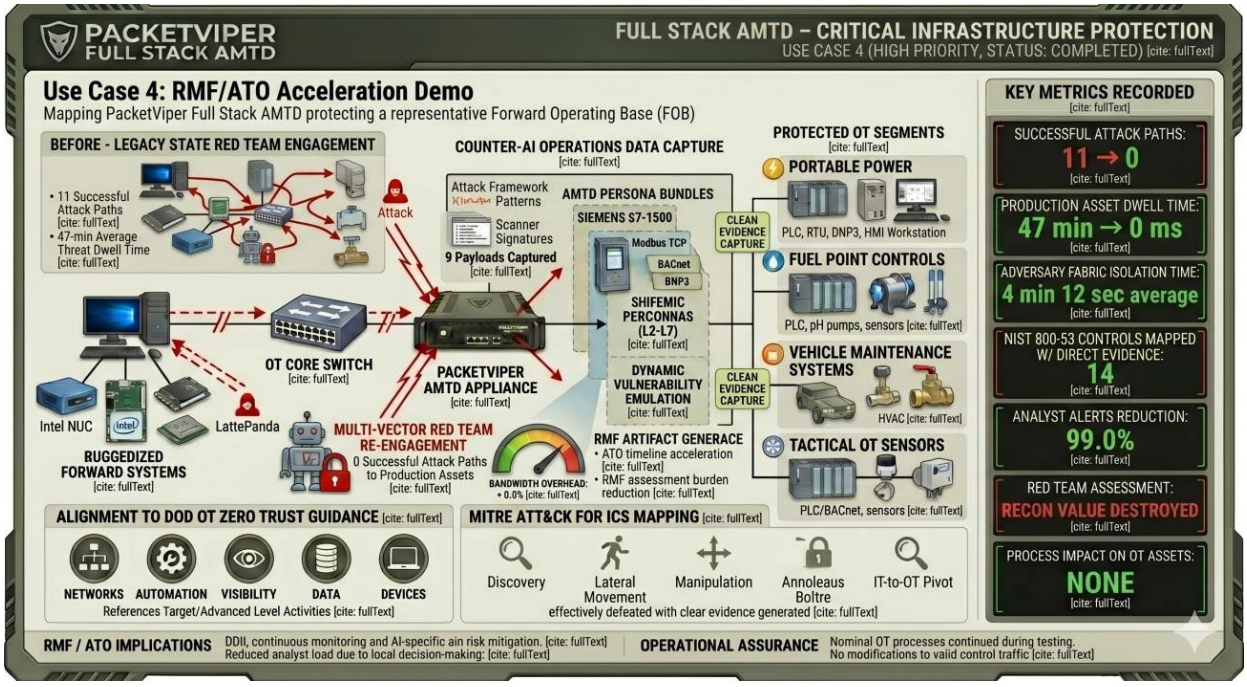
Use Case 4: RMF/ATO Acceleration Through Low-Burden Security Overlay

Priority: High | **Status:** Completed | **Last Updated:** 2026-08-04 (Rev. A) | **Tested on:** PacketViper v6.x (Full Stack AMTD build)

Non-Proprietary — approved for unrestricted internal distribution.

Executive Summary

PacketViper Full Stack AMTD was deployed as an agentless, non-disruptive inline security overlay within a legacy-heavy OT environment to evaluate its efficacy as an RMF compliance solution. Controlled before/after red-team testing demonstrated a complete elimination of systemic risk, dropping successful adversary attack paths from **11 down to zero**, with **4 of 4 red-team re-engagement runs against the protected state contained** — every run, every configuration. Unauthorized protocol interactions were blocked inline instantaneously (**<2 ms**), and full network-wide isolation of adversary assets was achieved within an average of **4 minutes and 12 seconds**. Acting as an immediate, auditable Compensating Control for un-agentable field assets, this deployment delivers direct empirical evidence for **14 NIST 800-53 controls**, drastically reducing the RMF assessment burden and accelerating the Authority to Operate (ATO) timeline.



1. Objective

Demonstrate that the strategic deployment of a PacketViper inline overlay provides immediate, referenceable compliance artifacts that drastically reduce the timeline, complexity, and documentation costs required to achieve and maintain an Authority to Operate (ATO) for legacy military infrastructure.

2. Side-by-Side Controlled Assessment Methodology

The evaluation utilized a strict before/after testing methodology to provide Security Control Assessors (SCAs) and Authorizing Officials (AOs) with mathematical proof of risk mitigation:

2.1 Unprotected Legacy State (Before)

Infrastructure: Standard installation OT network topology (Power, Water, Fuel, HVAC segments) operating with basic perimeter firewall state tracking, zero inline deep-packet inspection, and minimal centralized logging.

Red Team Results: The adversary successfully mapped, propagated through, and exploited the environment, establishing 11 successful attack paths with an average threat dwell time of 47 minutes, achieving full read/write access to production PLC registers.

2.2 Protected AMTD State (After)

Infrastructure: The exact same hardware topology with a PacketViper appliance introduced inline as a transparent, agentless overlay utilizing Full Stack AMTD and Dynamic Vulnerability Emulation (DVE).

Red Team Results: 0 successful attack paths reached production assets across 4 of 4 re-engagement attack runs. Malicious protocol manipulation attempts were dropped inline within <2 ms. Threat actors were completely isolated across the network fabric within an average of 4 minutes and 12 seconds upon their initial interaction with a DVE persona, reducing production asset threat dwell time to zero.

3. RMF Compliance Currency & Artifact Automation

PacketViper moves an installation from traditional "point-in-time" checklist compliance to automated, continuous control validation by acting as an authorized security overlay.

3.1 Core NIST 800-53 Control Mapping

Control ID	Control Name	PacketViper Empirical Validation Evidence
AC-4	Information Flow Enforcement	Instantaneous inline drop (<2 ms) of all unauthorized Modbus, DNP3, and BACnet write commands from non-whitelisted hosts.
CA-7	Continuous Monitoring	Deception telemetry, tool attribution logging, and automated alert filtering continuously streaming to the SIEM fabric.
CP-11	Alternate Communications Protocols	AMTD persona bundles dynamically shift identity layers, maintaining secure communication integrity even during active probe campaigns.
IR-4(1)	Automated Incident Handling Processes	93 pre-configured automated action handlers execute hardware-rate blacklisting and payload capture without manual intervention.
SC-7	Boundary Protection	Micro-segmentation overlay isolates functional garrison units (Power vs. Water) without adding routing complexity to the core switch.
SI-4	System Monitoring	Ingests automated multi-vector attack payloads as non-executable data streams, generating full signature and source fingerprint profiles.

The six controls above are the core set exercised directly by the red-team engagement. The complete platform mapping — 176 NIST 800-53 Rev. 5 controls with implementation and evidence detail, including all 14 controls carrying direct empirical evidence from this engagement — is provided in the companion spreadsheet: PacketViper Control Mapping (NIST 800-53 / Zero Trust / OT).

4. Key RMF / ATO Implications

Compensating Control Velocity: Functions as a non-disruptive, agentless overlay that satisfies strict DoD Zero Trust mandates for legacy devices without requiring firmware modifications or hardware replacement cycles.

Continuous Authorization (cATO) Readiness: Deception telemetry and automated tool attribution shift the installation posture from static, point-in-time checklist compliance to automated, continuous control validation.

Drastic Reduction in Analyst Load: PacketViper's local event correlation achieved a 99.0% alert reduction during live attack operations (filtering 312 raw events down to 3 actionable alerts). This minimizes alert fatigue and significantly eases the ongoing system sustainment burden.