Case Study:

Global High-Frequency Trading Exchange and Market Data Provider

Reliable Network Monitoring to Protect Against Cyberattacks, Maximize Performance, and Gain Competitive Advantage

Customer

The customer is a Fortune 500 provider of financial marketplace infrastructure, market data services, and related technology solutions. It operates financial trading exchanges and clearing houses globally and provides financial data and listing services. The organization owns and operates exchanges for financial and commodity markets and operates several regulated exchanges and marketplaces. The high-frequency trade (HFT) transactions it facilitates and the financial market data it provides meet the stringent speed and low latency requirements. Timeliness, accuracy, completeness, and security are paramount because its end users' financial gains and risks are impacted by the quality and consistency of its services.

Challenges

For the customer, providing market data and facilitating financial trades rely on a global network at the core of these complementary services (as generalized and shown in Figure 1). Ensuring high-resolution and accurate network monitoring for the services it provides ensures the success of the organization and its end-users. The breadth of the data services, organization size, and its global network drove the following IT objectives and challenges:

- Ensure consistent high-frequency trading and market data without gaps
- Manage network usage to maximize experiences and revenue
- Capture precise data for regulatory compliance
- Strengthen security to prevent cyberattacks
- Maximize the infrastructure return on investment (ROI)
- Leverage familiar UI and workloads across on-premises and cloud

Performance and Experience Monitoring

Time is money, and fractions of a second matter when placing high-stakes and/or high-risk trades that rely on fast trade execution and timely market data. Timeliness is critical because investors and investment managers seek to maximize gains, even from small market price movements. Tick-to-trade latency is a crucial metric that measures the time between receiving a price movement in the market (a "tick") that could be acted on as an opportunity to execute a trade for financial gain (a "trade"). Therefore the "tick-to-trade" time to respond to market data determines success. Market exchanges must operate secure networks at high data rates and the lowest possible latency and jitter to offer the best possible tick-to-trade service. The networks also must have sufficient headroom to avert data loss that can be caused when capacity overruns occur due to bursts/microbursts. A single microburst can cause packets to be dropped and can cause missed trade order placements, missed trade confirmations, and gaps in market data, any of which will cause financial losses when pursuing hedging and other trading strategies.

Benefits

- **High-Precision Monitoring**
  Lossless brokering, timestamping, counting, and characterization of traffic, latency, and jitter with millisecond precision
- **Profiling Microbursts with "cBurst"**
  Microburst profiling with sub-millisecond precision concurrently on all ports helps identify capacity shortcomings
- **Detecting Market Data Gaps**
  Detect gaps by counting network packets and measuring latency to assure quality information for trading decisions
- **Strengthen Security Posture**
  Provide streamed and stored network packets to security analysts and their tools for detection, response, and forensic analysis
- **Maximize Performance & ROI**
  Maximize hybrid workload performance and optimize 100Gbps WAN link capacity using network visibility, KPIs, and cBurst
- **Ensuring Regulatory Compliance**
  Capture and store data for regulatory record keeping and reporting

In this case, market information is collected and distributed in streams that, along with other transactions, must traverse internal and wide-area networks (WAN). A custom UDP-type protocol is used for some transactions to minimize overhead and hence maximize transmission speed. Parallel feeds provide scale to accommodate growth. Precise monitoring that includes timestamping activity with nanosecond precision is necessary to assure and validate that all feeds provide the exact same "fairness" delivery times to all end-users so that no recipient has an unfair advantage.

High-resolution monitoring with microburst profiling also provides the customer with critical performance metrics such as steady-state traffic, roundtrip timing, bursts/microbursts, latency, jitter, and capacity trends for data streams and trade transactions. Visibility of such metrics is essential for Network Operations (NetOps) teams to effectively balance performance, cost and maximize the ROI of the infrastructure. Monitoring network utilization over the WAN when approaching their capacity thresholds is also critical. Knowing the causes and patterns of bursts that are often difficult to detect empowers the customer's NetOps team to make the appropriate decisions to rebalance loads if possible and when to add new WAN links because adding high-speed WAN links are costly to provision and take several months to put into service.

Regulatory oversight and compliance are common for financial services. So, it is also essential to leverage monitoring to reliably capture and store data for regulatory record keeping and reporting with the precision necessary to confirm fairness so that no end-user has a timing advantage due to faster receipt of market data feed and executing trades.

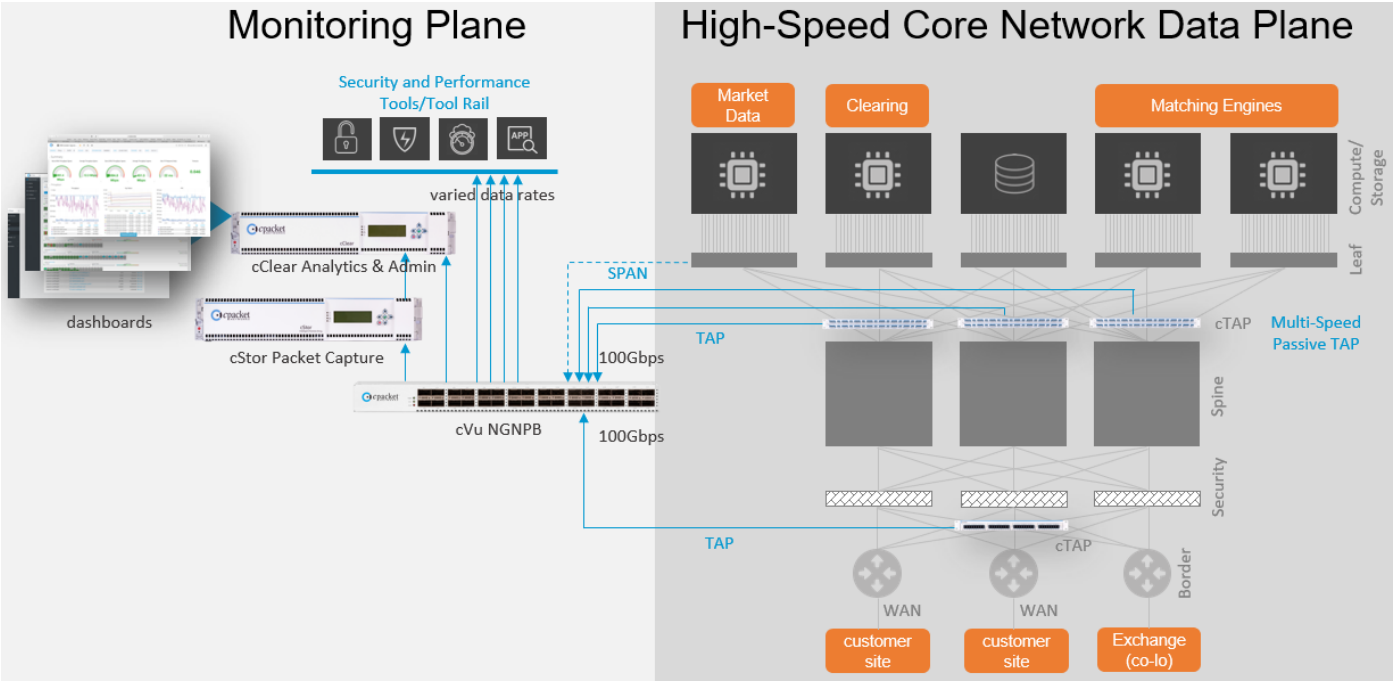

Figure 1: simplified architecture with network monitoring for high-frequency trading and market data

Cybersecurity

Strong cybersecurity is necessary, especially for financial trading services organizations that are attractive targets for cybercriminals. Monitoring provides visibility to the customer Security Operations (SecOps) team and vital data the tools they use to prevent cyberattacks and fraud effectively. To seamlessly protect against all types of cyberattacks across on-premises and cloud environments, the customer's SecOps team established the following requirements:

- Losslessly broker network packets to security and performance tools at 100Gbbps speed
- Capture every packet that arrives at and passes through the firewalls and retain them for several months
- Have visibility of activity occurring outside the firewall and see all traffic arriving at the perimeter to detect potential and actual denial-of-service (DoS) attacks quickly
- Analyze traffic outside and inside the firewall perimeter
- View traffic flows to identify flows of interest (i.e., suspicious behavior)
- Research issues by correlating flows of interest with packets and analyzing the 90-day packet history
- Know who is attempting to access the network, build profiles, and catalog connection attempts
- Use Kafka to stream packet data to an elastic repository for subsequent analysis

Solution

The customer's network visibility and business objectives were met using the cPacket Networks products listed below. The suite of products can decode their custom UDP-type transmission protocol, accurately timestamp packet transmissions with nanosecond resolution, store the packets, and provide analytics for performance, utilization, and market gap detection. cPacket's Visibility Fabric was chosen without a competitive bid because it is the only monitoring fabric that met the requirements listed below:

- Supports Network Operations' and Security Operations' requirements
- Timestamp and characterize traffic with millisecond precision for networks and WAN links operating at data rates from 10Gbps to 100Gbps
- Microburst profiling with millisecond resolution for WAN capacity planning (using the "cBurst" feature; refer to Figure *2* to see results)
- Link bandwidth monitoring with millisecond resolution characterization of latency and jitter
- Analytics for market data gap detection for trade executions
- Sustained capture-to-disk of network packet data at 40Gbps for up to 2 petabytes and the ability to stream packet data exported from the storage appliances using Kafka
- Adaptability to work with the customer's proprietary UDP-type data transmission protocol and implement functionality for market data gap detection
- Seamless monitoring that spans their on-premises and cloud hybrid environment

The customer's NetOps team initially began working with cPacket Networks to improve their ability to monitor and optimize the performance of their HFT and market data services. The footprint of the monitoring fabric and its uses expanded over the years to also include cybersecurity strengthening. The following products are deployed and used for NetOps and SecOps:

cPacket cVu® Series Network Packet Broker+ with distributed hardware-accelerated processing on all input and output ports reliably provides precise traffic metrics. It delivers the right data to the right personnel and the security and performance tools they use, without ever dropping packets, at data rates up to 100Gbps. The hardware-based acceleration includes a custom-developed application-specific integrated circuit (ASIC) and a field programmable gate array (FPGA). The programmability of the FPGA was leveraged to add real-time processing functions that operate at wire data rates to decode the customer's data transmission protocol and validate that market data streams are received reliably by verifying that packets are not missing, out of order, or duplicated. If packets are duplicates, the duplicates are removed.

cPacket cStor® Packet Capture Appliances capture network traffic at sustained rates of up to 60Gbps (and bursts at up to 100Gbps) to persistent storage that meets the customer's retention requirement. Historical data is security and performance evidence used for forensic analysis to strengthen the security posture, validate trade execution by matching orders with confirmations, and support regulatory record-keeping and reporting. Data can be queried and retrieved using the onboard browser-based UI, API, and streamed via Kafka.

cPacket cClear® Analytics Engine presents actionable network intelligence via out-of-the-box and custom dashboards that present traffic data, KPIs, and microburst details from data retrieved from the packet broker and packet capture appliances. It also includes a unified administration console for orchestrating and managing the Visibility Fabric and its configuration settings and workflows. The dashboards and administration console are viewed in a single-pane-of-glass using a browser.

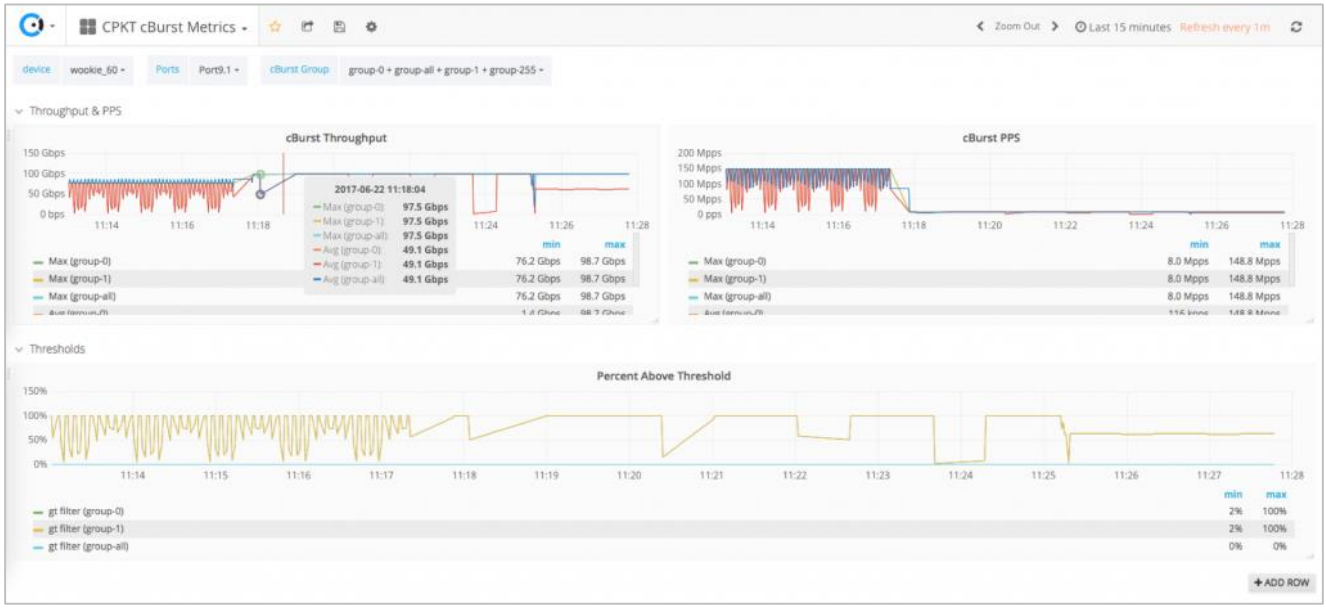

Figure 2: microburst visualization with high-resolution details using the cBurst feature

Results

The customer's NetOps team readily installed the cPacket monitoring fabric components listed above without disrupting their core network, then immediately gained the benefits listed below. Soon after, the SecOps initiated a program to increase all traffic visibility attempting to gain access to its network (per the cybersecurity requirements listed above). The organization's lead network architect recommended that the SecOps team evaluate the monitoring fabric already in place. After a favorable evaluation, the SecOps team embraced it and began expanding the footprint to strengthen the cybersecurity posture. The customer also values the seamless monitoring and resultant visibility across on-premises, cloud, and hybrid environments as they look to expand their infrastructure using public cloud offerings.

In addition to gaining reliable 24x365 network monitoring, the customer gained a trusted advisor, technological agility, and competitive advantages by thoroughly collaborating with cPacket Networks. Over several years, the collaborative relationship expanded, as did features and functionality that increased the breadth and depth of their visibility. The customer used analytics that streamlined their NetOps by eliminating other monitoring and analysis tools, which filled gaps in their network intelligence and strengthened their security posture.

After several years of success and collaboration the NetOps team recommended cPacket monitoring fabric to their SecOps team for their cybersecurity strengthening efforts. The SecOps team quickly recognized it met their requirements and moved forward. Since then, the organization has continuously expanded the monitoring footprint and the ways it benefits from trustworthy Network Visibility.

Some of the strategically important security and performance benefits the customer realizes include:

1) Strong security posture that leverages real-time plus historical data from outside and inside their firewall perimeter.
2) Maximized end-user experiences and customer satisfaction by being able to cost-effectively measure and hence minimize latencies and jitter at scale. Subscribers to their services experienced reliable and timely market data and order execution that gave them confidence in accuracy and fairness. This was made possible because packets were not dropped and were delivered in the correct order.
3) Maximized ROI of their WAN links by balancing existing capacity by using analytics to know the links that are carrying the most traffic and are most often subjected to microbursts. Costly new WAN link and other infrastructure upgrade costs are only incurred when necessary.
4) Increased end-user revenue by using analytics to know when to sell additional services to end-users who were reaching their contractually agreed-to bandwidth and capacity limits.
5) The ability to query data and generate compliance reports to regulatory authorities with the granularity and accuracy required to confirm that no stream or customer had an unfair timing advantage for receiving market data and executing trades.

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.