Case Study:

Fortune 100 Financial Services Company Benefits from Cloud Visibility

Replicated, Streamed, and Stored Network Packets are Vital for Securing Public Cloud and Hybrid Infrastructure

Benefits

- **Network Packet Replication**
  Straightforward and cost-effective way to deliver packets from one source to multiple destinations at scale
- **Network Packet Acquisition from custom Vantage Points**
  Gain Network Visibility from custom strategic vantage points for thorough security monitoring and intelligence
- **Interoperability with Third-Party Security Solutions**
  The universality of network packets and the open API enables interoperability with XDR/NDR, SIEM, and other security solutions
- **Scalability**
  Elastically and persistently scales across physical, single-cloud, multi-cloud, and hybrid networks.

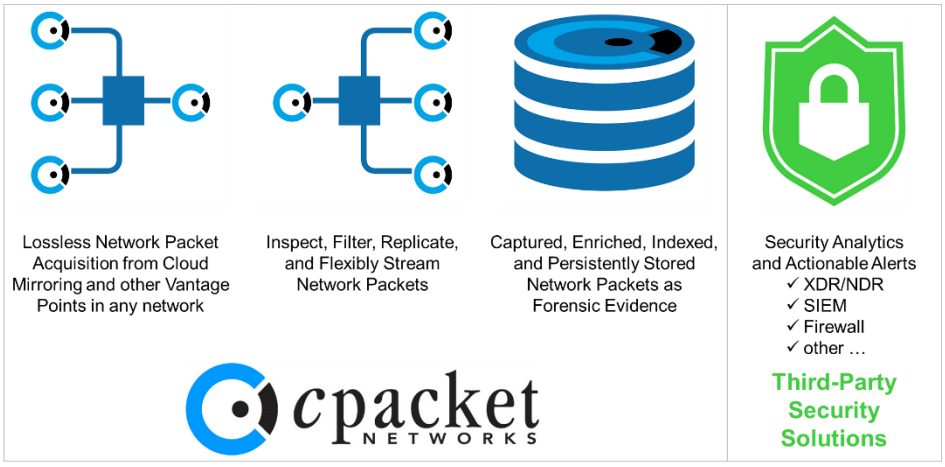
"We needed to get network packets from point sources to multiple destinations in our new cloud environment just like in our self-managed physical data centers. We also needed an easily managed and cost-effective solution. Fortunately, our long-term Network Visibility vendor, cPacket Networks, has the ideal solution to extend our visibility into the cloud."

- Global IT Security Operations Leader

Customer

The organization is a global financial services provider and one of the largest banks in the world, with branch offices in many countries. Services include consumer, commercial, corporate, and investment banking. Those services are available online, resulting in over 50 million transactions daily. The organization's IT operations are critical to revenue, profit margins, growth, and the ability to provide financial assistance to customers who rely on continuous availability, protection of their private data, and fraud prevention., Therefore, it is critical to minimize the risk of detrimental consequences to itself and its customers from unplanned service disruptions, data and identity theft, ransomware extortion, and other cybercrimes.

The organization sought to consolidate and reduce the number of self-managed data centers using public cloud infrastructure to supplement its existing data centers, resulting in a globally distributed hybrid data center. The consolidation effort necessitated migrating approximately two thousand applications to run in public cloud infrastructure. Data necessary for the applications to run also had to be migrated. Strong security measures had to be firmly in place before any migration could occur.



Challenges

Maintaining a strong security posture is an ongoing challenge because of the unique attributes of elastic cloud infrastructure and how the virtualized network handles DNS resolution, east-west traffic, and north-south traffic. A related challenge is how network packets could be acquired from strategic vantage points within their public cloud infrastructure, stored, and become available to security analysts and tools at different locations. This requirement creates cost and administration challenges because the native mirroring service does not replicate packets, and each mirroring session has a cost. A single holistic view that seamlessly spans their hybrid infrastructure is necessary to ensure a strong security posture. Furthermore, managing many mirroring sessions becomes unwieldy and difficult to manage at scale.

Troubleshooting problems in complex hybrid IT environments is always a challenge. The organization needed to extend its network visibility and observability to include public cloud infrastructure to assure optimal performance of their new hybrid IT infrastructure.

Objectives

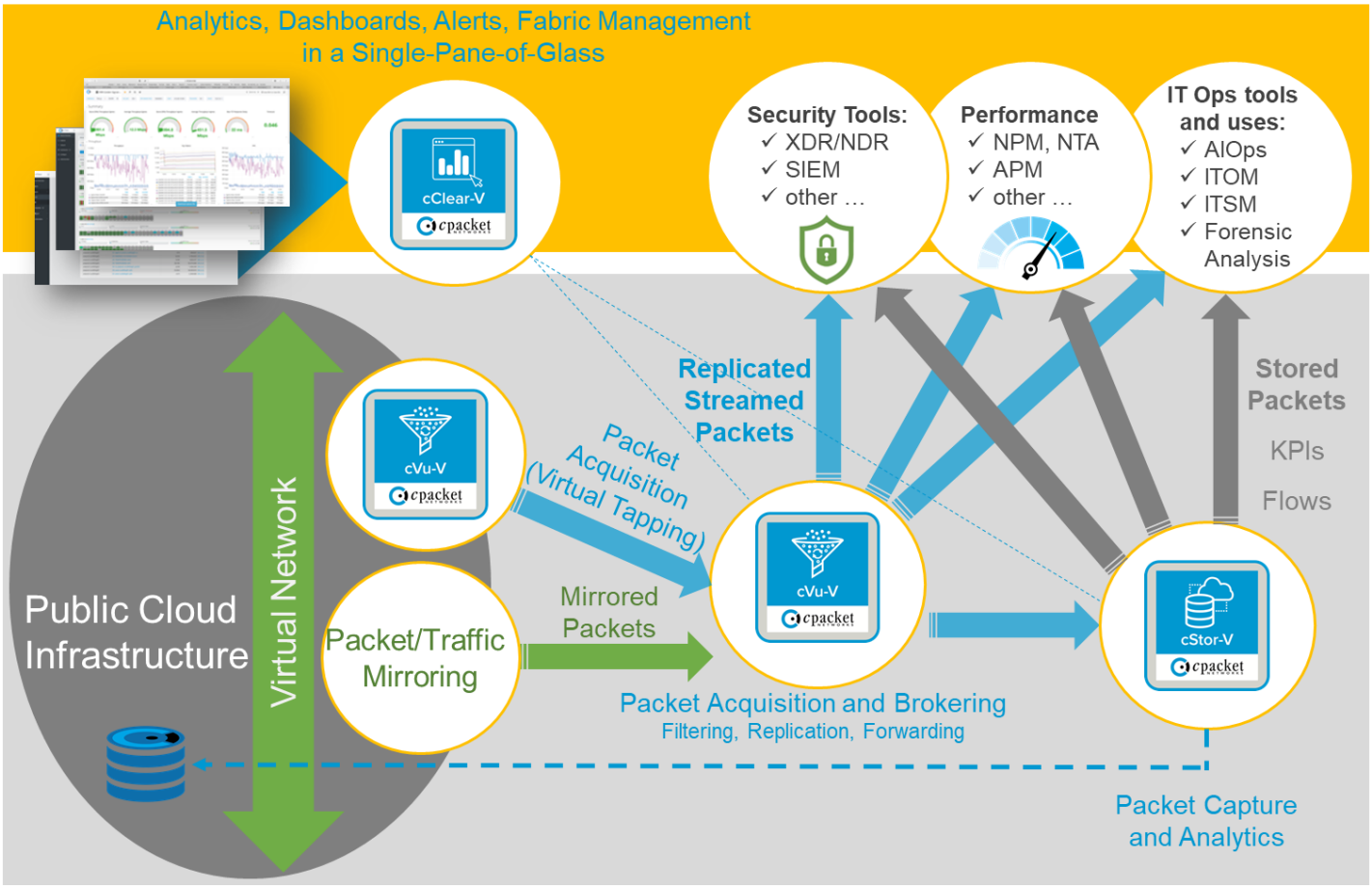
The primary objective is to ensure that all business units can secure data and workloads in the new hybrid IT environment before and after migration without using agents that increase attack surface area and hence cyber risks.

Additional objectives are to contain administration effort and variable cloud costs. With its many challenges and tasks, the organization's IT team expressly sought a visibility fabric that is straightforward to instrument and maintain, to have a low administrative burden. Incorporating public cloud infrastructure into its data center environment introduced consumption-based costs, including packet mirroring, that the organization needs to monitor and contain.

Solution

The organization deployed cPacket Networks' Intelligent Observability Platform in their self-managed data centers several years before their initiative to consolidate data centers and include public cloud infrastructure in their IT environment. Their positive experiences drove them to start by evaluating the cPacket cCloud™ Visibility Suite.

The IT team executed a combined security-first and cloud-smart plan – deploying a layered security strategy with multiple tools from several vendors, including Network Detection and Response (NDR), SIEM, Firewalling, and other security solutions before data and workloads were migrated. The foundation of their solution included using the cVu-V Virtualized Network Packet Broker for cost-effective acquisition, replication, and delivery of network packets to their SOC, multiple dashboards, security tools, and performance management tools.



high-level architecture that provides network-centric visibility and observability into public cloud infrastructure

The unique combination of network packet acquisition and brokering performed by the cVu-V Virtualized Network Packet Broker enabled acquiring, replicating, and forwarding network packet streams to security tools provide visibility and data that elastically scales with growth across the hybrid environment. Network packets and traffic are *tapped* from native vantage points accessible from the Cloud Service Provider's mirroring service and custom vantage points using the packet acquisition function (virtual tapping). Packets are filtered to match the needs of the target destinations then replicated and delivered. Among the destinations are instances of the cStor-V Virtualized Packet Capture appliances that store and analyze network packets. Analytics applied to the streamed and stored packets provide actionable insights to security analysts, XDR/NDR and SIEM security analytics, and other security tools. The combination of streamed packets, stored packets, and analytics results greatly helps the entire IT team to assure security, performance, and end-user experiences.

The solution provides visibility and data across their distributed hybrid environment with these benefits:

- Visibility and network packets from custom vantage points that are seamlessly aggregated with visibility and packets from native mirroring for complete cloud visibility
- Packet replication contains the cost of delivering packets to multiple targets
- A single holistic view that is accessible to security analysts working at different locations and the security tools they use that are hosted at various sites
- Unified management that simplifies administration of the visibility fabric that scales elastically and persistently

The solution used the following self-hosted virtual appliances that seamlessly interoperate with the organization's existing physical visibility fabric components to provide holistic visibility and network packets throughout their distributed hybrid IT network:

cClear®-V Virtualized Analytics Engine and Administration Console – Presents user interfaces for provisioning, fabric management, and data visualization in predefined customizable dashboards, all in a single-pane-of-glass. A single instance of this virtual appliance displays interactive dashboards that give the entire IT team observability with actionable network intelligence that consists of real-time network health, status, KPIs, baselines, anomalies, and other analytics results.

cCVu®-V Virtualized Network Packet Broker – The multi-function virtualized network packet brokering augments and extends cloud-native mirroring by acquiring network packets from native and custom vantage points. It filters, replicates, and delivers packet streams to multiple locations, tailoring them to match each target's intake requirements. The packet brokers also collect metrics and KPIs used by the cClear-V appliance for visualization using the solution's dashboards. Packets and KPIs are also externally accessible via an open API.

cStor®-V Virtualized Packet Capture to Storage – Provides stored network packet data and analytics for threat hunting, forensic analysis, and regulatory requirements. Forensic analysis and troubleshooting leverage comprehensive querying and searching and the ability to use stored packet data to replay network traffic before, during, and after an event to understand what happened. The high velocity and volume of network packets are captured, enriched with metadata, indexed, stored, and analyzed. Specific packet data can be queried, recalled, replayed, and analyzed by time and tags; data is tagged using an open API (e.g., to associate packets to a specific security event). Packets, KPIs, and analytics results are also externally accessible via an open API. Packets can also be grouped and exported as PCAP files.

Results

The organization strengthened and extended its security posture to include public cloud infrastructure before migrating data and workloads to the cloud. Their InfoSec and SecOps teams, collaboratively with the entire IT team, implemented security measures in their public cloud infrastructure that match their self-managed physical data centers.

The organization continues to realize the following benefits:

- A strong infrastructure-wide security posture driven by reliable continuous network packets delivered to several security analysts, analytics, and related tools
- Packet mirroring cost containment versus a more than fivefold cost-bloat (if they had to use several parallel mirroring sessions, multiplied by thousands of nodes)
- Elastic and persistent scalability to address intermittent and temporary growth
- Democratized availability of streamed and stored packets, network traffic KPIs, and other network analytics results that business units could use to secure their specific data, workloads, and VPC environments
- Straightforward and seamless administration of the hybrid visibility fabric
- Leverage the visibility and streamed and stored network packet data for performance management and regulatory compliance uses

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.