SALES PULSE RESEARCH

Technology Trends

Sales Pulse Research Update **December 20, 2018**

Cyber Security Trends - Market Dynamics - NGFW Vendors - PANW, FTNT, CHKP, CSCO

As you know, Sales Pulse has had an ongoing effort to watch the market closely to understand how the move of workloads to the cloud is impacting IT spending on infrastructure and on security. In this note, we explore the current state of this transition, the impact we currently see and the impact we expect on leaders in the NGFW segment.

NGFW - We're not dead yet… A recent article summarizes the bear case for the NGFW vendors. In The NGFW is dead the author makes the case for the death of the NGFW based upon:
- The network perimeter is gone
- NGFW's are not designed for cloud architectures
- Cloud providers are (or will) offer the same capabilities at a fraction of the cost
- The NGFW is not effective.

The argument is well stated and identifies real threats but determining the timing of the impact to the NGFW vendors is the challenge. The full bear case depends on most organizations moving to "cloud-native" architectures. Although some organizations continue to rapidly move application workloads to the cloud, the vast majority have chosen hybrid architectures and are expected to maintain those hybrid architectures for an extended period. As organizations have evaluated what to move to the cloud, most have found applications that don't make sense to move to the cloud for reasons including cost, control, security, complexity and/or performance. In the most recent sign that hybrid cloud is a legitimate path forward, AWS announced Outpost, at AWS: re:Invent to deliver AWS services on-premise. Microsoft made a somewhat similar move a year ago with Azure Stack.

Current status - Based upon input from field contacts in this security segment our view is that the consumption of NGFWs has been impacted by the cloud in the following ways:
- As organizations have reviewed their applications and architectures in the process of deciding what to move and what to keep on-prem, they have uncovered security exposures resulting in a short-term boost to NGFW spending.
- Virtual FW instances are increasing as a percentage of FWs ordered, putting downward pressure on total deal sizes and pricing. Subscription revenue, attached and unattached, continues to provide the most growth for NGFW vendors.
- The latest generations of appliances, especially from Palo Alto and Fortinet, have significantly boosted price/performance, also putting downward pressure on deal sizes. This has been partially offset by the need for increased processing power, especially for SSL decryption / encryption.

So, that leads us to where we are now, with slowing growth for NGFW appliances and sustained, or accelerating growth for subscription services. Growth in cloud workloads and more adoption of cloud-native architectures will lead to even greater headwinds for appliances. The timing of a fall-off in appliance sales is still difficult to predict but the broad acceptance of hybrid cloud architectures gives vendors more time to figure out their relevance in initially the hybrid cloud, but eventually in a world where customers have little, if any, technology in their own data centers. As always, we are working with the channel to stay on top of demand trends and be able to pinpoint when the fall-off begins in earnest.

Cloud-native vs. Lift and Shift

In addition to the move of applications to the cloud or hybrid cloud, a significant factor in determining the demand for legacy solutions is the adoption of cloud-native architectures vs. lift and shift of a current application stack into the cloud.

Cloud native = design of new (or heavily rearchitected) applications using advanced DevOps or DevSecOps techniques that take advantage of native cloud capabilities that provide architecture advantages in security as well as application performance, scalability, and recovery.

Lift and Shift (Sometimes known as Lift and Pray) = moving existing applications to the cloud without making architectural changes and therefore maintaining the security and operational characteristics and dependencies from their legacy deployment.

How do these different approaches impact the adoption of security solutions? With cloud-native implementations, there are no central, high volume inspection points. Instead of a limited number of high-speed ingress ports where all traffic is filtered and policed by NGFWs, individual end user sessions access applications. Identity and application and data management are the primary tools for security. Multi-tenant cloud platforms by their fundamental design provide for isolation of applications and therefore less of a security exposure on some dimensions. So, few FWs and appliance-based solutions are needed.

Lift and Shift largely preserve the same security controls that have been developed over the past 20+ years to serve premise-based applications. Some hardware-based appliances (FWs, ADCs) may be replaced by virtual instances, but functional requirements are preserved.

How is the transition to cloud progressing considering the choice between cloud native and Lift and Shift? Although some end users are embracing cloud-native approaches, we have been surprised by the extent that hybrid and on-premise concepts continue to impact the designs and architectures for customers. It is clear that hybrid cloud will be around for a while.

Some of the demand for cloud-based FWs is about inertia. If security is driving architecture, then you see traditional controls. If application groups are driving architecture then you are more likely to see new concepts to build security into the application stack. A more efficient design pattern for hybrid cloud is one that centralizes all connectivity from cloud to traditional data centers. At that central point, you install a virtual NGFW and closely monitor that network (called a Transit VPC). But you aren't putting a virtual firewall in every cloud stack nor front ending access to the cloud with these perimeter devices. Not everyone buys into the Transit VPC concept… yet. But that's a much better architecture to handle hybrid infrastructures. Additionally, Amazon introduced a new offering called Transit Gateway at the recent re:Invent conference, further validating and making this architecture easier to embrace. This will likely have a significant impact on using virtualized network security devices in the Transit VPC.

Select comments on vendors:

Palo Alto has been the most aggressive vendor in buying cloud security companies and defining their solutions for the hybrid cloud. Check Point recently announced their acquisition of Dome9, which is an early mover in offering network security in cloud environments. It appears to be a

good move, but the two approaches of these vendors are fundamentally different. And Palo Alto and Check Point get the vast majority of their revenue from the traditional network security appliances. So they are vulnerable if that revenue stream slows.

Do they now have more runway? As we have noted in previous updates, predicting the timeframe for this transition is challenging and we rely on our ongoing checks to provide near-term views. Palo Alto is currently executing well and continues to pick up market share. End users, field teams and their channels believe they are making the right moves to solve customer problems in a hybrid cloud environment and to continue their market leadership. Yet to maintain their growth rate over the long term they will have to significantly transition their business. Their product enhancements and recent acquisitions (Evident.io and RedLock) have given channels and end users confidence in their direction and leadership. Channels are currently indicating healthy sales pipelines going into 2019 (see our recent notes on security spending).

Fortinet has been executing better lately and leveraging strong price/performance that their ASIC-based architecture enables. Fortinet appeals to the segment of the market that is not willing to pay for Palo Alto's cost and vision and that includes much of the mid-market, which may give them more runway as well, given a portion of those customers will lag in terms of cloud adoption.

In our view, Check Point may be impacted far earlier because they are getting squeezed by Palo Alto at the high end and Fortinet from below. Dome9 was a start to understand the cloud threat (and neutralize it), but Check Point is not seen as an innovator nor particularly a strategic security provider for their customers.

Cloud is a much bigger initiative for Cisco than just security. But they run the risk of providing an overly broad and muddled message. Cloud offerings are also lagging and with the exception of acquiring Observable Networks, have made few moves to prepare for this cloud-based reality. OpenDNS (now Umbrella) provides the basis for their cloud-strategy, but it hasn't been well defined or communicated at this point.

Comments from channel contacts:

"Although moving to the cloud is reducing the need for security appliances and resulting in lower $ deal sizes in some cases, at this point the cloud VM firewall business that we are seeing appears to be mostly additive. And, shifting traffic to the cloud does require beefy powerful firewalls to support the increased traffic from the to the Internet Gateway Firewall."

"The edge firewall is still the best solution when performance is crucial. VM firewalls don't have the same performance characteristics or functionality. SSL inspection is a growing requirement and decryption requires a ton of horsepower, only available in the most recent versions of appliance firewalls from Palo Alto and Fortinet. In many environments SSL traffic is 50%+ of traffic and it must be inspected. Within 5 yrs SSL could be 90% of traffic. The latest version of TLS 1.3 is not widely implemented yet but will require even more horsepower to decrypt. SSL and TLS 1.3 decryption could be a factor in prolonging the relevance of appliance based firewalls, certainly good for the firewall manufacturers."

"The Transit VPC is a design that is getting more consideration because it's like the old hub and spoke. Often companies want to deploy apps in cloud, and since they are internal (hosted in cloud), they want to insure they are only interacted with appropriately and the Transit VPC is a good design to check and enforce. They also want the ability to route and inspect all outbound traffic, from the cloud, and this supports that objective. This can be achieved via an appliance but often done via VM because it's still new, and hard to predict future throughput requirements."

"As a channel providing security solutions, we have some concern that Amazon, and potentially Microsoft, could become competitors to Palo Alto, Fortinet, etc. and therefore to our product and services business. Amazon does claim to have some firewall features but they are only old school access lists. The "pay and you go" model at the cloud players is also a concern for vendor reps and channels because it's hard for the channel to track end user usage and hard for the reps to get paid, even though it's relatively small "rental income" at this time. Amazon, particularly, is considered "dictatorial" when it comes to how they work."

"We are not seeing any appliance firewalls being decommissioned and replaced with VMs in the cloud. One of the problems brought up is when the VM is deployed in cloud the performance is tied to the underlying infrastructure. When using appliances they know how it will perform because it's riding on top of Fortinet's ASICS or Palo Alto's Single Pass Architecture. In the cloud, this does not exist so they cannot control the impact on performance or insure the VM is not oversubscribed."

"The most exciting area of growth created by the move to the cloud is for protection of branch services, SD-WAN and mobile users. Palo Alto (GPCS), Zscaler, Forcepoint have various levels of solutions for this. This area is seeing tremulous growth and we are still in the very early stages."

"Today's move to the cloud seems similar to what VMW went through 10 yrs ago when they started moving from simply consolidating servers/hardware, to virtualizing mission critical, revenue generating, applications. Many companies are exploring downsizing or sunsetting data centers and moving to the cloud. It feels like we are in the 3rd to 4th inning of these moves. New Apps and new workloads are certainly cloud candidates and most often developed with the cloud in mind. And some companies are sunsetting apps and rebuilding to work in the cloud. When it comes to lift and shift, companies often find apps don't work as expected (because they were not developed as cloud apps) and often storage and compute costs are more expensive than anticipated. These legacy apps have architectures that are not optimized for the cloud, and don't/can't take advantage of the cloud optimization capabilities."

As always, we are happy to discuss in more detail.

SALES PULSE RESEARCH

Offices:

Atlanta, GA
Charlotte, NC

Tom Morphis
404-240-0916
tom@salespulse.net

Steve Thompson
704-467-6749
steve@salespulse.net

Important Disclosures

Facts and the other information contained in this report have been obtained from public sources considered reliable but are not guaranteed in any way. No independent confirmation of the truth, correctness or accuracy of the information presented has been made by Sales Pulse Research, LLC.

This report is published solely for information purposes and is not an offer to buy or sell or a solicitation of an offer to buy or sell any security or derivative. Sales Pulse Research, LLC accepts no responsibility for any loss or damage suffered by any person or entity as a result of any such person's or entity's reliance on the information presented in this report. Opinions and estimates expressed herein constitute judgments as of the date appearing on the report and are subject to change without notice.

All of the recommendations and views about the securities and companies in this report accurately reflect the personal views of the analyst(s) of Sales Pulse Research, LLC. No part of analyst's compensation was, is, or will be directly or indirectly related to the specific recommendations or views expressed by the research analyst. Employees of Sales Pulse Research, LLC may from time to time acquire, hold or sell a position in the securities mentioned herein in this report.

The information contained herein has been obtained from sources believed reliable but is it not necessarily complete and accuracy is not guaranteed.