Data Sheet

cStor® S Packet Capture & Analysis Observability Nodes

Captured Packet Data Facilitates IT Observability for Maximizing Availability, Performance, and Security

cStor S series observability nodes enable you to:

- Maximize the observability of your IT network infrastructure, and application workloads
- Understand how your network is performing and know how to resolve problems
- Use captured network packet data for efficient troubleshooting and fast incident response to minimize service outages and disruptions
- Use captured network packet data for threat hunting and forensic analysis to maximize the IT security posture
- Meet regulatory data capture and reporting requirements
- Analyze feeds to help market data providers assure that consumers have timely and accurate data to drive financial decisions
- Provide stored network packet data to analysts, analytics, and IT performance management and security tools

Capture and Analyze Network Packet Data for Observability

Network packet data is foundational for making IT infrastructure, especially the network, observable. The cStor S series packet capture and analysis observability nodes offer the highest performance available in the industry achieving a lossless, sustained packet capture-to-disk (CTD) rate at up to 60Gbps with a burst CTD of up to 100Gbps. The maximum capture-to-disk ingestion rates, storage capacity, encryption, and other functionality features vary by model, so refer to the specifications section. For virtualized and hybrid-cloud environments, seamlessly interoperable functionality is provided by the cStor-V capture and analysis virtual observability node (see cCloud™ Visibility Suite data sheet).

The cStor S series nodes combine fast network interfaces, storage, advanced software, and Wireshark integration to capture, store, analyze, and transfer a time-series history of network traffic that can be replayed, analyzed, and used for observability. Stored network packet data is vital to maximize the performance and security of IT infrastructure and application workloads.

Stored network packet data, KPIs, and analytics data contribute to network observability so the team can maximize the security posture, connectivity, and application performance experiences by helping the IT team detect and resolve:

- Service disruptions and outages in a multi-hop service-chain
- Performance issues, such as bottlenecks, latencies, dropped connections, etc.
- Network forensics for threat investigations and incident response
- Stored network packet data also supports regulatory compliance data retention and reporting requirements and third-party solutions

The cStor S nodes capture network packets in real-time on one or more input ports from network switch ports, Test Access Points (TAPs), and Network Packet Brokers (NPB) such as the cPacket cTap® TAPs and cVu® packet brokering and monitoring observability nodes, respectively. The cVu nodes enrich the network packet data with timestamps and custom tags (e.g., to identify specific events). The data is indexed and stored for fast retrieval and analysis.

The cStor S nodes also generate high-resolution network KPIs that include TCP, UDP, and RTP traffic metrics, transmission timing, and latencies (e.g., TCP, DNS lookup, and HTTPS handshake response times). The cStor S nodes also generate unique application and use-case specific metrics, KPIs, and other analytics, which are available immediately after being captured and you can view as follows:

- Directly on specific models that run Wireshark using a browser
- Using the cClear® observability layer and its interactive visualizations combined into customizable dashboards
- By transferring it to analysts and third-party analytics and tools via Kafka, API queries, and exported PCAP files

High-Fidelity Observability for IT Derived from Stored Network Packet Data

All cStor models store and generate TCP analytics, flow, and KPIs information that is indispensable for detecting, pinpointing, troubleshooting, and resolving IT problems to

minimize outages and strengthen IT cyber risk resilience. The network packet data and KPIs provide the necessary observability to know what is happening with your IT network, infrastructure, and application workloads. The cStor S nodes are components of the cPacket Intelligent Observability Platform. This full-stack solution spans reliable data acquisition to actionable IT and security operations intelligence via alerts and dashboards.

Analytics

The following network-centric analytics are applied to stored network packet data to generate actionable intelligence about the network and, more broadly, the IT infrastructure, including servers, services, and application workloads. Stored data and

analytics results are retrieved by the cPacket cClear® observability layer for additional analysis and presentation. KPIs and analytics results are also presented via interactive dashboards (refer to the cClear data sheet for details). Similarly, the data is available to non-cPacket devices, dashboards, analytics, and other software.

- Flow Analytics – Gives traffic flow insights useful for assessing throughput, detecting bottlenecks, and planning capacity.
- TCP Analytics – Conveys a network's health and helps troubleshoot problems, including stateful analysis and details about latencies (see next), response times, roundtrip times, session duration, and transmission errors (e.g., retransmissions, dropped packets, etc.).
- Latency/Jitter Analytics – Conveys one-way and roundtrip latency and jitter metrics that help troubleshoot problems that adversely impact performance and experiences, particularly with streaming data (i.e., multimedia data).
- Real-Time Protocol Analytics (e.g., multicast, UDP) – Conveys the quality of real-time transmission for data and use cases when network packets must be in order, without dropouts, and minimal or non-perceptible latency and jitter.
- Market Feed Gap Detection – Provides gap detection, out-of-orders, and sequence errors. This feature is for providers and consumers of market feed to make real-time trading decisions, ensure data delivery, have evidence for troubleshooting, and customer support, and meet regulatory requirements.
- VPN Analytics – Conveys errors, reconnections, and other KPIs specifically for VPN tunnels.

Data Enrichment and Indexing

Network packets are losslessly captured at sustained ingestion data rates of up to 60Gbps and are naturally stored as time-series data. Timestamps and optional custom tags are appended to add context. The data is indexed to facilitate fast querying, searching, forensic analysis, and regulatory reporting. cStor S nodes always attach timestamps to captured packets using one of the following methods:

- Internal clock
- Precision Time Protocol (PTP) Extended timestamp format
- Captured from a cPacket cVu packet broker observability nodes using either its native format or an Arista compatible (48-bit format; specific cVu models only, refer to the cVu data sheets for details)

The onboard analytics preferentially use timestamps from cVu nodes for the highest accuracy because those timestamps are associated with packets when they are acquired from a source with the least possible bias and timing skew.Tags are received via a RESTful API from external sources. For example, a firewall can send a tag correlating a packet series to a breach alert. Analysts and other end-users can group packets to replay the activity of a specific event, analyze only those packets, and export those packets for further analysis and evidence.

Data Access: Query, Search, and Export

You can query, search, access, and integrate the stored data immediately after it is stored.

- You can directly log into a cStor S node to search for and view data; search options include strings, IP addresses
- Wireshark is installed to easily view and analyze the network packet data without first having to download
- A RESTful API enables issuing queries and receiving data and analytics results (KPIs) matching the query
- Data can be streamed to a target device via Ethernet and optionally using Kafka

- Data can be grouped and exported in the industry standard PCAP file format; grouping can be by timeframe, tag, and Berkeley Packet Filters (BPF)

Data / Event Replay

The data is inherently time series and is stored and organized accordingly. You can view time-series data in sequence, or in other words, "replay" the data to convey the network perspective history of an event from before, during, and after an event.

Role-Base Access

A browser is used to interact with cStor S nodes and access and view the stored data. Authentication is facilitated using LDAP and TACACS+. End-users are added, deleted, and modified (passwords and read/write access permissions) by an admin using the internal Administration screen.

Extensible Storage and Data Encryption

All cStor S nodes have onboard storage that is cost and rack-space optimized; storage capacities vary by model from 44 to 576 TB. Some models can be expanded with additional storage capacity using a cPacket Extensible Storage unit that can increase per-node capacity up to a maximum of roughly 2 PB. You can also add nodes to increase storage capacity in your IT infrastructure. Data captured and stored across multiple nodes can be queried, searched, and retrieved as one logical and unified view. Stored data is automatically encrypted on Self-Encrypting Drives (SED). SED availability varies by model, so refer to the technical specifications and ordering information.

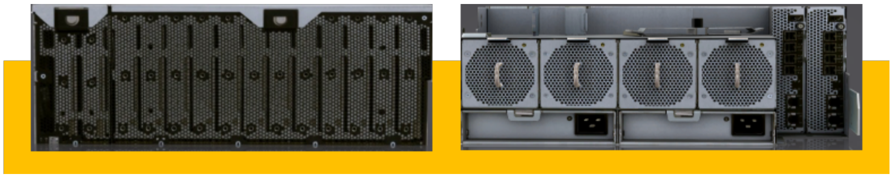

Figure 1: cPacket Extensible Storage (CES)

Open Architecture and Interoperability

The cStor S nodes receive network packets via Ethernet directly from the infrastructure and cPacket cVu® Network Packet Brokers. They also can receive network packets from any vendor's Network Packet Brokers, TAPs, and network infrastructure ports. Therefore, the cStor S nodes readily integrate into physical networks.

Hybrid-Cloud IT Infrastructure

A comprehensive range of hardware and virtual observability nodes allows you to deploy cStor S where needed in any IT environment. Using the physical nodes described in this data sheet and the cStor-V virtual nodes, you can seamlessly extend the capture and storage capacity to span physical and cloud environments. A single instance of cClear (or cClear-V) observability platform manages the full hybrid-cloud deployment, with customizable off-the-shelf dashboards that show traffic, analytics results, and other network-centric KPIs.

The cPacket hybrid-cloud observability is a full-stack solution. It includes the following components that maximize the observability of your IT network with network packet pipelining, analytics, actionable alerts, and visualizations:

cVu packet broker and monitoring observability nodes – provide network data consolidation, packet processing, pipelining with lossless acquisition and KPIs for certain real-time monitoring.

cStor packet capture and analysis observability nodes – provide lossless packet capture with on-board/off-board storage and historic KPIs; all of which can be accessed by queries, streaming, and as exported PCAP files.

cClear observability platform – provides analytics, additional KPIs, alerts, and interactive visualizations via customizable dashboards. It also hosts the user interface for managing the observability nodes.

Deployment

The rackmount cStor S nodes are for physical networks in a data center, campus, and branch environments. The nodes have one or more input ports that connect to a core network, TAP, or NPB. All captured packets are merged into the time-series database when packets are simultaneously ingested from multiple input ports. Receiving network packets from an NPB allows high-precision timestamping and filtering of the packet streams to reduce the volume of stored data.

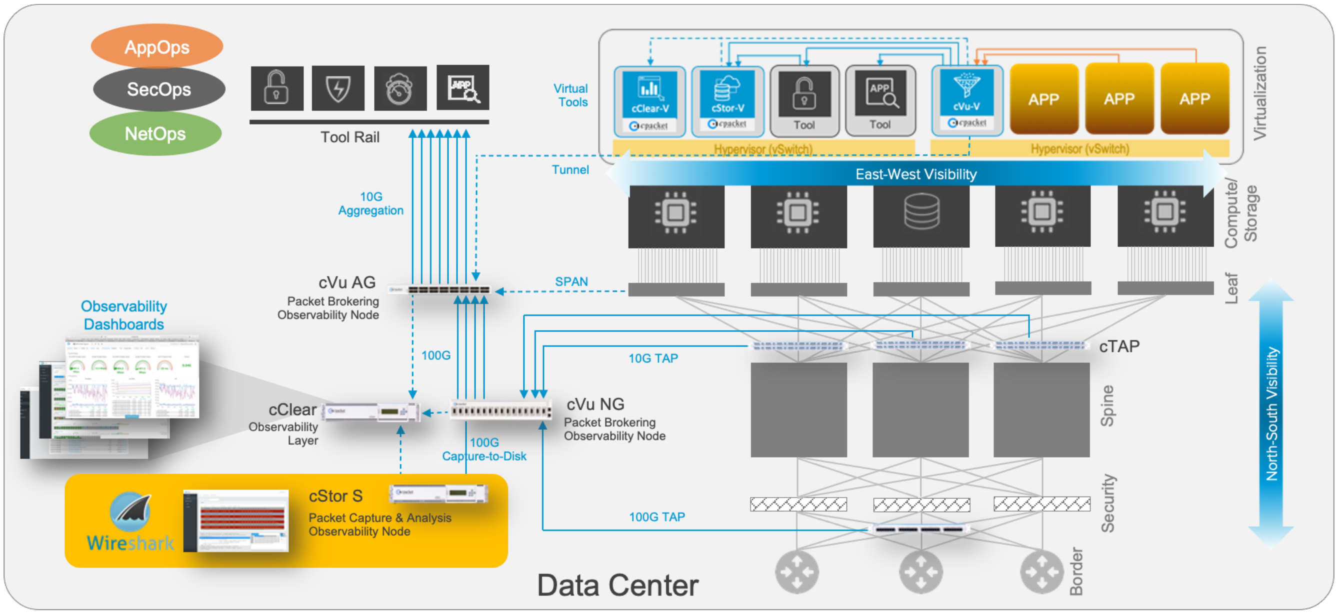

Figure 2: Reference Design for Complete Observability of North-South and East-West Network Traffic

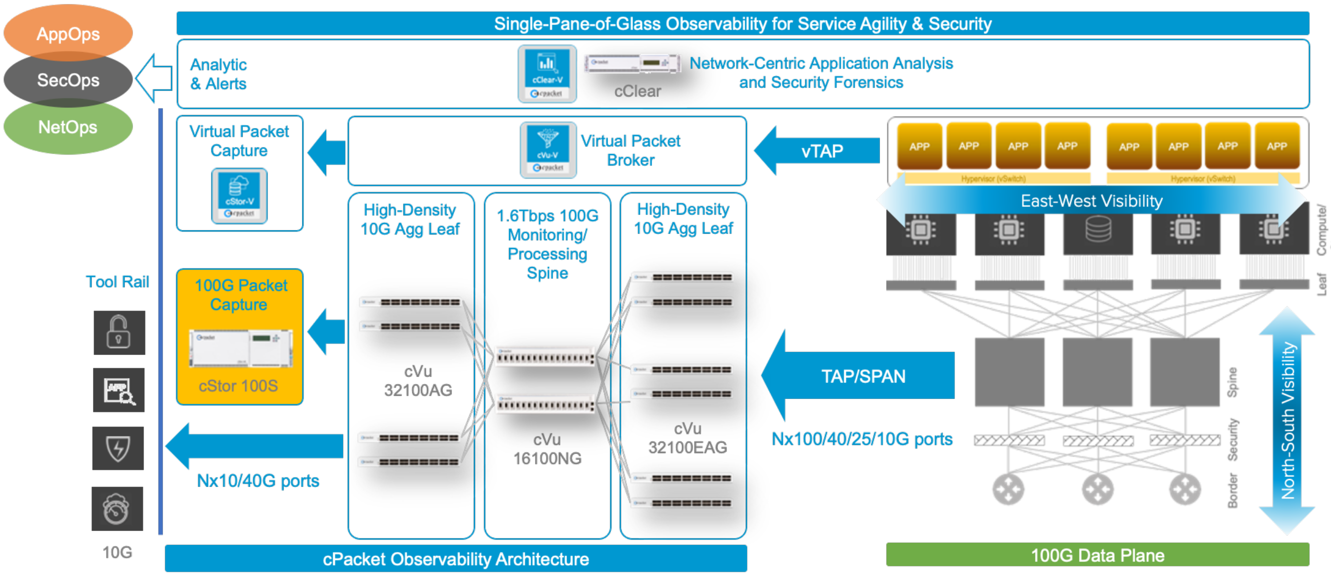

Figure 3: Reference Design for a 2-Tier Scalable Observability Architecture

Technical Specifications

Key Features:

	cStor 10S	cStor 20S	cStor 30S	cStor 40S	cStor 100S
Precision Time (PPS)	Yes*	Yes*	Yes*	Yes*	Yes*
Packet Indexing	Yes	Yes	Yes	Yes	Yes
Fast/Expedited Querying	Yes	Yes	Yes	Yes	Yes
Multiple Capture Merge	Yes	Yes	Yes	Yes	Yes
Flow Analytics	Yes	Yes	Yes	Yes	Yes
TCP Analytics	Yes	Yes	Yes	Yes	Yes
Latency/Jitter Analysis	Yes	Yes	Yes	Yes	Yes
Real-Time Protocol Analysis	Yes	Yes	Yes	Yes	Yes
Multicast Video Analysis	Yes	Yes	Yes	Yes	Yes
Market Data Feed Analytics (cMDF)	Yes	Yes	Yes	Yes	Yes
VPN and Tunneling Protocol Analytics	Yes	Yes	Yes	Yes	Yes
Hardware Accelerated Data Encryption	Yes	Yes	Yes	Yes	Yes
Filter and View Data with a browser	Yes	Yes	Yes	Yes	Yes
Wireshark (local, pre-installed)	Yes	Yes	Yes	Yes	Yes
Integration and Interoperability					
Packet Ingestion from cVu NPB	Yes	Yes	Yes	Yes	Yes
Packet Ingestion from third party NPB	Yes	Yes	Yes	Yes	Yes
Packet Ingestion from Network Ports	Yes	Yes	Yes	Yes	Yes
Packet Ingestion from Network TAPs	Yes	Yes	Yes	Yes	Yes
cClear Observability Dashboards	Yes	Yes	Yes	Yes	Yes
cClear Admin Console	Yes	Yes	Yes	Yes	Yes
Other analytics, dashboards, etc. (DIY, 3rd party)	Yes	Yes	Yes	Yes	Yes
Network Packet Data Access / Export					
Direct Streaming via Kafka	No	No	No	No	No
RESTful API (queries)	Yes	Yes	Yes	Yes	Yes
PCAP download	Yes	Yes	Yes	Yes	Yes

* Timing info received from a cPacket cVu NPB nodes

Interface and Storage Options:

	cStor 10S	cStor 20S	cStor 30S	cStor 40S	cStor 100S
10 GbE Ports (SFP+)	1	4	8	8*	8*
40 GbE Ports (QSFP+)	N/A	N/A	N/A	2	2**
100 GbE Ports (QSFP28)	N/A	N/A	N/A	N/A	2
Burst Capture Rate	N/A	N/A	N/A	80 Gbps	100 Gbps
Burst Capture Duration	N/A	N/A	N/A	1 sec (every 1 min)	1 sec (every 1 min)
Sustained Capture Rate	10 Gbps	20 Gbps	30 Gbps	40 Gbps	60 Gbps
Default Storage	44/88 TB	192 TB	192 TB	288TB	288 TB
SED Storage Option	44 TB	192 TB	192 TB	288 TB	288 TB
Extensible Storage (CES)	N/A	1696 TB	N/A	1696 TB	1696 TB
Max Total Storage	88 TB	1.88 PB	192 TB	1.98 PB	1.98 PB
Storage Reliability	Yes (SW)	Yes (SW)	Yes (SW)	Yes (SW)	Yes (SW)

* Using QSFP+ breakout box/cables   ** Using QSFP+ supported transceivers

Dimensions and Weight:

Capture Unit	cStor 10S	cStor 20S	cStor 30S	cStor 40S	cStor 100S
Height/Rack Unit	3.5" (8.9 cm) 2U	3.4" (8.7 cm) 2RU	7" (17.8 cm) 4RU	7" (17.8 cm) 4RU	7" (17.8 cm) 4RU
Width	17.2" (43.7 cm)	16.9" (43 cm)	17.2" (43.7 cm)	17.2" (43.7 cm)	17.2" (43.7 cm)
Depth	23.6" (59.9 cm)	28" (71.1 cm)	28" (71.1 cm)	28" (71.1 cm)	28" (71.1 cm)
Weight	52 lbs. (23.6 kg)	66 lbs. (30 kg)	132 lbs. (60 kg)	132 lbs. (60 kg)	132 lbs. (60 kg)

Extensible Storage Modules	CES 512TB	CES 1024TB	CES 1696TB
Height/Rack Unit	7" (17.8 cm) 4RU	7" (17.8 cm) 4RU	7" (17.8 cm) 4RU
Width	17.2" (43.7 cm)	17.2" (43.7 cm)	17.2" (43.7 cm)
Depth	45" (114.3 cm)	45" (114.3 cm)	45" (114.3 cm)
Weight	66 lbs. (30 kg)	132 lbs. (60 kg)	132 lbs. (60 kg)

Operating Conditions:

Capture Unit	cStor 10S	cStor 20S	cStor 30S	cStor 40S	cStor 100S
Operating Temperature	41° F – 95° F	60° F - 95° F	60° F - 95° F	50° F - 95° F	50° F - 95° F
Operating Humidity	50% – 90%	50% – 90%	50% – 90%	8%- 90%	8%- 90%

Extensible Storage Modules	CES 512TB	CES 1024TB	CES 1696TB
Operating Temperature	60° F - 95° F	50° F - 95° F	50° F - 95° F
Operating Humidity	50% – 90%	8%- 90%	8%- 90%

Power and Cooling:

Master Unit	cStor 10S	cStor 20S	cStor 30S	cStor 40S	cStor 100S
Airflow	Front-to-Back	Front-to-Back	Front-to-Back	Front-to-Back	Front-to-Back
Power Redundancy	1+1 AC 100-240 VAC 50-60 Hz	1+1 AC 100-240 VAC 50-60 Hz	1+1 AC 100-240 VAC 50-60 Hz	1+1 AC 100-240 VAC 50-60 Hz	1+1 AC 100-240 VAC 50-60 Hz
Max. Power Consumption	650 W	1170 W	1373 W	1373 W	1373 W
Heat Dissipation	2216.5 BTU/hour	2195.3 BTU/hour	4597.4 BTU/hour	4597.4 BTU/hour	4597.4 BTU/hour

Extensible Storage Modules	CES 512TB	CES 1024TB	CES 1696TB
Airflow	Front-to-Back	Front-to-Back	Front-to-Back
Power Redundancy	1+1 AC 100-240 VAC 50-60 Hz	1+1 AC 100-240 VAC 50-60 Hz	1+1 AC 100-240 VAC 50-60 Hz
Max. Power Consumption	1183.2 W	1373 W	1373 W
Heat Dissipation	2860 BTU/hour	4597.4 BTU/hour	4597.4 BTU/hour

Ordering Information

Product SKU:

CP_CSTOR_100S_2100_288TB	cPacket cStor 100S packet capture and analysis observability node in 4RU, 100Gbps burst, 60Gbps sustained capture-to-disk rate, 2x100GbE QSFP28 ports, and 288TB onboard disk storage. CES expansion supported. Maintenance not included.
CP_CSTOR_100S_2100_288TB_SED	cPacket cStor 100S packet capture and analysis observability node in 4RU, 100Gbps burst, 60Gbps sustained capture-to-disk rate, 2x100GbE QSFP28 ports, and 288TB self-encrypting drive (SED) onboard disk storage. CES expansion supported. Maintenance not included.
CP_CSTOR_40S_240_288TB_SED	cPacket cStor 40S packet capture and analysis observability node in 4RU, 40Gbps sustained capture-to-disk rate, 2x40GbE QSFP+ ports, and 288TB self-encrypting drive (SED) onboard disk storage. CES expansion supported. Maintenance not included.
CP_CSTOR_40S_240_288TB	cPacket cStor 40S packet capture and analysis observability node in 4RU, 40Gbps sustained capture-to-disk rate, 2x40GbE QSFP+ ports, and 288TB onboard disk storage. CES expansion supported. Maintenance not included.
CP_CSTOR_30S_810_192TB_SED	cPacket cStor 30S packet capture and analysis observability node in 4RU, 30Gbps sustained capture-to-disk rate, 8x10GbE SFP+ ports, and 192TB self-encrypting drive (SED) onboard disk storage. Maintenance not included.
CP_CSTOR_30S_810_192TB	cPacket cStor 30S packet capture and analysis observability node in 4RU, 30Gbps sustained capture-to-disk rate, 8x10GbE SFP+ ports, and 192TB onboard disk storage. Maintenance not included.
CP_CSTOR_20S_410_192TB_SED	cPacket cStor 20S packet capture and analysis observability node in 2RU, 20Gbps sustained capture-to-disk rate, 4x10GbE SFP+ ports, and 192TB self-encrypting drive (SED) onboard disk storage. CES expansion supported. Maintenance not included.
CP_CSTOR_20S_410_192TB	cPacket cStor 20S packet capture and analysis observability node in 2RU, 20Gbps sustained capture-to-disk rate, 4x10GbE SFP+ ports, and 192TB onboard disk storage. CES expansion supported. Maintenance not included.
CP_CSTOR_10S_110_88TB	cPacket cStor 10S packet capture observability node in 2RU, 10Gbps sustained capture-to-disk rate, 1x10GbE SFP+ ports, and 88TB onboard disk storage. Maintenance is not included.
CP_CSTOR_10S_110_44TB_SED	cPacket cStor 10S packet capture and analysis observability node in 2RU, 10Gbps sustained capture-to-disk rate, 1x10GbE SFP+ port, and 44TB self-encrypted drive (SED) onboard disk storage. Maintenance not included.
CP_CSTOR_10S_110_44TB	cPacket cStor 10S packet capture and analysis observability node in 2RU, 10Gbps sustained capture-to-disk rate, 1x10GbE SFP+ port and 44TB onboard disk storage. Maintenance not included.
CP_CES_CSTOR_1696TB	cPacket extensible storage unit (CES) 1.6PB disk storage in 4RU for cPacket cStor packet capture and analysis observability nodes. Maintenance is not included.
CP_CES_CSTOR_1024TB	cPacket extensible storage unit (CES) 1PB disk storage in 4RU for cPacket cStor packet capture and analysis observability nodes. Maintenance is not included.
CP_CES_CSTOR_512TB	cPacket extensible storage unit (CES) 512TB disk storage in 4RU for cPacket cStor packet capture and analysis observability nodes. Maintenance is not included.
CP_CCLOUD_CSTOR_V_SUB-xG	For details refer to the Cloud and Virtual cStor-V datasheet: https://www.cpacket.com/resources/cstorv/

You can learn more about the cStor S observability nodes at https://www.cpacket.com/products/cstor/

About cPacket Networks

cPacket powers hybrid-cloud observability through its Intelligent Observability Platform. It reduces service outages through network-centric application analysis, strengthens cyber security through high-resolution network data for threat detection, and accelerates incident response through network forensic analysis. The result is increased service agility, experience assurance, and transactional velocity for the business.
Find out more at www.cpacket.com.