is asking but never what is being asked for.

The second thread is the management plane at the edge. Firewall administration, overlay-network sockets, ERP servlets and store admin panels all sit one hop from the internet or from a single compromised device. Where those planes were fenced off, the same flaws scored lower and reached fewer victims. Exposure, not the bug itself, decided who had a bad week.

Third, AI now sits on both sides of the ledger. Models helped find this week's kernel and runtime bugs. Intruders reportedly used agentic tooling and automation to enumerate, launder and exploit. Investors, meanwhile, asked what all the AI spending actually returns. Defenders should treat machine-speed activity as a detection signal and AI spend as a governed budget line.

Finally, speed. Exploitation, laundering and reinfection ran on minutes and hours. Many organisations still verify on days and quarters. Next week's work is unglamorous: verify running versions, clean up what patching leaves behind, and test the controls you assume are independent.

THIS WEEK'S THEMES

- **Trust without verification.** Signers, editors and sign-in pages did exactly what authenticated callers asked, so controls must inspect intent as well as identity.
- **Edge management planes.** Administrative interfaces on firewalls, overlay networks and business apps decided real-world exposure more than the underlying bugs did.
- **AI on both sides.** Models found two of the week's critical bugs (kernel and Brotli) and attackers reportedly automated intrusions, while markets questioned the bill for the AI build-out.

BY THE NUMBERS

~\$6.4B

stolen from Binance, most of it in about 20 minutes (tracker estimates range from USD 6.36B to 6.43B)
1,2

USD 2.7B-2.85B

of the Binance haul frozen or seized, almost all of it stablecoins
1,2

953

stores, mostly Magento, that Sansec ties to one CMS-block loader operator since July 2025
23

~53 min

for Anthropic's proof of concept to leak a kernel pointer and reach root command execution
39

618

SkyW4lker sandbox analyses ANY.RUN logged through October 21
41

-2.86%

Nasdaq Composite close on October 30, its worst day since June
44,45

INSIDE THIS ISSUE

Twelve stories. Twelve field guides.

Each feature summarizes verified, attributed reporting, then a technical page turns it into a defensive reference architecture, the controls behind it, and steps to verify those controls on systems you are authorised to test.

01	Binance loses billions in minutes	p. 4	07	Patched Magento stores keep skimming	p. 16
	CRYPTO / INCIDENT RESPONSE			E-COMMERCE / WEB SECURITY	
02	Chainalysis discloses internal-tool intrusion	p. 6	08	Brotli bug reportedly added to CISA KEV	p. 18
	DATA BREACH / IDENTITY			RUNTIME / OPEN SOURCE	
03	PHP2Shell turns firewalls into footholds	p. 8	09	Kernel TCP race reaches remote root	p. 20
	NETWORK DEFENSE / ACTIVE EXPLOITATION			LINUX / VULNERABILITY RESEARCH	
04	Tailscale patches Tailworm SSH and Serve flaws	p. 10	10	SkyW4lker phishes Microsoft 365 device codes	p. 22
	ZERO TRUST / REMOTE ACCESS			IDENTITY / PHISHING	
05	Oracle EBS flaw draws early probes	p. 12	11	AI spending fears sink Nasdaq	p. 24
	ENTERPRISE APPLICATIONS / ERP			MARKETS / AI BUSINESS	
06	Backdoored Claude Code builds hit Cursor	p. 14	12	OpenAI reportedly trims funding target	p. 26
	SOFTWARE SUPPLY CHAIN / ENDPOINTS			AI BUSINESS / REPORTED DEVELOPMENT	
			+	Weekly roundup · What to watch · Defender tips	p. 28

How to read this edition. Reported facts are attributed to their sources; numbers in brackets refer to the source list at the back. “Why it matters”, actions, diagrams and checks are original MAG212 defensive interpretation, not incident findings. Architecture diagrams are illustrative reference designs, not reconstructions of any victim’s systems. Commands and queries are read-only examples that were not executed against production systems; confirm syntax against vendor documentation. Editorial photographs are AI-generated conceptual illustrations.

CRYPTO / INCIDENT RESPONSE · STORY 01

Binance loses billions in minutes

Attackers got Binance systems to sign valid withdrawals across 10-11 chains, and freezes clawed back under half within hours.

Theft Oct 29, 2026 (from about 20:05 UTC); updates through Oct 31 | Sources:^{1,2,3,4}



AI-GENERATED EDITORIAL ILLUSTRATION · CONCEPTUAL, NOT INCIDENT EVIDENCE

REPORTED FACTS

TRM Labs puts the October 29 theft at USD 6.36B across 10 chains, most of it moved in about 20 minutes from 20:05 UTC¹. Elliptic counts USD 6.43B across 11 chains, adding NEAR² and Chainalysis says about USD 6.4B³. Binance first blamed a compromised DevOps engineer's laptop that reached a service container and submitted unauthorized withdrawals, with no evidence that private keys were exposed. It later reported "additional points of breach"^{2,4}. On Ethereum, 50 validly signed EIP-7702 authorizations turned a hot wallet into an attacker-controlled sweeper^{1,2}. Issuers and L2 councils froze or seized USD 2.7-2.85B^{1,2}. TRM (high confidence) and Chainalysis attribute the theft to North Korea's TraderTraitor, while Elliptic calls that "likely". No government has confirmed attribution².

WHY IT MATTERS

Elliptic's reading holds the lesson: the attacker did not need to steal keys, only to make Binance's own systems sign². CEO Richard Teng said the EIP-7702 activity "did not pass through our normal approval controls"². That suggests the policy checks covered transfers but not delegation payloads. A signer that signs whatever an authenticated internal service submits is functionally a key leak. Freezes worked almost entirely on stablecoins (94%, per Elliptic). Apart from small L2 council seizures, the native ETH, and all of the BTC, stayed with the attacker^{1,2}.

DEFENDER ACTIONS

- 01** Decode and policy-check every signable payload, including EIP-7702 authorizations and delegatecall, before release.
- 02** Enforce per-wallet velocity limits and a cross-chain circuit breaker inside the signer itself.
- 03** Keep pre-agreed freeze contacts and evidence packs ready for stablecoin issuers and L2 councils.

ASK YOUR TEAM

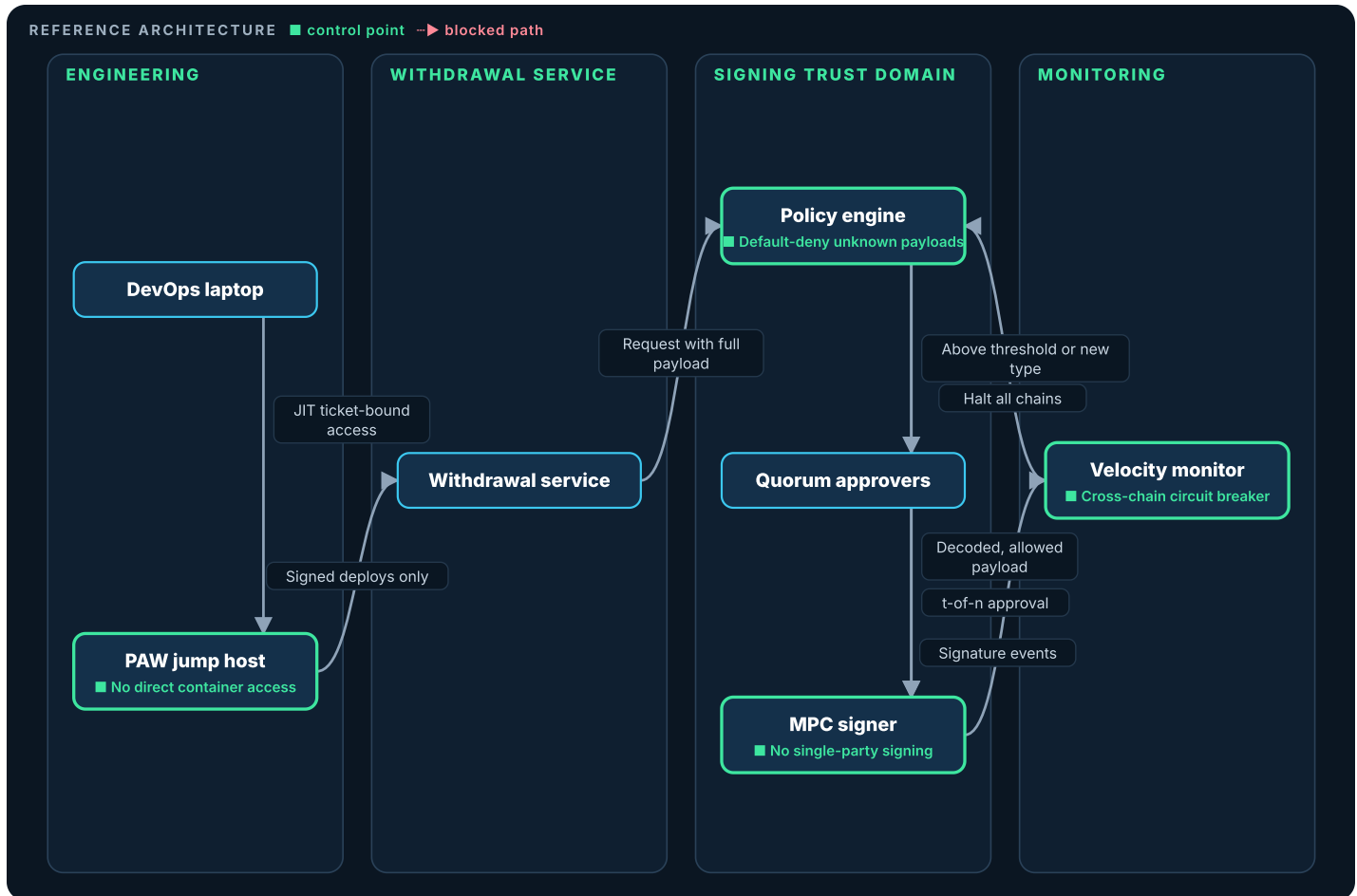
Which payload types can our signer approve without a human ever seeing the decoded intent?

Evidence boundary. Binance has published no root cause, the "additional points of breach" are undisclosed, and attribution remains a private-sector assessment.

TECHNICAL PAGE 01 · DEFENSIVE ARCHITECTURE

Gate everything the signer signs

Custody engineering | Independent signing policy



CONTROLS EXPLAINED

Payload-aware policy engine

Run the policy engine in a separate trust domain, ideally an HSM, enclave or MPC co-signer, and have it decode every signable object before a signature is released. That covers transfers, approve and permit calls, EIP-7702 authorizations, setCode delegations and multisig delegatecall. Anything it cannot parse is denied. On exchange hot wallets, block EIP-7702 authorizations unless a change-managed exception exists.

Quorum and limits inside the signer

No single service or credential should be able to produce a signature. Above defined thresholds, require t-of-n approvals from people on separate devices, each of whom independently re-renders the decoded transaction. Enforce value and velocity limits per wallet, chain, asset and time window inside the signer, not the caller. Halt every chain when anomalies appear on several at once.

Isolated build and deploy path

Elliptic notes that both Bybit and Binance trace back to a developer or DevOps endpoint². DevOps laptops should never reach signing containers directly. Route administration through privileged-access workstations with just-in-time, ticket-bound access. Ship only signed container images through admission control. Keep cold and warm tiers on separate signing stacks, each with its own admin identities.

VERIFICATION STEPS

1. Export the signing-policy configuration and confirm that EIP-7702, approvals and delegatecall are explicitly handled or denied.
2. On a testnet or staging signer only, submit a crafted EIP-7702 authorization and confirm rejection or quorum escalation.
3. Review 90 days of signer logs for signature requests with no linked ticket or approval record.
4. Diff the hot-wallet destination allow-lists against approved change records.
5. Run a tabletop: a DevOps laptop is compromised. Time the all-chain halt and the contact with each stablecoin issuer.

Illustrative MAG212 design. Binance's signing architecture is undisclosed and is not depicted here. Context:^{1,2,3}.

DATA BREACH / IDENTITY · STORY 02

Chainalysis discloses internal-tool intrusion

An attacker reached internal tools and customer contact data, but Chainalysis says it found no evidence of access to investigations, credentials or session tokens.

Notice Oct 30, 2026 (21:14 UTC); reporting Oct 31 | Sources:^{5,6}



AI-GENERATED EDITORIAL ILLUSTRATION · CONCEPTUAL, NOT INCIDENT EVIDENCE

REPORTED FACTS

Chainalysis's public notice, dated October 30, says the company was "recently the target of a cybersecurity incident, similar to many other tech platforms in recent weeks." It found no evidence of access to investigation content, authentication credentials or session tokens⁵. It says the incident is unrelated to the Binance theft and that it has notified all customers⁵. The Block quotes the customer notice: an unidentified hacker used "offensive agentic techniques" this month to reach Chainalysis systems and internal tools. The hacker accessed user IDs, full names, email addresses and organization role labels for provisioned users⁶. It has not disclosed the entry point, detection date or number of affected customers. It advises customers to enable 2FA and watch for unexpected password-reset or authentication prompts⁶.

WHY IT MATTERS

The names, emails and role labels of investigators, compliance staff and law-enforcement users make a ready-made target list for spear-phishing and help-desk impersonation. An attacker needs no password when a caller can name a real colleague and a real account. The "agentic" framing also points to intrusions that enumerate tools at machine speed, which human-paced alerting can miss. The claim that the incident is unrelated to Binance comes from Chainalysis and has not been independently verified.

DEFENDER ACTIONS

- 01** Warn exposed users to expect targeted phishing, fake reset prompts and impersonation of known colleagues.
- 02** Require out-of-band identity verification before any MFA reset, password reset or privileged access change.
- 03** Baseline per-identity request rates on internal tools and alert on sequential enumeration or bulk export.

ASK YOUR TEAM

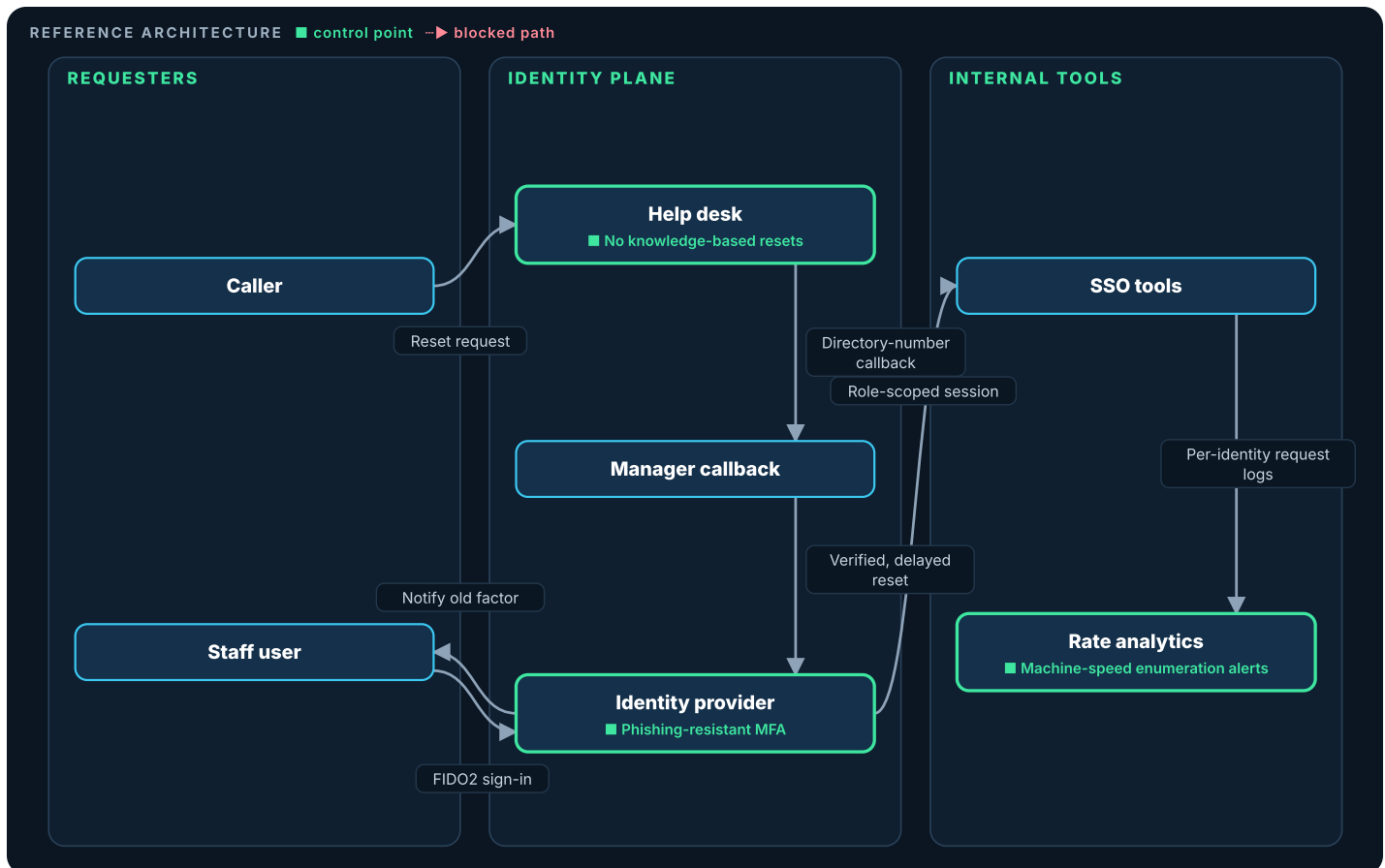
Would our help desk reset a factor for a caller who knows a real name, email address and job title?

Evidence boundary. The access vector, the dwell time and what the "agentic techniques" actually were are undisclosed, and no independent investigator has confirmed the company's account.

TECHNICAL PAGE 02 · DEFENSIVE ARCHITECTURE

Harden recovery and internal tools

Identity engineering | Help desk and automation detection



CONTROLS EXPLAINED

Phishing-resistant MFA, support staff first

CISA calls FIDO/WebAuthn or PKI-based MFA the "gold standard." It recommends rolling it out first to the help desk and IT administrators, and prioritising email, remote access and identity servers⁷. Extend it to every internal tool through SSO and remove local accounts. Treat any internal tool that cannot federate as a scheduled exception with a named owner and an end date.

Verified, observable account recovery

Never reset a password or MFA factor on knowledge-based answers: exposed names, emails and roles make those answers easy to give. Require a video or in-person ID check, a manager callback to a directory number, and a waiting period that notifies the old factor. Log every reset with its operator, verification method and approver, and review the log every week.

Automation-aware access monitoring

Set per-identity baselines for internal APIs and admin consoles. Alert on sequential enumeration such as iterating user IDs, on new API tokens or OAuth grants, on headless user agents, and on sessions from new ASNs. Restrict bulk export of user directories. Run quarterly access reviews and expire unused access, which shrinks what an automated intruder can harvest.

VERIFICATION STEPS

1. Run an IdP report of admins, help-desk staff and internal-tool users who lack phishing-resistant factors.
2. Review 30 days of resets and confirm each records the verification method, the approver and old-factor notification.
3. Run an authorised, scripted mystery-shopper call, with no real reset, to test whether staff follow the procedure.
4. Search internal-tool logs for bulk listing or export events by human accounts.
5. List API tokens and OAuth grants older than policy allows, and assign an owner to each.

ENTRA ID | KQL | READ-ONLY (illustrative)

```
// Illustrative: password resets, last 30 days
AuditLogs
| where TimeGenerated > ago(30d)
| where OperationName has "reset"
| project TimeGenerated, OperationName,
InitiatedBy, TargetResources
```

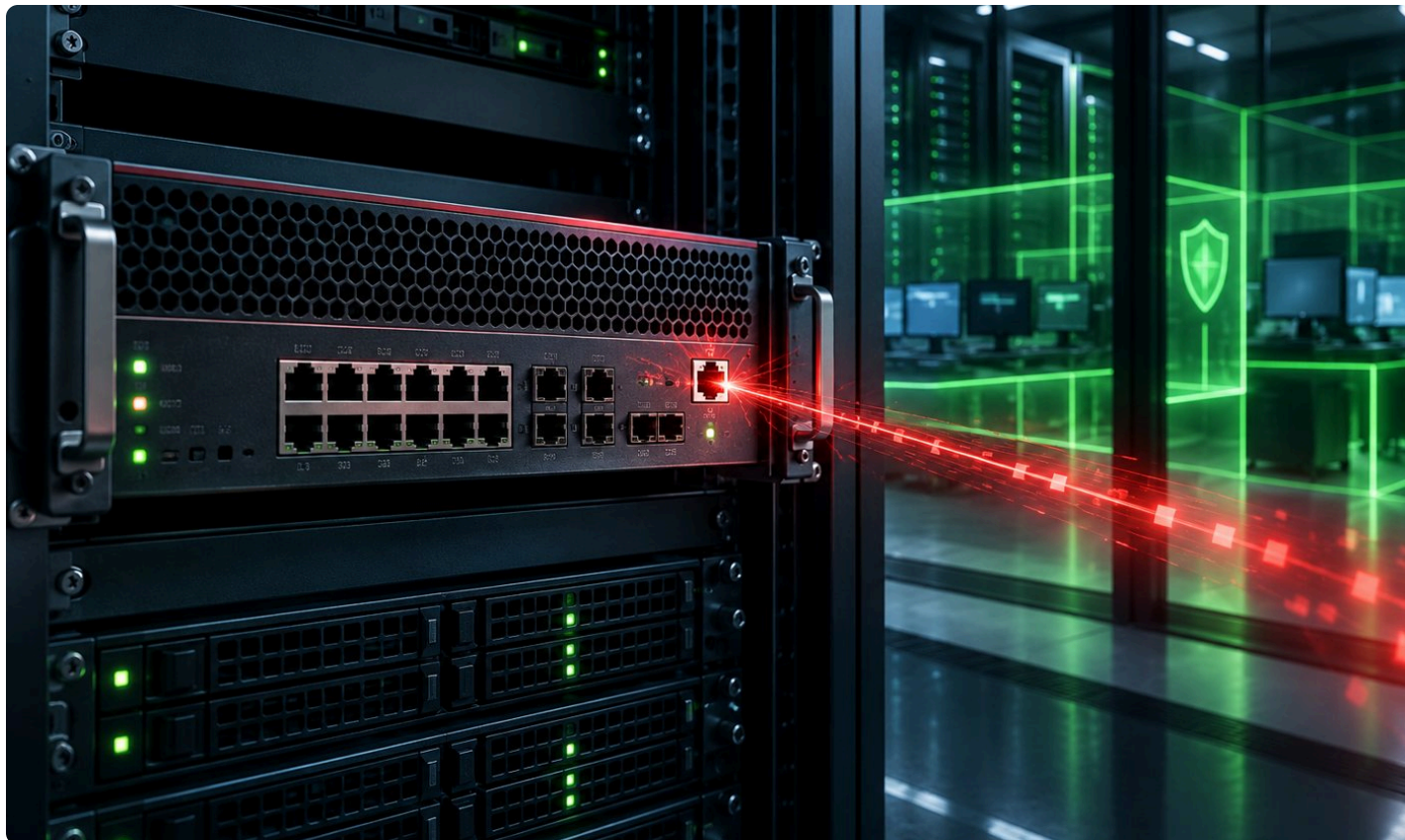
Illustrative MAG212 design. It makes no claim about Chainalysis procedures, and the access vector is undisclosed. Context: ^{5,6,7}.

NETWORK DEFENSE / ACTIVE EXPLOITATION · STORY 03

PHP2Shell turns firewalls into footholds

Attackers chained critical PHP flaws in PAN-OS management interfaces with a kernel bug for root, and CISA reportedly set a three-day deadline.

Advisory Oct 21; hotfixes Oct 25-29; KEV Oct 26; Unit 42 update Oct 29, 2026 | Sources: ^{8,9,10,11}



AI-GENERATED EDITORIAL ILLUSTRATION · CONCEPTUAL, NOT INCIDENT EVIDENCE

REPORTED FACTS

Palo Alto Networks rates CVE-2026-109618 as CVSS 4.0 9.2 Critical, with exploit maturity "Attacked." Hotfixes released October 25-29 fix both it and CVE-2026-109619 across PAN-OS 10.2, 11.1, 11.2, 12.1 and 12.2⁸. Only the management web UI and XML API are affected, plus any dataplane interface that carries a management profile. GlobalProtect is not affected⁸. Unit 42 confirmed exploitation of internet-exposed management interfaces. It independently verified tooling that chained PHP2Shell with a Linux kernel privilege escalation to gain root. About 0.02% of the installed base was exposed⁹. Dream Research reported 25 compromised servers and theft of LDAP service-account credentials, and identified the kernel bug as CVE-2026-46300¹⁰. CISA added both CVEs to KEV on October 26 with an October 29 due date, according to TNW¹¹.

WHY IT MATTERS

Attackers compromised the device that enforces network policy through its own administrative plane, which PAN says is not internet-exposed by default⁸. The small exposed population shows that management-plane hygiene, not dataplane defence, decided who was hit. PAN's own scoring falls from 9.2 to 5.2 when management sits behind a jump box⁸. Because LDAP service credentials were stolen, patching alone does not close an incident on a device that was already exposed¹⁰.

DEFENDER ACTIONS

- 01** Compare every firewall and Panorama build against the fixed-hotfix table for its PAN-OS train.
- 02** Remove internet reachability of management interfaces and management profiles on untrusted dataplane interfaces.
- 03** Treat previously exposed devices as suspect: hunt, rotate LDAP and service credentials, and replace management certificates.

ASK YOUR TEAM

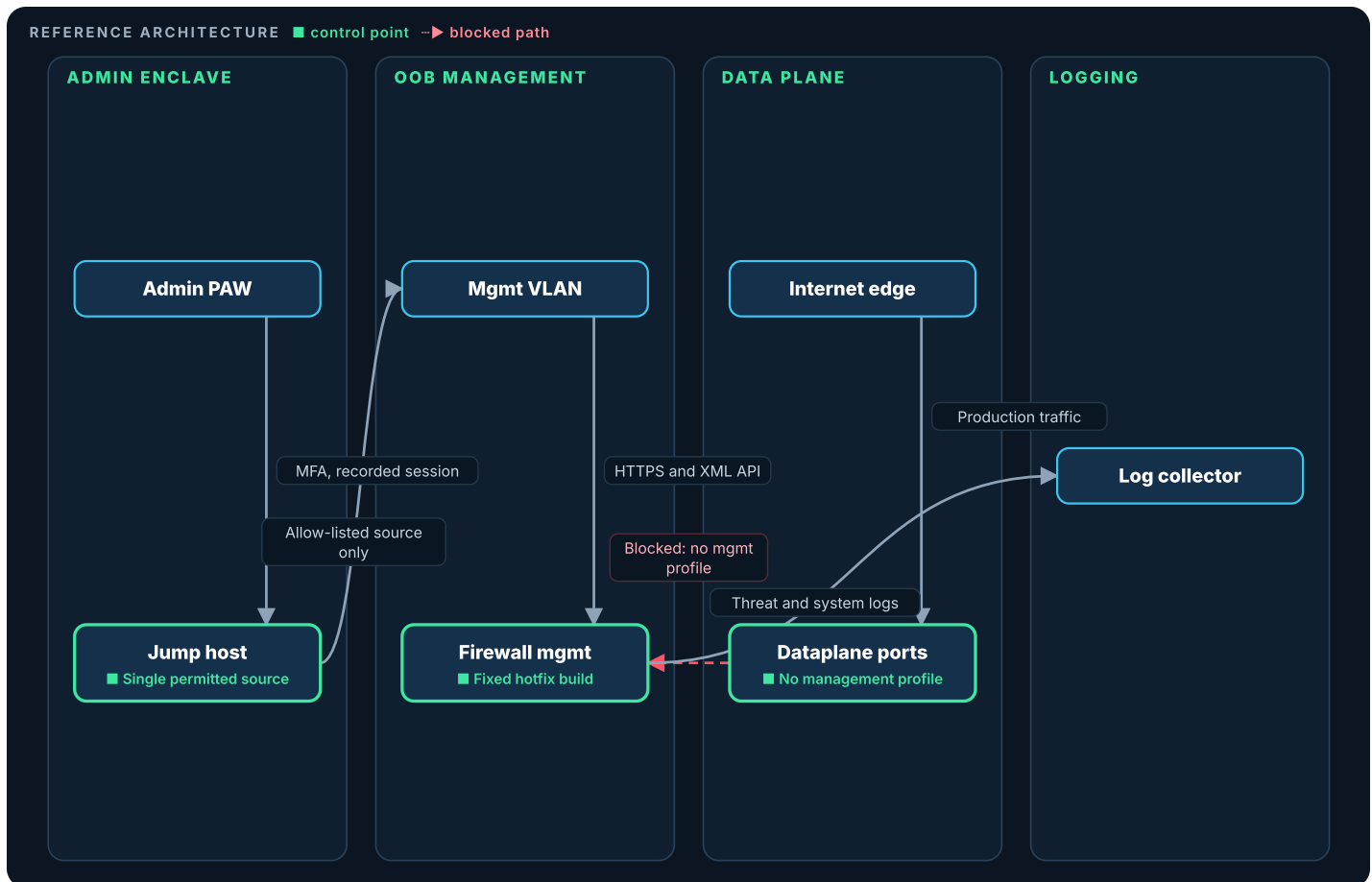
Can anyone reach a firewall login page from the internet, including through a forgotten interface profile?

Evidence boundary. Unit 42 published no IOCs and Dream withheld vendor details. Neither says whether PAN-OS needed its own kernel fix for CVE-2026-46300.

TECHNICAL PAGE 03 · DEFENSIVE ARCHITECTURE

Isolate the firewall management plane

Network engineering | Management versus data plane



CONTROLS EXPLAINED

Out-of-band management access

Put firewall and Panorama management interfaces on a dedicated management VLAN. Make it reachable only from a hardened jump host or privileged-access workstation with MFA and session recording. PAN's advisory lowers the score to 5.2 when access is restricted this way, because the attack then needs an adjacent network instead of the open internet⁸. Review the Permitted IP Addresses on every management interface.

Interface management profile hygiene

The dataplane becomes vulnerable only when a management profile is attached to it⁸. Audit every Layer 3 interface for profiles that enable HTTPS or the XML API, especially temporary exceptions on internet-facing zones. Where inbound management traffic must cross the dataplane, PAN recommends routing it through a dataplane port with a management profile for decryption and Threat Prevention inspection⁸.

Content-based virtual patching and hunting

PAN released threat signatures, including Threat ID 543004, which need Applications and Threats content 9162, 9163, 9164 or later⁸. Confirm your content version. Then run Unit 42's NGFW threat-log query for inbound hits from public IPs, and its Cortex XDR query for suspicious child processes under PHP workers, which can produce false positives⁹. Signatures buy time; only the hotfixes fix the flaw.

VERIFICATION STEPS

1. Run show system info and compare sw-version with the advisory's fixed hotfix for that train.
2. Confirm that app-version is content 9162 or later so the Threat IDs are active.
3. Review the Permitted IP Addresses and every management profile attached to a Layer 3 interface.
4. From an authorised external vantage point, test TCP 443 and 4443 on your public IPs for a login page.
5. Query threat logs for Threat ID 543004 hits from public source addresses since October 20.

PAN-OS | CLI | READ-ONLY (illustrative)

```
# Illustrative; confirm syntax in PAN docs
show system info | match sw-version
show system info | match app-version
# GUI: Device > Setup > Interfaces > Management
# Then review Interface Mgmt Profiles on L3
```

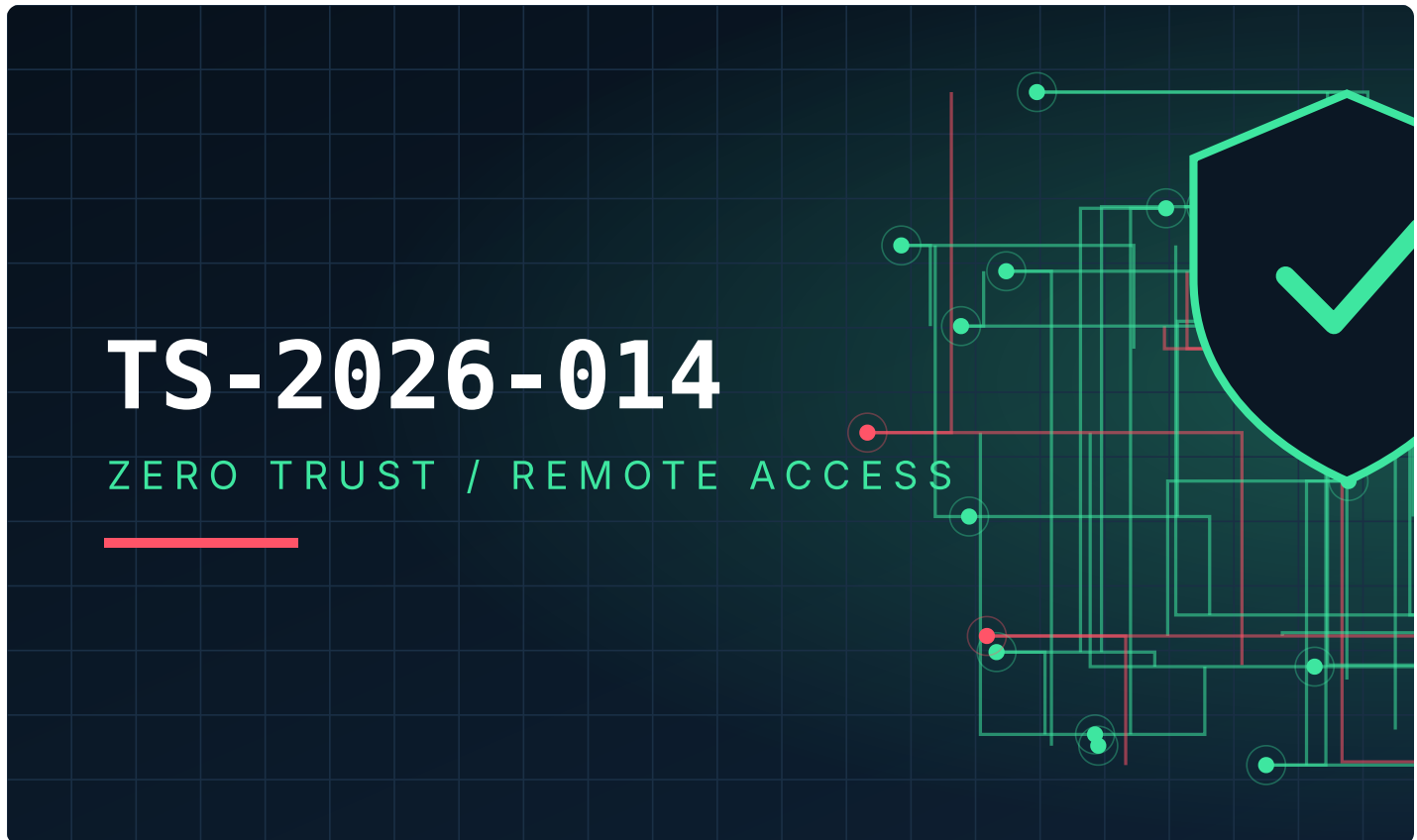
Illustrative MAG212 design, not a depiction of any victim network. The commands are standard PAN-OS syntax, not quoted from the advisory. Context:^{8,9,10}.

ZERO TRUST / REMOTE ACCESS · STORY 04

Tailscale patches Tailworm SSH and Serve flaws

Four bulletins fix root-socket access, memory exhaustion and capability leaks, and every one needs an authenticated tailnet or local foothold first.

Audit Oct 22-24; bulletins dated Oct 26; v1.104.4 released Oct 28, 2026 | Sources: ^{12,13,14}



MAG212 EDITORIAL GRAPHIC · CONCEPTUAL

REPORTED FACTS

Tailscale published bulletins TS-2026-014 to TS-2026-017, all dated October 26. Each lists 1.104.4 or newer as the fix, and none carries a CVE or severity rating¹². TS-2026-014 let peers with forwarding permission reach root-only Unix sockets, such as Docker's or the tailscaled LocalAPI. TS-2026-015 allowed unbounded memory growth that could get tailscaled killed for running out of memory. TS-2026-016 let Serve forwards dial Unix sockets as root. TS-2026-017 leaked app capabilities across HTTP/2 streams¹². Version 1.104.4 shipped on October 28¹³. Researcher Erica Windisch audited v1.104.2 and headscale v0.29.5 on October 22-24. She published 11 findings as "Tailworm" before patches were available, in an attack chain that assumes an already-trusted device¹⁴.

WHY IT MATTERS

None of these flaws is an unauthenticated internet attack, but in a mesh network one trusted device is all an attacker needs. Windisch reported that a rogue policy change reached every SSH-permitted device in under a second. She also captured an enrollment key, because Tailnet Lock is off by default¹⁴. The socket bugs turn the Docker socket or LocalAPI into a route to full node takeover¹². Overlay networks need the same least-privilege and node-admission rigour as firewalls.

DEFENDER ACTIONS

- 01** Upgrade every node to 1.104.4 or later, using the admin console's version filter to find stragglers.
- 02** Where upgrades lag, set `TS_SSH_DISABLE_FORWARDING=1` for tailscaled and restart, as Tailscale advises.
- 03** Enable Tailnet Lock and remove Serve forwards that point at Unix sockets.

ASK YOUR TEAM

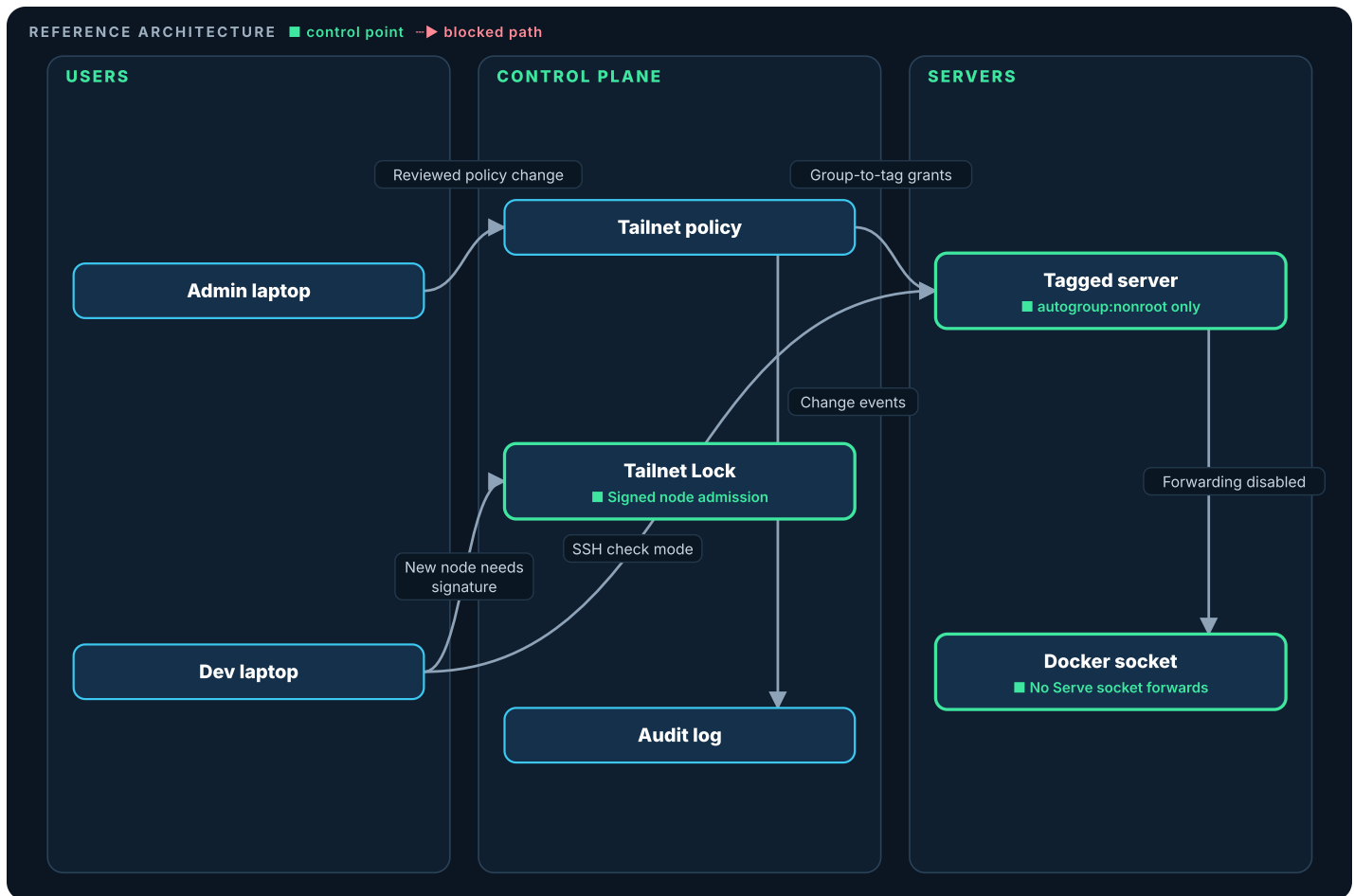
If one laptop on our tailnet were compromised, which nodes could it reach as root?

Evidence boundary. Tailscale lists no CVEs, affected-version floor or credits. The status of a headscale fix and any in-the-wild exploitation are unconfirmed.

TECHNICAL PAGE 04 · DEFENSIVE ARCHITECTURE

Contain a compromised tailnet node

Zero trust networking | Node admission and least privilege



CONTROLS EXPLAINED

Signed node admission

Tailnet Lock requires trusted keys to sign every new node, so a stolen auth key alone cannot add a rogue machine. That blocks the enrollment step in Windisch's chain, which worked because the feature is off by default¹⁴. Pair it with short-lived, pre-approved, tagged auth keys, and review every node addition in the audit log. Treat any unsigned node as an incident.

Least-privilege grants and SSH rules

Replace wildcard rules with specific group-to-tag grants, and land SSH sessions on autogroup:nonroot rather than root. Use check mode with a check period on sensitive tags so users re-authenticate, bearing in mind that it gates login, not what happens afterwards. Allow port forwarding only where a named workflow needs it, because TS-2026-014 required forwarding permission¹².

Socket and Serve hygiene

TS-2026-014 and TS-2026-016 both ended at root-owned Unix sockets¹². Inventory Serve configurations and remove TCP forwards to Unix sockets. Keep the Docker socket off nodes that accept SSH from broad groups, and restrict who can write Serve configuration locally. Fixed clients now run forwarding as the authenticated user and revalidate backends on every connection¹³.

VERIFICATION STEPS

1. Run tailscale version on each node, or filter the admin console Machines list by version.
2. Run tailscale serve status and record any forwards that point at Unix sockets.
3. On hosts awaiting upgrade, confirm the mitigation variable is set in the tailscaled service environment.
4. Run tailscale lock status to confirm Tailnet Lock is enabled and the trusted keys are current.
5. Review audit logs since October 20 for node additions, policy changes and auth-key creation.

LINUX | BASH | READ-ONLY (illustrative)

```
# Illustrative; confirm syntax before use
tailscale version
tailscale serve status
tailscale lock status
systemctl show tailscaled -p Environment
```

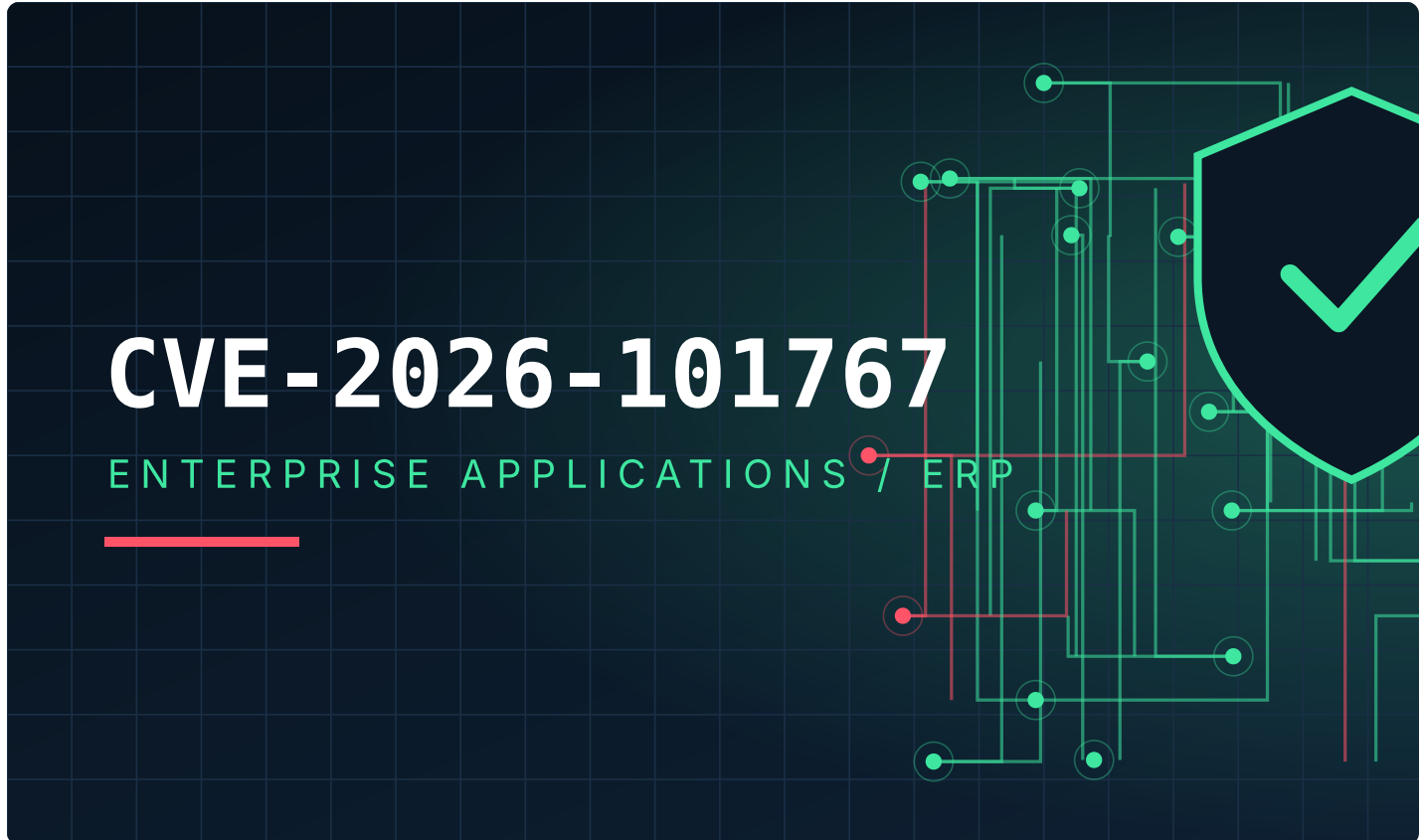
Illustrative MAG212 design, not any victim tailnet. The feature descriptions come from general product knowledge. Context: ^{12,13,14}.

ENTERPRISE APPLICATIONS / ERP • STORY 05

Oracle EBS flaw draws early probes

An unauthenticated EBS servlet flaw chains SQL execution as APPS into OS commands, and honeypots logged probing within a week.

Reported to Oracle Jul 24; CPU Oct 20 (Rev 2 Oct 26, unrelated); probes Oct 27, 2026 | Sources: ^{16,17,18}



MAG212 EDITORIAL GRAPHIC • CONCEPTUAL

REPORTED FACTS

Oracle's October 2026 Critical Patch Update, released October 20, fixes CVE-2026-101767. Oracle credits Horizon3.ai researchers Brandon Peterson, Jimi Sebree and Noah King¹⁶. Rescana reports a CVSS 3.1 score of 9.8 for the Application Object Library (Core), which can be exploited over HTTP without authentication in supported EBS releases 12.2.3-12.2.15. Earlier releases are untested but likely affected¹⁷. The Hacker News, describing Horizon3's findings, calls it SQL injection in the TCF servlet /OA_HTML/AppsTCFServer. The injected SQL runs as the APPS database user, and OS commands then run as the EBS application account¹⁸. Defused Cyber's decoys recorded exploratory attempts on October 27¹⁸. The October 26 revision of the CPU changed credits and Siebel versions, not this CVE¹⁶.

WHY IT MATTERS

EBS holds payroll, HR, financial and procurement records. Its exploitation history, including CIOp's use of CVE-2025-61882, makes fast weaponisation plausible¹⁸. Shadowserver counted about 950 internet-exposed instances in July¹⁹ but Horizon3 notes that internal instances can be exploited from any network that reaches the servlet¹⁸. So far the activity is probing, not confirmed compromise, and "under active attack" headlines go beyond the evidence.

DEFENDER ACTIONS

- 01** Apply the October 2026 CPU to production, DR, test and clone EBS instances, following MOS Note KA923.
- 02** Remove AppsTCFServer from the EBS URL firewall allowlist and restrict the web tier to trusted networks.
- 03** Hunt for unauthenticated POSTs to AppsTCFServer and for oracle-account shells spawned by Concurrent Manager.

ASK YOUR TEAM

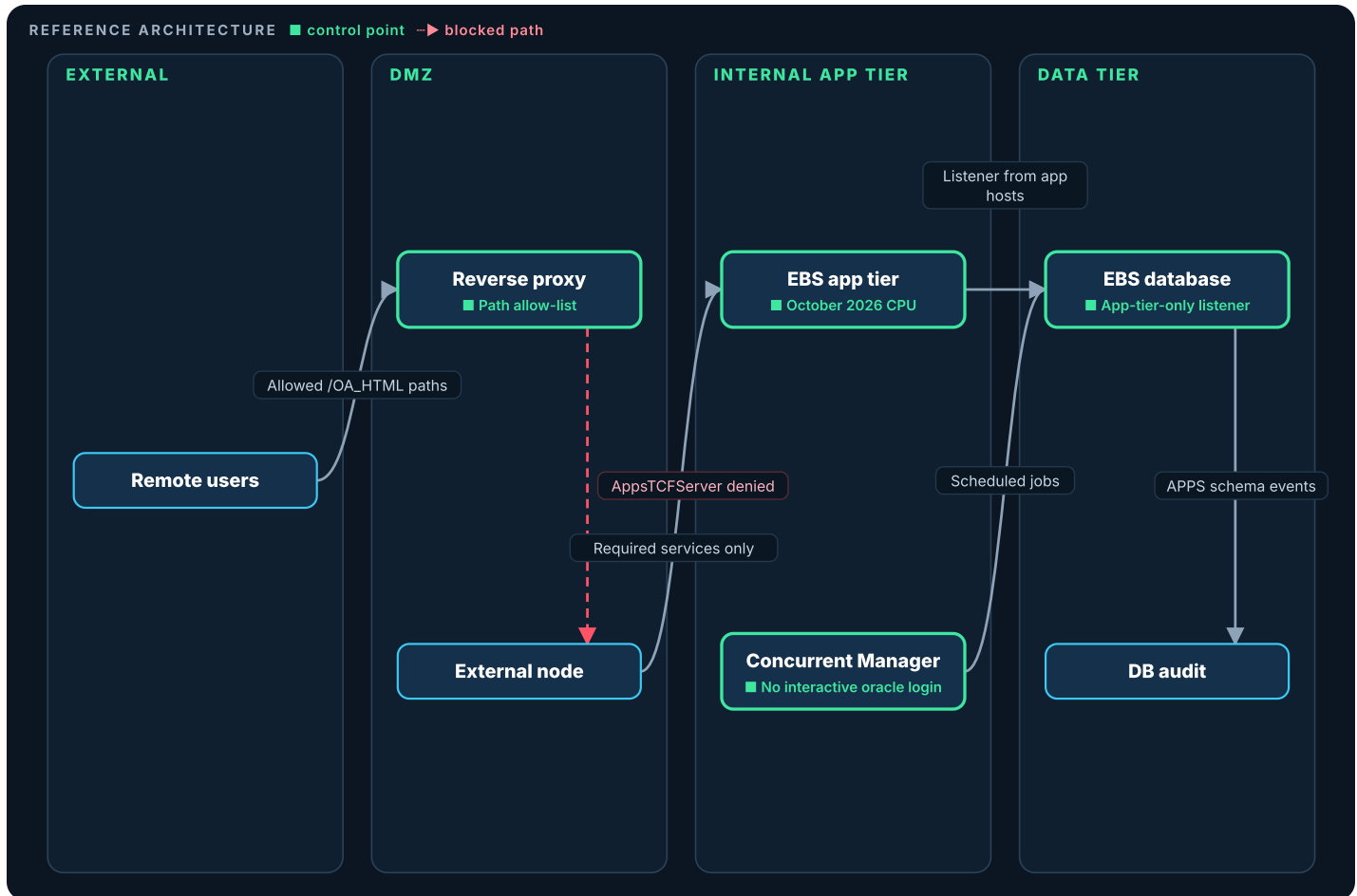
Which internal networks can reach our EBS web tier, and does anyone still need AppsTCFServer?

Evidence boundary. No confirmed compromises, NVD score or KEV listing were found, and the Previdian telemetry and GitHub proof-of-concept claims remain unverified.

TECHNICAL PAGE 05 · DEFENSIVE ARCHITECTURE

Fence the ERP web tier

Application security | Tiered EBS exposure



CONTROLS EXPLAINED

Path allow-listing at the edge

If EBS must be reachable from outside, publish only DMZ external nodes behind a reverse proxy or WAF. The proxy should allow only the specific /OA_HTML paths users need and explicitly deny /OA_HTML/AppsTCFServer. As reported, Horizon3 advises removing the servlet (oracle.apps.fnd.tcf.SocketServer) from the EBS URL firewall allowlist and restricting the web tier to trusted networks¹⁸.

Tier segmentation and account hardening

Let only application-tier hosts reach the database listener. Give the oracle OS account no interactive login and tightly restricted outbound access. That limits the step from SQL running as APPS to commands running as the application account¹⁸. Apply the same rules to DR, test and clone environments, which often lag behind production on patching and segmentation.

Database and host telemetry

Enable auditing on the APPS schema and forward it to the SIEM. Reported indicators include POSTs to AppsTCFServer that instantiate GanttDataServer, SQL reconnaissance of the database version, current user and directory objects, unexpected files in \$APPLPTMP, and the oracle account spawning /bin/sh through Concurrent Manager¹⁸. Correlate web, database and process events rather than alerting on each in isolation.

VERIFICATION STEPS

1. Confirm the patch level through adop patch history or the patch-check queries documented in MOS.
2. Grep exported copies of web-tier or proxy access logs for AppsTCFServer requests and POSTs.
3. Check that the URL firewall configuration no longer allowlists AppsTCFServer.
4. From an authorised external vantage point, confirm the EBS hostnames are unreachable, and send no payloads.
5. List files in \$APPLPTMP modified since October 20 and review any you do not recognise.

LINUX | BASH | READ-ONLY (illustrative)

```
# Illustrative; run on exported log copies
grep -c 'AppsTCFServer' access_log*
grep 'POST /OA_HTML/AppsTCFServer' access_lo
g*
ls -lt "$APPLPTMP" | head -20
```

Illustrative MAG212 design based on vendor and Horizon3 guidance, not a depiction of victim systems. Context: ^{16,17,18}.

SOFTWARE SUPPLY CHAIN / ENDPOINTS · STORY 06

Backdoored Claude Code builds hit Cursor

Two tampered extension builds planted an SSH key, a reverse tunnel and persistence during a roughly 11-hour marketplace window.

Reported by Cursor Oct 29; Microsoft analysis Oct 30, 2026 | Sources:²¹



AI-GENERATED EDITORIAL ILLUSTRATION · CONCEPTUAL, NOT INCIDENT EVIDENCE

REPORTED FACTS

Microsoft reports that Cursor's extension marketplace served tampered anthropic.claude-code builds 2.1.312 and 2.1.313. Cursor puts the exposure window at about 2:27 AM to 1:35 PM PDT²¹. Injected JavaScript ran when the module loaded. It collected host details and the names, though not the values, of up to 40 secret-like environment variables. It then appended an "svc-telemetry" Ed25519 key to authorized_keys, opened a reverse SSH tunnel to 134.209.82.225 and wrote platform-specific persistence²¹. Microsoft says the package never appeared on the Visual Studio Marketplace or npm. Anthropic told Microsoft its systems were not compromised²¹. Cursor took the builds down server-side but says that does not remove artifacts already on devices. On most macOS and Windows hosts, errors and admin-permission requirements blocked SSH access²¹.

WHY IT MATTERS

A familiar publisher ID and consecutive version numbers made this look like a routine update. Microsoft's "installed or auto-updated" wording implies that some machines received it without any user action²¹. Uninstalling the extension does not remediate a host, because the keys, LaunchAgents, cron entries and scheduled tasks live outside the extension directory. Collecting secret names maps where credentials live, ready for a later visit. How the builds reached the marketplace is still unexplained.

DEFENDER ACTIONS

- 01** Identify hosts that installed or auto-updated to 2.1.312 or 2.1.313, and preserve evidence before cleanup.
- 02** Remove the svc-telemetry key only after confirming its fingerprint, then remove persistence and .stk_ files.
- 03** Restrict extensions to approved publishers and add an installation cooldown for new versions.

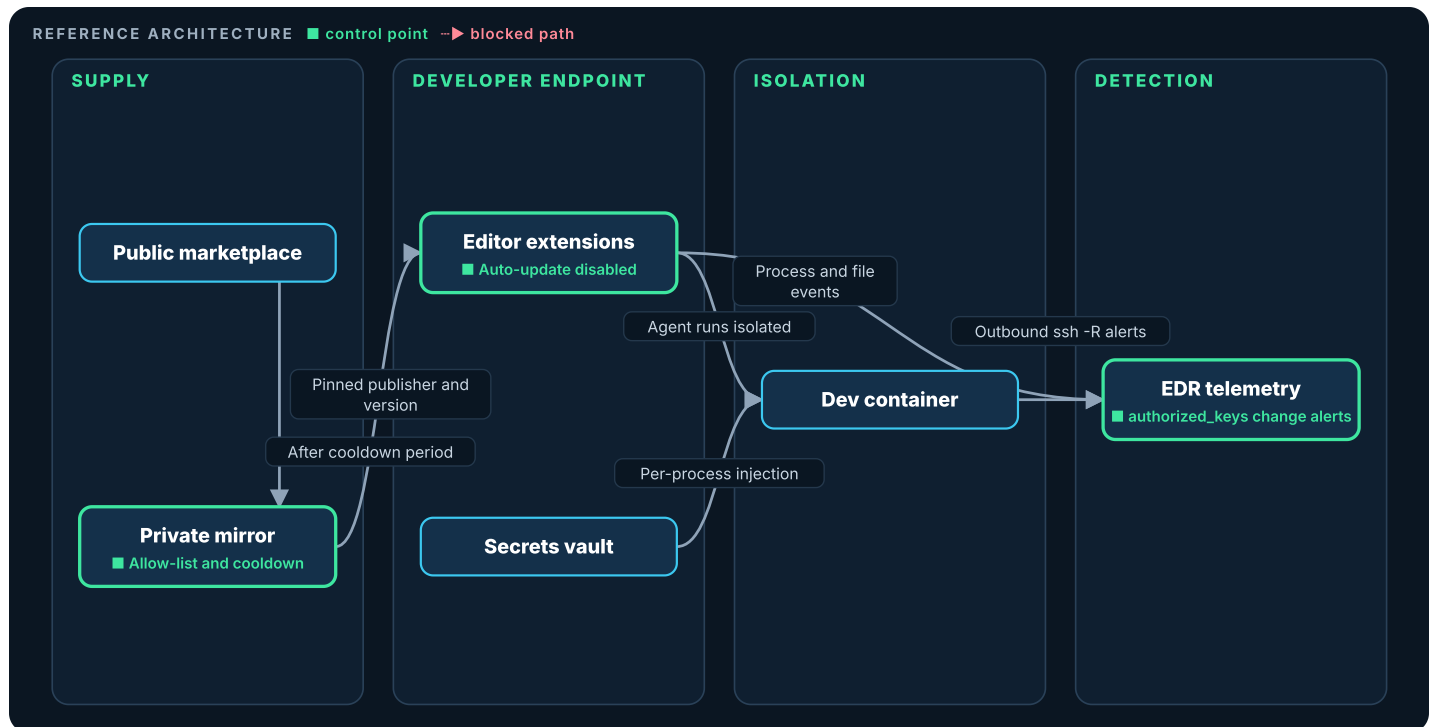
ASK YOUR TEAM

Can we list every editor extension, version and marketplace origin across developer machines today?

Evidence boundary. The marketplace insertion method, the install count and the text of Cursor's own notice are unknown, and the exposure date is assumed to be October 29.

Govern developer extensions like code

Endpoint engineering | Extension supply chain



CONTROLS EXPLAINED

Curated extension source

Serve extensions from an allow-listed source pinned to publisher and version, and hold each new version for a cooldown before release, as Cursor itself now recommends²¹. Disable extension auto-update on managed fleets so that a single marketplace compromise cannot reach every laptop within hours. Record the marketplace of origin, because Microsoft says the evidence so far points to a single marketplace²¹.

Isolated agents, no ambient secrets

Run AI coding agents and their extensions in dev containers or VMs, and keep inbound sshd off laptops unless it is required. On macOS, leave Remote Login disabled. Store secrets in a vault or OS keychain and inject them per process. This loader listed environment-variable names containing KEY, TOKEN, SECRET, PASS, AWS and GCP²¹, which shows attackers mapping ambient secrets.

Endpoint detection for persistence

Alert on new `authorized_keys` entries, outbound ssh with `-R`, `autossh` launches, new `LaunchAgents`, `@reboot` cron lines and new scheduled tasks. Microsoft's hunting covers the IP, the entry-point hash, the `.stk_temp`-file pattern, the "SysMon" task and `com.apple.sysmond.plist`, mapped to T1098.004, T1572, T1053.003 and T1053.005²¹. Inspect what each object actually runs, not its name.

VERIFICATION STEPS

1. List installed extensions with versions, and look for `anthropic.claude-code` 2.1.312 or 2.1.313.
2. Grep `authorized_keys` for `svc-telemetry` and compare fingerprints with Microsoft's published IOC.
3. On macOS, check for `com.apple.sysmond.plist` and `~/config/smt` files. On Linux, review `@reboot` crontab lines.
4. On Windows, query the SysMon scheduled task and check both `authorized_keys` locations.
5. Search firewall, proxy or DNS logs for 134.209.82.225 and beacons to port 8099.
6. Look for `.stk_` temp files and for running `autossh` or `ssh -R` processes.

MACOS/LINUX | SHELL | READ-ONLY
(illustrative)

```
# Illustrative; Cursor CLI flags may differ
cursor --list-extensions --show-versions
grep -n 'svc-telemetry' ~/.ssh/authorized_keys
ssh-keygen -lf ~/.ssh/authorized_keys
crontab -l | grep -n '@reboot'
ls -la "$TMPDIR:-/tmp"/.stk_* 2>/dev/null
ps aux | grep -E 'autossh|ssh.*-R'
```

Illustrative MAG212 design, not a depiction of victim systems. The Cursor CLI's behaviour is assumed to match VS Code's. Context:²¹

E-COMMERCE / WEB SECURITY · STORY 07

Patched Magento stores keep skimming

One operator's database-resident loader survives PolyShell patching, and Sansec ties it to 953 compromised stores since July 2025.

APSB26-73 Jul 14; Sansec report Oct 24; KEV reportedly Oct 27 (due Nov 10), 2026 | Sources:^{22,23,24}



MAG212 EDITORIAL GRAPHIC · CONCEPTUAL

REPORTED FACTS

Adobe's APSB26-73, published July 14 and updated August 11, rates CVE-2026-48356 Critical. The flaw is an unrestricted file upload with a CVSS 3.1 score of 9.6. Adobe lists numbered builds such as 2.4.7-p10 and 2.4.8-p5 as affected and the "-2026-jul" builds as fixed, and says it is not aware of any exploits²². Sansec reported on October 24 that one operator has compromised 953 stores since July 2025 with a JavaScript loader stored only in the cms_block table. Its newest domain, deepveindrilling.com, appears on 83 stores²³. A 2.4.7-p10 store that Sansec considered fully patched was re-injected on October 23 through a rogue admin account²³. Rescana reports that CISA added the CVE to KEV on October 27, due November 10. That has not been confirmed with CISA directly²⁴.

WHY IT MATTERS

Patching closes the upload path, but it leaves database-resident scripts, rogue admins and stolen database credentials in place²³. File-integrity monitoring misses code stored in CMS blocks. The loader also caches its payload in each visitor's localStorage, so returning shoppers re-run it even when the domain is blocked²³. Version 2 hides from automated browsers²³, so scanners can report a clean store while its customers are being skimmed.

DEFENDER ACTIONS

- 01** Install the APSB26-73 and APSB25-88 fixed builds, checking for "-2026-jul" naming rather than numbered patch levels.
- 02** Query cms_block and cms_page for fpCode, se_referrer and localStorage.getItem on a read-only replica.
- 03** Review admin_user for unknown accounts, then rotate admin, database and deploy credentials.

ASK YOUR TEAM

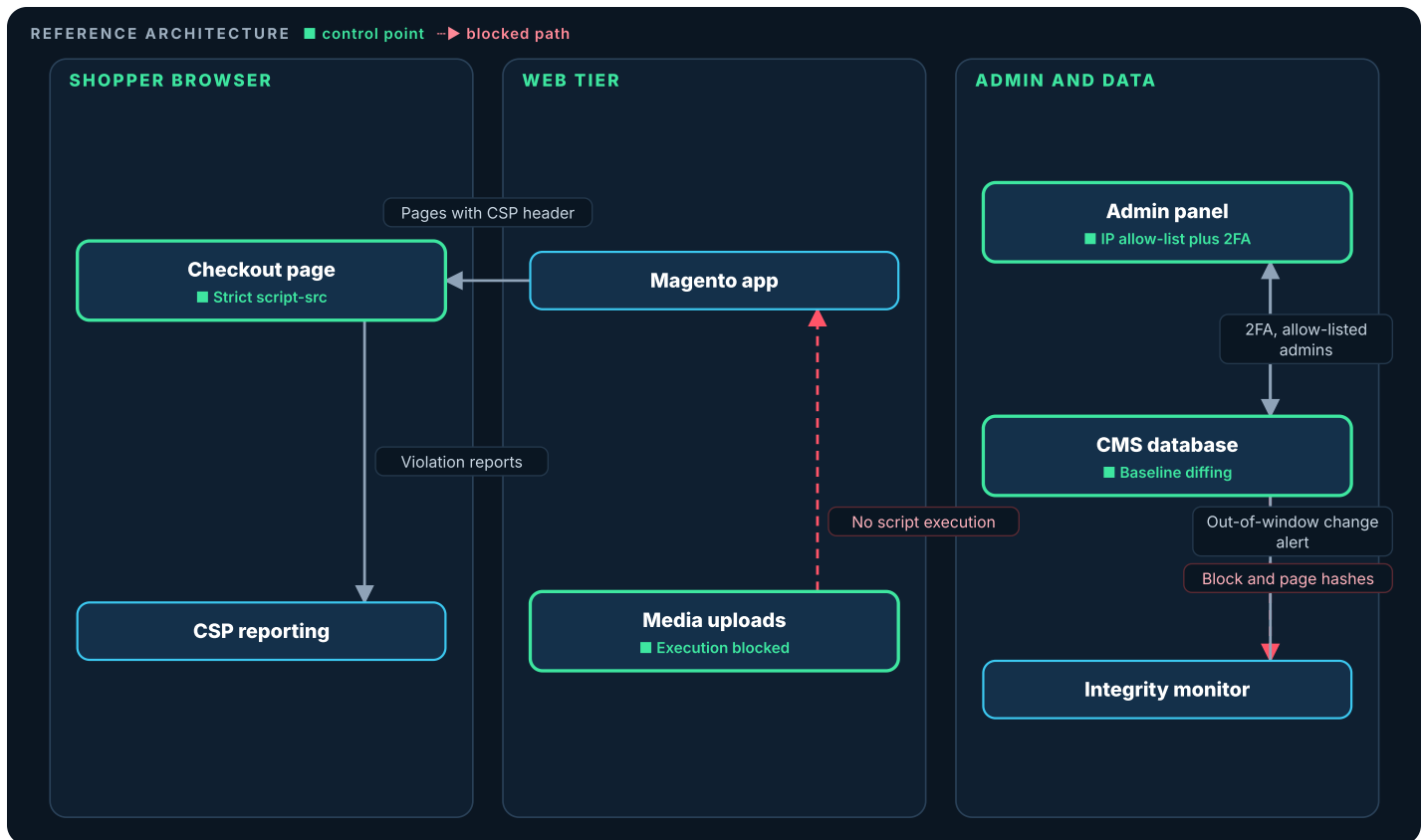
If our store were re-infected an hour after a clean scan, which control would notice?

Evidence boundary. The final payload has not been captured, the KEV listing is second-hand, and it is unclear whether Sansec's "patched" store had Adobe's isolated patch.

TECHNICAL PAGE 07 · DEFENSIVE ARCHITECTURE

Patch, then clean, then rotate

Web application security | Checkout integrity



CONTROLS EXPLAINED

Content Security Policy with reporting

Deploy a strict script-src allow-list on checkout. Start in Report-Only mode using Magento's built-in CSP module, and enforce once the reports are clean. Add Subresource Integrity to third-party scripts. A loader that fetches from an unknown domain then triggers a violation report. Cached localStorage payloads that run inline also need a policy that restricts inline scripts.

CMS content integrity

This loader lived only in cms_block, not in configuration or theme files²³. Hash or diff cms_block and cms_page against a known-good baseline, and alert on any update_time change outside approved change windows. Run the checks from a real browser profile as well, because version 2 returns an empty response to automated browsers²³. A clean scan alone proves little.

Admin and database least privilege

Removing a script does not remove the attacker's database write access²³. Use a custom admin path, a VPN or IP allow-list, and mandatory 2FA, and review admin_user regularly. Give the web application's database user least privilege, separate from deploy credentials. Block script execution under pub/media at the web server to blunt upload flaws such as PolyShell.

VERIFICATION STEPS

1. Run `bin/magento --version` and `composer show` to confirm the installed product version.
2. Run Sansec's `cms_block` query on a read-only replica, then repeat it for `cms_page`, adding any table prefix.
3. List `admin_user` accounts by creation date and last login, and investigate unknown entries.
4. Find non-`.htaccess` files under `pub/media/custom_options` and `pub/media/customer_address`, and any `accession.php`.
5. Check the checkout page's response headers for Content-Security-Policy.

MAGENTO | MYSQL | READ-ONLY (illustrative)

```
-- Illustrative; read-only replica only
SELECT block_id, identifier, update_time
FROM cms_block
WHERE content LIKE '%fpCode%'
OR content LIKE '%se_referrer%'
OR content LIKE '%localStorage.getItem%';
SELECT username, created, logdate
FROM admin_user ORDER BY created DESC;
```

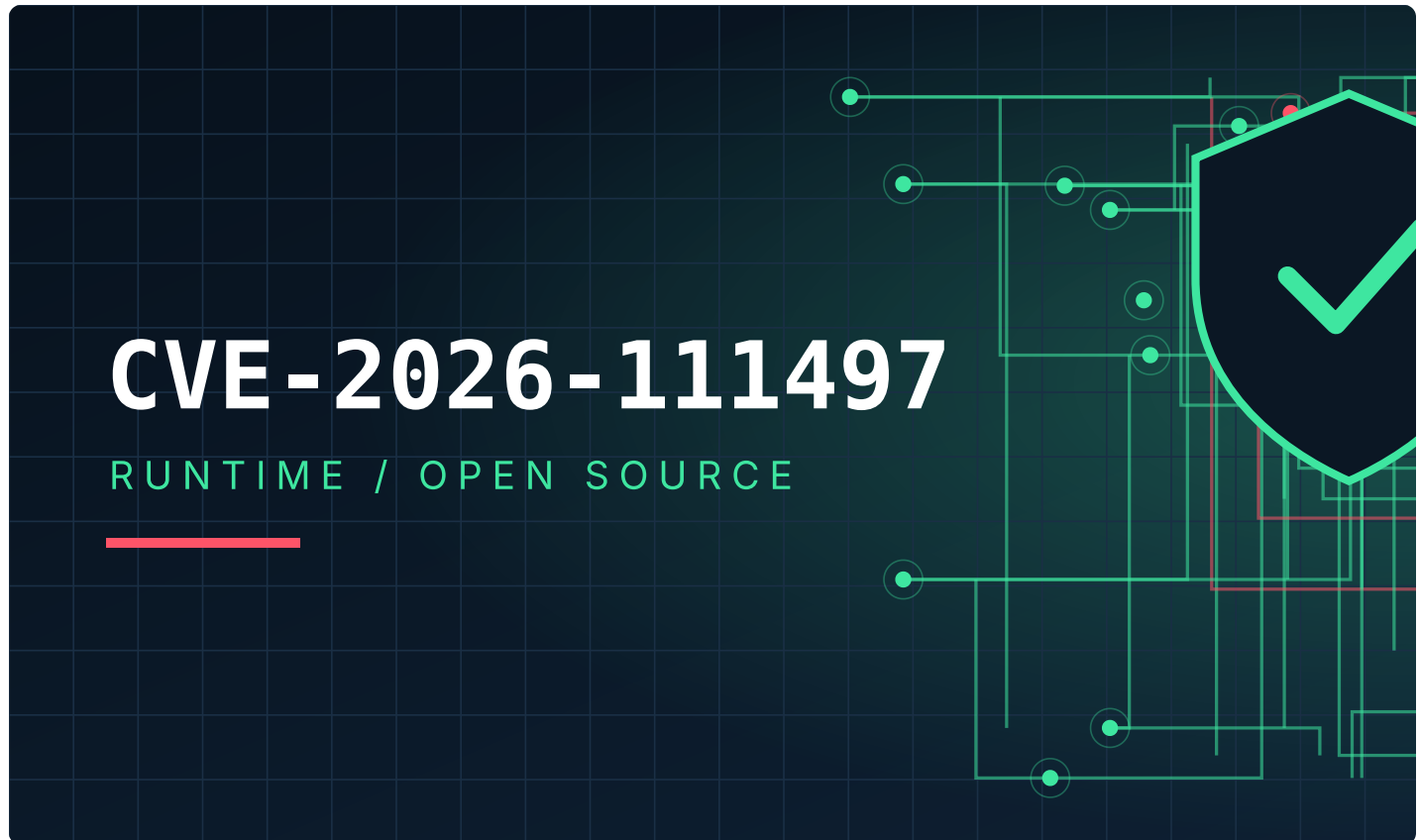
Illustrative MAG212 design, not a depiction of victim stores. The cms_block query is adapted from Sansec. Context:^{22,23}.

RUNTIME / OPEN SOURCE · STORY 08

Brotli bug reportedly added to CISA KEV

A Brotli decoder flaw in Node.js and other runtimes is reportedly on CISA's exploited list, though RCE on standard builds is unproven.

Node.js fix Oct 21; KEV Oct 27 (due Nov 10); Cyber Centre alert Oct 28, 2026 | Sources: ^{27,28,29,30}



MAG212 EDITORIAL GRAPHIC · CONCEPTUAL

REPORTED FACTS

On October 21, Node.js fixed CVE-2026-111497, rated High, in versions 22.23.4, 24.22.1 and 26.12.1. It was one of 10 CVEs in that release²⁷. The decoder treated an invalid block switch as a need for more input, so it kept writing past an 8-byte buffer. Attacker-supplied Brotli data decompressed with node:zlib can therefore cause a crash, a memory disclosure or RCE²⁷. OpenAI Codex Security reported the flaw²⁷. Upstream Brotli is fixed in 1.0.10, 1.1.1 and 1.2.1. The Canadian Cyber Centre also lists .NET, PowerShell, Bun, Envoy, Istio and Python packages as affected²⁹. BleepingComputer reports that CISA added the flaw to KEV on October 27, due November 10³⁰. As of October 22, the public PoC had achieved code execution only on a deliberately weakened build²⁸.

WHY IT MATTERS

The exposure sits wherever untrusted Brotli data is decoded. That includes inbound bodies sent with Content-Encoding: br, and responses an application fetches from other servers, which edge rules such as Vercel's do not cover²⁸. Vulnerable copies can hide inside containers, Electron apps and bundled runtimes. Node 20.x and earlier get no fix²⁸. The KEV listing likely reflects exploitation attempts, crashes or leaks rather than working RCE, but that is an assessment, and crash-loops alone can take services down.

DEFENDER ACTIONS

- 01** Upgrade Node to 22.23.4, 24.22.1 or 26.12.1, then restart processes and rebuild container images.
- 02** Inventory Brotli bundled in .NET, Envoy, Istio, Bun and Python packages, and patch each separately.
- 03** Strip or block Content-Encoding: br at the edge where Brotli is not needed.

ASK YOUR TEAM

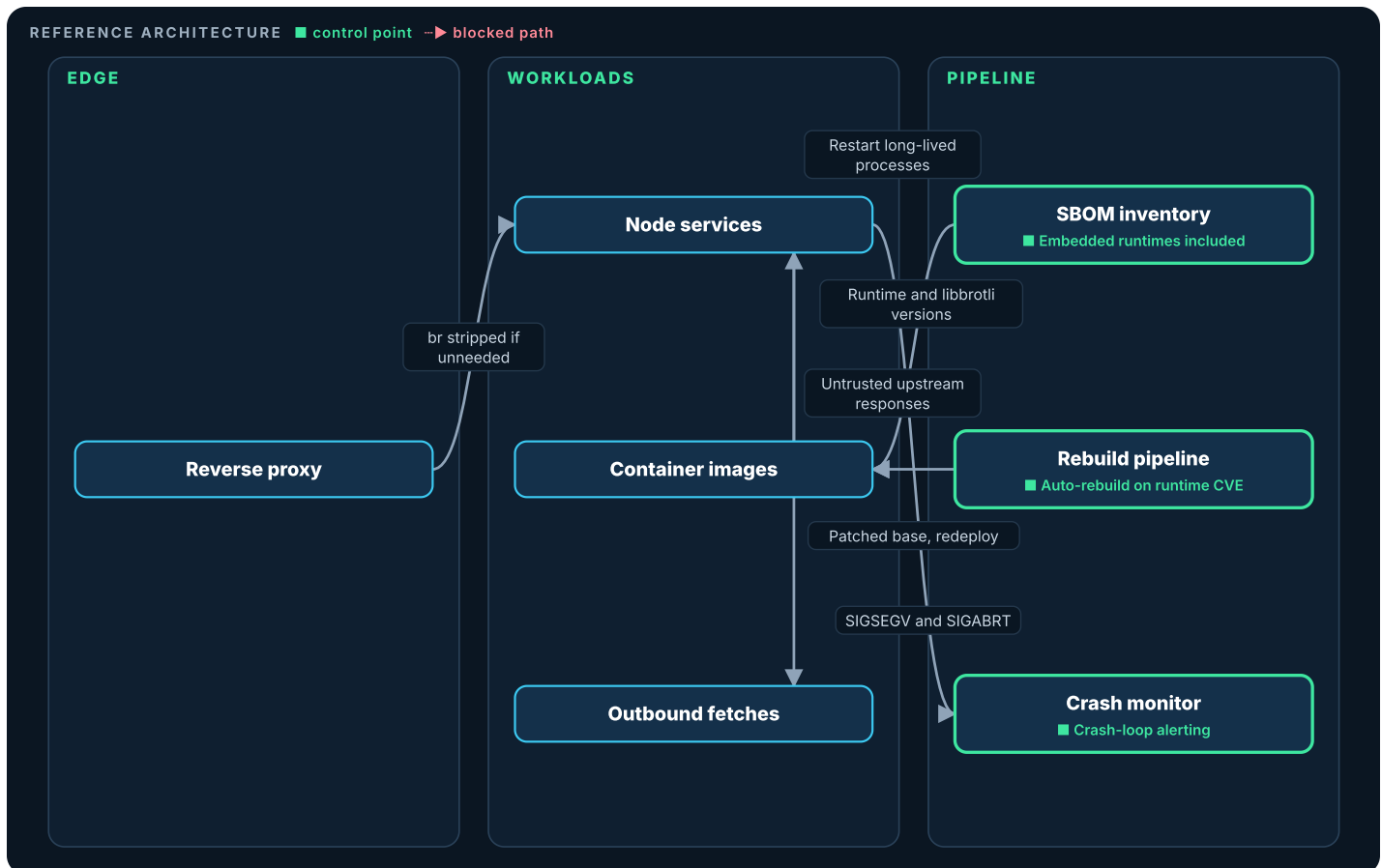
Where do we decompress Brotli from sources we do not control, including outbound fetches?

Evidence boundary. The KEV listing is second-hand, no actors or confirmed compromises are named, and the CNA's numeric CVSS score has not been verified.

TECHNICAL PAGE 08 · DEFENSIVE ARCHITECTURE

Find every hidden Brotli decoder

Platform engineering | Runtime inventory and rebuild



CONTROLS EXPLAINED

Runtime-aware inventory

Package scanners often miss runtimes embedded in containers, Electron apps and single-executable apps, as well as the system libbrotli that other software loads. Build an SBOM or runtime inventory that records the Node version in each image and every copy of Brotli, including the downstream products the Cyber Centre names²⁹. Treat Node 20.x and older as unfixable and schedule their migration.

Automatic rebuild and restart

Upgrading a package does not patch a running process or a stale image. Pin base images and trigger rebuild-and-redeploy automatically when a runtime CVE lands, then restart long-lived processes, as BleepingComputer's interim advice stresses³⁰. Gate releases on the minimum fixed version for each line: 22.23.4, 24.22.1 or 26.12.1²⁷. Track restart completion, not just merged pull requests.

Decode only what you need

Strip Content-Encoding: br at the edge for services that do not need it, or disable Brotli decoding³⁰. Remember that outbound fetch() and undici calls can decode responses from untrusted upstreams, which inbound firewall rules miss²⁸. The maxOutputLength option limits decompression bombs, not this memory-corruption bug, so pair it with crash-loop alerting on SIGSEGV and SIGABRT.

VERIFICATION STEPS

1. Run `node -v` on every host and inside each container image.
2. Print `process.versions` to record the bundled Brotli version.
3. Check the `node_shared_brotli` build variable to see whether Node uses a system library.
4. List system Brotli packages with `dpkg` or `rpm`, plus the Python `brotli` and `brotlicffi` packages.
5. Pass only Node 22.23.4, 24.22.1, 26.12.1 or later on each line, and flag any 20.x.

LINUX | BASH | READ-ONLY (illustrative)

```
# Illustrative; replace IMAGE with your tag
node -v
node -p "process.versions.brotli"
node -p "process.config.variables" | grep br
ot
docker image inspect IMAGE --format \
  '{{.Config.Env}}'
ldconfig -p | grep -i brotli
pip show brotli brotlicffi
```

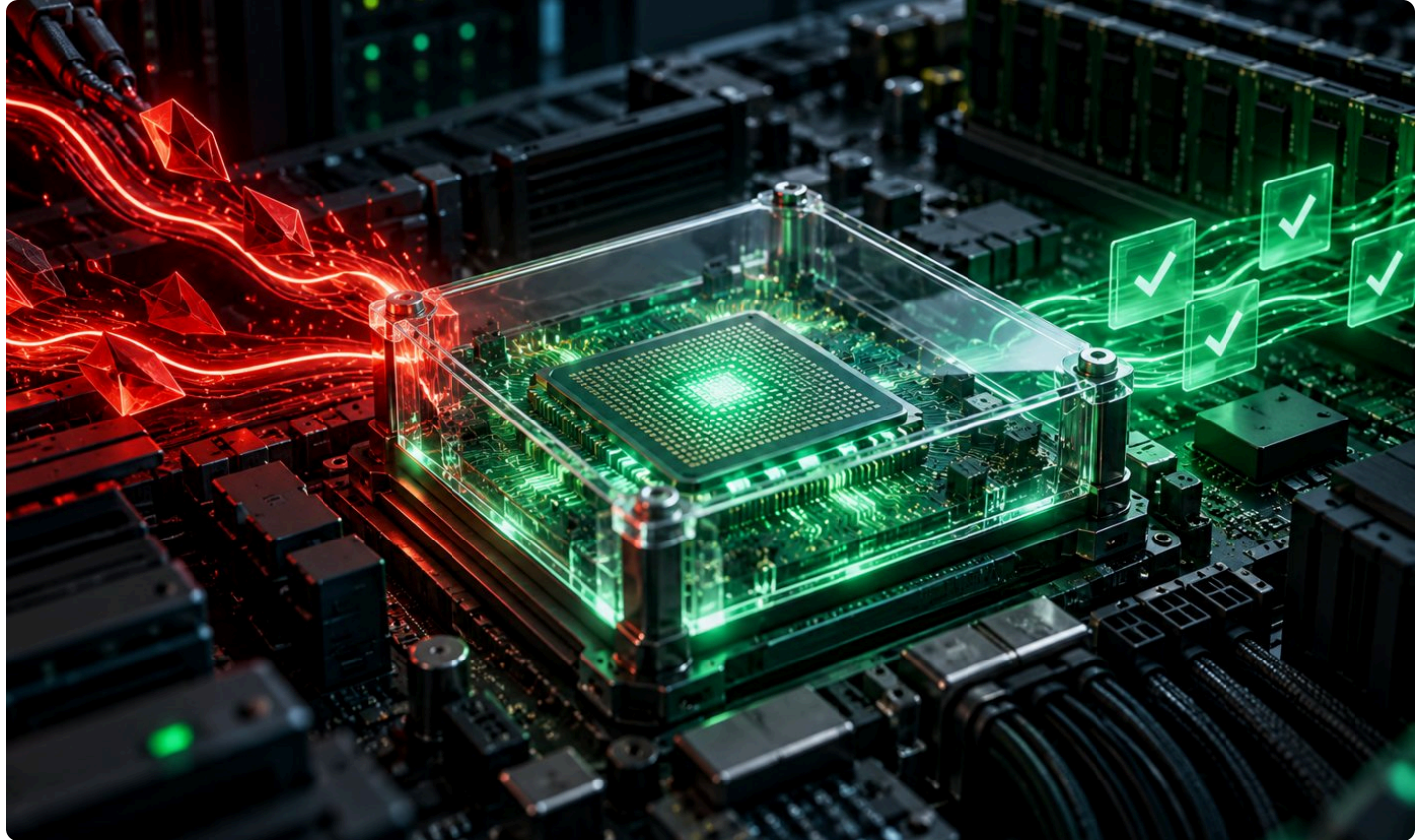
Illustrative MAG212 design, not a depiction of victim systems. The `process.versions.brotli` key is assumed. Context:^{27,28,29,30}

LINUX / VULNERABILITY RESEARCH · STORY 09

Kernel TCP race reaches remote root

An IPv4 TCP use-after-free present since Linux 4.4 gave Anthropic's researchers zero-click root against servers running MPTCP listeners.

CVE Oct 15; Red Hat rescore Oct 24; Anthropic Oct 27; distro updates Oct 29-30, 2026 | Sources: ^{32,34,35,39}



AI-GENERATED EDITORIAL ILLUSTRATION · CONCEPTUAL, NOT INCIDENT EVIDENCE

REPORTED FACTS

CVE-2026-98432, published by the kernel CNA on October 15, is a use-after-free in IPv4 TCP request-socket handling. IP options shared between a child socket and a concurrent SYNACK are freed without an RCU grace period³². Present since Linux 4.4, it is fixed upstream (e3f33b0a1d89, 7.3-rc7) and in stable releases including 6.1.190, 6.6.159 and 6.12.113^{32,38}. On October 27, Anthropic reported zero-click, unauthenticated remote root against servers with a multipath TCP listener. Its exploit took 48 minutes to leak a kernel pointer and five more to run commands³⁹. Red Hat raised its score from 5.9 to 9.8 Critical on October 24^{32,33}. By October 30, Debian had fixes, SUSE some, Ubuntu and Red Hat none^{34,35,36,37}. No in-the-wild exploitation is reported³².

WHY IT MATTERS

Anthropic says the fix was "backported to all maintained stable kernel branches"³⁹, but that is not the same as patched distribution kernels. RHEL and Ubuntu users were still waiting on October 30^{34,35}. The CVE text names generic IPv4 TCP, not MPTCP³², and Red Hat says any host accepting inbound TCP connections is the most directly exposed³⁴. A lost race only fails the handshake, so an attacker can keep retrying without crashing the target³⁹.

DEFENDER ACTIONS

- 01** Track your distribution's advisory, install the fixed kernel, and confirm the running kernel after reboot.
- 02** On RHEL, test and then apply Red Hat's nftables rule dropping inbound IPv4 TCP with IP options.
- 03** Disable MPTCP where unused, as hardening only; no vendor documents it as a mitigation.

ASK YOUR TEAM

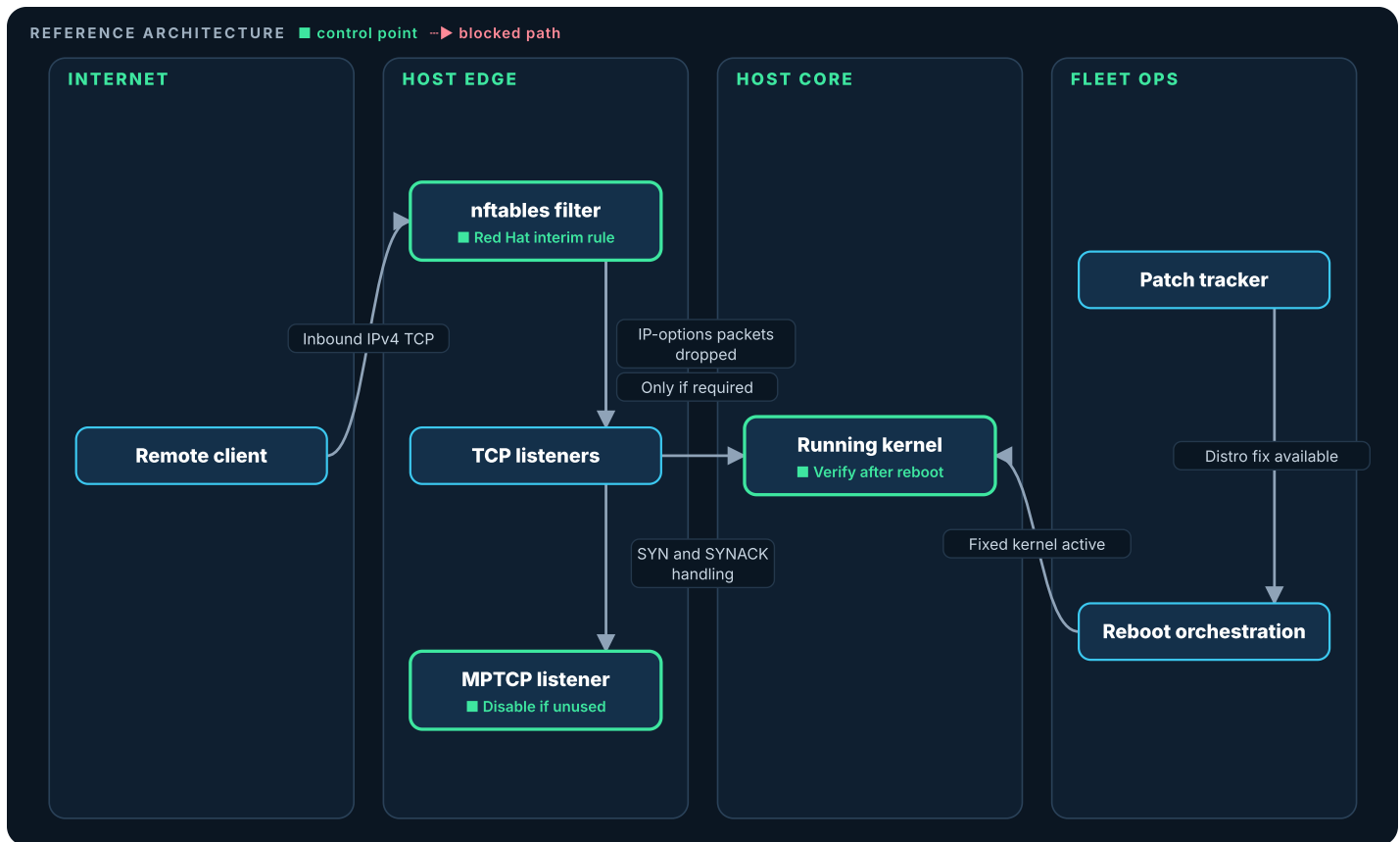
Which internet-facing Linux hosts still run a pre-fix kernel, and which of them have MPTCP listeners?

Evidence boundary. No source says whether the RCE requires MPTCP or MPTCP merely made it practical, or whether Red Hat's rule covers that path.

TECHNICAL PAGE 09 · DEFENSIVE ARCHITECTURE

Bridge the kernel patch gap

Linux engineering | Interim filtering and runtime verification



CONTROLS EXPLAINED

Distribution-matched patching

Distributions backport fixes, so check your vendor's tracker rather than upstream version numbers. Debian lists 6.1.190-1 and 6.12.113-1, SUSE released several SLES kernels on October 29, and Ubuntu advises against cherry-picking updates^{35,36,37}. An installed kernel package protects nothing until the host boots it, so record the running kernel after every maintenance window.

Interim IP-options filter

Red Hat's bulletin publishes an nftables table, inet cve_2026_98432, at input priority -310³⁴. Its rule drops inbound IPv4 TCP packets whose header length exceeds five words, which means packets carrying IP options. Red Hat says it reduces exposure but cannot fully prevent exploitation, and that it must be tested first. Check legitimate traffic using IP options, and remove the rule after patching.

Listener and feature minimisation

Anthropic's remote-root demonstration targeted MPTCP listeners³⁹. Inventory which services open MPTCP sockets and turn MPTCP off where no application needs it. Present this as hardening rather than a fix, because no vendor lists it. Keep net.ipv4.tcp_migrate_req at its default of 0 (third-party sources, not vendors, suggest this partly narrows the migration path), and cut the number of publicly reachable TCP listeners wherever you can.

VERIFICATION STEPS

1. Record `uname -r` and compare it with your distribution's security tracker, not upstream version numbers.
2. List installed kernel packages with `rpm -q kernel` or `dpkg -l`.
3. Check `sysctl net.mptcp.enabled`, and list MPTCP listeners with `ss -Mltn` where `iproute2` supports it.
4. List all TCP listeners with `ss -lnt`, because any host accepting inbound TCP is exposed.
5. Confirm that `net.ipv4.tcp_migrate_req` is 0.
6. On RHEL, confirm the interim table is loaded with `nft list table`.

LINUX | BASH | READ-ONLY (illustrative)

```
# Illustrative; read-only inventory
uname -r
sysctl net.mptcp.enabled
sysctl net.ipv4.tcp_migrate_req
ss -Mltn
ss -lnt
nft list table inet cve_2026_98432
```

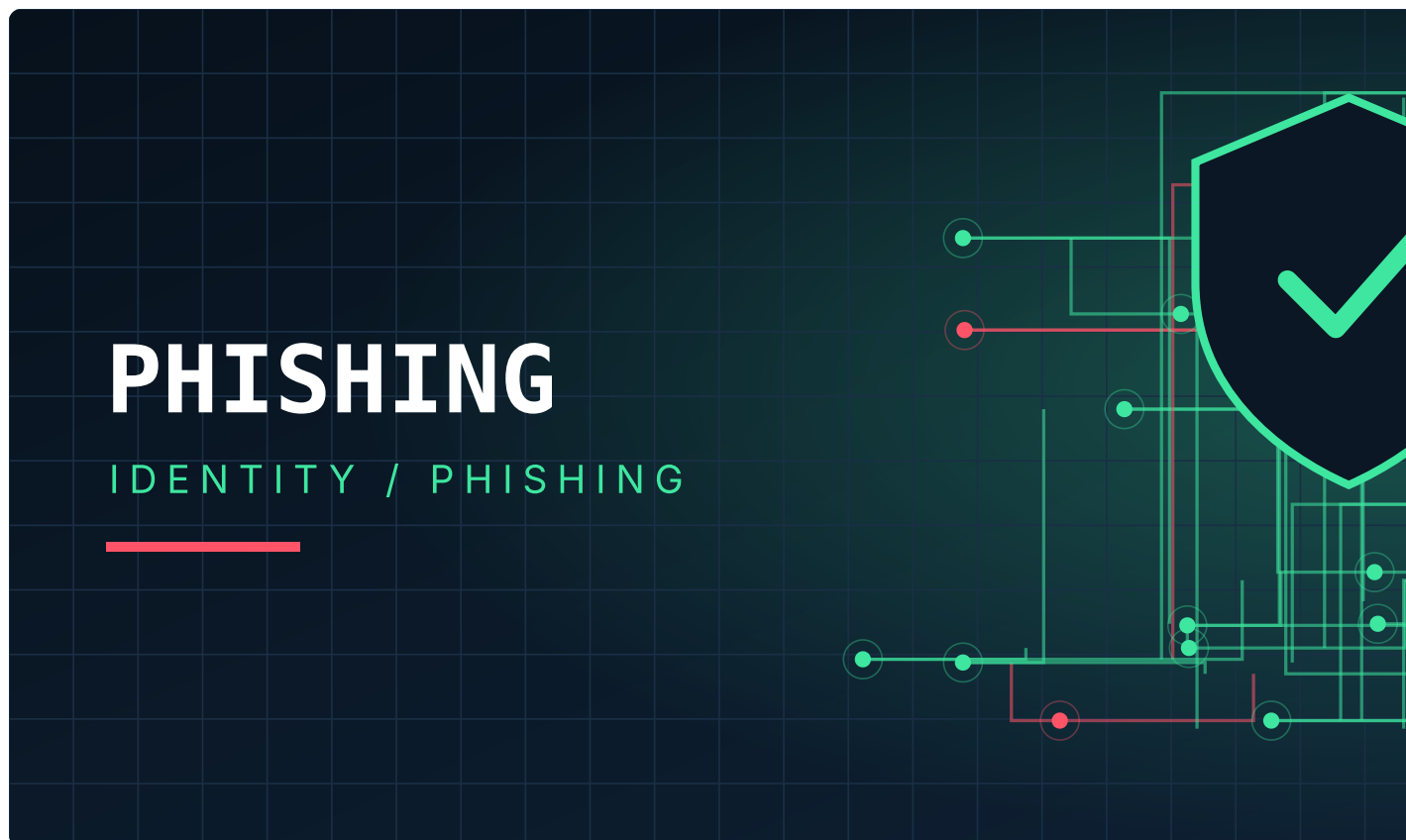
Illustrative MAG212 design, not a depiction of victim systems. The MPTCP steps are hardening, not vendor mitigation. Context:^{32,34,39}.

IDENTITY / PHISHING · STORY 10

SkyW4lker phishes Microsoft 365 device codes

A kit abusing OAuth device-code sign-in has victims complete real Microsoft MFA while the attackers collect the tokens.

First seen Jun 23; ANY.RUN report Oct 27, 2026 | Sources: ^{41,42}



MAG212 EDITORIAL GRAPHIC · CONCEPTUAL

REPORTED FACTS

ANY.RUN reported on October 27 that SkyW4lker, first seen on June 23, abuses the OAuth 2.0 device authorization grant⁴¹. The victim enters an attacker-requested code on Microsoft's genuine sign-in page and completes MFA. The attacker's backend, which polls session_public.php, then receives the tokens⁴¹. Lures arrive as password-protected PDF, DOCX or XLSX attachments. A CAPTCHA follows, sometimes with a page on Miro, Google Sites or Zoom⁴¹. ANY.RUN counted 618 sandbox analyses through October 21, rising from 20 a month in June to 200 in September. It also logged 92 backend IPs and 173 domains⁴¹. It assesses with high confidence that SkyW4lker shares a developer with the Gabagool credential-phishing kit⁴¹. Sandbox submissions are not a count of victims.

WHY IT MATTERS

The kit never takes a password, so phishing-resistant MFA does not stop it: the user authenticates legitimately for a session the attacker started. Microsoft recommends blocking device code flow wherever possible and allowing it only where it is needed⁴². Organisations that left device code open for conference-room devices or command-line tools may now have a working token-theft path, while their MFA dashboards still look healthy.

DEFENDER ACTIONS

- 01** Block device code flow and authentication transfer with Conditional Access, testing in report-only mode first.
- 02** Hunt for device-code sign-ins that follow suspicious emails, correlating email events with identity events.
- 03** Hunt proxy logs for session_public.php, confirm_visit.php and the kit's JavaScript module paths.

ASK YOUR TEAM

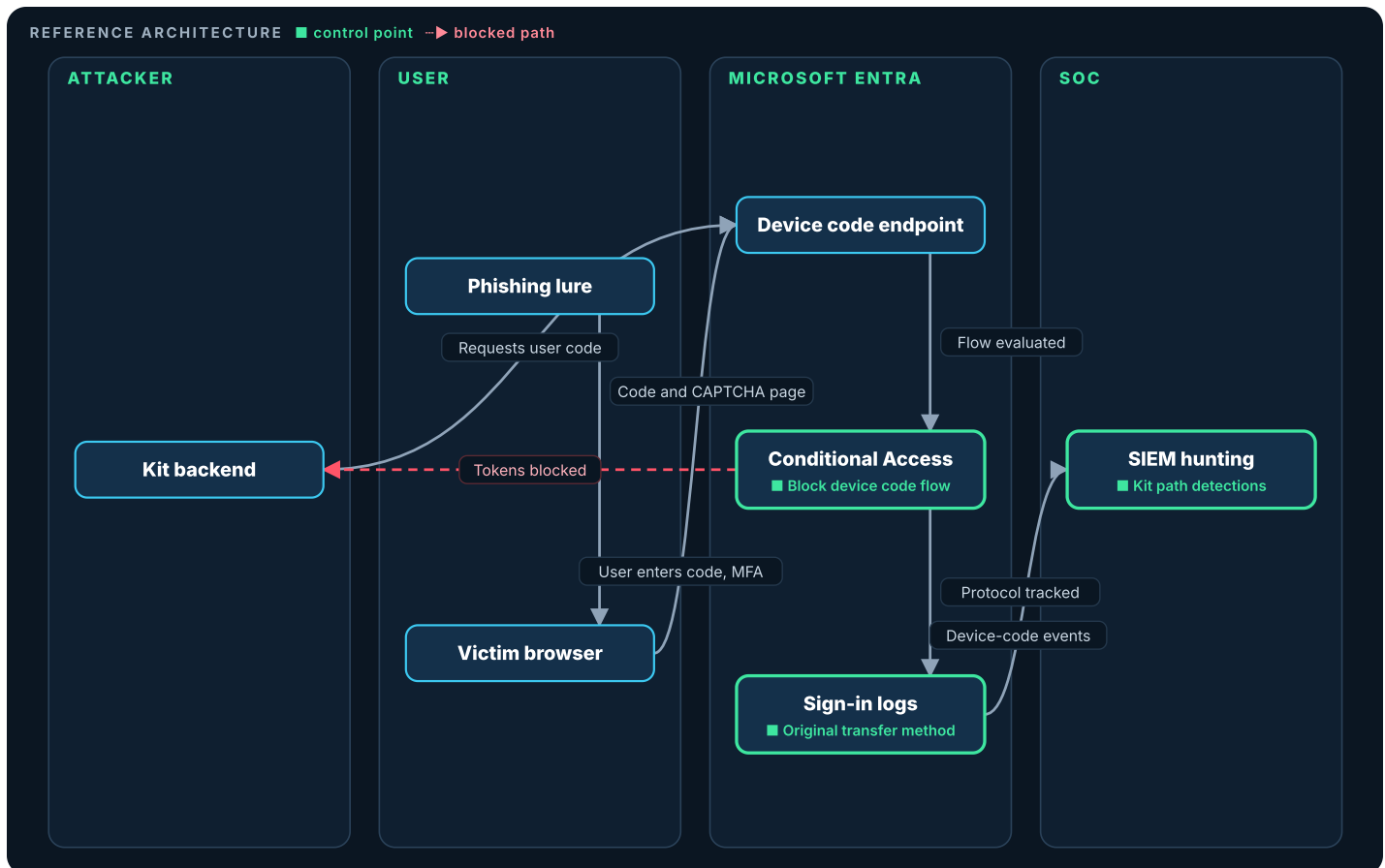
Who in our tenant genuinely needs device code sign-in, and is everyone else blocked?

Evidence boundary. ANY.RUN names no operator, Microsoft client ID or confirmed account takeovers, and no other vendor has independently corroborated its findings.

TECHNICAL PAGE 10 · DEFENSIVE ARCHITECTURE

Close the device-code side door

Identity engineering | Conditional Access authentication flows



CONTROLS EXPLAINED

Authentication-flows policy

Conditional Access authentication-flows policies can block device code flow and authentication transfer. Microsoft advises allowing device code only where necessary, combined with other conditions such as device platform or location⁴². Start in report-only mode. Since September 2024, policies that target all resources also cover the Device Registration Service, so exclude its client ID only if legitimate registration needs it⁴².

Protocol tracking and narrow exceptions

Sessions that began with device code are protocol-tracked, so later sign-ins from them can also be blocked. The Original transfer method property shows "Device code flow" for these sessions⁴². Limit exceptions to named service accounts or device groups, document an owner for each, and review them quarterly. Brief help desks on AADSTS530036, the error Microsoft documents when a protocol-tracked session is blocked (shown as a refresh-token-invalid error)⁴².

Email-to-identity correlation

ANY.RUN recommends watching for unexpected device-code sign-ins after suspicious emails, and correlating email events with identity events⁴¹. Combine attachment telemetry for password-protected documents with sign-in logs filtered to the Device code authentication protocol. Give Tier 1 analysts clear escalation criteria. After a compromise, review Microsoft 365 activity before declaring the incident contained⁴¹.

VERIFICATION STEPS

1. In the sign-in logs, filter Authentication protocol to Device code for the last 30 days.
2. Review the Original transfer method for sessions that started with device code flow.
3. Confirm that a Conditional Access authentication-flows policy exists, and check its report-only results.
4. List the exclusions on that policy and confirm each has a documented owner.
5. Search web proxy logs for requests to session_public.php and confirm_visit.php.

SENTINEL | KQL | READ-ONLY (illustrative)

```
// Illustrative; verify column values
SigninLogs
| where TimeGenerated > ago(30d)
| where AuthenticationProtocol == "deviceCode"
| summarize Count=count()
  by UserPrincipalName, AppDisplayName
| order by Count desc
```

Illustrative MAG212 design, not a depiction of victim tenants. Check the KQL string values against your schema. Context: ^{41,42}.

MARKETS / AI BUSINESS · STORY 11

AI spending fears sink Nasdaq

Intel's outlook and Amazon's AI-driven cash burn sent the Nasdaq to its worst day since June on October 30.

Trading session Oct 30, 2026; next session Nov 2 | Sources: ^{44,45,46}



AI-GENERATED EDITORIAL ILLUSTRATION · CONCEPTUAL, NOT INCIDENT EVIDENCE

REPORTED FACTS

On October 30, according to Yahoo Finance closing data, the Nasdaq Composite closed down 2.86% at 25,437.00. The S&P 500 fell 1.82% to 7,580.07 and the Dow 1.09% to 51,770.31⁴⁴. For both the Nasdaq and the S&P 500, it was the worst day since June⁴⁵. Intel closed down 28.58%. It had guided fourth-quarter revenue to \$15.0B-16.0B and adjusted EPS to 25 cents, against 43 cents expected⁴⁵. Amazon closed down 1.41%. AWS grew 39%, but trailing twelve-month free cash flow was -\$42.4B, which Amazon attributed mainly to AI spending⁴⁵. Reuters, in a syndicated report, framed the open as Amazon and Intel adding to "AI spending woes"⁴⁶. October 31 fell on a Saturday, so there was no recovery session⁴⁵.

WHY IT MATTERS

The pattern suggests investors punished AI capital spending that drives cash flow negative, rather than AI demand itself: AWS grew 39% and Intel's data-center and AI revenue rose 78%⁴⁵. For security and IT leaders, that pressure tends to travel downstream as price changes, tighter usage limits and harder questions about return on investment. Vendors under margin pressure renegotiate. Buyers who already measure their cost per useful result can negotiate from strength.

DEFENDER ACTIONS

- 01** Put per-team token and spend quotas with hard cut-offs on every production AI integration.
- 02** Track cost per accepted result, not cost per call, for each AI use case.
- 03** Review AI contracts for price-change notice, usage caps and data-return terms before renewal.

ASK YOUR TEAM

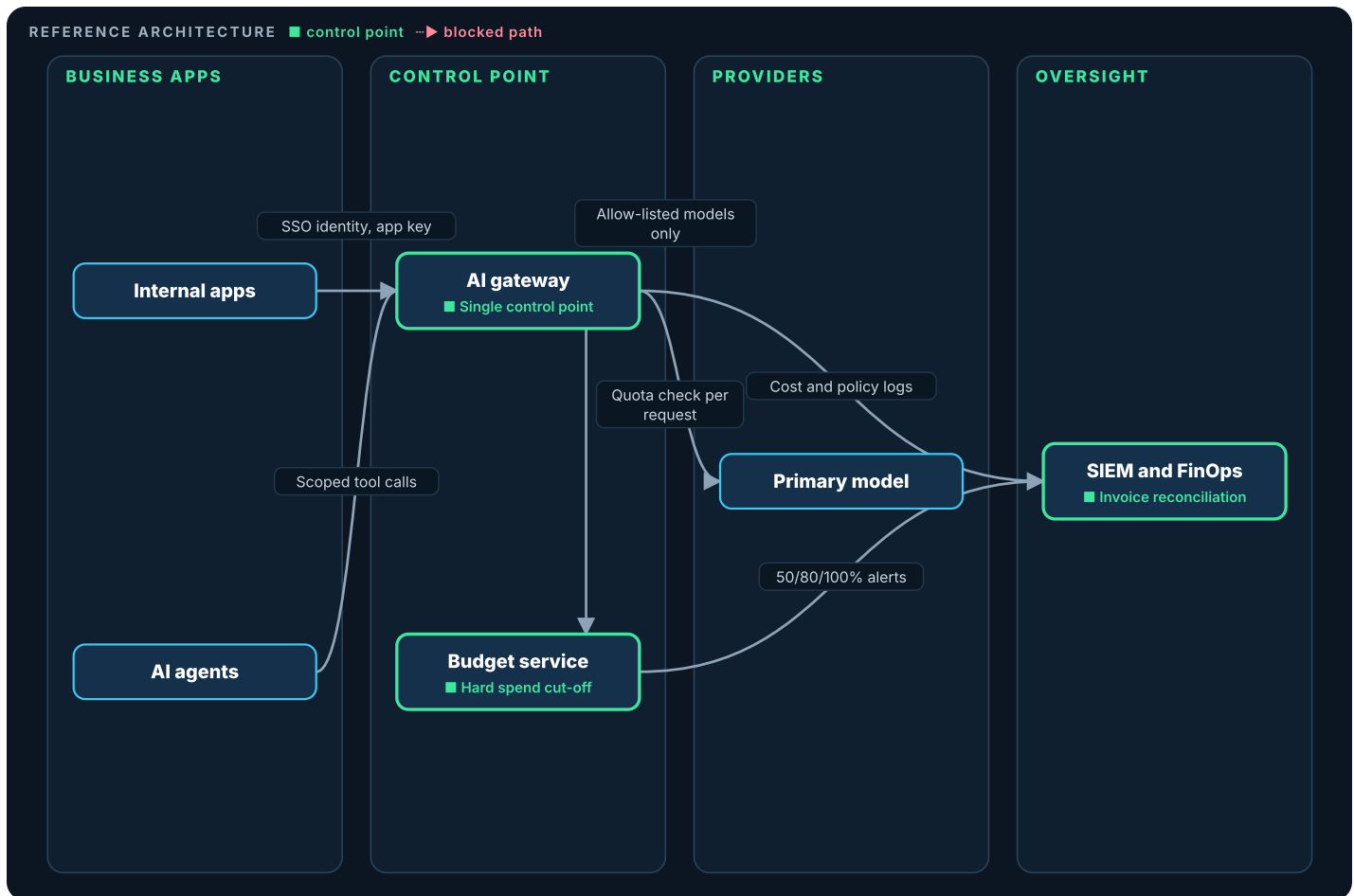
If our AI provider raised prices sharply next quarter, which workloads would we cut first?

Evidence boundary. A single session does not prove a lasting repricing, intraday and closing figures differ across outlets.

TECHNICAL PAGE 11 · DEFENSIVE ARCHITECTURE

Put a budget gateway around AI

Technology operations | Cost and rate governance



CONTROLS EXPLAINED

Single AI gateway

Route every model call, whether to SaaS LLMs, internal models or agents, through one gateway that enforces SSO identity, per-application keys and model allow-lists. That shuts out shadow AI and gives one place to apply policy. It maps to the Govern and Map functions of the NIST AI RMF⁵⁰ and it creates the logs that both finance and security need.

Budget and rate controls

Set token and spend quotas per team and per application, plus per-request token caps, timeouts and concurrency limits. Alert at 50, 80 and 100 percent of budget, then stop hard. This directly addresses OWASP LLM10, Unbounded Consumption⁴⁹ and protects you if providers chasing returns change their pricing. Keep budgets outside prompts, where models cannot alter them.

Cost-per-accepted-result metric

Divide total AI spend, including tokens, infrastructure and review labour, by the number of outputs accepted without rework, and track it per use case. The metric separates genuine productivity from token burn. It also gives CFOs the kind of return evidence markets demanded of hyperscalers this week. Reconcile gateway logs against provider invoices: calls that are billed but not logged indicate bypass.

VERIFICATION STEPS

1. Drive a test application past its quota and confirm the hard stop, the alert, and that no overrun is billed.
2. Reconcile one month of gateway logs against provider invoices and investigate any unlogged calls.
3. Confirm every production AI integration has an owner, a budget and a model allow-list entry.
4. Sample cost per accepted result for two use cases and compare it with the baseline workflows.
5. Confirm budgets are enforced at the gateway, not in prompts or client code.

Illustrative MAG212 governance design. No pilot outcomes or forecasts are claimed. Context: ^{44,45,49,50}.

AI BUSINESS / REPORTED DEVELOPMENT · STORY 12

OpenAI reportedly trims funding target

The FT reports that OpenAI cut its round to about \$20 billion at a \$1.25 trillion valuation as investors pulled back.

FT report Oct 30; Reuters syndication Oct 31 UTC, 2026 | Sources:^{47,48}



AI-GENERATED EDITORIAL ILLUSTRATION · CONCEPTUAL, NOT INCIDENT EVIDENCE

REPORTED FACTS

The Financial Times reported on October 30, citing people with knowledge of the matter, that OpenAI had cut its fundraising target by \$10 billion to about \$20 billion. The valuation is \$1.25 trillion, and the cut followed some investors reducing their commitments during the AI selloff⁴⁸. OpenAI had previously sought \$30 billion at \$1.4 trillion. Friday was the commitment deadline, and the first close is expected to raise less than \$20 billion⁴⁷. UAE investors including MGX are expected to be the largest backers. Founders Fund, Coatue, Sequoia and Andreessen Horowitz also plan to invest⁴⁸. The WSJ reports that OpenAI has raised less than half of the \$30 billion it sought⁴⁸. OpenAI did not respond to Reuters⁴⁸ and the company has not confirmed any of this.

WHY IT MATTERS

The reported valuation target has fallen from \$1.4 trillion to \$1.25 trillion this month, and the round has shrunk by a third⁴⁷. Supplier conditions in AI can change faster than procurement cycles. Reuters reports that OpenAI wants to close the round before Anthropic's expected mid-November listing, because the two draw on overlapping investors⁴⁸. None of this signals that any service will degrade. It is a reason to make provider dependence explicit and tested.

DEFENDER ACTIONS

- 01** Document which critical workflows depend on a single model, API or proprietary tool.
- 02** Keep a second provider or open-weight model behind a provider-neutral abstraction layer.
- 03** Run quarterly failover drills that measure reroute time and output quality against a fixed evaluation set.

ASK YOUR TEAM

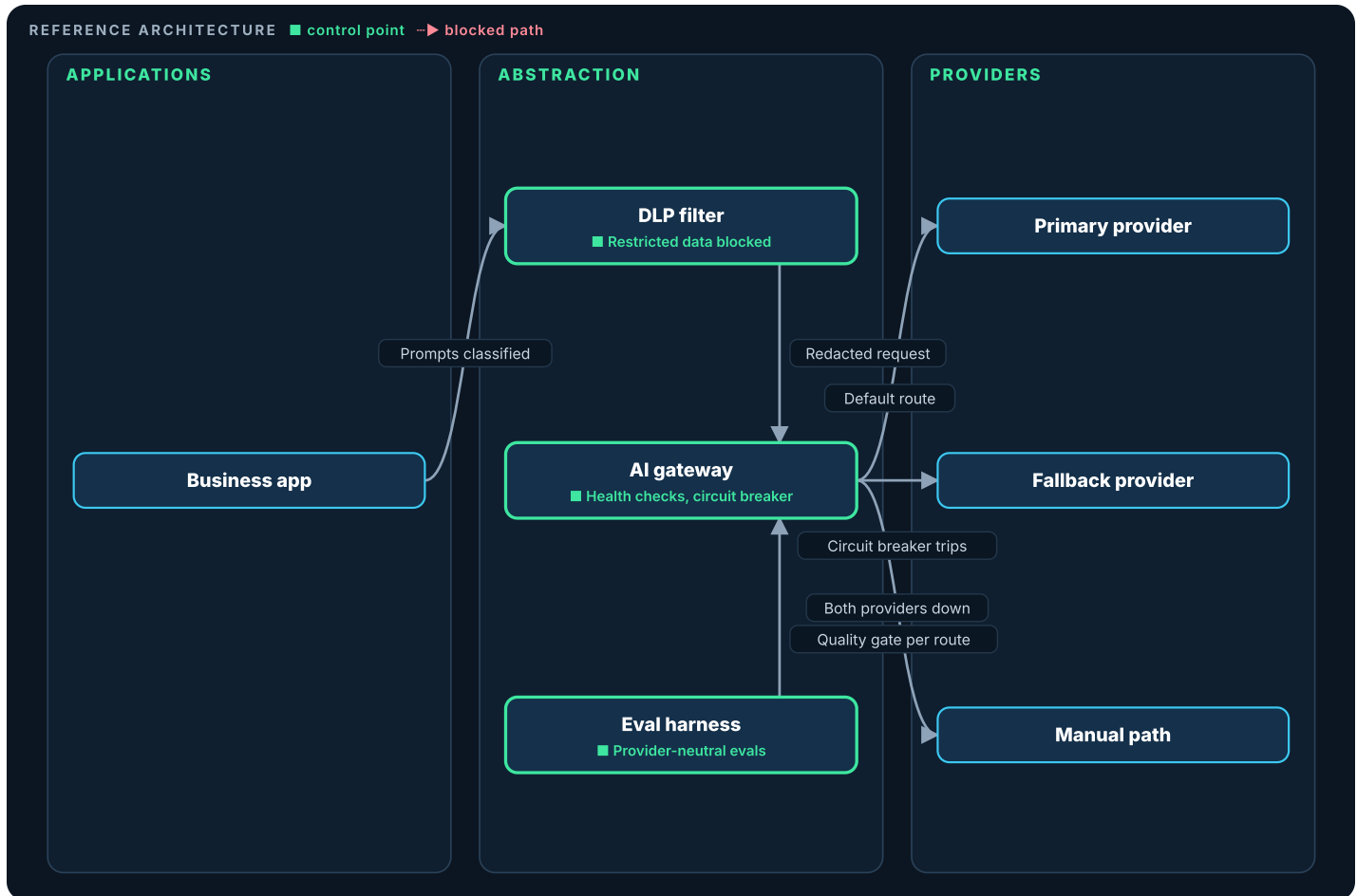
Could our most important AI workflow keep running if its provider changed pricing or limits?

Evidence boundary. The report rests on unnamed sources. The final size, closing date and investor allocations are unconfirmed, and OpenAI has made no statement.

TECHNICAL PAGE 12 · DEFENSIVE ARCHITECTURE

Design for AI provider portability

Enterprise architecture | Continuity and supplier risk



CONTROLS EXPLAINED

Provider fallback behind an abstraction

Keep at least two providers, or one provider plus an open-weight model, behind a single abstraction layer with health checks, circuit breakers and tiered routing. The abstraction isolates authentication, request formatting and error handling, but models still differ in tool calls, structured outputs and context limits. This addresses OWASP LLM03, Supply Chain⁴⁹, and the risk of concentrating on one vendor.

Provider-neutral evaluation

A second endpoint is not continuity until its outputs have been tested. Maintain a representative evaluation set, keep prompts provider-neutral, and set pass criteria in advance, such as maximum reroute time and an acceptable quality difference. Include timeouts, rate limits and malformed outputs in the tests. Keep a documented manual path for tasks the business cannot pause.

Contract and data controls

Map where prompts and outputs are stored, which subprocessors are involved, and how data comes back at exit. Prefer zero-retention or no-training terms. Redact personal data, secrets and regulated data at the gateway before requests leave, which addresses OWASP LLM02, Sensitive Information Disclosure⁴⁹. Review exit clauses at renewal, not in the middle of a crisis.

VERIFICATION STEPS

1. Each quarter, block the primary provider at the gateway for a test workload.
2. Measure time to reroute, error rate and the quality difference on the fixed evaluation set.
3. Seed canary personal data and secrets in prompts, then confirm redaction or blocking and a log entry.
4. Confirm that each provider contract specifies data return, retention and exit terms.
5. Run the manual procedure once with its named owner and record the gaps.

Illustrative MAG212 reference design. No OpenAI service change is implied. Context:^{47,48,49}.

ALSO THIS WEEK · NOT COVERED ABOVE

Weekly roundup

The other confirmed stories of October 25–31 that defenders should know about, in brief.

Oct 29

CISA lists GitLab and Cisco firewall flaws

CISA added GitLab CVE-2026-97229 (CVSS 10.0) and Cisco ASA/FTD CVE-2026-76418 (CVSS 8.6) to KEV, due Nov 1. Ruby fixed regex-engine bugs behind four GitLab RCEs^{51,52}.

Oct 30

Drupal Commerce Core flaw exploited in the wild

SA-CONTRIB-2026-254 covers CVE-2026-118539, rated "Highly critical." Fixes are reported in 3.3.13 and 8.x-2.41, so confirm the version boundary against Drupal's advisory⁵³.

Oct 27

FBI seizes Virtualine bulletproof host

A court authorised seizure of virtualine.net, alleged to support laundering, CSAM distribution, phishing, carding and spam. No arrests or charges have been announced⁵⁵.

Oct 29

Syrian Electronic Army hacker gets 42 months

Ahmad Umar Agha was sentenced for the 2013 AP Twitter hijack, whose fake explosion report DOJ says briefly erased \$136B from Dow stocks⁵⁶.

Oct 29

ARTEX AI framework hit 200-plus organizations

CrowdStrike says China-linked Vapor Panda used ARTEX, a Go framework coordinating several LLM backends, against over 200 organizations, with post-exploitation confirmed at nine⁵⁷.

Oct 28

WordPress 7.1.4 fixes heavily attacked core RCE

The CVSS 8.1 flaw affects core 4.7 to 7.1.3 and has no CVE. Wordfence blocked 62,969 attacks in 24 hours⁵⁸.

Oct 30

Trezor and Ledger warn of implanted wallets

Trezor told anyone who bought from CryptoBilis since March 2026 to move funds to new seeds. Singapore police warned of tampered Ledger devices⁵⁹.

Oct 29

Telegram Android voice-call flaw disclosed

NebuSec says answering a call could run attacker code in versions 8.6.2 to 12.10.3. Version 12.10.4 fixes it, and no exploitation has been seen⁶⁰.

Oct 26

Sweden blocks browser AI chatbots at work

The Swedish government blocked work computers from reaching browser-based ChatGPT and Claude, citing concerns about sensitive data⁶¹.

Oct 29

Microsoft Authenticator AuthMask flaw patched

Enclave found that an Android app with no permissions could obtain tokens from the Authenticator broker. CVE-2026-80097 is now patched^{62,63}.

Oct 30

TeamViewer flaw lets hosts attack controllers

The Hacker News reports a TeamViewer flaw that lets a remote computer attack the user connecting to control it. Check the vendor's details for fixed versions⁵⁴.

Oct 29

nOn ransomware leaks AI-built toolkit

SOCRadar found an exposed server with AI-generated tooling, credential stuffing against 305 FortiGate VPNs, and 23 victims in 14 countries⁶⁴.

Get MAG212 CYBER every week.

The weekly magazine, daily editions and new field guides, free in your inbox.

cyber.mag212.com/subscribe-free →

LOOKING AHEAD · NOVEMBER 2026

What to watch, and what to do

ON THE RADAR

Nov 1

KEV deadline for GitLab and Cisco

Federal civilian agencies must remediate GitLab CVE-2026-97229 and Cisco ASA/FTD CVE-2026-76418⁵¹.

Early November

Binance withdrawals and reserves report

Binance hoped to resume withdrawals before Sunday and planned a Proof of Reserves report for Monday. As of October 31, neither had been confirmed².

Nov 10

Patch Tuesday and Fortinet disclosures

Fortinet will publish advisories for the flaws fixed in its Oct 22 hardening release, which makes patch diffing likely⁶⁵.

Nov 10

KEV deadline for Brotli and PolyShell

The reported federal due date for CVE-2026-111497 and CVE-2026-48356; confirm both with CISA^{24,30}.

Mid-November

OpenAI round versus Anthropic listing

Reuters reports OpenAI wants to close its round before Anthropic's expected listing⁴⁸.

Pending

RHEL and Ubuntu kernel fixes

Watch for Red Hat errata and Ubuntu packages for CVE-2026-98432, then retire the interim nftables rule^{34,35}.

Ongoing

Trezor lab results and Virtualine charges

Trezor's analysis of the implanted device is pending, and no Virtualine operators have been charged^{55,59}.

Ongoing

EU Cyber Resilience Act reporting

Manufacturers' 24-hour reporting duties for actively exploited vulnerabilities have applied since Sept 11, so expect early enforcement news⁶⁶.

DEFENDER TIPS FOR NEXT WEEK

- 01** Before Monday, list every internet-reachable admin interface you own, including firewalls, VPNs, ERP and wallets, and give each one a named owner.
- 02** On anything exposed before its fix, treat "patched" as the start of incident review: hunt, rotate credentials and check for rogue admins.
- 03** Close tickets on running versions, not installed packages: reboot kernels, restart Node services and rebuild images first.
- 04** Pause automatic updates for developer extensions on managed fleets this week, and review which marketplaces your engineers actually use.
- 05** Tell help-desk staff that attackers may now know real names, emails and roles, and rehearse one recovery call against procedure.
- 06** Ask custody and payments teams to show a decoded example of every transaction type their signers accept.
- 07** Pull a 30-day report of device-code sign-ins and justify every remaining exception with a named owner.
- 08** Add AI vendor concentration and pricing changes to the quarterly supplier-risk review, alongside a tested manual fallback.

PRACTISE THIS WEEK'S LESSONS ON CYBER.MAG212.COM

Phishing quiz

Spot device-code and lookalike lures: 10 random scenarios.

Incident response checklist

The first 60 minutes, minute by minute.

Learning paths

Security basics, network engineer, SOC and IR tracks.

Email header analyzer

See where a suspicious email really came from.

FOLLOW THE EVIDENCE

Sources

Click any link to open the original report. Vendor advisories take precedence over this edition when versions or mitigations change. Sources accessed October 31, 2026.

- 1 TRM Labs | North Korea steals USD 6.36 billion from Binance in the largest hack in history | Oct 29, 2026
<https://www.trmlabs.com/resources/blog/north-korea-steals-usd-6-36-billion-from-binance-in-the-largest-hack-in-history>
- 2 Elliptic | Binance: the largest hack in history | Oct 30, 2026 (updated Oct 31)
<https://www.elliptic.co/insights/binance-largest-hack-in-history/>
- 3 Chainalysis | Binance exploit: latest findings and response | Oct 30, 2026
<https://www.chainalysis.com/blog/binance-exploit-latest-findings-and-response/>
- 4 Forbes | Binance's \$6.3 billion hack started with one engineer's laptop | Oct 30, 2026
<https://www.forbes.com/sites/digital-assets/2026/10/30/binances-63-billion-hack-started-with-one-engineers-laptop/>
- 5 Chainalysis | Security incident, October 30 | Oct 30, 2026
<https://www.chainalysis.com/blog/security-incident-october-30/>
- 6 The Block | Chainalysis says hacker using offensive agentic techniques accessed its customers' names and emails | Oct 31, 2026
<https://www.theblock.co/news/business/2026-10-31-chainalysis-says-hacker-using-offensive-agentic-techniques-accessed-its-customers-names-and-emails-432244>
- 7 CISA | Implementing Phishing-Resistant MFA (fact sheet) | Oct 2022
<https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf>
- 8 Palo Alto Networks | Security advisory CVE-2026-109618 | Oct 21, 2026 (updated Oct 29)
<https://security.paloaltonetworks.com/CVE-2026-109618>
- 9 Palo Alto Networks Unit 42 | Threat brief: CVE-2026-109618 and CVE-2026-109619 (PHP2Shell) | Oct 29, 2026 update
<https://unit42.paloaltonetworks.com/cve-2026-109618-cve-2026-109619/>
- 10 Unite.AI | Dream reports PHP2Shell attack chain that compromised 25 servers | Oct 27, 2026
<https://www.unite.ai/dream-reports-php2shell-attack-chain-that-compromised-25-servers/>
- 11 TNW | PHP2Shell flaws exploited, added to CISA KEV | Oct 28, 2026
<https://thenextweb.com/news/php2shell-flaws-exploited-cisa-kev>
- 12 Tailscale | Security bulletins (TS-2026-014 to TS-2026-017) | Oct 26, 2026
<https://tailscale.com/security-bulletins>
- 13 Tailscale | Changelog (v1.104.4) | Oct 28, 2026
<https://tailscale.com/changelog>
- 14 IT-Connect | Tailworm: 11 unpatched Tailscale flaws, including root access via Tailscale SSH | Oct 26, 2026
<https://www.it-connect.tech/tailworm-11-unpatched-tailscale-flaws-including-root-access-via-tailscale-ssh/>
- 15 MAG212 CYBER | Tailscale SSH vulnerabilities TS-2026-014 (Tailworm) | Oct 28, 2026
<https://cyber.mag212.com/tailscale-ssh-vulnerabilities-ts-2026-014-tailworm/>
- 16 Oracle | Critical Patch Update Advisory, October 2026 | Oct 20, 2026 (Rev 2 Oct 26)
<https://www.oracle.com/security-alerts/cpuoct2026.html>
- 17 Rescana | Oracle E-Business Suite CVE-2026-101767: prepare now | Oct 21, 2026
<https://www.rescana.com/post/oracle-e-business-suite-cve-2026-101767-prepare-now>
- 18 The Hacker News | Hackers target critical Oracle E-Business Suite flaw | Oct 2026
<https://thehackernews.com/2026/10/hackers-target-critical-oracle-e.html>
- 19 Security Affairs | Oracle E-Business Suite flaw under active attack, 950 systems exposed | Jul 1, 2026
<https://securityaffairs.com/194599/security/oracle-e-business-suite-flaw-under-active-attack-950-systems-exposed.html>
- 20 MAG212 CYBER | CVE-2026-101767 Oracle EBS vulnerability | Oct 28, 2026 (modified Oct 30)
<https://cyber.mag212.com/cve-2026-101767-oracle-ebs-vulnerability/>
- 21 Microsoft Security Blog | Inside a malicious Claude Code-branded Cursor extension with a persistent SSH backdoor | Oct 30, 2026
<https://www.microsoft.com/en-us/security/blog/2026/10/30/inside-malicious-claude-code-branded-cursor-extension-persistent-ssh-backdoor/>
- 22 Adobe | Security bulletin APSB26-73 (Adobe Commerce) | Jul 14, 2026 (updated Aug 11)
<https://www.adobe.com/trust/security/products/commerce/apsb26-73.html>
- 23 Sansec | Magento CMS block loader (deepveindrilling) | Oct 24, 2026 (modified Oct 25)
<https://sansec.io/research/magento-cms-block-loader-deepveindrilling>
- 24 Rescana | Adobe Commerce / Magento CVE-2026-48356 file upload RCE, KEV October 2026 | ~Oct 28, 2026
<https://rescana.com/post/adobe-commerce-magento-cve-2026-48356-file-upload-rce-kev-october-2026>
- 25 The Hacker News | Hackers infect 953 online stores | Oct 26, 2026
<https://thehackernews.com/2026/10/hackers-infect-953-online-stores-with.html>
- 26 MAG212 CYBER | PolyShell CVE-2026-48356 Magento CMS block loader | Oct 2026
<https://cyber.mag212.com/polyshell-cve-2026-48356-magento-cms-block-loader/>
- 27 Node.js | October 2026 security releases | Oct 21, 2026
<https://nodejs.org/en/blog/vulnerability/october-2026-security-releases>
- 28 The Hacker News | Node.js Brotli decoder bug could allow code execution | Oct 22, 2026
<https://thehackernews.com/2026/10/nodejs-brotli-decoder-bug-could-allow.html>
- 29 Canadian Centre for Cyber Security | AL26-027: Critical vulnerability impacting Google Brotli (CVE-2026-111497) | Oct 28, 2026
<https://cyber.gc.ca/en/alerts-advisories/al26-027-critical-vulnerability-impacting-google-brotli-cve-2026-111497>
- 30 BleepingComputer | CISA warns of hackers now exploiting critical Node2Shell flaw | Oct 28, 2026
<https://bleepingcomputer.com/news/security/cisa-warns-of-hackers-now-exploiting-critical-node2shell-flaw>
- 31 MAG212 CYBER | CVE-2026-111497 Node.js Brotli vulnerability | Oct 2026
<https://cyber.mag212.com/cve-2026-111497-nodejs-brotli-vulnerability/>
- 32 OpenCVE | CVE-2026-98432 | Oct 15, 2026 (updated Oct 30)
<https://app.opencve.io/cve/CVE-2026-98432>
- 33 Red Hat | CVE-2026-98432 | accessed Oct 31, 2026
<https://access.redhat.com/security/cve/cve-2026-98432>
- 34 Red Hat | RHSB-2026-016 security bulletin | Oct 30, 2026
<https://access.redhat.com/security/vulnerabilities/RHSB-2026-016>
- 35 Ubuntu | CVE-2026-98432 | Oct 15, 2026 (updated Oct 30)
<https://ubuntu.com/security/CVE-2026-98432>

SOURCES, CONTINUED

36	Debian Security tracker: CVE-2026-98432 accessed Oct 31, 2026 https://security-tracker.debian.org/tracker/CVE-2026-98432	53	The Hacker News Hackers actively exploit highly critical Drupal Commerce flaw Oct 30, 2026 https://thehackernews.com/2026/10/hackers-actively-exploit-highly.html
37	SUSE CVE-2026-98432 Oct 30, 2026 https://www.suse.com/security/cve/CVE-2026-98432.html	54	The Hacker News TeamViewer flaw lets remote computers attack connecting users Oct 30, 2026 https://thehackernews.com/2026/10/teamviewer-flaw-lets-remote-computers.html
38	stack.watch CVE-2026-98432 accessed Oct 31, 2026 https://stack.watch/vuln/CVE-2026-98432/	55	The Record FBI seizes Virtualine bulletproof hosting domain Oct 28, 2026 https://therecord.media/fbi-seizure-csam-virtualine
39	Anthropic Discovering vulnerabilities with Claude Oct 27, 2026 https://www.anthropic.com/research/discovering-vulnerabilities-with-claude	56	The Hacker News Syrian hacker behind fake tweet that rattled markets sentenced Oct 30, 2026 https://thehackernews.com/2026/10/syrian-hacker-behind-fake-tweet-that.html
40	Wiz Vulnerability database: CVE-2026-98432 accessed Oct 31, 2026 https://www.wiz.io/vulnerability-database/cve/cve-2026-98432	57	The Hacker News Chinese hackers use AI-powered ARTEX framework Oct 30, 2026 https://thehackernews.com/2026/10/chinese-hackers-use-ai-powered-artex-to.html
41	ANY.RUN SkyW4lker phishing kit analysis Oct 27, 2026 https://any.run/cybersecurity-blog/skyw4lker-phishing-kit-analysis/	58	The Hacker News WordPress RCE flaw draws nearly 63,000 attacks Oct 30, 2026 https://thehackernews.com/2026/10/wordpress-rce-flaw-draws-nearly-63000.html
42	Microsoft Learn Conditional Access: authentication flows updated Mar 24, 2026 https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-authentication-flows	59	The Hacker News Trezor warns of suspected hardware implant Oct 30, 2026 https://thehackernews.com/2026/10/trezor-warns-of-suspected-hardware.html
43	MAG212 CYBER SkyW4lker device-code phishing targets Microsoft 365 Oct 28, 2026 (updated Oct 30) https://cyber.mag212.com/skyw4lker-device-code-phishing-microsoft-365/	60	The Hacker News Telegram Android flaw lets attackers run code via voice calls Oct 29, 2026 https://thehackernews.com/2026/10/telegram-android-flaw-lets-attackers.html
44	Yahoo Finance Stock market today, Friday October 30: Dow, S&P 500, Nasdaq, Amazon, Intel, AI sell-off (live blog) Oct 30, 2026 https://finance.yahoo.com/markets/live/stock-market-today-friday-october-30-dow-sp-500-nasdaq-amazon-intel-ai-sell-off-191429143.html	61	Euronews Swedish government blocks ChatGPT and Claude: here's why Oct 26, 2026 https://www.euronews.com/2026/10/26/swedish-government-blocks-chatgpt-and-claude-heres-why
45	StockTitan Stock market today live, October 30, 2026 Oct 30, 2026 https://www.stocktitan.net/articles/stock-market-today-live-october-30-2026	62	The Hacker News ThreatsDay bulletin: critical firewall flaws and more Oct 29, 2026 https://thehackernews.com/2026/10/threatsday-critical-firewall-flaws.html
46	Investing.com (Reuters) Nasdaq tumbles at open as Amazon, Intel add to AI spending woes Oct 30, 2026 https://www.investing.com/news/stock-market-news/nasdaq-tumbles-at-open-as-amazon-intel-add-to-ai-spending-woes-4988016	63	Enclave AuthMask: we made Microsoft Authenticator hand over tokens Oct 2026 https://enclave.ai/blog/authmask-we-made-microsoft-authenticator-hand-over-tokens
47	Investing.com OpenAI cuts funding target by \$10 billion to \$20 billion - FT Oct 31, 2026 https://ng.investing.com/news/company-news/openai-cuts-funding-target-by-10-billion-to-20-billion--ft-2772582	64	SOCRadar n0n ransomware: AI-assisted extortion Oct 2026 https://socradar.io/blog/n0n-ransomware-ai-assisted-extortion/
48	TNW OpenAI funding round target cut to \$20bn (FT) Oct 31, 2026 https://thenextweb.com/news/openai-funding-round-20bn-target-cut-ft	65	Fortinet Fortinet releases security hardening release for multiple products Oct 21, 2026 https://www.fortinet.com/blog/ciso-collective/fortinet-releases-security-hardening-release-for-multiple-products
49	OWASP GenAI Security Project OWASP Top 10 for LLM Applications 2025 2025 https://genai.owasp.org/llm-top-10/	66	Jones Day EU Cyber Resilience Act: 24-hour reporting duties start September 11, 2026 Jul 2026 https://www.jonesday.com/en/insights/2026/07/eu-cyber-resilience-act-24-hour-reporting-duties-start-september-11-2026
50	NIST AI Risk Management Framework accessed Oct 31, 2026 https://www.nist.gov/itl/ai-risk-management-framework	67	MAG212 CYBER Heists, hijacked scripts, hostile regex: MAG212 CYBER, October 30, 2026 Oct 30, 2026 https://cyber.mag212.com/heists-hijacked-scripts-hostile-regex-mag212-cyber-october-30-2026/
51	The Hacker News CISA adds actively exploited GitLab RCE (and Cisco ASA/FTD) to KEV Oct 30, 2026 https://thehackernews.com/2026/10/cisa-adds-actively-exploited-gitlab-rce.html	68	MAG212 CYBER The edge, the cloud and the code: MAG212 CYBER, October 29, 2026 Oct 29, 2026 https://cyber.mag212.com/the-edge-the-cloud-and-the-code-mag212-cyber-october-29-2026/
52	The Hacker News Ruby fixes three regex-engine bugs behind critical GitLab RCE flaws Oct 2026 https://thehackernews.com/2026/10/ruby-fixes-three-regex-engine-bugs.html	69	cside Polymarket client-side supply chain attack Jun 26, 2026 https://cside.com/blog/polymarket-client-side-supply-chain-attack

Publication notes. Author and editorial direction: El Mostafa Ouchen. Summaries, technical field guides and defensive commentary prepared for MAG212 CYBER with AI assistance, from public sources listed above; this edition does not reproduce source articles and claims no independent forensic access. Items that could not be confirmed against a primary source were left out. Read and subscribe free: cyber.mag212.com/subscribe-free