cPacket

SOLUTION BRIEF

Network Security:
Every packet counts

Today's network security requires packet delivery, capture and analytics at line speed without a single dropped packet.

Ensuring robust network security and seamless operations is critical, especially for domains like finance, healthcare, the military, real-time logistics and first responders, where the cost of failure is exceptionally high. cPacket's integrated suite of products, including cPacket cVu data brokering and cPacket cStor data capture and analytics, provides a comprehensive solution for line-speed packet delivery and capture—essential for detecting and mitigating network threats. cPacket's agentless hybrid-cloud architecture simplifies deployment and management and offers a cost-effective approach to handling network security demands.

Today's enterprise networks face ever increasing security threats. And many organizations have an even higher bar to clear because of the high cost of failure for their operations. Enterprises in domains including finance, healthcare, the military, real-time logistics and first responders demand zero downtime and can't afford even the slightest network disruption due to a security breach.

For financial institutions, quoting and trading data must be delivered on time and accurately, 100% of the time. And in healthcare, military and first responder organizations, even a minor disruption can literally cost lives.

These enterprises also face regulatory and ethical requirements to protect confidential information and secure infrastructure against compromise.

Keeping networks secure and 100% available requires comprehensive observability and security solutions. Reliable and accurate packet data is essential. Packet delivery, capture and analytics must operate concurrently, at line speed, across on-premises and hybrid, multi-cloud environments.

Put simply: Packet data is foundational for a network observability solution. Every packet could contain information essential to stopping an attack.

Packets are the single source of truth on the network. A bad actor can delete evidence from servers or desktops but not from network traffic. And a single infected packet can be the vector for attack—that's why failing to inspect even a single packet matters. Security defense needs to find that one infected packet and act on it

Why capturing every packet matters

More than 80 years ago, aviation was dangerous business. Development of the flight recorder, known colloquially as the "black box," was a big step to making flight safer. Flight recorders create detailed records of cockpit activity and aircraft instrumentation for analysis after a disaster. The first flight recorder was deployed in 1939, and since then, the data from those devices help protect against disasters recurring.

The networking industry needs the equivalent of a flight recorder—a black box that continuously runs lossless packet-data capture in a hybrid-cloud infrastructure and uses this data to investigate every incident to protect against repetition.

Capturing every network packet in real-time is essential to fulfilling the range of network security responsibilities:

Detecting unauthorized activity. Real-time packet capture permits immediate detection of suspicious network activities, which can include attempts to access restricted areas, brute force attacks, and other forms of malicious activity.

Forensic analysis. In the event of a security incident, having a complete record of network traffic allows for a thorough forensic analysis. This can help in understanding how a breach occurred, what data was accessed, and how similar incidents can be prevented in the future.

Compliance and legal requirements. Many industries have regulatory requirements around data security and may require real-time packet capture to ensure compliance. Additionally, having a record of all network traffic can be useful in legal situations where network activity data is required.

Performance Monitoring. By monitoring network traffic in real-time, organizations can monitor network performance and ensure that the network is operating efficiently. This can also help identify any unusual traffic patterns that might indicate a problem.

Threat Hunting. Proactively hunting for threats is an essential part of modern network security. Real-time packet capture enables security teams to sift through network traffic to identify patterns associated with malicious activity before a full-blown attack occurs.

Incident Response. In the case of a security incident, real-time data is crucial for a timely and effective incident response, enabling the incident response team to understand the scope of the incident and take necessary measures to mitigate the damage.

Mitigating ongoing attacks. Real-time data allows quicker mitigation strategies to be employed against ongoing attacks, blocking malicious IP addresses, adjusting firewall rules and taking other necessary steps to halt the attack and minimize damage.

By losslessly capturing packet data in real-time, organizations are better placed to maintain a strong security posture, comply with legal and regulatory requirements, and ensure their networks' overall integrity and performance.

Anywhere and anytime

Network analytics tools must satisfy multiple challenging requirements to enable network security. Analytics tools must:

- Capture and track packets sourced from all environments and store them locally: On-premises, virtualized, from co-location facilities, and multi-cloud sources.
- Perform lossless packet capture at data rates of 100Gbps+
- Operate without agents on servers or in applications.
- Always be available.
- Easily integrate with other components of the security stack.

Each of these packet sources can illuminate a potential source of disruption. Together, they enable comprehensive observability that solves growing complexity and decreasing reliability.

cPacket is the one solution that meets those needs

cPacket cVu packet broker and cStor packet capture appliance, operating in conjunction with the cClear dashboard for analytics and management, comprise the one solution that can affordably deliver on enterprise observability requirements.

The cVu packet broker is best-in-class—the only packet broker that operates fully featured, concurrently, at full line speed on every port. It reliably feeds packets to security tools, with Smart Analytics at wire speed up to 100Gbps and 100% packet accountability. That makes cVu the industry-leading packet broker under load.

cVu processes every bit of every packet for intelligent brokering, including deduplication, truncation, header stripping and other analytics requirements.

It efficiently brokers pre-processed packets to intended tools, including network detection and response (NDR), intrusion detection systems (IDS) and security information and event management (SIEM) to maximize utilization.

Packets are sourced from all environments: On-prem, virtualized, multi-cloud and hybrid cloud.

cVu's performance is enabled by a unique distributed architecture, cPacket's proprietary software algorithms, and processing provided by FPGAs and ASICs on every port.

Both the packet broker and cStor packet capture appliances are agentless. Network management teams don't need to install specialized agent software to meet security requirements, enabling intelligent alerting and reporting to ensure the continuous smooth operation of security tools. As part of the agentless architecture, cPacket partners with leading cloud service providers.

Market-leading total cost of ownership (TCO)

cPacket slashes the cost of securing your network in several ways:

cPacket reduces the number of security tools required, by efficiently delivering only the relevant packets to the tools. cPacket's packet broker and capture appliances offload pre-processing that security tools typically perform, so fewer tools are needed. cPacket's tools liberate security tools to do their critical jobs.

cPacket data broker can be set to send security tools only the packets those tools need. cPacket can send just the headers, decrypted content, tagged content, and custom reporting on custom APIs—all at line rate performance.

Other factors leading to cost savings:

- cPacket's list prices are competitive with other products—but cPacket does more.
- cPacket provides the only solutions with every port fully enabled with every feature—no incremental licensing or hardware required to unlock additional capabilities. You don't get surprises down the line; when you need change, every feature is available to you.
- Using cPacket's cClear management appliance, cPacket provides single-pane-of-glass administration and reporting for all its devices, reducing management overhead.
- cPacket requires fewer appliances than the competition. While the competition requires 4-6 appliances to achieve 100Gbps analytics, a single cPacket appliance can achieve an even better result. Choosing cPacket reduces infrastructure and maintenance costs. Likewise, cPacket offers the highest storage density in the market, reducing data center space requirements when compared with the competition.
- cPacket is friendly to non-security operations teams. With less rack space per box, fewer boxes, and fewer connections, our solutions present minimal hassles.
- cPacket data brokering is agentless in the cloud and in a virtual environment, which contributes to reduced hassle for operations teams. The security team handles all the maintenance, including software patches and updates, without needing to offload that work to other groups or use other groups' resources.
- That low-hassle profile extends to ongoing operations. For security teams, cPacket is set and forget.

Best-in-class packet capture for forensics

cPacket leads the industry in packet capture for forensics, leading to rapid remediation and evidence collection. We provide the industry's only fully featured line-speed performance for simultaneous capture, query and retrieval, delivering third-party verified lossless packet capture at up to 100Gbps under load. cPacket provides the fastest search and retrieval time for critical, complex, multi-variable queries to quickly pinpoint and retrieve desired packets.

This combination is what's unique about cPacket solutions. Any one of these capabilities can be duplicated by competitors, but only cPacket does it all at the same time—for example, capture at line speed while simultaneously performing advanced searches and retrieval without dropping a single packet.

Packets are seamlessly stored from and in all environments: On-premises, virtualized, multi-cloud and hybrid cloud. We provide the only agentless solution for the cloud, partnering with the leading cloud providers.

cClear provides single-pane-of-glass, simultaneous querying of all cPacket devices, producing comprehensive, intuitive reports and retrievals and delivering immediate, simultaneous, intuitive access to all devices that security teams require.

cPacket enables fast search and retrieval. Competitors capture first, then index, then search, and then retrieve, but we're doing all of that at the same time. cPacket captures and retrieves at full bandwidth, bidirectionally and concurrently. Using real-time analytics, the packet broker can quickly communicate with the firewall to block dangerous traffic before it threatens vital business infrastructure and information resources.

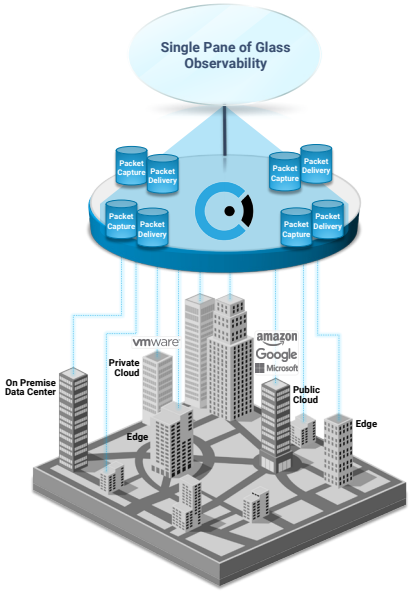
Better together

cPacket provides two main products that work together to provide a comprehensive solution for packet monitoring: cStor for packet capture and cVu for packet brokering.

Each of these products is available as a physical appliance for the data center and as software to run in virtualized/cloud environments.

At the hub is our third product, cClear, which provides management for cStor and cVu devices, such as provisioning and pushing out firmware updates, as well as network packet traffic visualization. cClear's single-pane-of-glass view is an improvement over multiple vendors providing separate management consoles for packet capture and brokering/delivery.

Each module offers standalone functionality, scalable with the addition of new modules. Each module takes maximum advantage of the other modules' specialized features to make them even more effective and efficient in combination. Taken together, the visualization and insights empower security teams to make better decisions to protect the network.



Conclusion

In an era where digital security is paramount, cPacket cVu and cStor provide the best, comprehensive solution for real-time packet capture and analysis, ensuring seamless network operations, especially for high-stake sectors like finance, healthcare, and the military. Find out more about how cPacket solutions can help you.

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 around the world 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 **cpacket.com**.