VECTRA SECURITY THAT THINKS® | cpacket NETWORKS

SOLUTION BRIEF

Vectra and cPacket Networks deliver NDR with fast forensics

The challenge

Modern cybercriminals now employ AI with machine learning (ML) to identify and exploit visibility and security gaps. AI is also used to create deep fakes that trick humans and systems into helping to execute their missions.

When business reputation is at stake, it is vital to ensure data privacy, secure experiences and operational continuity, while avoiding theft and fraud. And it requires using adversarial AI with ML to stop hidden attackers.

The right data with the right context

Together, the Cognito® Network Detection and Response (NDR) platform from Vectra® and the cPacket Networks visibility solution swiftly identify and mitigate cyberattacks across cloud, data center, IoT, and enterprise networks.

The strength of the security provided by this integrated solution is maximized because the Cognito NDR platform captures, analyzes and stores metadata at scale from all network traffic and enriches it with security insights about every threat.

These rich insights, with detailed context about each attack, enable security teams to perform more conclusive incident investigations and faster AI-assisted threat hunting. The information you need to stop an attack is always at your fingertips.

To speed-up response time, the Cognito NDR platform integrates and shares the same context and insights with third-party security solutions – cPacket Networks, as well as EDR, SIEMs and SOAR tools – for end-to-end threat management, visibility and response automation.

End to end solution to swiftly identify and mitigate cyberattacks

BUSINESS BENEFITS

- Operational continuity – Stop attacks with deep visibility inside networks and high-fidelity attacker behavior detections.
- Robust cybersecurity – Robust full-stack threat-detection and network intelligence protects business assets and client data.
- Reputation preservation – Prevent customer churn due to reputation and experience loss caused by a data breach.

TECHNOLOGY BENEFITS

- Reliable security – Lossless real-time packet data brokering to the Cognito NDR platform across cloud, data center, IoT, and enterprise networks.
- Rich and fast forensics – Historical packet retrieval for forensics investigation is now possible for any segment of the network.
- Full hybrid visibility – Access to packet data with consistent workflows across the hybrid environment for efficient security operations.

Data drives threat intelligence

Capturing data with zero loss, analyzing that data for threats, and initiating defensive actions create a security-delivery chain that is only as strong as its weakest link.

That security-delivery chain – one that reliable, consistent, complete with zero loss, and accurate – must integrate with NDR platforms for real-time protection and historical forensics. The cPacket cVu®/cVu-V® series Network Packet Broker+ (NPB) meets these requirements due to its scalable and distributed architecture.

That security-delivery chain – one that reliable, consistent, complete with zero loss, and accurate – must integrate with NDR platforms for real-time protection and historical forensics.

The Cognito NDR platform uses AI-derived machine learning algorithms to automatically detect, prioritize and respond to in-progress attack behaviors that pose the highest business risk – inside cloud, data center, IoT, and enterprise networks.

By automating manual and mundane Tier-1 and Tier-2 security tasks, the Cognito NDR platform significantly reduces the workload in security operations centers, analysts more time to investigate incidents and hunt for threats.

The combined techniques and integration of Vectra and cPacket provide robust security at scale. Data privacy is assured because the Cognito NDR platform only analyzes metadata from packets – not the payload.

Detecting malicious footprints

Malware is cleverly implemented to execute during times of high network traffic to evade detection amid noise and expectations of lost packets, intentionally hoping that footprints are not detected and lost forever.

Because the wire sees all and holds the truth, the source, target and method of attack – no matter how sophisticated, cloaked, slow or fast – can be found by analyzing network packets. The inability to access and analyze 100% of the packets exposes businesses to significant risk.

Malicious activity leaves footprints in network packets because all data exchanged through a network at Layer 3 and above is packetized. This is why network packet data is extremely important for network and security analytics – to quickly and accurately detect footprints and initiate remediation.

The Cognito Recall™ investigative workbench, which runs on the Cognito NDR platform, provides additional footprint detection using forensic analysis that queries historical data to detect compromised hosts, devices, privileges, and accounts involved in an attack, as well as for retrospective threat-hunting.

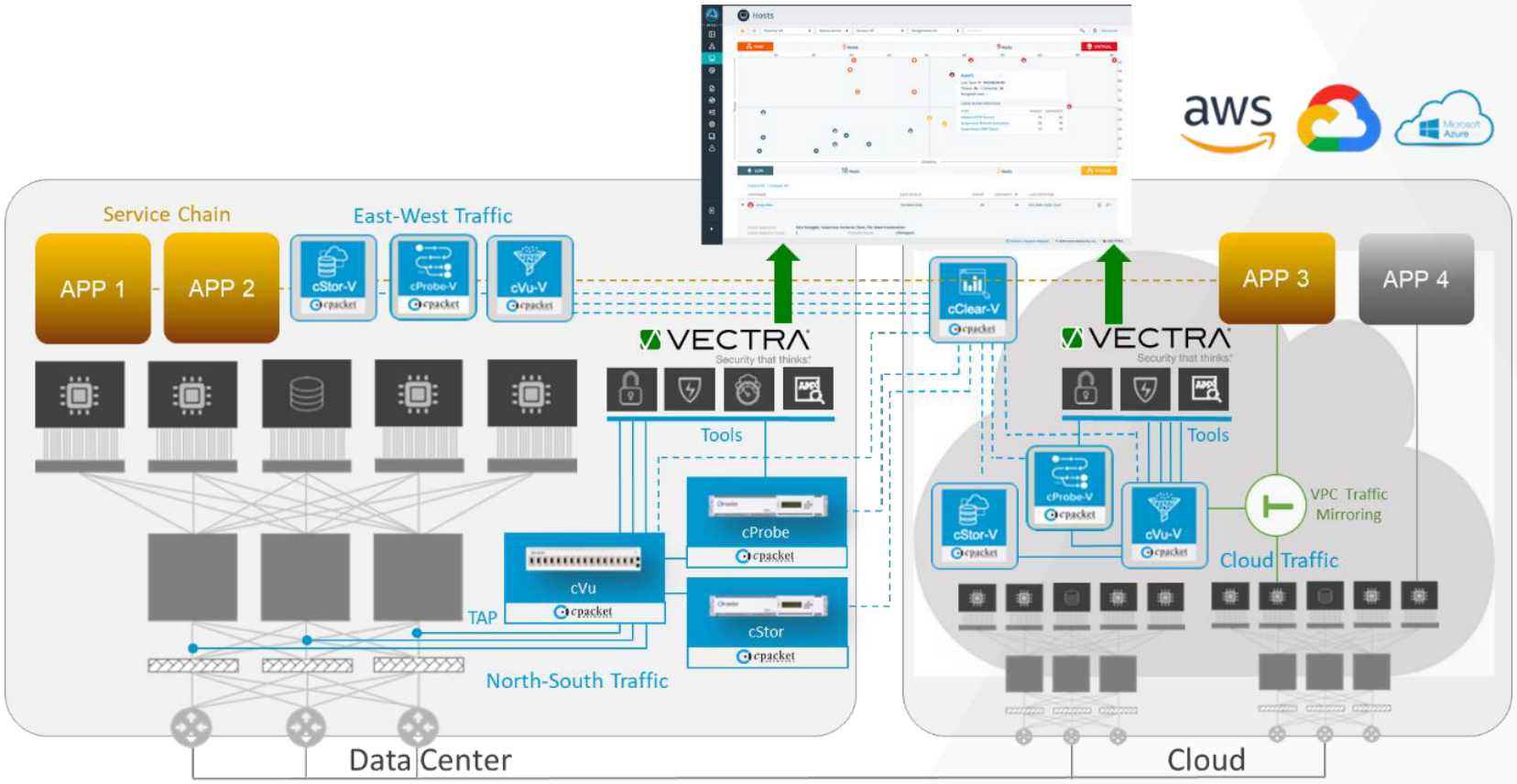
Data can also be routed to the cPacket physical cStor® and virtual cStor-V® appliances for persistent storage, additional forensic analysis, and compliance record keeping.

Because the wire sees all and holds the truth, the source, target and method of attack – no matter how sophisticated, cloaked, slow or fast – can be found by analyzing network packets.

Seamless integration and interoperability

Integrating cPacket network visibility and the Cognito NDR platform from Vectra is straightforward and seamless. cVu receives packets from cTap devices and SPAN ports, and cCu-V receives mirrored packets in virtualized and cloud environments. In both cases, packets are routed from cVu/cVu-V to the Cognito NDR platform.

Integrating cPacket network visibility and the Cognito NDR platform from Vectra is straightforward and seamless.



About Vectra

Vectra® protects businesses by identifying and stopping cyberattackers before they spread throughout the IT infrastructure – across, cloud, data center, IoT, and enterprise networks. As a leader in network detection and response (NDR), Vectra AI is the premier choice among cybersecurity professionals around the world to automate attacker discovery, prioritize threats and respond with unparalleled speed. Vectra is equally adept at protecting IaaS, PaaS and SaaS deployments, resulting in true enterprise-scale threat coverage. For more information, visit vectra.ai.

About cPacket Networks

cPacket enables IT through network-aware application performance and security assurance across the distributed hybrid environment. Our AIOps-ready single-pane-of-glass analytics provide the deep network visibility required for today's complex IT environments. With cPacket, you can efficiently manage, secure, and future-proof your network - enabling digital transformation. cPacket solutions are fully reliable, tightly integrated, and consistently simple. cPacket enables organizations around the world to keep their business running. Our cutting-edge technology enables network, application, and security teams to proactively identify issues before negatively impacting the business. The result: increased security, reduced complexity, and increased operational efficiency. Learn more at cpacket.com, read our blogs, or follow us on Twitter, LinkedIn, Facebook, YouTube, and BrightTalk.

For more information please contact a service representative at sales-inquiries@vectra.ai.

Email info@vectra.ai vectra.ai