

Chainhound: Endpoint Detection and Response for the XRP Ledger

Cove Chainhound and Cove Shield whitepaper

October 30, 2026 · @Matt

This paper describes Chainhound and Cove Shield as built in October 2026 (services/backend v0.3.0, walletd 0.51, Cove 0.4.29), and marks what is planned but not yet built. It is a companion to the Cove Wallet whitepaper, Split-Authority Custody, and to the Cove Key.

Abstract

Chainhound finds attacks on the XRP Ledger as they happen, and Cove Shield stops every Cove wallet from paying the attacker within minutes of a person approving the block.

It brings the model of enterprise endpoint security to a public ledger:

- **Sensors**: Cove's own XRP Ledger nodes read every validated ledger, and each wallet reports its device security posture once a day.
- **Detection engines**: seven signatures, each built from real XRP Ledger incidents, score what they find from 0 to 100 and explain every score.
- **An analyst console**: graphs, cases, tags, watches and alerts for investigation.
- **A definitions feed**: Cove Shield, lists of blocked addresses signed with Ed25519 keys that every wallet pins, delivered within minutes.
- **An agent on every endpoint**: walletd, the wallet's signer, refuses to sign a payment to a blocked address, and enforces the user's own policy before every signature.

The design rule is simple: software may detect and nominate, but only a second person can approve a block, and only a signed feed can deliver one. No legitimate account is blocked by a heuristic alone, and a compromised Chainhound cannot block anything by itself.

1. The problem: theft on a ledger that settles in seconds

An XRP Ledger payment is final in 3 to 5 seconds, and XRP has no issuer that can freeze it. Once a victim signs, nothing reverses the theft. Defence has to act before the signature.

The largest losses show the scale:

- **Bitget, September 2026**: about 102.9 million XRP moved through one new account in under five hours, then split into round lots.
- **Chris Larsen's personal wallets, January 2024**: about 213 million XRP left one account in eight payments in a single day.
- **D'CENT and XRPH app wallets, September 2026**: more than 10,000 wallets emptied in waves, each into one or two accounts created hours before.

These attacks leave patterns on the ledger, and the patterns repeat. Many use the ledger's own features: partial payments that display one amount and deliver another, regular keys and signer lists that hand control to a stranger, and tokens anyone can issue under any name.

2. Why enterprise endpoint security belongs on the blockchain

Enterprises stopped relying on users to spot every attack a long time ago. They put an agent on every laptop and phone, feed it telemetry from a sensor network, run detection engines centrally, push new definitions to every endpoint within minutes, accept only signed code, and enforce policy from a management console. Self-custody wallets today work like the unmanaged PC of twenty years ago: every user alone, every decision theirs, every mistake final.

Cove applies those controls to the wallet without taking the keys away from the user.

Enterprise control	What it does in an enterprise	Cove's equivalent
Endpoint agent	Runs on every device, enforces policy locally, can't be turned off by the user's apps	**walletd**, the only code that holds keys and signs. It checks Cove Shield, the address book, the PIN and the user's presence before every signature; the app's interface can't skip it (whitepaper, Sections 4 and 7)
Sensor network	Telemetry from endpoints and the network, gathered centrally	Cove's own **rippled and Clio** read every validated ledger; each wallet's **daily check-in** reports device security signals (root or jailbreak, hooking tools, a debugger, an emulator, no screen lock, a copy not signed by Cove) without keys, addresses or balances
Detection engines	Signatures and behaviour rules, versioned, tested, explainable	**Seven detectors** (Section 6), each a pure function with a version, unit and replay tests, and a per-point explanation
Definitions updates	New indicators pushed to every agent within minutes	The **rapid Shield feed**: approved addresses reach every wallet within about 10 minutes, signed in Cloud KMS, and lapse within 14 days unless the offline-signed list carries them
Code signing	Only code from a trusted publisher runs	Every document a wallet acts on is **signed and pinned**: the main and rapid Shield feeds, the reviewed trading pairs and the fee config, each with its own key and signing domain, so none passes as another. Android builds check they are signed by Cove's certificate
Device compliance	Non-compliant devices lose access	A store build **won't open the wallet on an insecure phone**: no secure hardware, no screen lock, an unlocked bootloader or unverified system (from Android key attestation), or a copy not signed by Cove
Mobile device management (MDM) policy	Granular, per-device rules set by an administrator	**Policy the user sets and walletd enforces**: a Spend key that locks when idle, an address book that only the PIN and the system sheet can add to, a co-signer on Save, a hold that makes Save transactions wait days, and a duress wallet. Cove's own staff get **role-based access** in Chainhound and the Console (viewer, editor, admin), with four eyes on every block
Incident response	Analysts investigate, contain, and record	**Chainhound's console**: graphs of accounts and ledgers, cases, tags, watches with text and email alerts, and an audit log kept two years

What is different from enterprise MDM, on purpose. An enterprise owns its devices and can wipe them. Cove does not own the user's money, so Cove's console never holds a key and can never move funds or change a wallet's policy remotely. Its only power over a wallet is to deliver a signed list of addresses the wallet refuses to pay, bounded in time when signed online. Everything else stays with the user.

How it fits with Cove's other papers.

- Split-Authority Custody describes the endpoint: keys in the phone's Secure Enclave or Android Keystore and on a Cove Card's secure element, signer lists on the ledger that decide which keys can move each account, recovery from any single loss, and a signing component that shows the user exactly what it signs on the phone's own system sheet.
- The Cove Key describes the backup: a standard 24-word BIP-39 key written as 12 rows with check values that name the row a mistake is on, so a backup is proven before it's needed.
- This paper describes the network around those endpoints: the sensors, detection, approval and delivery that let every wallet learn about an attacker within minutes of the first victim.

Each layer works without the next: a wallet signs and recovers with no backend at all; Chainhound adds detection; Cove Shield adds enforcement.

3. Platform architecture

Chainhound sits between Cove's own ledger nodes and Cove Shield: it watches every ledger, and what it finds reaches wallets only through a person's approval and a signed feed.

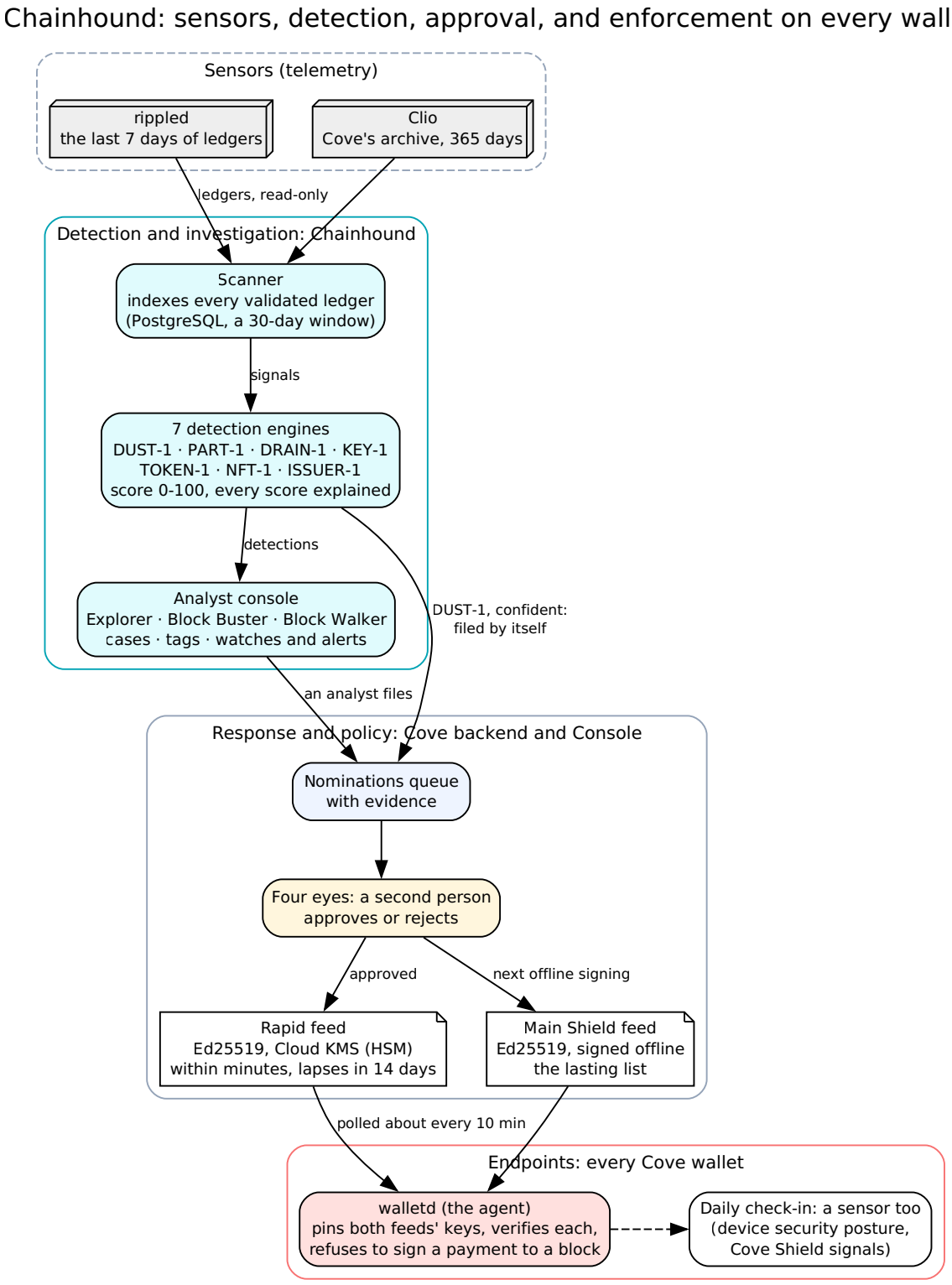


Figure 1. Sensors, detection and investigation, response and policy, and the endpoint that enforces it.

- **Sensors.** rippled keeps the last 7 days of ledgers; Clio keeps Cove's own archive, 365 days by default. The scanner reads them over a private network with two read-only methods (`server_info`, `ledger`).
- **Detection.** The scanner indexes each validated ledger into PostgreSQL (about 6.5 KB a ledger) and routes what it finds to the detectors.

- **Investigation.** Analysts work in Chainhound's console: the Explorer, Block Buster (live ledgers as a graph), Block Walker (one ledger at a time), Block Timeline, account graphs, cases, tags, and watches that alert by text message or email.
- **Response.** Nominations go to Cove's backend, where a second person approves or rejects them in the Console.
- **Enforcement.** Every Cove wallet verifies the signed feeds and refuses to sign a payment to a blocked address.

4. Attacks on the XRP Ledger and how Chainhound answers them

Every common theft on the XRP Ledger maps to at least one Chainhound detector or analyst view. Each row comes from Chainhound's incident records, which hold the sources and the accounts and transactions checked on Mainnet.

Attack	How it works	Real incidents	Chainhound detection	Shield category
Address poisoning	A look-alike address sharing the first and last characters of one the victim pays sends a tiny payment, so the victim later copies the wrong address from history	Dust sent to the receivers of the Larsen theft (Jan 2024) and to every hop of the Bitget thief (Sep 2026)	DUST-1, with a look-alike	`poisoning`
Dusting and phishing lures	Tiny payments sprayed at many accounts, with a link or "airdrop" in the memo leading to a site that collects secrets	"Ripple is releasing 3 billion XRP" (Feb 2020, about 2.1M XRP stolen); fake giveaways (2020 to 2026)	DUST-1, without a look-alike	`dusting`
Display spoof	A partial payment shows a large Amount but delivers dust, to look like a real deposit	A campaign showing about 100 XRP and delivering 744 drops to 15 accounts (Mainnet check, Oct 2026)	DUST-1 (display spoof)	`dusting`
Partial-payment deposit fraud	A service credits the displayed Amount instead of the delivered amount and pays out the difference	Beaxy (Aug 2019); a payment showing 25.6 billion XRP sent to Bitfinex (Jan 2024)	PART-1	`exploit`
Mass drain with stolen keys	Many unrelated accounts emptied into one new account within hours	GateHub (2019, 14.4M XRP collected from 37 accounts); XRPH (4,011 wallets) and D'CENT (6,678 or more), Sep 2026	DRAIN-1	`theft`
Takeover by regular key or signer list	The victim is tricked into signing SetRegularKey or SignerListSet, handing control to the attacker, who empties the account	Fake Ripple giveaway asking Xumm users to sign SetRegularKey (Jul 2022)	KEY-1	`drainer`
Copycat token	A token issued under a known code, such as RLUSD, by another issuer and sold on the DEX and in AMM pools	Fake RLUSD before and after Ripple's launch (Dec 2024 onward)	TOKEN-1	`impersonation`
NFT offer trap	A priced NFT sell offer aimed at a victim, presented as a "reward" to accept	"Reward" NFT offers in giveaway campaigns	NFT-1	`scam`

Attack	How it works	Real incidents	Chainhound detection	Shield category
Issuer honeypot	An issuer turns on clawback or freezes its token after people buy it	Honeypot tokens	ISSUER-1	`exploit`
Exchange or treasury theft	Large sums move from a service's wallets to a new account, then split into round lots	Bitget (Sep 2026, about 102.9M XRP); Larsen (Jan 2024, about 213M XRP)	Analyst views: Block Buster, the account graph, watches. The Larsen accounts are on Shield's confirmed list	analyst's choice
Supply-chain backdoor	A trojaned library sends seeds to the attacker; the theft appears later as a drain	xrpl.js on npm (Apr 2025, CVE-2025-32965)	DRAIN-1 once the stolen seeds are used; Cove's builds pin every dependency exactly	`theft`

5. Hidden payloads on the ledger

The ledger can carry encoded content that is not a theft by itself but leads to one: lure links in memos, NFT metadata that points to files, and currency codes that spell a familiar name. Chainhound and Cove treat all of it as inert data, never as something to run or render.

- **Memos.** Any transaction can carry hex-encoded memos. The scanner decodes their text, and links and lures count toward DUST-1 and NFT-1.
- **Currency codes.** TOKEN-1 decodes currency codes and compares them as a reader sees them, so a code that is spelled differently but reads the same is still a copy.
- **NFT files.** Cove's IPFS gateway refuses content a browser would run (HTML, SVG, scripts, XML) and serves the rest with a sandboxing content security policy; the wallet shows only PNG, JPEG, GIF and WebP images, and its fetcher refuses local and private network addresses and caps the size.
- **The console.** Chainhound shows everything from the ledger as escaped text; nothing from a memo, tag or case note is rendered as HTML.

Chainhound does not yet classify binary malware inside memos or NFT files. It finds the delivery pattern (the spray, the lure, the look-alike) and blocks the sender. Scanning decoded payloads against known malware and phishing indicators is on the roadmap.

6. The detection engines

Chainhound runs seven detectors on every validated ledger, all automatically. Each is built from real incidents on the XRP Ledger: it scores what it finds from 0 to 100 against a set of rules, and records why, with the transactions behind it. The same ledgers and rules always give the same scores.

DUST-1 files its most confident findings to Cove Shield by itself. The six **technique detectors** flag findings for an analyst, who decides whether to nominate. Lower scores are kept for the record. An allowlisted account (a tagged exchange, issuer or service) is never scored. Nothing reaches a wallet without a second person's approval.

DUST-1's rules change only with four eyes: an editor proposes a change, it is replayed against recent senders, and a different admin approves it.

The rules themselves, their weights and their thresholds are not published, so an attacker can't tune a campaign to stay under them. Analysts see each rule, and every point of every score, in Chainhound. What each detector looks for:

DUST-1: Dusting and address poisoning

Tiny payments. Address poisoning plants a look-alike of an address the victim really uses in their history, so they copy it next time. Dusting sprays tiny payments at many accounts, often with a lure in the memo. DUST-1 tells the two apart. It also catches partial payments dressed up to look like a real deposit. A payment to someone the sender already deals with isn't poisoning.

PART-1: Partial-payment fraud

A partial payment shows a large amount but delivers far less. A service that credits what the payment shows, rather than what arrived, pays out the difference. PART-1 finds the senders who aim such payments at services.

DRAIN-1: Mass drain

Many unrelated accounts emptied into one new account within hours. This is the trace left by leaked keys, a trojaned library or a wallet bug being exploited.

KEY-1: Account takeover by key

A victim tricked into signing SetRegularKey or SignerListSet hands control of their account to the attacker's key, and the account is then emptied. KEY-1 follows keys that take over several accounts.

TOKEN-1: Copycat token

A token issued under the code of a known one, such as RLUSD, by another issuer, so that it trades on the real one's name. Codes are compared as a person reads them, not byte by byte.

NFT-1: NFT sell-offer trap

Priced NFT sell offers aimed at many accounts and presented as a "reward" to accept. Accepting one pays for a worthless NFT.

ISSUER-1: Issuer clawback or freeze

An issuer that claws tokens back from its holders, or freezes them all, after people buy in: a honeypot token.

Tuned on live Mainnet

Rules that looked right on paper were tightened after running against live traffic, each change with a test. At first, ordinary DEX trading, airdrops to token holders and bots moving funds between their own accounts were flagged. They are now told apart from attacks. Over 18,748 Mainnet ledgers after those changes, DUST-1 sent 3 senders to an analyst and filed none by itself.

Exchanges, issuers and services tagged by analysts are allowlisted automatically, and the allowlist follows the tag.

7. From detection to enforcement

An approved address is blocked in every Cove wallet within minutes, and nothing is blocked without a second person's approval.

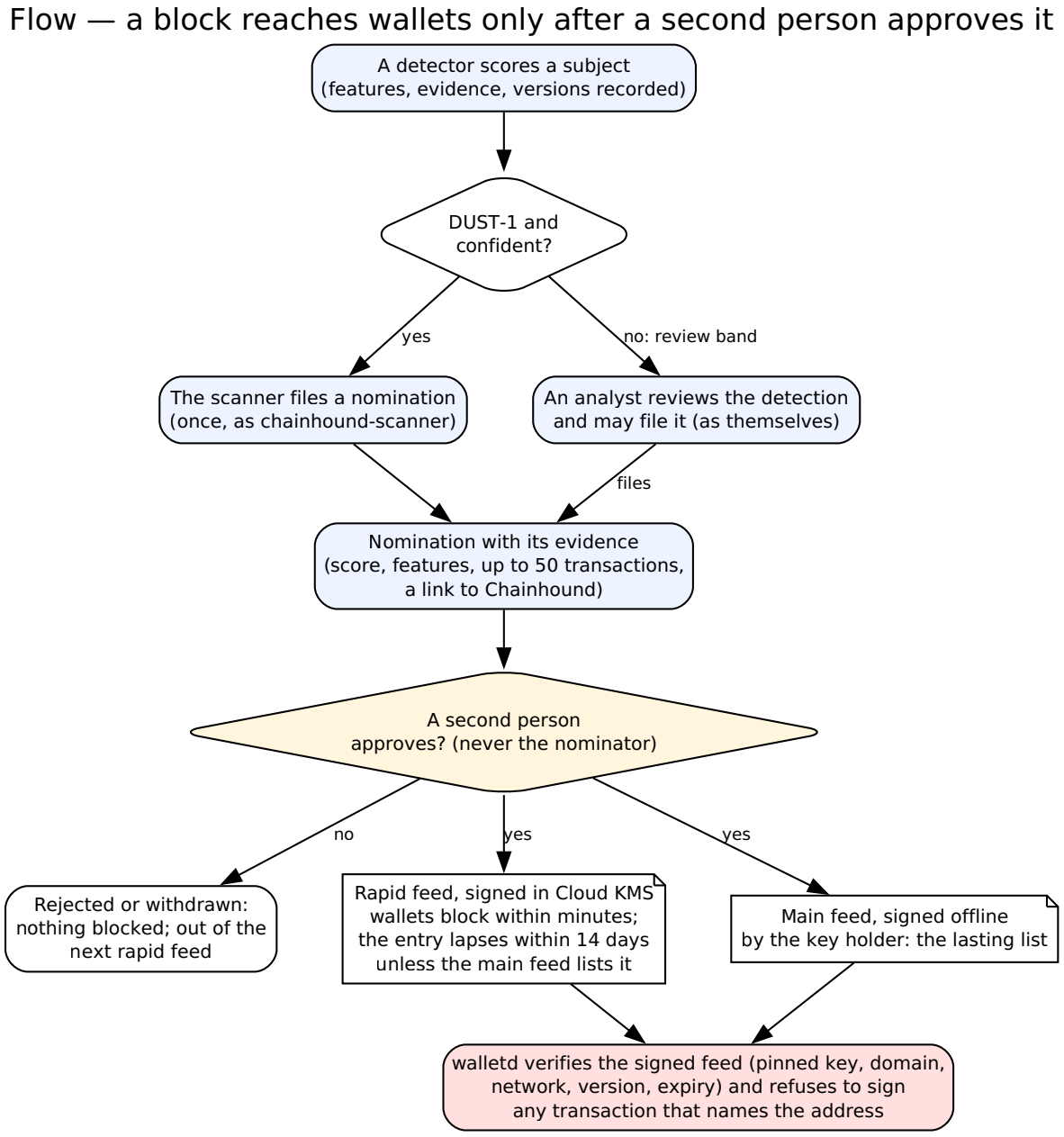


Figure 2. Two decisions and two feeds between a detection and a wallet.

Every nomination carries its evidence: the detector and ruleset versions, the score and each feature behind it, up to 50 transactions, and a link to Chainhound. Admins can decide a whole campaign's nominations at once, with one audit entry per address. Wallets poll the rapid feed about every 10 minutes; a withdrawn nomination is unblocked at the next poll, because each rapid feed replaces the last.

8. Cryptography and security controls

Every block a wallet enforces is signed with an Ed25519 key the wallet pinned when it was built, and no single person or server can add a permanent block.

Control	How it works	What it prevents
Two signed feeds, two key sets	The main Shield feed is signed offline by the key holder. The rapid feed is signed online by a key in Google Cloud KMS (`EC_SIGN_ED25519` , HSM protection, FIPS 140-2 Level 3, not exportable). Wallets pin each set separately	A forged feed, and one feed's key being used for the other
Domain-separated signatures	Rapid signatures cover `cove-shield-rapid-v1` and the payload, so a main-feed signature never verifies as a rapid one, or the reverse	Cross-feed replay
Strict verification	Ed25519 strict verification; exact JSON fields; checksum-valid addresses; network match; version rollback refused; issue and expiry times checked	Tampered, replayed, stale or wrong-network feeds
A bounded online key	A rapid entry lapses within 14 days unless the offline feed carries it; the rapid key can never touch the main list	A compromised backend blocking for long, or unblocking a main-list address
Four eyes	The person who nominates an address can't approve it (enforced in the store). Ruleset changes need a second admin	One insider blocking or silencing an address
Least-privilege tokens	Chainhound's intake token reaches six routes: file, list, read and withdraw nominations, look up an address, read what is blocked. It can't approve, publish feeds, push or manage installs	A compromised Chainhound approving its own nominations
Keys on the phone	walletd keeps keys in the iOS Secure Enclave and Keychain or the Android Keystore (StrongBox, or TEE), opened with the PIN and biometrics	Key theft from the app or a backup
Enforced in the signer	walletd checks every account a transaction names against Shield before signing, token issuers included, at any depth	A compromised or buggy interface paying a blocked address
Sign-in and audit	Analysts sign in through Google with a verified email; roles are viewer, editor and admin. Every action is in an audit log kept two years; every KMS signature is in Cloud Audit Logs	Anonymous or untraceable actions
Network isolation	The scanner reads the ledger read-only; containers can't reach the cloud metadata server; admin ports are reachable only through Google IAP or from Chainhound's own VM	Lateral movement from a compromised container

The trade, stated plainly. Before the rapid feed, a compromised backend could only withhold updates. With it, someone holding the backend and its KMS key can block an address for up to 14 days, or drop rapid entries early. Cove accepts this for blocking within minutes. They can never touch the offline-signed list. Chainhound's intake token can also withdraw a nomination after approval, which takes it out of the next rapid feed; whether that power stays with Chainhound or moves to the Console is an open decision.

9. Operations, limits and roadmap

Operations.

- **Deployment.** Chainhound and its scanner run on a Google Cloud VM of their own; rippled and Clio run on the backend's VM, reached over a private network. The data disks are snapshotted daily and kept 30 days.
- **History.** The scanner indexes a window of the ledger (30 days by default) at about 6.5 KB per ledger, about 150 MB a day.
- **Health.** The Nodes page shows how far behind each source the scanner is; the scanner reports unhealthy when its newest ledger is more than 5 minutes old, and restarts if any of its tasks stops.
- **Explainability on demand.** `cove-chainhound-scanner explain <address>` scores one sender and prints every feature and its evidence.

Limits.

- Only DUST-1 files nominations by itself. The technique detectors need an analyst, and their rules are fixed in code, without four-eyes rulesets yet.
- The scanner sees only its window: a look-alike of a counterparty from before it is missed until history is deeper.
- TOKEN-1 checks one named token (RLUSD) by name, and the rest against established issuers in the index.
- Shield protects Cove wallets. It can't stop a payment signed in another wallet, and it can't freeze XRP already stolen.
- Exchange-scale thefts are found through analyst views and watches, not by a dedicated detector.

Roadmap.

1. Four-eyes rulesets for the technique detectors.
2. A detector for exchange-scale outflows: a new account taking very large sums, then splitting them into round lots.
3. More checked tokens for TOKEN-1.
4. Scanning decoded memo and NFT content against known malware and phishing indicators.
5. Acting on the device security verdicts the wallets already report, as a compliance rule the user opts into.
6. Sharing approved indicators with other wallets and exchanges in a signed format.

Conclusion

Chainhound turns the XRP Ledger's public record into telemetry, its attack history into signatures, and Cove's wallets into endpoints that enforce a signed, reviewed list before they sign. The user keeps the keys and the policy; Cove contributes detection, a second pair of eyes, and delivery within minutes.

Sources

Incident figures come from Chainhound's incident records (`services/backend/crates/chainhound/src/incidents.rs`), which cite these sources and list the accounts and transactions checked on Mainnet. Detector and feed details come from `services/backend/docs/chainhound-scanner.md` and `docs/shield-rapid-feed.md`, and the scanner's code.

- Larsen theft: ZachXBT, The Block, US forfeiture complaint, N.D. Cal. 4:25-cv-02324
- Bitget hack: Bitget incident update, Bitcoin.com, CoinDesk
- GateHub hack: XRP Forensics, Cointelegraph
- xrpl.js backdoor: XRPL disclosure, GHSA-33qr-m49q-rxfx
- Partial payments: XRPL documentation, rippled issue 3043, Cointelegraph on Bitfinex
- XRPH and D'CENT drains: crypto.news, CryptoSlate
- SetRegularKey phishing: The Crypto Basic, Xaman: how to rekey
- Copycat tokens: Ripple RLUSD token addresses, U.Today
- Giveaways and phishing: Decrypt, Bithomp, Cointelegraph on the fake Ledger app