cpacket NETWORKS

Tech Brief

Network Packet Storage and Forensics for Hybrid IT

Captured Packets and Analytics Empowers Security Operations to Troubleshoot Cyberattacks

Technology Benefits

- **Lossless Packet Capture for Physical, Virtualized and Cloud Networks**
  Network packets from an entire network facilitates detailed forensic analysis
- **Optimized Search**
  Fast queries and data retrieval complement fast packet capture with simultaneous store and indexing to respond quickly
- **Network Packet Archival Storage for Incident Response**
  Capture-and-store packets enriched and indexed with metadata

Business Benefits

- **Optimized Root Cause Analysis**
  Replay and forensically analyze historical network data for cybersecurity and incident response
- **Reducing Production downtime**
  Reduce mean-time-to-resolution for stateful (TCP) and real-time (UDP/RTP) applications
- **Operational Efficiency**
  Pervasive visibility allows you to optimize applications, security posture, and Hybrid networks

The Challenge

The frequency and types of cyberattacks are increasing and becoming more damaging. Perimeter security methods such as firewalls and signature-based intrusion detection systems (IDS) are necessary but not able to catch newer and innovative attacks, especially those leveraging human frailty. More attackers exploit the network or "data in motion" channel to mix into the regular enterprise traffic and then progressively execute a DDoS, ransomware, or other attack types. Although End-Point Detection and Response (EDR) can help to protect mobile devices, servers, the most sophisticated attacks demand the use of counter through Network Detection and Response (NDR). NDR relies on high-quality network packet data to detect and respond to new and dwelling threats and attacks in the process.

There are multiple reasons to capture and archive packet data so that the Security Operations team can mount a timely and effective Incident Response:

- Investigate what happened, when it happened, how it happened, where it happened, and why it happened? So that you can zero in on the suspicious activity and the culprit.
- To have evidence for what happened and for taking legal action
- To help identify the threat actors and to know how to prevent future occurrences.
- To find out from what point onwards to restore anything corrupted by an attack, such as business data, personal data, system configurations, etc.

Collectively, these activities are aspects of an effective Incident Response (IR) to contain and neutralize an attack and to stop further damage to your business, customers, and reputation.

When it comes to capturing, storing, and analyzing packet data, it's not an easy task due to further technical challenges:

- It's challenging to ingest losslessly, process, and write data to disk at speeds of up to 100Gbps, and simultaneously provide visualizations.
- Evolving hybrid architectures adds further complexity to capture network packets across on-premises physical, virtualized, and multi-cloud environments and where to save them. Managing multiple distributed physical and virtualized capture appliances can also be a challenge.
- How to quickly find, analyze specific data (e.g., find data pertaining to a specific event, timeframe, or both) and provide holistic views when needed – which relies on good indexing and fast search capabilities.

The Technology

The cPacket cStor® series appliances are an integral part of the cPacket's Intelligent Observability Platform and are engineered for lossless capture-to-disk at up to 100Gbps burst and 60Gbps sustained data rates. Fast data retrieval even while writing data leveraging the cPacket's Time Series Database (TSDB) gives you immediate access to forensic evidence. The TSDB is built specifically for handling metrics and events or timestamped measurements and is optimized for measuring change over time. Properties that make time series data very different than other data workloads are data lifecycle management, summarization, and large range scans of many records.

Persistently stored stateful data is enriched with timestamps and event tags to provide easily retrievable snapshots of traffic before, during, and after events that allow replaying breaches, lateral movement, and data exfiltration. The ability to replay the network activity gives a clear understanding of what happened and is happening so you can respond quickly, effectively and prevent future occurrences. Fast query execution and data retrieval using an open API facilitate cyber threat hunting and analysis by security tools for effective NDR, such as Security Information and Event Management (SIEM) and Intrusion Prevention and Detection Systems (IPS/IDS).

Analytics applied to historical data assist the entire IT team in response to threats and attacks in progress. Data is stored on media that can be extended by adding capacity for a total of up to 2PB per device (check datasheet and Quick Reference Guide). For virtualized, cloud, and hybrid environments, similar and seamless functionality is provided by the cStor-V component within the cPacket cCloud® Visibility Suite. This provides quick and easy "Point in Time" visualizations based on the network's IP addresses to show what was happening during that specific time period.

The cPacket physical and virtualized cStor appliance supports simultaneous data feed store, indexing, and search. Smart Query is provided by *parallel indexing* and *fast expedited querying* handling of large amounts of unstructured data at velocity.

The Solution

cPacket provides a scalable and cost-optimized single solution for hybrid environments. Diagram 1 shows an example of hybrid architecture with the cPacket cClear® Analytics Engine deployed in the cloud. The virtualized cClear appliance provides the visualizations in dashboards and facilitates retrieving historical network packets that can be grouped and exported as PCAP files for sharing and analysis.

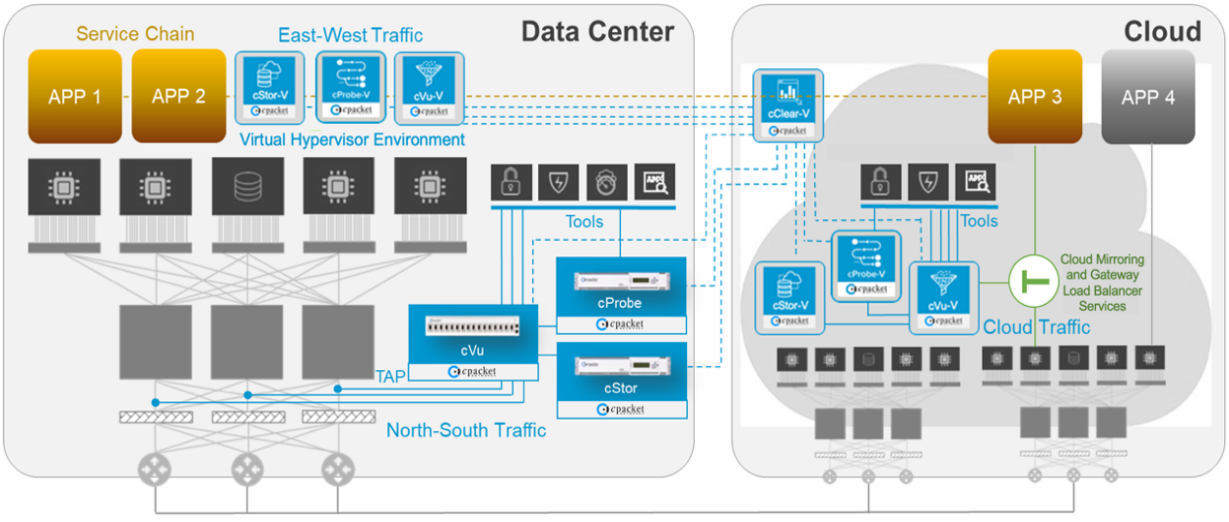

Diagram 1 – cPacket Hybrid Visibility Architecture

Diagram 2 shows an incident response point-in-time view with active sessions data for a specific server. Other metrics include server response, server latency, and active sessions during the time of the breach.

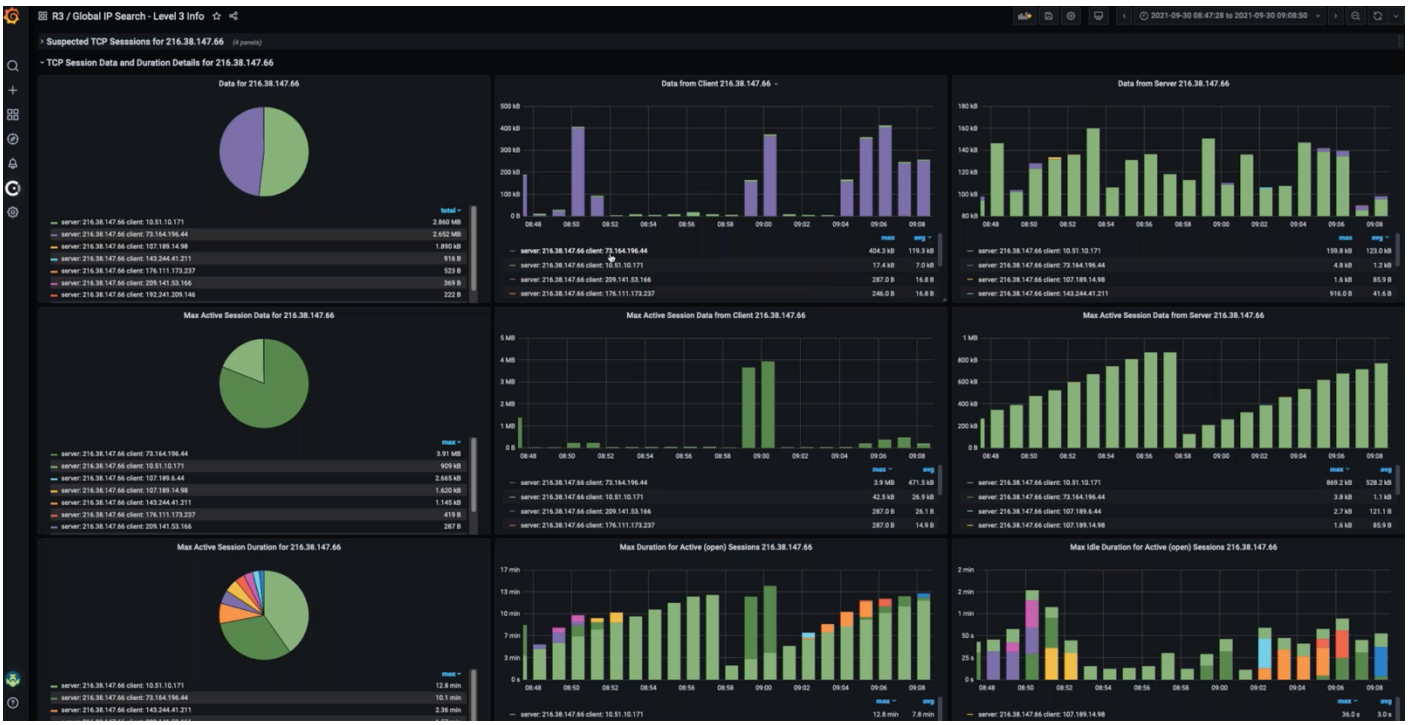

Diagram 2 – Example Server KPIs Visualization for Incident Response

Diagram 3 shows an incident response PCAP download example. This example shows that the data is easily combined using three cStor appliances and captured packets from vantage points strategically located in the network. The range settings option provides custom selectable "Point-in-Time" for an incident's required date and time. Filter Type options provide rich filtering customization, including but not limited to IP addresses, ports, VLANs, time range, and multiple cStor appliances.

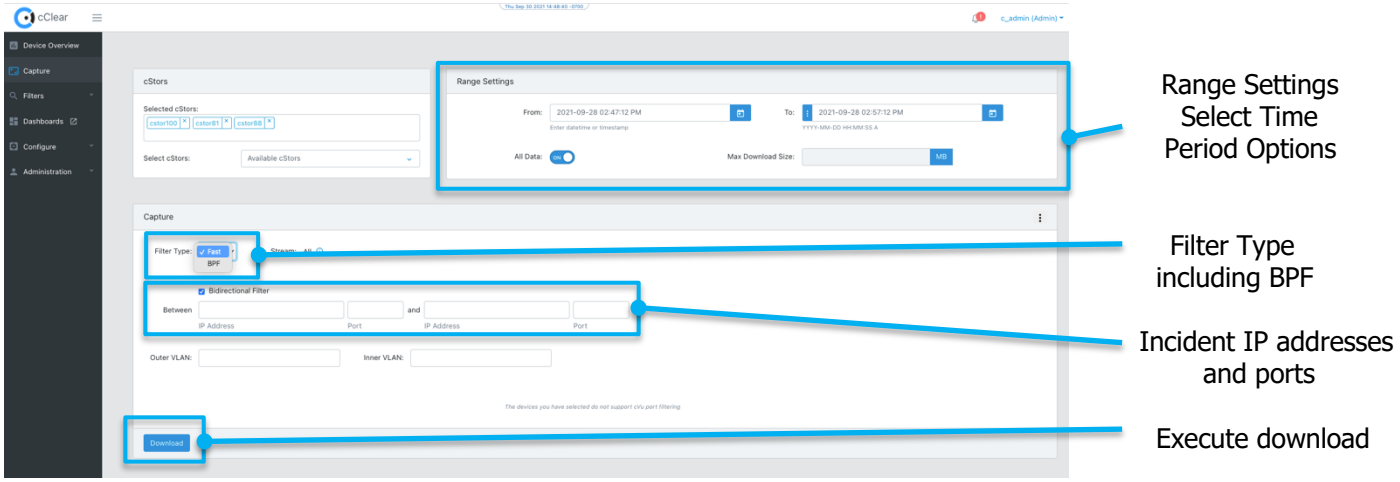

Diagram 3 – Incident PCAP download options

NDR solutions provide alerts on the cyber kill chain when the packets are replicated and forwarded from the network infrastructure and raise threat indicators, such as lateral movement, C2, and exfiltration. cClear provides visualizations to reduce MTTR and enables BPF (Berkley Packet Filter) filtered download PCAP files by including date and time, network monitor, host IP address, etc. Diagram 4 shows an example of a historic PCAP download using Wireshark for network forensic analysis (Ips obscured).

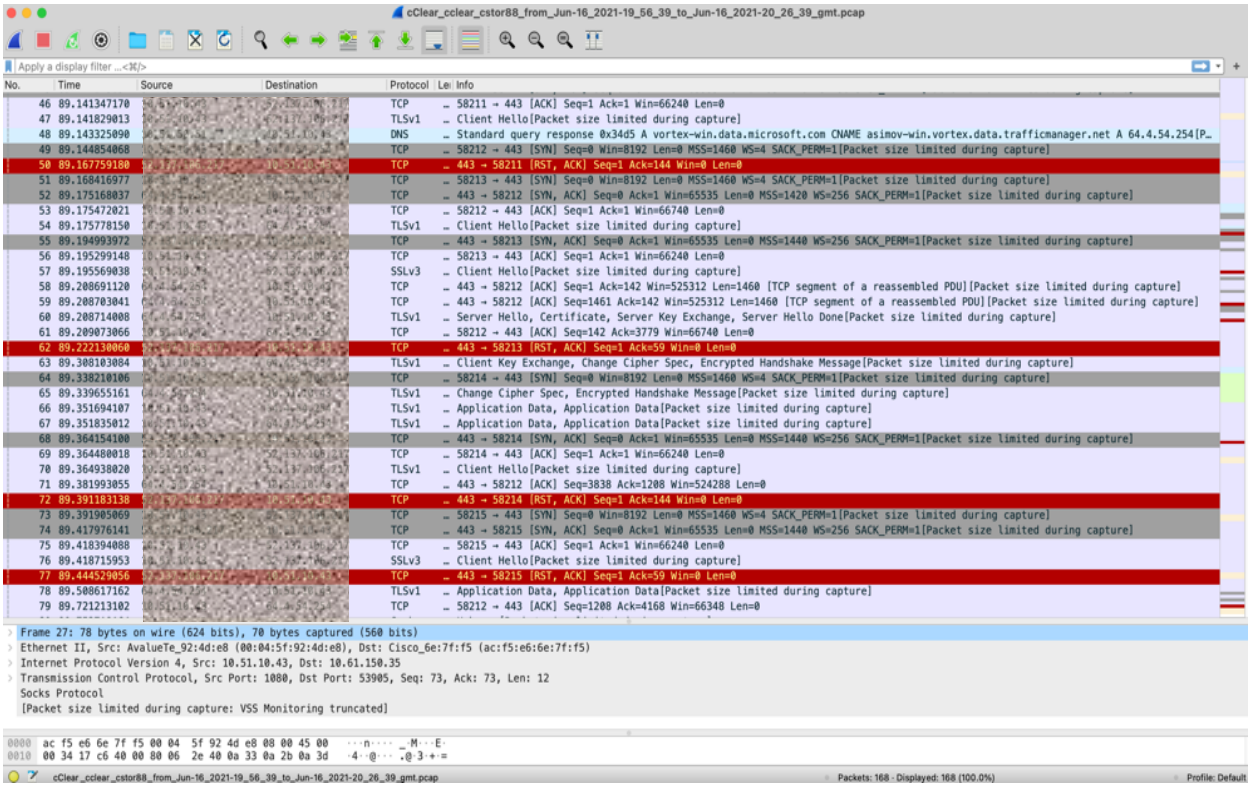

Diagram 4 – Example Historic Forensic PCAP

In summary, the cPacket Intelligent Observability Platform solution enables the following three key use cases and beyond:

- **Lossless Full Packet Capture and Forensic Evidence:** analyzing by link, port, and server for high-speed core networks enables Network Detection and Response.
- **Provides archival network packet storage for analysis:** bringing insightful point-in-time views for faster troubleshooting, breakfix resolution, reducing MTTR, and insight into network Key Performance Indicators (KPIs).
- **Optimized search and retrieval for Incident Response:** supporting simple, fast access to network flows and data to assist forensic investigations.

About cPacket Networks

cPacket Networks 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 www.cpacket.com