cpacket NETWORKS
VISIBILITY YOU CAN TRUST

VECTRA
Security that thinks.®

Solution Brief

Network Detection and Response for Cybersecurity

cPacket and Vectra Integrated Solution Provides Robust Threat Detection and Fast Forensic Analysis

Business Benefits

- Robust Cybersecurity
  Robust full-stack network detection and response solution protects business assets and client data
- Operational Continuity
  Proactive security posture and visibility mechanisms prevent mission-critical down time
- Reputation Preservation
  Prevent customer churn due to reputation and experience loss incurred through a data breach

Technology Benefits

- Reliable Data for Cybersecurity
  Lossless real-time packet brokering to the Vectra Cognito platform for on-premises and cloud security
- 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

The Challenge

Cyber-attacks occur from both the outside and within. They are cleverly implemented and cloaked 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. Cybercrime is also well-funded, arming criminals with technology including Machine Learning (ML) and Artificial Intelligence (AI) to identify and exploit visibility and cybersecurity gaps. AI is also used to create "deep fakes" that trick humans and systems into helping execute their mission. Cybersecurity therefore must be robust because data privacy, secure experiences, theft, fraud, operational continuity, and business reputations are at stake. Cybersecurity measures must also leverage ML and AI at machine speed to defend against attacks and threats that are increasingly more sophisticated, stealthy, and persistent.

The right data with the right context drives strong security

The Solution

The combination of cPacket Networks' visibility solution integrated with Vectra's Cognito platform for Network Detection and Response (NDR) offers prevention of cyber-attacks against data and infrastructure seamlessly spanning on-premises and cloud. The strength of the security provided by this integrated solution is maximized because the Cognito platform has consistently reliable access to all network packets.

Rich Network Data Drives Threat Intelligence

The cPacket visibility stack transforms network data into actionable network intelligence that drives security. The cPacket cClear® analytics and visualization product consumes data from Network Packet Brokers (NPBs) and cStor®. Network traffic metrics shown by cClear dashboards reveal specific attacks and common malware behaviors such as "floods" that cause Denials of Service (DoS) and lengthy sessions with low amounts of data transferred. Deeper threat intelligence and automated responses come from the Cognito platform that uses AI and ML driven behavioral detection algorithms to analyze metadata to transform the network data into actionable threat intelligence using event correlation, host scoring, and other techniques to detect behaviors that may jeopardize key assets that are of strategic value to attackers. All phases of persistent stealthy attacks are detected, including hidden command-and-control communications, internal reconnaissance, botnet monetization, lateral movement, and data exfiltration. When the Cognito platform detects attacks and threats, it initiates remediation and response actions natively through lockdown or through integrations with other cybersecurity solutions and technologies such as SOAR, SIEM, firewalls, and endpoint policy managers. The combined techniques, integrations, and overall solution provides robust security at scale, and upholds data privacy because only enriched packet metadata is analyzed.

A Reliable Security Delivery Chain

Losslessly capturing data, analyzing it for threats, and initiating defensive actions is a "security delivery" chain that is only as strong as the weakest link. Therefore, it is necessary that data delivered to cybersecurity solutions for real-time protection and historical forensics is reliable and consistent, complete with zero loss, and accurate. cPacket's cVu®/cVu-V® series Network Packet Broker+ (NPB) products meets these data quality requirements because of its scalable and distributed architecture.

A security delivery chain is only as strong as the weakest link. Detecting cyber-attacks and their footprints requires high-quality data and reliable visibility you can trust to thwart cybercriminals and malware that exploit known weaknesses such as data and visibility gaps that occur when other vendor's NPBs drop packets.

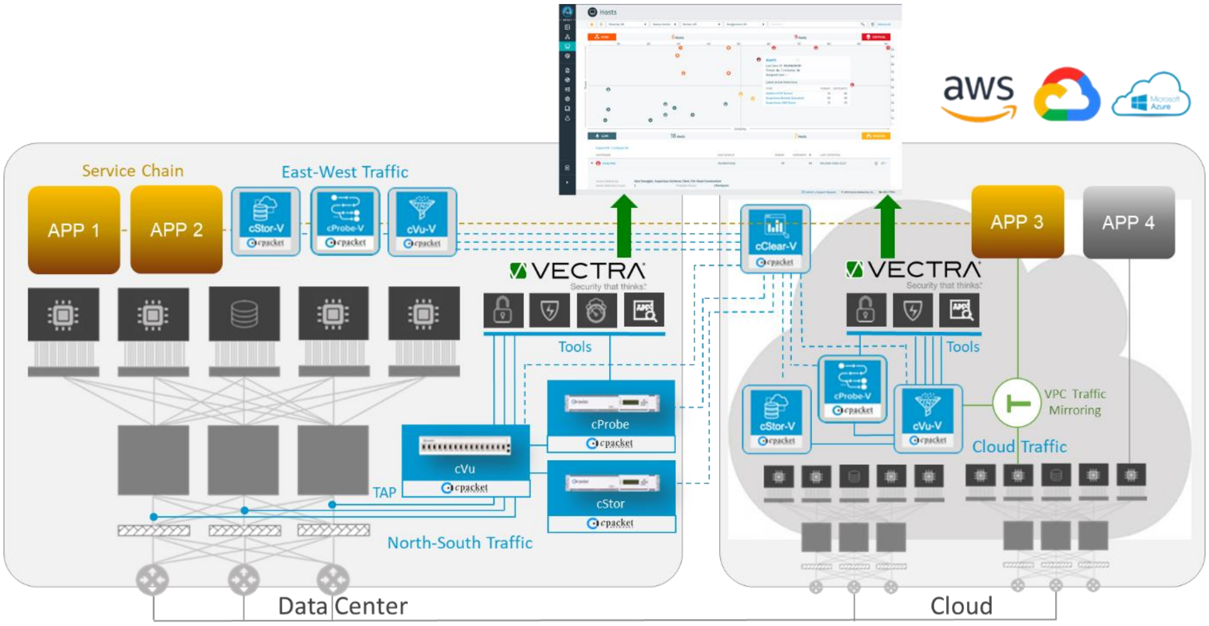
Detecting Malicious Footprints

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. "The wire sees all and holds the truth." This means that the source, target, and method of attack, no matter how sophisticated, cloaked, slow, or fast can be found by analyzing network packets. Any solution that cannot access and analyze 100% of the packets is a huge exposure and risk because criminals and malware will find, exploit, and share such weaknesses. Malicious activity leaves footprints in network packets because all data exchanged through a network at layer-3 and above is packetized. This is why lossless access to network packets is extremely important for network and security analytics – to quickly and accurately detect footprints and initiate remediation.

Cognito Recall (a Cognito platform component) facilitates forensic analysis by security analysts who can query historical data to identify hosts, devices, accounts, and attackers that were involved in a security event, as well as for retrospective threat-hunting. Data can also be routed to cPacket's physical cStor® and virtual cStor-V® appliances for persistent storage, additional forensic analysis, and compliance record keeping.

Seamless Integration and Interoperability

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



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.

About Vectra

Vectra® is the leader in network detection and response – from cloud and data center workloads to user and IoT devices. Its Cognito® platform accelerates threat detection and investigation using artificial intelligence to enrich network metadata it collects and stores with the right context to detect, hunt and investigate known and unknown threats in real time. Vectra offers three applications on the Cognito platform to address high-priority use cases. Cognito Stream™ sends security-enriched metadata to data lakes and SIEMs. Cognito Recall™ is a cloud-based application to store and investigate threats in enriched metadata. And Cognito Detect™ uses AI to reveal and prioritize hidden and unknown attackers at speed. For more information, visit vectra.ai.