Termguardium Suite

The problem Termguardium solves

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

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



Executive summary

Enterprises still depend on **green-screen and character-mode applications**: IBM i (5250), z/OS (3270), Unix and Linux over Telnet, VT, TLS, and SSH. These workloads rarely expose HTTP APIs, yet they carry high-value transactions, privileged operations, and regulated data.

Termguardium is a coordinated product family that places a **security and evidence layer** in the path of terminal emulator sessions—while giving users modern **browser or Windows desktop** access. Four products divide responsibility cleanly:

Product	Role
Sentinel	Session relay, evidence capture, semantic policy, fraud-oriented detection, forensics
Portal	**Web terminal emulator** and managed session client
Director	Identity, profiles, channels, SSO—and orchestration for **Identity Guard** (legacy ZTNA)
Station	**Desktop terminal emulator** for Windows; standalone or Director-managed

A **shared terminal decode engine** keeps IBM and VT behavior consistent across Portal, Sentinel, and Station—so forensics and on-screen rendering stay aligned.

The problem Termguardium solves

Traditional PAM and web WAAP tools were built for **HTTP and RDP**. Terminal emulator sessions are opaque byte streams unless you **decode screen semantics**—fields, protected areas, screen transitions, and user actions.

Without in-path visibility, organizations face:

- **Weak user activity monitoring (UAM)** on the systems where fraud and insider abuse actually happen
- **Audit gaps** when recording is optional, client-side only, or not replayable
- **Flat network access** to legacy listeners with no per-user admission or channel ACL
- **Operational friction** forcing every user to install unmanaged terminal emulators with no central policy

Termguardium treats **terminal screens as the enforcement surface**—the same interpreted stream powers recording, search, replay, rules, and (with Identity Guard) zero-trust admission.

How the products work together

```
User ──► Portal (web terminal emulator) or Station (desktop terminal emulator)
                │
                ▼
         Sentinel (relay + evidence + policy + admission)
                │
                ▼
         Legacy host (IBM i, z/OS, Unix, …)

Director ──► users, groups, roles, connection profiles, channel mapping, SSO
```

- **Director** is the **control plane**: who exists, which profiles they see, how channels map to Sentinel listeners.
- **Portal / Station** are **terminal emulators and data-plane clients**: they render the session and (when configured) route through Sentinel.
- **Sentinel** is the **sensor and gate**: it records ordered evidence, evaluates rules, enforces step-up and kill, and (Identity Guard) issues single-use connect tokens.

Profiles that **bypass Sentinel** (direct Telnet to host) do not receive Sentinel forensics—an intentional deployment choice. Production UAM deployments standardize on **via Sentinel** profiles.

Identity Guard (legacy ZTNA)

Identity Guard is a **cross-product capability**, not a separate installable product. It combines:

- Director/Portal **identity and entitlement**
- Sentinel **channel ACL, MFA-at-admission, connect tokens, session limits, SIEM/SOC hooks**

Scope is **3270, 5250, and VT-class hosts through Sentinel**—not a replacement for enterprise ZTNA for arbitrary SaaS.

Where to read next (PDF)

- **Security / fraud / audit:** Termguardium Sentinel (PDF)
- **Web terminal emulator:** Termguardium Portal (PDF)
- **Administration and ZTNA:** Termguardium Director (PDF)
- **Desktop terminal emulator:** Termguardium Station (PDF)
- **Website:** comfixsoftware.com