cpacket NETWORKS

Business Brief

Network Detection and Response Reduces Cyber Risks

Network Visibility Enables Your Security Analysts and Analytics to See and Stop Cyberthreats and Cyberattacks

Business Benefits

- Strengthens Your Security Posture

  Reliably provides network packets to any vendor's XDR or NDR security analytics so your SecOps team or MDR provider can detect and respond to security breaches before they become costly and chaotic

- Helps Eliminate Vulnerabilities

  The agentless, out-of-band, and security hardened hybrid Network Visibility Fabric does not introduce new vulnerabilities into your network or IT infrastructure

- Security Evidence

  Captured-and-stored network packets are evidence for threat hunting, forensic analysis, identifying the attacker, vulnerability testing (by red and blue teams), and complying with regulatory record keeping requirements

cPacket Uniqueness

- Full Network Visibility solution

  Seamless physical and virtualized packet brokering and capturing that losslessly acquire and deliver streamed and stored network packets to security analytics

- Any Network at Any Scale

  Acquires and aggregates packets from as many vantage points and mirroring services as needed from a physical, single-cloud, multi-cloud, or hybrid network

- Unified Fabric

  The entire hybrid network visibility fabric is managed in a single-pane-of-glass

Featured Products

cClear® and cClear®-V physical and virtualized Analytics Engine Appliances

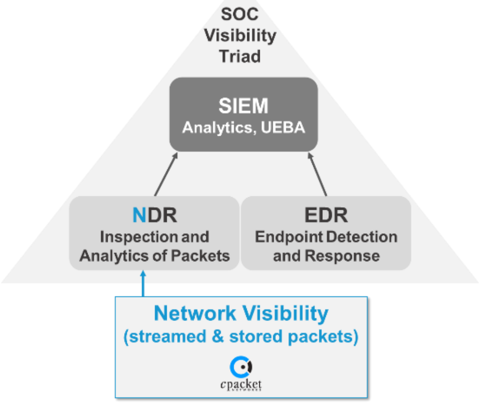
cVu® and cVu®-V physical and virtualized Network Packet Brokers

cStor® and cStor®-V physical and virtualized Packet Capture Appliances

Your SecOps team must defend against increasingly challenging threats using layered security measures that must include *detection and response*.

Extended/Network Detection and Response (XDR/NDR)

XDR/NDR interoperates with SIEM and other security solutions to facilitate a timely and appropriate response. XDR/NDR solutions continuously inspect and analyze network packets in real-time to identify threats, attacks in progress, and what has been compromised. Therefore, the strength of your security posture depends on reliable availability of network packets.

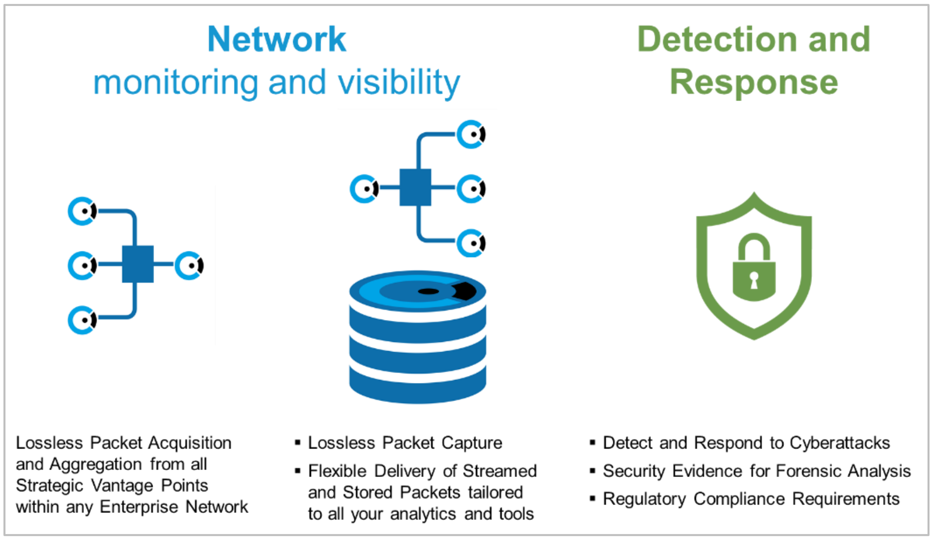


Stored packets are a rich source of security evidence for threat hunting that augments automated detection. Stored network packets provide actionable details that help you respond, recover, and identify vulnerabilities to prevent future occurrences.

Performance Matters, Good Enough is a Vulnerability

Your network visibility must work flawlessly under all conditions to provide visibility into what is in your network and what is happening in your network, especially suspicious Indicators of Compromise that identify threats and active attacks. Network visibility also provides security evidence for threat hunting, forensic analysis, and regulatory compliance.

The following diagram highlights that network packet data is vital and universal for detecting and responding to threats and active attacks. Partial visibility, intermittent visibility, and visibility siloes are vulnerabilities that cybercriminals will exploit. Our network visibility fabric provides consistent access to streamed and stored network packets all the time to eliminate such vulnerabilities.



Lossless Packet Acquisition and Aggregation from all Strategic Vantage Points within any Enterprise Network

- Lossless Packet Capture
- Flexible Delivery of Streamed and Stored Packets tailored to all your analytics and tools

- Detect and Respond to Cyberattacks
- Security Evidence for Forensic Analysis
- Regulatory Compliance Requirements

The cPacket Network Visibility Fabric possesses lossless performance and unified visibility breadth that maximizes threat detection effectiveness and responsiveness to security events. Additional unique capabilities include:

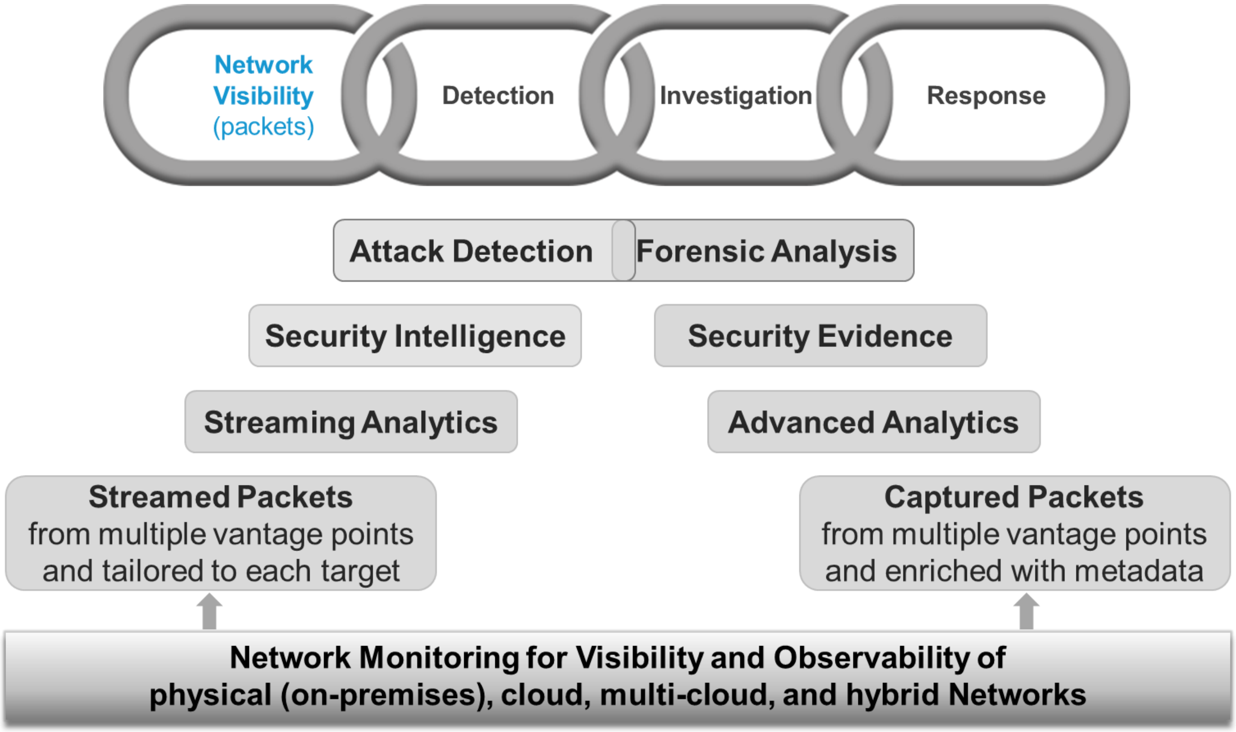
- Not inadvertently introducing new vulnerabilities by being agentless, out-of-band, and security-hardened
- Lossless acquisition of packets providing visibility that is free of blind spots under all operating conditions
- Capturing and storing packets enriched with timestamps and metadata to add context to the security evidence
- Seamless aggregation of packets from all strategic vantage points throughout a distributed physical, cloud, multi-cloud, or hybrid network

Interoperability

Network packets are uniform for specific protocols and encapsulations. Therefore, with few exceptions, most any Network Visibility Fabric, including cPacket's, is fully compatible and interoperable with any vendor's XDR or NDR implementation, or MDR service, that ingests and analyzes network packets. Our solutions interoperate with and cost-effectively extend native packet and traffic services such as mirroring, gateway load balancing, and ingress routing.

Streamed and Stored Network Packets for Automated and Manual Detection & Response

Security Analysts, the SOC, and XDR/NDR solutions continuously analyze network packets acquired, aggregated, and streamed from the cPacket Network Visibility Fabric. Tailoring and managing packets from multiple vantage points requires using cVu® and cVu®-V physical and virtualized Network Packet Brokers, respectively. The cStor® and cStor®-V Packet Capture appliances capture and store packets for evidence that facilitates threat hunting to augment real-time detection with actionable details about breaches so you can respond quickly and appropriately. Advanced analytics applied to stored packets surfaces patterns, trends, and deep insights. The insights, plus forensic analysis, help identify the attacker and the tactics, techniques, and procedures that advanced persistent threats use to penetrate enterprise networks to prevent future occurrences. Capturing packets is optional, though highly recommended because the benefits of accessible and easily queried evidence and having a large dataset for analysis often outweigh the cost.


Network Visibility (packets)
Detection
Investigation
Response
Attack Detection
Forensic Analysis
Security Intelligence
Security Evidence
Streaming Analytics
Advanced Analytics
Streamed Packets from multiple vantage points and tailored to each target
Captured Packets from multiple vantage points and enriched with metadata
Network Monitoring for Visibility and Observability of physical (on-premises), cloud, multi-cloud, and hybrid Networks

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.