IT Teams

Here's how PacketWatch provides answers other solutions simply can't.

DIAGNOSE

1. **Troubleshoot** performance, availability, policy violations, and security issues.
2. **Explore** traffic patterns, network assets, and subnets.
3. **Reveal** misconfigurations, unauthorized communications, unexpected behaviors, and Shadow IT.
4. **Determine** root causes by comparing expected and actual activities.

Complete, timely, and trustworthy data for confident cybersecurity decisions.

Different teams will ask different questions when looking at the same IT infrastructure. But they all want answers based on defensible forensic evidence.

packet watch

Cyber Teams

Here's how PacketWatch provides answers other solutions simply can't.

FORENSICS

1. **Investigate**, find, and contain threats proactively before they trigger conventional alerts.
2. **Complete Visibility** with full-packet capture and experienced threat hunters for full reconstruction of threat actor activities.
3. **Source of Truth** when log data is deleted, damaged, incomplete, or inconclusive.
4. **Evidence-based** threat data and forensics to make more confident decisions; know exactly what happened.

Complete, timely, and trustworthy data for confident cybersecurity decisions.

Different teams will ask different questions when looking at the same IT infrastructure. But they all want answers based on defensible forensic evidence.

packet watch

GRC Teams

Here's how PacketWatch provides answers other solutions simply can't.

PROVE

1. **Independent** validation that security controls are operating as documented.
2. **Translates** cybersecurity activities into risk, compliance, and governance contexts.
3. **Improves** security incident documentation, risk treatment, and board-level reporting and decisions.
4. **Conveys** security and compliance posture over time, supporting governance as an ongoing discipline.

Complete, timely, and trustworthy data for confident cybersecurity decisions.

Different teams will ask different questions when looking at the same IT infrastructure. But they all want answers based on defensible forensic evidence.

packet watch

Audit Teams

Here's how PacketWatch provides answers other solutions simply can't.

VALIDATE

1. **Objective** time-stamped "Source of Truth" data not reliant on system-generated logs.
2. **Defensible** high-fidelity, forensic evidence of packet-level network activities.
3. **Supports** control validation, incident review, policy compliance, and documentation.
4. **Demonstrates** security and compliance posture over time.

Complete, timely, and trustworthy data for confident cybersecurity decisions.

Different teams will ask different questions when looking at the same IT infrastructure. But they all want answers based on defensible forensic evidence.

packet watch