Zealot Engagement — Security & Workflow Modernization White Paper

Author: Daniel Brewster
Date: September 22, 2025
Client: Zealot
Engagement Type: Vendor Security Evaluation & Production-Ready Controls Implementation aligned to MPAA/TPN Best Practices

---

Executive Summary

Zealot Inc. (flagship studios in **New York, Los Angeles, and London**) engaged Daniel Brewster to architect and operationalize a multi-site, **Apple-native**, TPN-aligned postproduction platform spanning editorial, finishing, and campaign production. Between **2015–2022**, the engagement supported Zealot's **expansion into the Los Angeles market**, delivered **RAID-based high-performance storage** and **10Gb/40Gb high-speed networking**, implemented **secure firewall architectures**, and guided the organization to **Trusted Partner Network (TPN) certification**. The result is a unified, film/TV-grade infrastructure that pairs **Dolby Atmos sound environments**, **pro editorial suites**, and **enterprise-level security**—engineered for speed, reliability, and seamless client collaboration across global markets.

Outcomes at a glance - **TPN alignment & certification:** Control stack mapped and evidenced across facilities and workflows.
- **Scalable performance:** RAID-backed storage tiers with deterministic throughput for editorial/finishing.
- **Market expansion:** LA studio brought online with standardized builds and secure connectivity to NY/LON.
- **Operational clarity:** SOPs, runbooks, and training to sustain day-2 operations across sites.

Background & Objectives

From **2015–2022**, Zealot grew from a bi-coastal presence to a **tri-continental** creative network. Growth in studio/streamer mandates, client confidentiality requirements, and hybrid work demanded a cohesive security and performance foundation—without sacrificing creative velocity.

Objectives 1. Stand up a **full-stack creative infrastructure** for LA and unify with NY/LON under common standards.

2. Implement **RAID storage** and **high-speed networking** for editorial, finishing, and sound (incl. **Dolby Atmos** rooms).
3. Design and enforce **secure firewall configurations** and network segmentation across sites.
4. Achieve and maintain **TPN certification** with audit-ready evidence.
5. Codify **policies/SOPs** that reflect real workflows and scale with growth.

Role & Contributions (Highlights)

- Supported **expansion into Los Angeles** for feature film trailer editorial and finishing.
- Implemented **RAID storage tiers** and **10/40GbE networking** with secure, segmented infrastructure.
- Designed and oversaw **firewall architectures** and access controls across NY/LA/LON.
- Led **TPN certification** effort: control mapping, remediation, evidence binder, and staff training.
- Delivered day-2 **runbooks**, **incident response playbooks**, and **change control** practices.

Scope of Work

- **Assessment:** Interviews, control walkthroughs, evidence review, and limited technical validation.
- **Policy & Governance:** Drafting/refresh of core policies: Disaster Preparedness & Recovery; Remote Access; Content Transfer; Acceptable Use; Media Handling; Incident Response; Vendor Management.
- **Control Design & Implementation:** Practical controls mapped to TPN families (Physical, Logical, Network, Content Security, Vulnerability Management, Logging & Monitoring, IR, HR/Training).
- **Runbooks & Playbooks:** Day-2 operational SOPs for common tasks and high-severity incidents.
- **Metrics:** Leading/lagging indicators and audit evidence package.

Out of Scope (for this phase)
Deep red-team exercises; DLP at endpoint kernel level; full SIEM buildout; enterprise PAM rollout; fully managed MDR. (Roadmap provided.)

Methodology

1. **Discovery & Evidence Collection** — Interviews with production, editorial, operations; inventory of content paths; sampling of access logs; facility walkthrough highlights.

2. **Threat Modeling** — Focus on content theft, accidental exposure, account takeover, rogue vendor access, and ransomware.

3. **Gap Analysis** — Mapping current controls to MPAA/TPN requirements; prioritization via risk, likelihood, and implementation effort.

4. **Remediation Design** — Control patterns favoring simplicity, audibility, and maintainability.

5. **Implementation & Handover** — Policy ratification, technical changes, training, and evidence binder.

Architecture & Control Overview (Target State)

Studios & Topology
- **NY / LA / London** connected via secure site-to-site tunnels; standardized stack per site.
- Apple-native editorial suites (Final Cut Pro / Premiere / Resolve), finishing bays, and **Dolby Atmos** mix rooms.

Identity & Access
- SSO/MFA; role profiles for editorial, finishing, producers, vendors; JML with <24h deprovision.

Network & Segmentation
- Production VLANs isolated from corporate; **firewall policy objects** with ticketed change control; NY–LA–LON interconnect with least-privileged routes.

Storage & Throughput
- **RAID-backed primary** (NVMe/SAS) for online edit; nearline RAID for work-in-progress; snapshot/replication policies.
- Deterministic bandwidth targets per bay; QoS for review/dailies windows.

Content Paths
- Ingress quarantine → checksum → metadata capture → project volumes; egress via approved, auditable tools with watermarking and link expiry.

Logging, Monitoring & IR
- Central log retention (90/365), privileged action alerts, egress anomaly detection; IR playbook and tabletop cadence.

Vendor & Remote Access
- Time-bound vendor accounts; project-scoped access; encrypted tunnels; posture checks for BYOD.

MPAA/TPN Control Alignment (Representative)

Control Family	Before	After	Evidence
Access Control	Shared accounts in some workflows	Named users + MFA + role profiles	SSO policy, MFA logs, access reviews
Content Transfer	Ad hoc tools & links	Approved transfer platform, policy-bound, link expiry	Transfer policy, system config, audit exports
Media Handling	Informal checks	Chain-of-custody forms; ingest quarantine & checksums	Ingest SOP, checksum logs
Network Security	Flat segments in places	Production VLANs; firewall policy objects; jump access	Network diagrams, rule exports
Logging & Monitoring	Partial coverage	Centralized logs, retention policy, alert rules	Log architecture, alert runbook
Incident Response	Undocumented tribal knowledge	Written IR plan; roles; comms templates; tabletop	IR plan, tabletop report
Vendor Management	One-time vetting	Onboard/offboard workflow; time-bound access; attestations	Vendor SOP, access records

---

Policies & SOPs Delivered (Highlights)

- **Disaster Preparedness & Recovery** — Roles, RTO/RPO targets, comms tree, failover steps.
- **Remote Access Policy** — Approved methods, MFA, device posture, session recording guidelines.
- **Content Transfer Policy** — Approved systems, encryption at rest/in transit, watermarking, link expiry, prohibited channels.
- **Media Handling SOP** — Intake → quarantine → checksum → metadata → approved volumes.
- **Incident Response Plan** — Severity matrix; containment actions; evidence preservation; notifications.
- **Vendor Access SOP** — Project-scoped, time-bound, auditable access with approval records.

Implementation Highlights

- Consolidated identity with MFA; removed shared credentials.
- Segmented network; enforced gateway-based privileged access.
- Rolled out secure transfer tooling and retired shadow channels.
- Stood up centralized logging for privileged actions and egress.
- Codified runbooks and trained staff; completed tabletop exercise.

Risk Reduction & Metrics

Key Risk Reductions
- **Account misuse** via MFA + least privilege + JML discipline.
- **Accidental data leaks** via policy-bound transfer workflows and watermarking.
- **Pivot/ransomware spread** via network segmentation and endpoint baselines.

Operational Metrics (representative; customize with Zealot's data) - Mean time to deprovision (target: < 24h)
- % privileged actions with corresponding change tickets (target: 100%)

- % egress via approved channels (target: 100%)
- Tabletop cadence and time-to-containment in drills
- Patch compliance > X% within Y days

Business Impact

- **Compliance & trust:** Studio/partner confidence via TPN-aligned controls and evidence.
- **Faster approvals:** Predictable, secure review/approval improved turnaround.
- **Reduced downtime:** Clear DR/IR playbooks; faster containment and recovery.
- **Talent productivity:** Secure defaults reduced cognitive load and rework.

Evidence Binder (Audit Package)

1. Policy documents (versioned PDFs)
2. Network & data flow diagrams
3. Access control matrix & quarterly reviews
4. Transfer system configuration & sample audit exports
5. IR plan, tabletop report, and lessons learned
6. Training attendance & acknowledgments
7. Change management tickets linked to firewall/identity changes

---

Roadmap (Next 3–6 Months)

- Endpoint telemetry unification and alert triage playbook
- Vulnerability management cadence with executive scorecard
- Privileged Access Management (PAM) pilot for editors/admins

- Expanded DLP patterns for exported review media
- Quarterly tabletop + semiannual third-party assessment

Engagement Timeline (2015–2022)

- **2015–2016:** Discovery, NY/LON baseline; LA facility planning and bill-of-materials.
- **2017–2018:** LA build-out; RAID + 10GbE core; firewall deployment; identity consolidation.
- **2019:** Content transfer hardening; SOPs; first TPN audit pass.
- **2020–2021:** Hybrid work enablement; remote editorial workflows; additional Dolby Atmos rooms.
- **2022:** Evidence binder updates, tabletop exercises, multi-site standards refresh.

Tools & Platforms (Representative)

- Identity/MFA (SSO provider), endpoint management (MDM/EDR), secure transfer platform, centralized logging, ticketing/change control, documentation wiki.

Note: Tool choices were driven by Zealot's existing investments, creative workflows, and cost/benefit—favoring the simplest solution that produces audit-grade evidence.

Credits & Roles

- **Engagement Lead:** Daniel Brewster — assessment, design, implementation leadership, policy authorship, training.
- **Stakeholders:** Zealot Production, Editorial, Operations, IT.

Contact

Daniel Brewster
Los Angeles Metropolitan Area
Email: dan@hstation.com
Phone: 310-450-2600
LinkedIn: linkedin.com/in/dabrewster

Appendix A — Control Mapping Checklist (Editable)

- Access Control (TPN-AC): MFA enforced; role profiles defined; quarterly reviews complete.
- Content Security (TPN-CS): Ingest quarantine; checksum; watermarking; approved egress.
- Network Security (TPN-NS): Segmentation; gateway access; documented rules.
- Logging & Monitoring (TPN-LM): Centralized logs; retention policy; alerting in place.
- Incident Response (TPN-IR): Plan, playbooks, on-call; tabletop conducted.
- Vendor Management (TPN-VM): Onboard/offboard SOP; attestations; time-bound access.
- Physical Security (TPN-PS): Visitor logs; restricted areas; media storage controls.
- HR & Training (TPN-HR): Security awareness; acknowledgments; sanctions policy.

Appendix B — Data Flows (Insert Diagrams)

- **Content Ingress** → Quarantine → Checksum → Catalog/Metadata → Project Volume
- **Editorial** → Render → Review/Approval (watermarked) → Archive/Delivery
- **Vendor Remote** → Auth → Posture Check → Project VLAN → Session Recording (where applicable)

Appendix C — Tabletop Scenario (Template)

- **Scenario:** Compromised vendor laptop exfiltrates watermarked review files.
- **Injects:** MFA fatigue attempt; unusual egress; transfer tool alert.
- **Measures:** Time to detect; time to contain; comms accuracy; evidence chain.
- **Improvements:** Playbook updates; access scoping; user training refresh.