cpacket NETWORKS

# Intelligent Observability Platform

Case Study:
## Visibility-Driven Network Detection and Response Strengthens Cyber Risk Resilience

**Government Protects its Distributed Hybrid Infrastructure and Sensitive Data from Cyberattacks**


## Customer

The Department of Defense (DoD) of a large, developed country uses Network Detection and Response (NDR) to mitigate cyber risks from recurring cyberattacks, many from state-sponsored attackers. Their IT infrastructure and network connect roughly 400 sites and consist of physical and virtualized resources that host numerous workloads and sensitive data.

## Challenge

Preventing attacks by state-sponsored actors across the IT infrastructure and its perimeter is a matter of national security. It is necessary to secure access to the country's DoD IT resources and sites from all north-south connections by meeting the following requirements:

- Losslessly delivering network-centric visibility to security analysts in the SOC and delivering network packet data to the security tools
- Seamless scalability across physical and virtual infrastructure at many sites
- Acquire and capture-and-store packets at data rates up to 100Gbps
- Easily add vantage points to monitor to protect all sites and links
- Interoperability with their security solutions (IDS, NDR, SIEM, etc.)
- A full stack network visibility solution ideally from one vendor consisting of acquisition, delivery, capture-to-disk, analytics, and an open API

## Solution

The DoD began its effort to strengthen its cybersecurity posture by evaluating network monitoring solutions for visibility from network packet data that is a vital source of immutable evidentiary truth of what happened and is happening within IT infrastructure. cPacket Networks was the only vendor with a visibility solution that met their requirements and passed their rigorous performance tests. Their lossless packet brokering and capturing-to-disk at the 100Gbps speed outperformed competing solutions.

> Security Analysts and Tools Are Only as Good as the Visibility and Data They Receive

For threat hunting, the Security Operations (SecOps) team uses the Corelight Open-NDR Platform that includes an enhanced version of the "Zeek" Network Security Monitor. Zeek transforms network packet data into rich security logs that security analysts use to hunt for and neutralize cyberthreats proactively. Zeek has a large user base, so other widely used complementary security solutions commonly ingest its security logs.

The DoD's Intrusion Detection System (IDS) is configured to send event tags to the packet capture devices using the cPacket API. The stored packet data also is enriched with timestamps. The devices automatically index the data by tags and timestamps to make it easy for security analysts and tools to recall specific data for analysis and easily replay specific traffic sequences.

## Benefits

- **Minimize Vulnerability**
  NDR is a vital component of a cyber defense arsenal to prevent all types of cyberattacks and their consequences.
- **Effective Threat Hunting**
  Proactively search for malicious activity across a wide range of tactics such as command and control, lateral movement, and data exfiltration in physical and/or virtualized IT infrastructure.
- **Uncompromised Visibility**
  The cPacket solution precludes blind spots by losslessly acquiring, delivering, and storing packet data from virtual and physical networks operating at up to 100Gbps.
- **Full Stack Visibility, One Vendor**
  The IT team benefits from a full stack visibility solution for hybrid infrastructure that includes network packet data acquisition, storage, and analytics with visualizations

*"We evaluated several network visibility solutions for NDR. Only one vendor, cPacket Networks, offers a full stack solution that met all of our requirements including seamlessly monitoring hybrid infrastructure with dependability."*

- Director of the Security Operations Center

Bad actors and malware in the IT infrastructure leave network artifacts and clues about what happened and is happening that are detectable by observing and analyzing real-time and historical network traffic. Stored network packet data that is indexed by events and time makes it easy to review the traffic and behavior to trace lateral movement that occurred throughout the entirety of the attack to gain a step-by-step understanding of the malicious activity as it unfolded. This granular detail gives the SecOps team a powerful tool for threat detection and threat hunting that provides a thorough understanding of the attack vectors, implantation methods, execution methods, data exfiltration, and the scope and impact of attacks that penetrated the IT infrastructure.

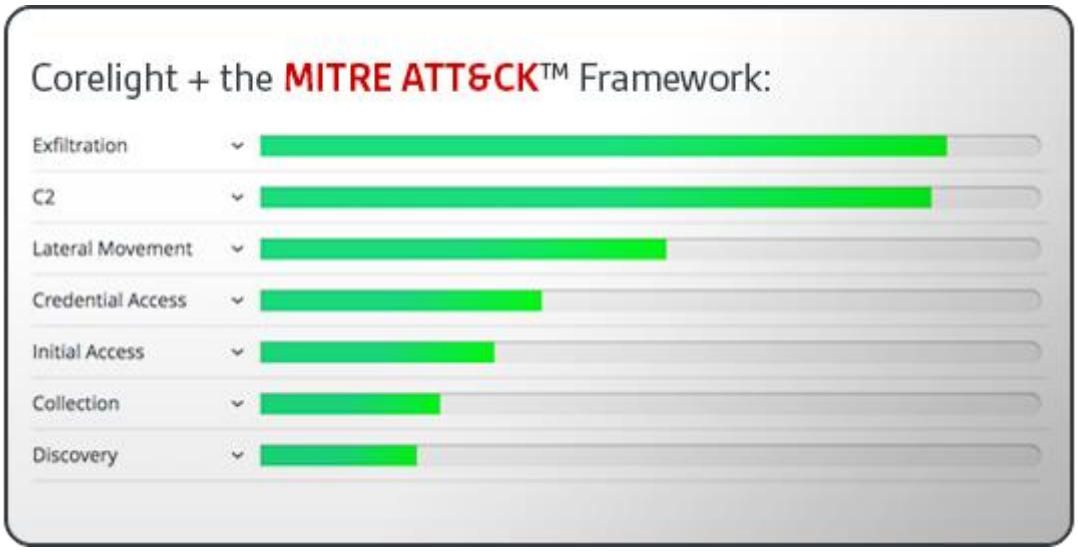


Figure 1: Adversary tactics and techniques that are detectable using the Corelight Open NDR Platform

The Network Operations (NetOps) and SecOps teams collaboratively designed the NDR solution, using Corelight sensors with Zeek preinstalled and the specific components of the cPacket Intelligent Observability Platform listed below. Except for cPacket cVu-V® agentless virtualized packet broker modules, all other components are out-of-band and therefore did not require downtime and do not disrupt, impact, or expose the core network. The entire implementation was straightforward. The NetOps team configured the network packet brokers to stream network packets to the NDR solution, other cybersecurity solutions, and the packet capture-to-disk appliances. A single instance of the cPacket cClear® Analytics Engine provides customizable dashboards with holistic KPIs plus the user interface to configure and manage the network monitoring fabric.

The following network monitoring fabric components deployed provide both real-time and captured-and-stored historical network packet data to the NDR solution:

**cClear®/cClear-V Analytics Engine** – Presents the user interfaces in a single-pane-of-glass for provisioning, managing, and visualizing traffic, KPIs, and other analytics results. A single instance provides customizable interactive dashboards that give the entire IT team actionable network intelligence that consists of real-time network status, KPIs, baselines, anomalies, alerts, and other analytics results.

**cVu®/cVu-V Network Packet Broker+** –cVu packet brokers acquire network packets from TAPs connected to ingress ports. cVu-V virtualized packet brokers are inserted into virtual infrastructure subnets. Packet replication, processing (e.g., filtering, deduplication, slicing), and data rate adjusting are configured so that each target receives data tailored to its intake requirements. The packet brokers also observe and collect metrics, KPIs, and microburst details for use by the cClear device for visualization in dashboards. Virtualized packet brokers acquire network packets from the virtualized infrastructure and delivered them to specific targets.

**cStor®/cStor-V® Packet Capture-to-Disk** – Physical and virtualized appliances capture packets and enrich them with timestamp and event tags (received from the DoD's IDS via API calls). Data is indexed for fast querying and is available to security analysts and the tools they use.

## Results

Built using cPacket's high-fidelity network visibility solution that makes their Zeek-based NDR and other security tools maximally effective, the SecOps team leverages broad and accurate detection of various attack vectors and types. The SecOps team leverages its effective threat hunting, detection, neutralization tools for incident response agility. The result is a resilient and robust cybersecurity posture that greatly helps guard against attacks intended to compromise or cripple the military and the entire government, including the public services it provides.

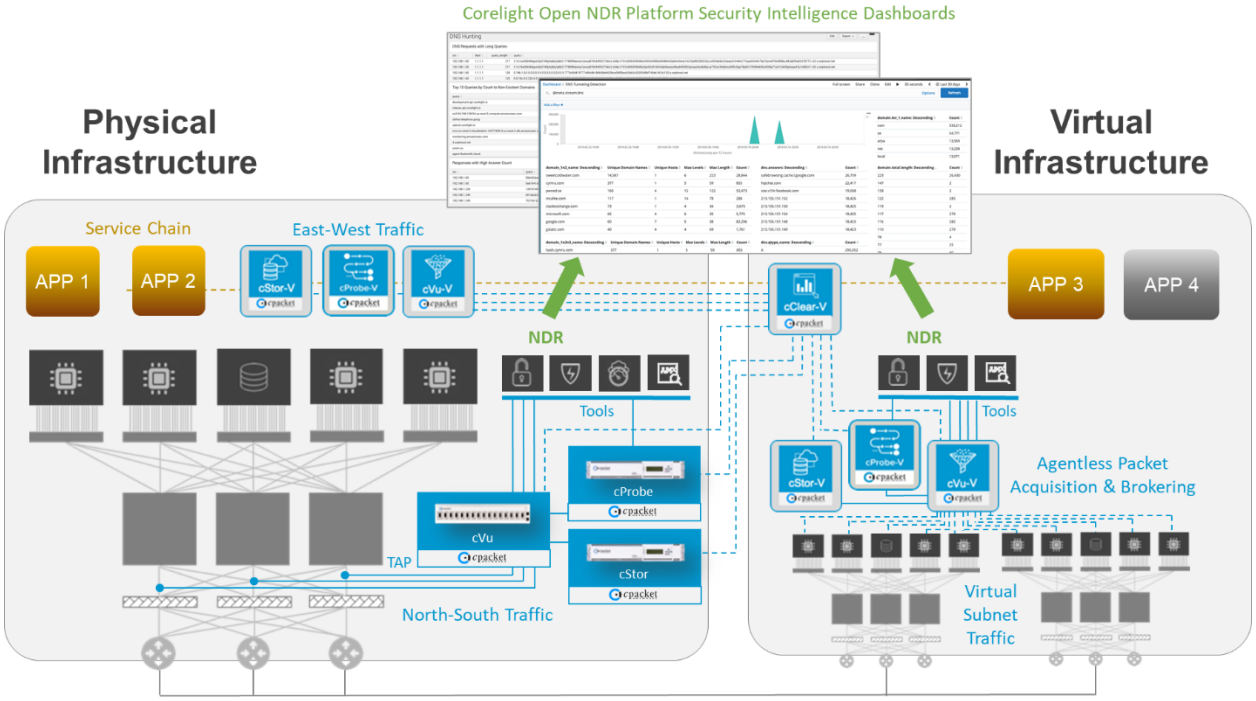


Figure 2: Visibility-driven Network Detection and Response architecture

The IT team also realized the following benefits:

- The mostly out-of-band deployment was quick and without disruption to their core network and IT workloads
- The cPacket and Corelight platforms work together naturally, so integration of the NDR solution was straightforward and problem-free, and ongoing management and total cost of ownership are low
- Other security solutions including SIEM tools and SOAR also have access to real-time and stored packet data
- Stored network packet data is always readily available to the SecOps team for use as forensic evidence and for complying with regulatory report requests
- The NetOps team has continuous real-time visibility that enables them to assist the AppOps and other IT teams to resolve performance problems

Learn more about how the cPacket Intelligent Observability Platform provides trustworthy delivery of visibility and data for NDR solutions at: https://www.cpacket.com/solutions/network-detection-response/

### 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 provides the deep network visibility required for today's complex IT environments. cPacket enables 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 www.cpacket.com.