REPORT REPRINT

cPacket bucks the big-iron trend with pervasive distributed network analysis

CHRISTIAN RENAUD

19 FEB 2016

The company's distributed analysis capabilities, paired with centralized policy management and overlay-protocol-friendly correlation, are well suited for forthcoming Internet of Things projects.

451 Research®

Distributed network visibility and monitoring firm cPacket continues to evolve its traffic-visibility offering as network and application performance management (NPM/APM) increasingly overlap with traditional network-monitoring tools. The company's distributed analysis capabilities, paired with centralized policy management and overlay-protocol-friendly correlation, are well suited for forthcoming Internet of Things projects.

THE 451 TAKE

The NPM, APM and network-visibility sectors are rapidly adapting to an increasingly virtualized and cloudy network, as well as the early effects of the Internet of Things. With its distributed approach to analysis for network data that can be summarized (such as IoT time-series data), cPacket conserves valuable bandwidth compared with traditional SPAN/RSPAN backhaul approaches. Its scale-out approach to application and network performance monitoring should result in a linear cost basis to customers when compared with the step function of new chassis purchases of competing approaches. Continuing to iterate on cPacket's proprietary ASIC technology, although beneficial for distributed analysis, will likely continue to be a cash drain on the small company.

CONTEXT

CPacket was founded in 2006, and currently has more than 30 employees between its headquarters in Mountain View, California, and Portland, Oregon, as well as additional sales offices in Europe. The company has raised three rounds of funding (the last coming in 2011), bringing its total raised to $15m. While, as a private company, it does not disclose revenue, the headcount and burn rate (and no funding since 2011) indicate that it has revenue in the $20-25m range. CPacket also recently kicked off a new marketing push with new branding and a redesigned website.

PRODUCTS

CPacket has always bucked the trends in the network- and application-visibility market. While other vendors are competing to see which can achieve the highest density in increasingly larger visibility switch chassis, cPacket has quietly (sometimes too quietly) continued to espouse a distributed scale-out approach of smaller network-analysis sensors. These devices, named cVu, utilize an internally developed custom application-specific integrated circuit (ASIC), which it has named the Algorithmic Fabric Chip. The AFC provides the horsepower for distributed analysis and summarization, using an information-theory-based approach, of data collected at the edges of the network. The policy and correlation of these distributed devices is performed by the company's centralized policy management and reporting system, the Stream and Packet Inspection Front End Environment.

The company has identified two other major trends in network deployments, namely the rapid growth of network virtualization and overlay technologies, such as VXLAN, and the regulatory need to retain specific traffic (network recording) using a storage device. CPacket released cClear in 2014, adding support for overlay networking technologies (notably, cClear is overlay-technology-agnostic), and addressing the concern of hybrid physical and virtual networks and the difficulty in troubleshooting network misconfiguration and performance issues. In 2014 the company also added cStor to its list of offerings, a custom appliance that can retain up to 128TB of network traffic. The company utilizes a rotating buffer of the traffic, allowing network administrators to look 'retrospectively' at conditions that led up to network or security incidents, in contrast to common approaches that begin recording once a condition is triggered, such as an alert from an IDS/IPS.

The Internet of Things is transitioning from proof-of-concept to production deployments, with 15% of enterprises claiming current IoT deployments and another 31% actively planning to deploy the technology, according to the 451 Research Voice of the Enterprise Datacenter panel in Q4 2015. IoT introduces another order of magnitude of connected devices to the IT network, further exacerbating network and application performance issues. CPacket's cVu devices can be scaled out to aggregate IoT devices (frequently a source of easily summarized time-series data), positioning the company well in contrast to large chassis-based offerings that would require a backhaul of the IoT traffic to a centralized location, saturating network bandwidth.

COMPETITION

CPacket primarily competes with network-visibility vendors such as Gigamon, NetScout and Ixia, as well as network-centric APM vendors such as ExtraHop and Corvil. Gigamon and Ixia both represent the incumbent/traditional approach to network visibility, using specialized networking switches with specialized 'packet grooming' capabilities to prepare traffic for ingestion by 'tool pool' devices such as intrusion-detection systems and traffic recorders. The market has been growing lately due to the combination of network virtualization, the standard drumbeat of datacenter speed increases (from 10Gb to 40Gb/100Gb) and the ongoing demands for security of the evolving datacenter (the latter of which has been a large revenue driver for Ixia and Gigamon).

Companies such as ExtraHop and Corvil take an application-in perspective to network visibility. ExtraHop creates and aggregates multiple data sources (from log data to network traffic to application performance) into a unified 'wire data' stream that it can analyze itself or hand to third-party tools such as Splunk. Corvil utilizes a specialized appliance to monitor network traffic and extract relevant applications and (within those applications) performance variables with minimal configuration. ExtraHop has shifted toward a more software-driven, cloud-friendly approach in recent releases, and Corvil has disaggregated its hardware and software pricing, potentially foreshadowing an offering of the company's software for use on virtual machines/servers or in the cloud.

SWOT ANALYSIS

STRENGTHS

Its distributed visibility and scale-out approach to adding small incremental sensor capability as the network grows make the offering a capex-friendly approach.

WEAKNESSES

CPacket has flown under the radar for many years as larger publicly traded competitors captured the majority of visibility wallet share. The company has its work cut out for it in growing brand awareness in the emerging IoT visibility and traffic-analytics market.

OPPORTUNITIES

IoT adoption is just now beginning in earnest, so a concerted push to position the company as a visibility 'safety net' for early deployments could carve out a large incremental market for the small company.

THREATS

As with most small companies, the largest threats are obscurity and an overall lack of awareness by paying customers. In IoT, the proliferation of both traditional OT- and new IT-based technologies could alter the landscape to tunneling proprietary protocols, complicating network analytics and visibility.