ComFix Software

Termguardium Sentinel

User activity monitoring and fraud detection for legacy terminal emulator sessions

> Termguardium — security and access for green-screen and character-mode enterprise applications.

Generated 2026-10-14 · Confidential — for customer and partner use

User activity monitoring and fraud detection for legacy terminal emulator sessions

ComFix Software



Executive summary

Termguardium Sentinel is a high-performance **session relay and security sensor** for Telnet, TLS, SSH, and IBM terminal protocols (TN3270, TN5250). It sits **in the network path** between your **web or desktop terminal emulators** and host systems, producing **evidence-grade audit trails**, **searchable forensics**, and **policy enforcement** grounded in what users actually see and type—not just TCP bytes.

For security and fraud teams, Sentinel delivers the missing **user activity monitoring (UAM)** layer on green-screen workloads: who connected, through which channel, which screens appeared, which keys were pressed (with redaction), which rules fired, and whether the session was stopped or stepped up for approval.

Sentinel is the **only product in the suite that enforces admission policy and owns session evidence**. Portal and Station are terminal emulators and clients; Director is the administration plane.

The challenge

Fraud, insider threat, and compliance investigations on IBM i, mainframe, and Unix terminal emulators suffer from three recurring gaps:

1. **No authoritative session record** — Host logs show job names, not screen-level behavior or correlated identity across jump paths.
2. **Recorder tools without semantics** — Packet capture stores bytes; investigators need **screens, fields, and timelines**.
3. **Detection too late** — Batch log review after a loss event instead of **in-session** alert, block, or step-up when a sensitive screen appears.

Sentinel addresses these by **decoding terminal traffic in real time**, retaining **ordered screen frames**, and applying **rules on interpreted content**—the same stream used for replay and analytics.

What Sentinel does

Universal session relay

- Listens on configured **channels** (per-port listeners) and forwards to upstream hosts.
- Supports **Telnet, TLS, SSH**, and IBM **3270 / 5250** display sessions (shared decode with Portal and Station terminal emulators).
- Optional upstream hardening: TLS, SSH host-key verification, client certificate requirements on listen paths (Identity Guard deployments).

Evidence and UAM

Sentinel captures a **coherent session story**:

Evidence type	Purpose
Audit log	OPEN/CLOSE pairs, user binding, channel, close reasons
Traffic log	Directional payload record
Screen log	Recv-side **screen snapshots** when the decoded grid changes materially
Combined log	Screens plus **keystrokes** with printable redaction
Structured artifacts	Versioned screen frames for replay APIs
Database / Elasticsearch	Optional enterprise search and retention backends

Integrity contract: When capture or persistence fails, sessions enter a **visible degraded state**—Sentinel does not silently pretend full visibility. Operators see integrity events in admin and audit output.

Forensics and investigation

- **Live sessions** and **historical sessions** with channel name, admitted user, and **screens captured** count.
- **Session replay**: screen-by-screen navigation, screen + keys mode, timeline, export.
- **Search** across traffic and screen text (file and database modes).
- **Analytics summary**: user journey hints, field edits, rule context, redaction status.

Investigators can answer: *What did this user see before the transfer? Which screen triggered the rule? Was evidence complete for this session?*

Fraud detection and policy enforcement

Sentinel applies **semantic policies** on decoded screens—not merely IP or port ACLs:

- **Screen and field rules** — Match titles, text, flows; actions include **allow**, **alert**, **block**, **escalate**, and **step_up**.
- **Step-up pause** — Session relay halts until an administrator approves or denies via admin console.
- **Live session kill** — Operator or SOC integration terminates an active relay.
- **Rule audit trail** — Rule firings and response markers in logs and optional database events.
- **DLP-oriented masking** — Sensitive field meanings and nondisplay regions masked in **logs** while preserving authorized replay artifacts where configured.
- **Protocol field awareness** — TN3270 field attributes (protected, MDT, nondisplay) merge into frames for field-aware predicates and masking.

AI-assisted meaning (screen templates, field suggestions) accelerates rule authoring; **user-defined rules remain authoritative**. Full autonomous fraud scoring is on the product roadmap—today's strength is **deterministic, explainable rules on captured semantics** plus rich replay for retrospective fraud analysis.

Identity Guard admission (with Portal + Director)

When **Identity Guard** is enabled:

- **Channel ACL** — Only assigned users/groups receive session admission to a channel.
- **Single-use connect tokens** — TCP handshake before host bytes; optional signed token mode.
- **MFA at admission** — Portal proves MFA in session-request metadata; Sentinel fails closed on mismatch.
- **Session limits** — Idle and maximum duration enforced at the relay.
- **SIEM webhook out / SOC kill in** — Operational hooks for security operations centers.

Sentinel is the **enforcement point**; Portal proves identity; Director holds assignments and profiles.

Key strengths

1. **In-path, client-agnostic recording** — Web and desktop **terminal emulators** that route through Sentinel share the same evidence pipeline.
2. **Screen-native security** — Policies speak the language of **5250 menus, 3270 maps, and VT applications**, not generic five-tuple rules.
3. **Investigation-ready artifacts** — Replay, export, and search reduce mean time to understand for fraud and audit cases.
4. **Fail-closed security posture** — Admission denials, token reuse rejection, degraded evidence signaling, and optional block-on-degraded enforcement.
5. **Enterprise runtime** — Designed for concurrent sessions, container deployment, and channel administration in production.
6. **Decode parity with Portal and Station** — One shared terminal engine so **what users see in the emulator matches what forensics captures**.

Typical use cases

- **Insider threat and fraud investigation** on IBM i payment or transfer screens after the fact, with frame-accurate replay.
- **Real-time control** — Block or step-up when a restricted function key or screen template appears.
- **Regulatory audit** — Demonstrate who accessed which host application and what they viewed, with redacted keystroke evidence.
- **SOC visibility** — Central session list, kill switch, and SIEM integration for terminal abuse.
- **Brokered access** — All Portal/Station terminal emulator traffic through Sentinel so **direct-to-host bypass** is eliminated in hardened deployments.

Deployment snapshot

Item	Typical value
Admin console	HTTPS on configurable port (default lab: port 63592)
Evidence storage	File (default), optional PostgreSQL / Elasticsearch
Integration	Portal and Station terminal emulators connect to Sentinel listen channels

Sentinel does **not** replace Director for user administration or Portal/Station for end-user terminal emulation—it **relays, records, enforces, and proves**.

Related reading (PDF)

- Termguardium Suite Overview (PDF)
- Termguardium Portal — Web Terminal Emulator (PDF)
- Termguardium Director — Administration & Identity Guard (PDF)
- Termguardium Station — Desktop Terminal Emulator (PDF)
- Product site: comfixsoftware.com