cpacket NETWORKS
VISIBILITY YOU CAN TRUST

Data Sheet

cPacket cStor®-V Virtualized Packet Capture

Network Packet Capture with Analytics for Cloud and Virtualized Environments

cStor-V Virtualized Packet Capture enables you to:

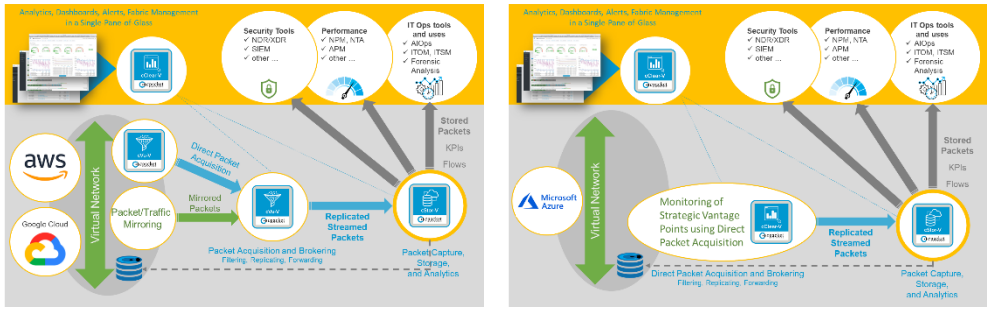
- Strengthen your security posture with security evidence for threat hunting, security analytics, forensic analysis, and replaying attack TTPs
- Efficiently troubleshoot problems, plan capacity, and analyze the network health, traffic, flows, and protocols (e.g., TCP, UDP, etc.)
- Query, search, and replay network traffic before, during, and after an event to understand what happened
- Provide information and evidence for regulatory compliance
- View detailed TCP, conversation, and flow statistics with flow indices by parsing layer 2-4 packet headers
- Export packet data as PCAP files for use with other tools (e.g., Wireshark)
- Democratize access with role-based permissions to people, analytics, and IT tools
- Scale to support temporary (elastic) and permanent growth
- Uniformly manage multiple capture nodes and the high volume of packets across any distributed, multi-cloud, or hybrid network
- Quickly get started leveraging stored network packet data by deploying self-hosted executable images with installation scripts in Amazon Web Services (AWS), Google Cloud, and Microsoft Azure[1]

cStor-V Virtualized Network Packet Capture

Streamed and stored network packet data is vital for maximizing security posture and observability of your network, IT infrastructure, and application workloads. This agentless solution facilitates the availability of stored network packet data, traffic analytics, and KPI metrics to IT personnel and the analytics and tools they use. It is a self-hosted component if the cCloud™ Visibility Suite that is ready to deploy, use, and scale with[1]:

- Public Cloud Infrastructure: AWS, Azure, Google Cloud
- Hypervisors: VMware ESXi, Microsoft Hyper-V, KVM, Cisco NFVIS

Stored packets are necessary to strengthen your security posture, efficiently troubleshoot network problems and capacity shortcomings, monitor performance vis-a-vis service level agreements (SLA), and provide information and evidence for regulatory compliance. Packets are captured, enriched with metadata, routed to persistent storage, and are available by API and direct queries. Captured packets are enriched with timestamps and event tags received via an open API (e.g., a breach alert from a firewall). Data is indexed and organized for fast recall and grouping. Packets can also be selected, grouped, and exported as a PCAP file.



high-level diagrams of typical Public Cloud deployments; direct packet acquisition is necessary for Azure

The virtualized and physical Packet Capture Appliances (cStor®-V and cStor®, respectively) interoperate to provide a single, seamless, and holistic view of your network from your choice of vantage points. You get elastic scalability and unified access to all stored packets from anywhere in a distributed or hybrid network, from all physical and virtual cStor Packet Capture nodes. Queries and searches also span across all nodes and all data.

All cStror-V nodes and captured-and-stored packet data are accessed using an API, the appliance's user interface, and the cClear® or cClear®-V Analytics Engine and Administration Console. Packet capture scales from just one VPN to a globally distributed hybrid network. Unified centralized administration lowers the effort to manage nodes and the high velocity and high volume of network packet data captured from multiple strategic vantage points in any network.

[1] go to www.cpacket.com for the current list of readily supported and validated environments

Key Benefits

Stored network packets complement streamed network packets by providing data for security and performance analytics, other tools, and dashboards. Use-case oriented benefits include:

- Historical network packet data is vital for security, performance management, and regulatory compliance uses
- Capture and store high volumes of packets enriched and indexed (by timestamp and tag metadata)
- Analytics for protocols, latency, jitter, market data gaps (cMDF), refer to the Technical Specifications for more
- Query and Search across all instances/nodes for strings, IP addresses, ports, etc., see the User Guide for details
- Export packets to PCAP files using Berkeley Packet Filtering and grouping by selecting timeframes and tags

IT operations personnel, especially NetOps, AppOps, CloudOps, SRE, SecOps, and InfoSec (security analysts, forensic analysts, red team, blue team, third-party vulnerability and penetration testers, and the analytics and tools they use) benefit from the rich insights available from stored network packets. The insights facilitate detecting cyberthreats and active attacks, validating network health, profile network performance, and identifying anomalies and other problems. Data, KPI metrics, and actionable insights are surfaced and visualized using the cClear® or cClear®-V Analytics Engine, Wireshark, and other third-party analytics.

Stored network packet data, especially when accumulated over time and analyzed, becomes a large dataset that holds and reveals:

- Patterns, trends, and many other insights are revealed by advanced analytics
- Forensic evidence that can be explored and analyzed automatically and manually to reveal cyberthreats, performance anomalies, and other actionable insights
- A record of communications, traffic, transactions, and other forensic evidence commonly required for regulatory compliance reporting
- Actionable insights derived from stored network packet data using analytics include application and server responsiveness, protocol performance details, TCP health, round-trip time, retransmits, flow information, latencies, jitter, utilization (e.g., "top talkers"), basic connectivity problems, and streaming performance
- Actual traffic before, during, and after events of interest by playing sequences of stored packets

Versatile Usage

Elastically deploy packet capture nodes to capture packets for analysis to understand threats, breaches, network health, performance problems, and to have data to meet regulatory requirements. Nodes can be located anywhere within your environment, including branch offices, remote sites, data centers, and public clouds. You can configure the cStor-V virtualized appliance to route captured packet data to local, virtual, and cloud storage (refer to the Technical Specifications for compatible storage types). Stored network packet data can be created and shared as PCAP files by grouping packets by time, tags, or both then exporting them as PCAP files.

Instances of cStor-V and cStor virtualized and physical appliances can be deployed at strategic vantage point nodes for visibility and packet capture that will scale across distributed and hybrid environments. When used with the cClear or cClear-V Analytics Engine, network packet data from all nodes are combined to present a unified view of the IT environment.

The cStor-V virtualized appliance can be run in virtualized Network Function Virtualization (NFV) environments in the Single-Root Input/Output Virtualization (SR-IOV) mode to capture/analyze the LAN/WAN traffic. It also interoperates with qualified Cisco ISRv virtual routers for gaining visibility, insights, and observability.

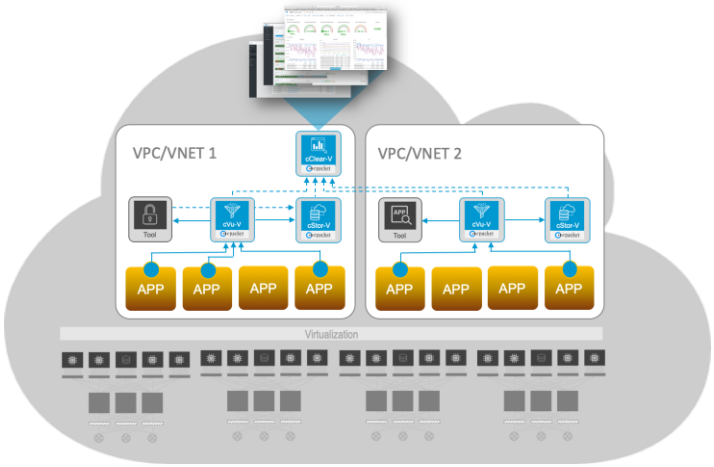
Open Architecture

Stored data is easily accessible by anyone, the cClear® or cClear®-V Analytics Engine, Wireshark, and other third-party analytics and tools. Data. Pan-network packet data can be queried or streamed for democratized use by all IT stakeholders, third-party analytics, AIOps solutions, and other IT tools by:

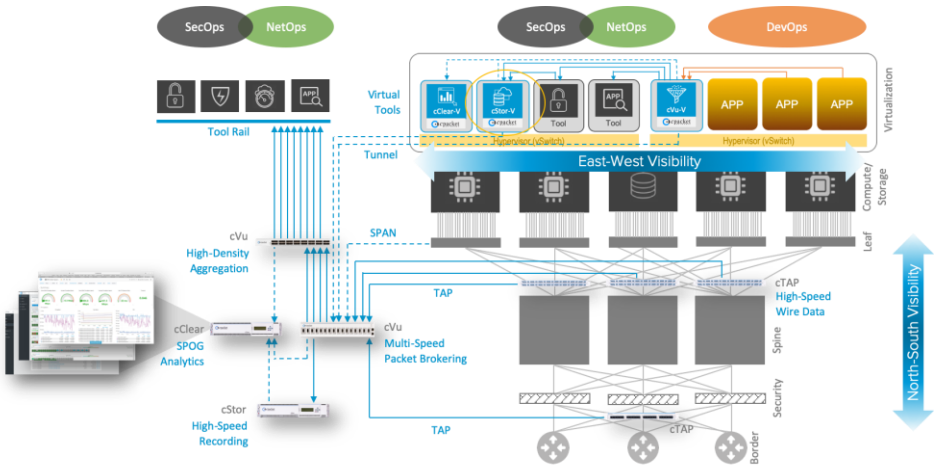
- Direct role-based access
- Remotely querying and retrieving using the open API
- Streaming using Kafka

Deployment and Use Case

Self-hosted instances can scale to meet temporary and permanent scaling needs. This flexibility gives you a cost-effective and easy way to monitor traffic at strategic vantage points or for specific periods (e.g., you can use an instance to troubleshoot a particular problem then decommission that instance).



architectural diagram for comprehensive public cloud visibility



architectural diagram for complete north-south and east-west visibility in a hybrid environment

On-premises deployments in the branch offices or data centers support capturing packet data through DPDK/SR-IOV direct mode, hypervisor-based virtual-switching with support for VMware Standard/Distributed vSwitch, and Open vSwitch (OVS) mode or overlay tunnels (VXLAN, ERSPAN).

The appliance captures network packets from public cloud infrastructure seamlessly scaled across multiple Virtual Private Clouds, Availability Zones, and the entire infrastructure (i.e., a multi-cloud environment). The same applies to hybrid environments that include physical infrastructure.

The cStor-V Virtualized Packet Capture appliance interoperates with all physical and virtualized Visibility Fabric appliances from cPacket Networks. It also readily integrates with third-party analytics and tools via its open API.

cStor-V virtualized packet capture self-hosted images can be deployed and run on a VM in virtualized software-defined data centers to gain visibility into east-west and north-south traffic. It is hardware-independent with ready support for common virtualized environments, including public cloud infrastructure. See the Technical Specifications for details.

The virtualized appliance captures packets from virtualized networks from native mirroring services, from instances of the cVu®-V Virtualized Network Packet Broker (NPB), or both (note that all diagrams in this datasheet show packets delivered via the cVu-V virtualized NPB). The cVu-V virtualized NPB operating in *packet acquisition mode* will monitor your choice of VPC subnets to acquire network packets in public cloud infrastructure that do not offer native packet/traffic mirroring services packets without the downsides of using agents. The virtualized NPB can be configured to filter network packets to tailor the contents and lower the volume of packet data delivered to network packet capture appliances. Network packets can also be captured from overlay tunnels such as VXLAN and ERSPAN to gain visibility. You can configure the repository where captured packets are stored (refer to the Technical Specifications for compatible storage repositories). While it is possible to route packets for storage outside of a public cloud, doing so will introduce additional latency and costs for transferring data out of your cloud environment.

Cost-Effective and Flexible Licensing

The cStor-V Virtualized Packet Capture appliance has flexible licensing that allows you to control, contain, and right-size cost with flexible licensing options, including bringing your own usage license (BYOL). The virtual appliances can be instantiated on-demand for timed use (e.g., hourly, weekly, monthly, etc.). The licensing options give you elastic flexibility to deploy software images in your target environments at the scale needed. Refer to the ordering information section for additional details.

Technical Specifications

Key Features:

	cStor-V
Packet Indexing	Yes
Fast/Expedited Query	Yes
Flow Information	Yes
Multiple Capture Merge	Yes
Latency and Jitter Analysis	Yes
Multicast / Video Analysis	Yes*
TCP Analytics	Yes
Real-Time Protocol Analytics	Yes*
Financial Protocol Analytics (e.g., for high-frequency trading)	Yes*
Financial Market Data Feed Analytics (cMDF)	Yes*
cClear/cClear-V Analytics Engine Integration	Yes
Role-Based Administration	Yes
Software Upgrade/Restore	Yes
Web-based GUI / CLI for System Management	Yes
TACACS+/RADIUS Authentication	Yes

* Roadmap or planned. Check with cPacket Networks or an authorized sales representative for the most current product availability and related information.

Performance and Specifications:

	cStor-V
Virtual Port (Management)	1
Virtual Port (Capture) / Instance	1
Capture Rate / Instance	Up to 10Gbps
vCPU	4
Memory	16GB
System Disk	40GB
Minimum Storage	1TB
Maximum Storage	Scalable*
Maximum Capture Throughput*	Scalable (Refer to Ordering Information)
Hypervisor Supported	VMware ESXi, MS Hyper-V, KVM, Cisco NFVIS
High-Performance Mode	DPDK/SR-IOV
Public Cloud	AWS, MS Azure, GCP
Cloud Data Mirroring	AWS VPC Traffic Mirroring GCP Packet Mirroring

* Storage scales with machine type selected

Ordering Information

SKU	Description
CP_CCLOUD_CSTOR_V_SUB-xG (Where X is the capacity. Options 1G, 5G, 1[illegible] 25G, 50G, 100G, 250G, 500G, 1TB)	cPacket cStor-V packet capture virtual appliance up to 5Gbps aggregate capture capacity, 1 year subscription. Deployable on top of VMware ESXi, Microsoft Hyper-V, KVM, Cisco NFVIS, and as part of cCloud BYOL solution in AWS, Google Cloud, and Microsoft Azure. Requires cClear-V subscription. Gold level maintenance included.
CP_CCLEAR_CON	Annual license to connect with cClear appliance or cClear-V software instance at 3% of the list price of the connected device.

For additional information, go to cCloud Visibility Suite product webpage.

About cPacket Networks

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 deep network visibility required for complex IT environments enabling Fortune 500 organizations worldwide to keep their business running. cPacket solutions are fully reliable, tightly integrated, and consistently simple. Our cutting-edge technology enables network, application, and security teams to proactively identify issues before negatively impacting the business. The result: increased service agility, enhanced experience assurance, and faster transactional velocity. Learn more at www.cpacket.com.