cpacket NETWORKS
VISIBILITY YOU CAN TRUST

VECTRA
Security that thinks®

Solution Brief

Strengthening Cybersecurity using Network Detection and Response

Lossless Visibility. High-Fidelity Threat Detection. Less Cybersecurity Risk.

Organizations are constantly under attack by cybercriminals who are stealthy, well-armed, and cleverly cloak their activity to blend in with normal network traffic to carry out nefarious missions. Cybercriminals and malware are smart; they monitor traffic to determine the best times to infiltrate. Preventing attacks and their consequences begins with monitoring network traffic and observing behaviors. Prevention is ideal, however when events occur, causation, containment, response, and recovery must proceed quickly and effectively. The Vectra Cognito Platform uses visibility from the cPacket Intelligent Observability Platform to provide effective NDR:

- Is reliable and lossless so you have thorough visibility without blind spots
- Acquires network packet data from many vantage points for security delivery
- Provides seamless detection across entire multi-cloud hybrid infrastructure
- Includes detailed high-resolution visibility into behaviors, patterns, and trends
- Leverages ML and AI at machine speed to defend against attacks and threats

WHAT WE OFFER - Integrated Network Observability and Threat Detection for Multi-Cloud Hybrid Infrastructure

The cPacket Intelligent Observability Platform and the KPIs and security delivery it provides is an ideal fit for Vectra's Cognito Platform. Together the Security Operations (SecOps) team receives high-fidelity actionable alerts versus an abundance of alert noise. The field-proven joint solution is applicable for hybrid-cloud and multi-cloud environments. The cPacket platform includes a unique agentless direct link method of packet acquisition that can tap into subnet traffic to acquire packets, hence providing a self-hosted packet mirroring service. This service is useful for acquiring packets in environments without native packet (or traffic) mirroring, and to supplement native packet mirroring to add strategic vantage points to the overall visibility. Alerts generated by an IDS can be sent via an API call to cPacket cStor® packet capture devices to tag the data enabling fast data queries, analysis of specific events, and replaying activity from before, during, and after events. Alerts, security intelligence, and captured packet data empower security analysts and automation solutions to quickly understand threats, contain them, and respond.

Vectra Threat Detection and Response:

The Vectra Cognito Platform collects network data from physical and/or virtual instances of cPacket cVu® Network Packet Brokers and enriches the data with metadata to customize the security analytics to each IT environment. It provides automated real-time enforcement by detecting, scoring, and sending prioritized alerts to the SecOps team who use the information for threat hunting and retrospective investigations. Security analysts to receive alerts quickly and are able to discern critical versus benign events, lowering the time from the compromise to incident detection and containment.

What our customers say:

" Alert noise can be paralyzing, especially when security events occur. The scored and prioritized alerts reduce the noise and give us time to focus on investigation, containment, and the best possible response. Security events will always be a crisis, but now they're a bit less stressful."

– Security Operations Team Leader
Large Utility Company

The cPacket Intelligent Observability Platform includes:

- Network packet acquisition using TAPs and virtualized packet acquisition (for cloud and other virtualized infrastructure)
- Physical and virtualized network packet brokering for reliably delivering network packet data to the Vectra platform
- Physical and virtualized packet capture, storage, and analytics
- Unified management of the cPacket monitoring fabric plus customizable dashboards for data visualization in a single-pane-of-glass

cPacket Networks + Vectra
A Winning Combination for Effective NDR

Key Benefits

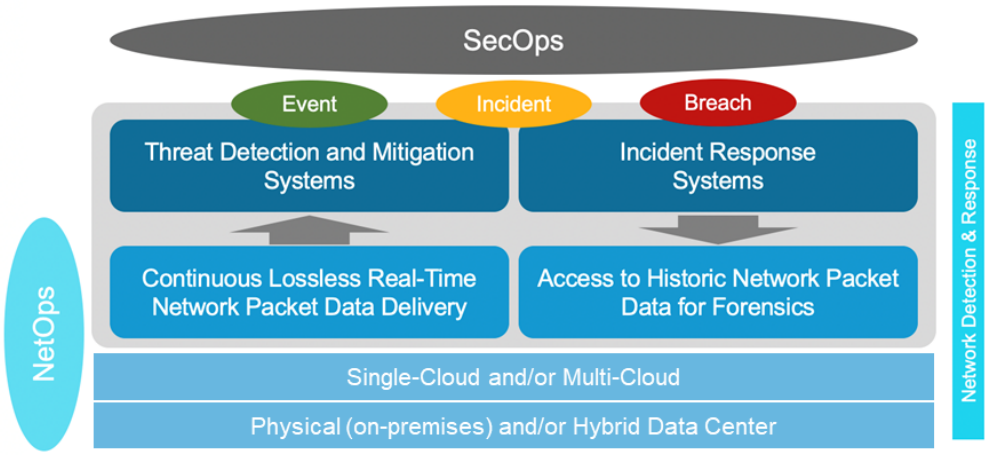
- **Strong Cybersecurity Posture**
  Integrated network observability with unique agentless self-hosted packet mirroring, security monitoring, intrusion detection, prioritized alerts, forensic analysis, and threat hunting.
- **Seamlessly Secure All IT Environments**
  Prevent attacks, breaches, fraud, cybercrime, and malicious activity across physical, public cloud, multi-cloud, and hybrid environments.
- **Fast and Easy Deployment**
  Field-proven interoperability with standard interfaces and open APIs make deployment and bring-up easy and fast.

Real-Time Cybersecurity Alerts and Intelligence with Enriched Data Enhances SIEM Effectiveness

Vectra combines security researchers who distill attacker behaviors sourced from securing the world's most sensitive assets with data scientists who codify behaviors across unsupervised, supervised, and deep learning models to generate security-enriched data that is streamed to SIEM tools and data lakes. The result is an AI-driven cybersecurity platform that detects attacker behaviors to protect hosts and users from being compromised, regardless of location. The platform automates security analyst tier-1 activities resulting in a 34x workload reduction that maps to 97% of the MITRE ATT&CK framework. Learn about Vectra Threat Detection and Response.

Security Begins with High-Fidelity Network Visibility

Monitoring to acquire network packet data and observing behaviors, patterns, and trends enriches the visibility provided to security analysts and the tools they use is the foundation for effective NDR. Prevention, threat hunting, investigation, forensic analysis, and incident responses all rely on the information derived from network packet data. Gapless and lossless visibility is especially important for distributed hybrid environments because visibility and data gaps due to dropped packets during peak network activity are vulnerabilities that attackers will exploit. Learn more about the cPacket cVu® Network Packet Brokers and cStor® Packet Capture devices that provide security delivery.



cPacket Networks de-risks IT I&O through network-aware service and security assurance across hybrid and multi-cloud environments. Our AIOps-ready Intelligent Observability Platform provides single-pane-of-glass analytics and provides the deep network visibility required for today's complex IT environments. The result: increased service agility, enhanced experience assurance, and faster transactional velocity. Learn more at www.cpacket.com