PacketViper - Cyber-Physical System (CPS) Comparative Analysis

Overview

PacketViper's analytics and visualization are powered by an AlertBox **platform**, providing advanced telemetry, behavioral analytics, and compliance visibility. With these capabilities, PacketViper's autonomous enforcement model eliminates the need for orchestration layers—achieving direct, immediate remediation of threats in real time. While **Claroty** remains valuable as an asset visibility and compliance management system, **PacketViper** provides full CPS protection, analysis, and compliance coverage.

CPS Architecture Layers and Roles

CPS Layer	Claroty	PacketViper	CPS Function Alignment
Physical Process Layer	Focuses on digital asset and network process visibility; limited physical sensing.	Integrates environmental sensors (motion, temperature, humidity, camera) and provides 360° visibility through dashboards, telemetry, and analytics.	PacketViper High — full cyber-physical and environmental visibility
Sensing & Actuation	Passive network sensing only; depends on external controls for enforcement.	Active deception, immediate threat remediation, and physical sensor-actuated responses without orchestration.	PacketViper High — autonomous feedback and enforcement loops
Communication Layer	Visualizes communication paths; relies on existing firewalls/NAC for control.	Enforces Zero Trust micro-perimeters, maintains secure communication in air-gapped or remote sites, and provides real-time monitoring through AlertBox analytics.	PacketViper High — secure, autonomous communication and continuous monitoring
Computation & Control Layer	Centralized analytics and policy logic; limited local autonomy.	Distributed control: local applied intelligence + CMU sync, live traffic visualization, Power BI analytics, and automatic remediation.	PacketViper High — distributed control and immediate response

Cyber Layer (Modeling)	Creates digital twin-like models for devices and topology mapping.	Behavioral modeling of boundaries, ports, and risk behaviors visualized via dashboards.	PacketViper High — operational and behavioral modeling with compliance insight
Cognition Layer (Decision & Intelligence)	Exposure management and risk scoring (platform unspecified).	Applied Intelligence: automatic blocking, alert correlation, Power BI-based analytics for decision support, and autonomous threat remediation.	PacketViper Higher — intelligent, self-acting decision system
Configuration Layer (Adaptation)	Policy-driven, manual orchestration for configuration.	Automatic decoy shifting, adaptive blacklist propagation, self-healing configuration, and zero orchestration required.	PacketViper High — self-adaptive and orchestration-free defense
HMI & Oversight Layer	Rich dashboards for analysts and compliance.	Operator-focused dashboards and compliance insight via AlertBox Power BI integration; direct visibility of threats and compliance checks.	Both High, but PacketViper integrates analysis and enforcement

---

CPS Role Comparison Summary

CPS Role	Claroty Strength	PacketViper Strength
System Awareness & Visibility	✓ Deep asset discovery, exposure visualization	✓ 360° visibility, telemetry dashboards, Power BI analytics, compliance tracking
Real-Time Protection & Control	—	✓ Inline deception, autonomous blocking, and remediation without orchestration
Zero Trust Enforcement	Partial (via integrations)	✓ Native micro-perimeter, port-level control, and full isolation of threats
Resilience & Autonomy (Air-Gapped Ops)	—	✓ Fully autonomous, decentralized RSUs capable of independent defense
CPS Lifecycle Support	✓ Governance and risk frameworks	✓ Operational defense, telemetry efficiency, compliance analytics, and continuous visibility
CPS Physical Correlation	—	✓ Environmental + cyber correlation with instant response and analytics

Compliance & Compensating Controls	✓ Compliance reporting support	✓ Built-in compensating control functions covering ~20 compliance categories (e.g., NERC-CIP, NIST, ISO 27001)

Visual Summary

Claroty:

- Governance ————> Visibility ————> Analytics ————> Policy Guidance

Top-down CPS management and exposure control (requires orchestration for action).

PacketViper:

- Sensing ————> Visibility ————> Deception ————> Enforcement ————> Adaptive Protection
- │
- └——► AlertBox (Power BI Analytics Platform)

Bottom-up CPS protection and visibility: real-time telemetry, Power BI analytics, no orchestration required, self-adaptive autonomy, and direct compliance alignment.

Final CPS Verdict

With **AlertBox analytics** and autonomous enforcement, **PacketViper** achieves comprehensive CPS alignment—handling visibility, analytics, remediation, and compliance without orchestration. Claroty continues to serve as a valuable **asset and compliance manager**, but **PacketViper** functions as both a **preventive defense system and compliance-enforcing control**.

Dimension	Claroty	PacketViper	Winner (CPS Fit)
Physical-Cyber Integration	🟡 Moderate	🟢 High	PacketViper
Distributed Autonomy	🔴 Low	🟢 High	PacketViper
Governance & Risk Oversight	🟢 High	🟢 High	Both
Preventive Defense	🟡 Medium	🟢 High	PacketViper
Visibility & Modeling	🟢 High	🟢 Very High	PacketViper
Adaptive Configuration	🟡 Medium	🟢 High	PacketViper
Operational Resilience	🔴 Low	🟢 High	PacketViper
Analytics Platform	❓ Unspecified	🟢 AlertBox (Power BI)	PacketViper

Compliance & Compensating Control	🟢 Moderate	🟢 Comprehensive (~20 compliance checks)	PacketViper
Analyst & Compliance UI	🟢 High	🟢 High	Both

Summary Statement

With orchestration no longer needed and real-time remediation built into PacketViper's architecture, **PacketViper** surpasses **Claroty** in nearly all CPS layers. Claroty remains a powerful governance and compliance asset manager, but **PacketViper** stands as the **most holistic CPS solution**—delivering visibility, analytics, compliance coverage, and autonomous protection.

> **Claroty** is the *CPS brain* — focused on governance, visibility, and policy management.
> **PacketViper** is the *CPS nervous, immune, and compliance system* — delivering continuous 360° visibility, immediate remediation, Power BI-based analytics, autonomous enforcement, and built-in compensating controls.

Together, they create a complete CPS defense fabric:

- Claroty for device insight and governance management.
- PacketViper for adaptive protection, compliance assurance, and orchestration-free automation.