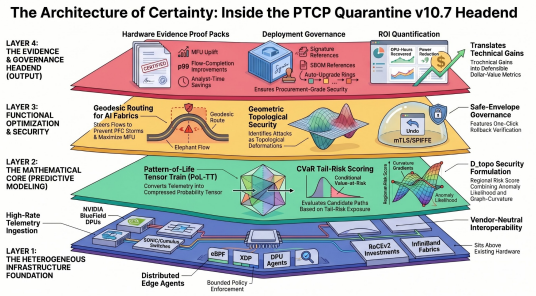
PTCP Zero-Day

Payload-blind, topology-native security for Living-off-the-Land, valid-credential abuse, encrypted exfiltration, lateral movement, AI-agent misuse, and OT threats.

No DPI dependency | No signatures required | No payload retention | Windows + Linux | Safe-envelope response

Built for the security blind spot

Traditional controls often look for known malware, command content, signatures, or decrypted payloads. PTCP Zero-Day measures how network behavior deforms topology - flow geometry, trust discontinuity, cut shifts, curvature changes, and Pattern-of-Life divergence - then renders rollback-ready containment.



PTCP topology quarantine architecture overview

Executive outcomes

1. **Find what content tools miss:** valid credentials, LotL, encryption, and topology abuse.
2. **Contain without panic:** staged kill switch with approvals and rollback.
3. **Preserve privacy:** rejects payload, prompt, token, command-line, and secret fields.
4. **Prove the decision:** hashes, signed actions, SBOM, provenance, and proof packs.

Product snapshot: D_topo + PoL-TT + QRE signal gates | staged kill switch | signed evidence | connector and hardware contracts | Windows/Linux API service

Problems solved by PTCP Zero-Day

A non-semantic security layer for attacks that look authorized, encrypted, or payload-clean.

The core problem: modern adversaries can use valid administrative credentials, built-in operating-system tools, encrypted channels, cloud identity, and legitimate control planes. That can make the packet or process content appear normal. PTCP Zero-Day scores the topology deformation around a node, service, identity, or route instead of searching for a malware string.

Valid-credential abuse

Attackers authenticate successfully and evade signature-only controls. **PTCP response:** scores identity/trust collapse, privilege discontinuity, impossible travel, and topology traversal.

Living off the Land

Built-in admin tools and LOLBins produce no new malware binary. **PTCP response:** detects remote-execution context, service/task creation geometry, and lateral movement patterns without command bodies.

Encrypted exfiltration

Payloads cannot be inspected or should not be retained. **PTCP response:** uses egress asymmetry, flow shape, elephant-flow deformation, cut changes, and destination-class drift.

East-west movement

The attacker moves laterally inside the network fabric. **PTCP response:** measures curvature gradients and cut-capacity shifts around affected regions.

AI-agent and cloud abuse

Automation can cross boundaries using valid tokens or orchestrators. **PTCP response:** scores non-semantic boundary crossing, unusual fan-out, trust collapse, and control-plane provenance drift.

Unsafe auto-quarantine

Isolation can create outages when blast radius is unknown. **PTCP response:** keeps active response gated by safe envelopes, approvals, change tickets, rollback, and dry-run defaults.

Market position: PTCP Zero-Day does not replace EDR, XDR, NDR, SIEM/SOAR, microsegmentation, ZTNA, or NGFW. It makes them stronger by adding a topology-native, payload-blind decision layer that detects non-semantic threats and outputs governed containment plans.

Core capabilities

From topology deformation to safe, auditable containment.

1. **Normalize**
   Flow, identity, trust, control-plane, OT, endpoint posture, and route metadata are normalized to dimensionless telemetry.
2. **Model PoL**
   Pattern-of-Life Tensor Train builds a bounded-memory normalcy map for local tenant behavior.
3. **Score D_topo**
   Anomaly likelihood, graph-curvature gradient, cut perturbation, and QRE-style drift generate a defect score.
4. **Contain safely**
   A Geometric Kill Switch plan is staged across connectors, policy-as-code, and hardware agents with rollback.

Payload-blind enforcement

Rejects raw payload, packet body, command line, prompt, token, cookie, authorization, password, raw log, file-content, and memory-dump fields before scoring.

D_topo topology defect score

Combines Pattern-of-Life density anomaly, curvature gradient, cut-capacity shift, trust collapse, and non-semantic movement features.

Operational QRE drift gate

Uses information-divergence and signal-energy gating to avoid low-signal false positives while catching geometry drift.

Geometric Kill Switch

Renders staged containment for boundary drops, node freeze, route drain, stronger auth, traffic sampling, and ticket/SOAR workflows.

Commercial evidence

Creates decision hashes, plan hashes, signed action hashes, rollback plans, proof packs, release provenance, OpenAPI, and SBOM artifacts.

Customer-local validation

Includes benchmark packs with precision/recall/F1, ROC/PR, false-positive impact, calibration drift, tail-risk reduction, and analyst-time savings.

Technical basis, bounded claims: The TNQG ideas are used as operational geometry - capacity, cut/area logic, inverse-capacity distance, information divergence, and curvature diagnostics - not as an unsupported physics guarantee. The PTCP concepts are implemented as normalized telemetry geometry, PoL-TT normalcy modeling, CVaR/tail risk, D_topo security scoring, and safe-envelope governance.

Why PTCP Zero-Day is unique and high value

A differentiated overlay for non-semantic zero-day security and governed containment.

Market category	Typical strength	PTCP Zero-Day advantage
EDR/XDR	Endpoint behavior and response.	Adds payload-blind topology evidence when actions use valid tools or credentials.
NDR/NGFW	Network visibility, rules, and selected DPI.	Works without packet content or decryption by scoring flow geometry and cut shifts.
SIEM/SOAR	Correlation, triage, and workflow.	Feeds deterministic defect scores, plan hashes, proof packs, and rollback-ready actions.
Microsegmentation / ZTNA	Policy enforcement and access control.	Calculates where to stage containment and verifies blast radius before active execution.
Legacy zero-day tools	Heuristics, IOCs, sandboxing, or signatures.	Detects non-semantic deformation: lateral motion, trust collapse, exfil shape, and topology warp.

v11.3 commercial readiness evidence*

48	15/15	7/7	1.00	0
OpenAPI paths	Connector SDK tests passed	Hardware contracts passed	Synthetic precision/recall/F1	Raw payload retention

Priority use cases

- Volt Typhoon-style valid-credential/LotL behavior
- Encrypted or opaque exfiltration
- East-west lateral movement
- AI-agent privilege boundary crossing
- OT/ICS topology drift
- Regulated environments that cannot retain payloads

Integration targets

- Microsoft Defender, CrowdStrike, SentinelOne, Palo Alto, Fortinet
- Splunk, Microsoft Sentinel, ServiceNow
- Illumio, Akamai Guardicore, Zscaler, Cloudflare
- Kubernetes/Cilium, cloud-flow, NDR/EDR/SIEM/SOAR
- Linux eBPF/XDP/TC, Windows WFP, DPU/SmartNIC, SONiC/Cumulus

Buyer value drivers

- Detect where signatures and DPI are blind
- Reduce sensitive data exposure
- Shorten time from suspicion to containment plan
- Add defensible proof packs for SOC/GRC
- Govern active response with rollback and approvals
- Augment existing tools instead of displacing them

Next step: Run PTCP Zero-Day in shadow mode against customer-owned non-semantic telemetry, calibrate tenant-local thresholds, certify connectors, and generate a buyer-ready proof pack before enabling active response.

*Evidence metrics are generated from release tests, synthetic/customer-local benchmark packs, and connector/hardware contract tests. Customer-specific claims require local calibration and validation. No product can guarantee prevention of every zero-day in every deployment.