Technology Brief...

June, 2017

J.Gold Associates LLC, 6 Valentine Road, Northborough, MA 01532, USA
www.jgoldassociates.com +1-508-393-5294
Research, Analysis, Strategy, Insight

INSIDE THIS ISSUE

1 Citrix as a Security Company?

2 Can VMware take IoT's Pulse?

3 Powering the "Mobile Data Center"

Citrix as a Security Company?

At its recent Synergy user conference, Citrix emphasized its refocused efforts to help enterprises and SMB become more secure within a growing world of hybrid cloud deployments and the plethora of device types making their way into the enterprise. Although we're not sure everyone in attendance got the new direction, given Citrix's continued reputation as primarily a VDI enabler, an area long ago expanded upon with many new capabilities, we nevertheless see this as an important new focus for the company. Citrix started out more than 20 years ago as a way to deploy "thin" clients, which often were not really such, but were often old technology repurposed to use on new app systems. Citrix then became a virtualization company when it was popular to use endpoint assets without having to have uniform device types. And then a cloud company when enterprise apps were migrating to the cloud. Now Citrix is morphing into a security company.

Citrix is primarily known for its long term position as a leader in the VDI space with its Xen family of desktop and mobile app delivery and management solutions, ShareFile file management, and NetScaler infrastructure capability. It has acquired a large installed base of users. It has recently been pursuing the integrated workspace market with a combined product suite offering, although that market has been slow to emerge. But with its primary market changing focus, Citrix has decided its best path forward is to rebrand itself as a security enabler, an approach that suits its technology and the markets it serves while maximally leveraging its core assets.

"…Citrix has decided its best path forward is to rebrand itself as a security enabler, an approach that suits its technology and the markets it serves while maximally leveraging its core assets.. enterprise users, particularly those already deploying Citrix products, should look at deploying these new capabilities in a timely fashion to enhance their overall security posture..."

We are impressed that Citrix is making this pivot towards being a security company and largely agree with its strategy. Citrix has always been in the security business, with many adopters in key regulated and security conscious industries such as finance, banking, retail, public sector, and healthcare. These enterprises were always concerned with keeping data safe and used VDI to eliminate risk at key endpoints. But in the past, Citrix defined its primary role as maximizing ROI/TCO by keeping IT costs low. While this is certainly a continuing concern, much more emphasis today is being placed on IT's role in managing complexity and the security issues created by the need to support both infrastructure and endpoint diversity. Add the complexity of partial cloud migrations to that mix as most enterprises will have a mixed environment of on-prem, private cloud and public cloud deployments for at least the next 5-7 years and probably beyond that.

This is not a technology restart, as Citrix can easily reposition its key technologies for its new focus on security. NetScaler started life as a WAN accelerator to enable better network performance and load balancing. Now it's a data visibility and security component of Citrix Cloud products and key to enabling secure next gen

work spaces. ShareFile is no longer a distinct data repository competing with Drop Box or SharePoint, but a secured and managed gateway to data wherever it resides from whatever device wishing to access it. Citrix Analytics Services provides automated policy driven security capability to shut down attacks and risks in near real time by leveraging data obtained from NetScaler (and partners Cisco and Microsoft) and utilizing the Xen and UEM (unified endpoint management) apps to enforce policies. Indeed, an automated policy driven analytics capability is key to making security work real time, with a current industry average of 60+ days to find a security breach/hack being common but totally unacceptable. All of this plays well not only into a targeted IT market where Citrix primarily markets its products currently, but also messages well for line of business, which is where we see 65%+ of product decisions being driven based on business need and not just IT preference. Companies that don't have a compelling message for both IT and LOB functions will have a difficult time being successful going forward.

Bottom Line: We believe it's a good move for Citrix to be remarketing itself to focus on security given all of the needs and threats now available. It's a refocus but not a true realignment of the products and services it offers. Leveraging to a growth market in security is a great way for Citrix to expand its potential footprint and what it's known for in the market. As a result many companies will look at Citrix in a new light, not as only a VDI approach to reduce TCO, but as a secure and safe enabler. However, Citrix's challenge will be to "sell" this new vision in a market that primarily knows Citrix for its legacy VDI business. Nevertheless, enterprise users, particularly those already deploying Citrix products, should look at deploying these new capabilities in a timely fashion to enhance their overall security posture.

Can VMware take IoT's Pulse?

Most vendors are racing to establish a position in the emerging area of IoT, and especially EoT (Enterprise of Things). Although still nascent, the emergence of EoT will have major impacts on most enterprises over the next 3-4 years as they deploy new devices, many of them consisting of user acquired and deployed products. This is the next mobile effect, but on steroids!

"…we expect the Pulse IoT Center product to be a welcome extension for those VMware customers looking to add EoT functionality to their already growing list of virtualized infrastructure components, especially as it will provide a single window pane into security and management …. Enterprises already invested in VMware should evaluate its new offering for EoT.…

Major concerns facing most implementations of EoT consist of easily on-boarding, securing and managing the devices, as well as obtaining useful data for actionable analysis and corresponding intelligent actions. Indeed, the major promises of EoT (a more efficient operation with new insights into business operations) can't be achieved without actionable intelligence that results in operating efficiencies beyond those available with current techniques. But the cart before the horse scenario says enterprises need to get the devices on-board, managed and secured before the big data and analytics can kick in. And companies have to manage and secure the devices and the data coming into and exiting their networks without having to rip and replace their existing infrastructure in the process. This requires a degree of architectural flexibility that many companies don't yet have in place and likely can't accomplish with older generation systems.

To this end VMware is announcing its Pulse IoT Center. Its primary target is to easily on-board both EoT devices and edge systems, securely tie them into the corporate infrastructure with minimal pain and manage and monitor them over their lifecycle. Leveraging its management/security and monitoring technology from AirWatch and vRealize, it should have great appeal to those users already invested in a VMware solution. With Pulse IoT Center, customers can extend segmented data flows and a virtualized network environment down to the individual device

level, while providing for visibility across the entire solution. This can be especially attractive for user-acquired devices.

To be sure, VMware has a good deal of competition in this space, ranging from Microsoft and AWS with cloud based platform alternatives, to GE Predix and other large scale infrastructure technologies attractive primarily to the industrial enterprises, to extended mobility/VDI capabilities from Citrix and the key EMM players like BlackBerry, Mobile Iron, IBM, etc. But VMware's product is most attractive to those companies who already have VMware in their data center for managing their devices and who want to extend their virtualized networks and infrastructure to upcoming EoT deployments. This "head start" could help both EoT implementations and virtualization initiatives expand beyond existing uses.

Many EoT products will require an intermediate edge server as a way to consolidate a myriad of data input devices (see our XXX). Virtualization could provide a key component of a broader edge strategy than having to put a "black box" at every node that has multiple sensor inputs. And while most people think of EoT devices as "dumb" sensors, many will have user interface requirements that can also benefit from a VDI approach to interface access and operation. Both of these scenarios can benefit from VMware's approach.

Bottom Line: We expect VMware over time to build on its Pulse platform and offer additional tools and capabilities, while also tying into related EoT products, just as it does with its infrastructure tools and technologies. However, VMware may be hard pressed to become a broad based provider of EoT infrastructure outside of their installed base. Nevertheless, we expect the Pulse IoT Center product to be a welcome extension for those VMware customers looking to add EoT functionality to their already growing list of virtualized infrastructure components, especially as it will provide a single window pane into security and management from the already in place management tools of VMware products. Enterprises already invested in VMware virtualization and management tools should evaluate its new offering for EoT.

Powering the "Mobile Data Center"

Everyone seems to be targeting autonomous vehicles as the next major "thing". And it's true that much progress continues to be made in automation, sensor development and AI associated computing necessary to make it a reality in the next few years. But what is often overlooked is the vast amount of data needing to be processed and then shared, and not just at the local vehicle level. That's why so many different players with a diverse set of technologies will be required to make this market a success.

"…The advances needed to achieve autonomous vehicles will take place both on and off the vehicle, and no one vendor will be able to accomplish this independently. Early leaders are unlikely to dominate the processing functions needed, and competing requirements will produce a large market opportunity for additional players....."

Let's look at some of the required technologies:

- Sensor systems to run the car – machine vision/processing, LIDAR, enhanced location information
- Localized and edge data processing to understand parameters about the ecosystem, including vehicle to vehicle communication standards, but also unified backend data services from various suppliers of data
- Reliable and high speed data transmission to keep the entire network of vehicles and related data in sync, and not only limited to vehicle to cloud
- Back end AI/ML/Huge Data processing from all of the vehicles to make sense of the entire picture of what is happening in the targeted areas of operation.

This is going to take a vast array of processing capabilities and products. Nvidia with its GPUs may have an early lead in some of the vision and sensor AI related operations capability. But high powered processors, like Intel Xeon, and specialized programmable chips like FPGAs will absolutely be needed, as well as newly announced AI/ML chips from Google (TPU) and Intel (Movidius). We expect these dedicated processors to capture an increasing share of the AI market going forward, at the expense of many general purpose devices like GPUs.

Without a reliable 5G network that can move data around in a low latency, highly deterministic real time way, the notion of autonomous vehicles will fall far short. Traditional wireless technology vendors like Qualcomm (chips) and Cisco (network infrastructure) will be required to enable such capability, as well as the carriers who implement the technology that will establish a robust 5G footprint. Finally, big data integrators/processors like Google, Microsoft, AWS, etc. will be needed to keep and process the large amount of data in the cloud needed to make the information available for proper operation, especially as it's required to do proper machine learning to advance localized processing functions in the vehicles themselves.

This is just a small indication of the complexity of making the next generation of autonomous vehicles operate effectively and efficiently. There are many more technology needs, like security, app management, systems health management, etc. But to concentrate solely on what is powering each individual vehicle misses the point of what will ultimately be needed if we are truly going to move to an autonomous vehicle future. The next 3-5 years will be dynamic and produce yet unrealized capabilities, many of which are just now at the concept stage.

Bottom Line: The advances needed to achieve autonomous vehicles will take place both on and off the vehicle, and no one vendor will be able to accomplish this independently. Early leaders (e.g., Nvidia) are unlikely to dominate the processing functions needed, and competing requirements will produce a large market opportunity for additional hardware (e.g., Intel, Qualcomm, Google, and many others) and software (e.g., BlackBerry QNX and Samsung Harman in vehicle; Google, AWS, Intel etc. in the backend), both in the car and in the cloud. Products now being deployed should be considered early implementations, with maturity taking at least 3-5 more years of evolution.

Recent Research

Contact us to request the following research reports:

Market Studies
- **The State of Enterprise Mobile Management (EMM)**
- **Mobile E-Commerce: Friend or Foe?**

Emerging Technology Trends
- Highlights our key emerging trends for the next 3-4 years

Commentary and Analysis
- Apple and IBM in Enterprise: Joined at the Apps

Research Reports
- Android in the Business Environment: Is it Safe?
- Your PC has an Identity Crisis: Saving the cost of hacks and other benefits of enhanced identity
- Replacing Enterprise PCs: The Fallacy of the 3-4 Year Upgrade Cycle
- Keeping Notebooks Past Their Prime: A Study of Failures and Costs

Whitepapers
- A Heuristic Approach to Mobile Security
- MDM- Where Do We Go From Here?

J.Gold Associates, LLC
6 Valentine Road
Northborough, MA 01532 USA

Phone:
+1-508-393-5294

Web:
www.jgoldassociates.com

Research, Analysis, Strategy, Insight

About J.Gold Associates, LLC.

J.Gold Associates provides advisory services, syndicated research, strategic consulting and in-context analysis to help its clients make important technology choices and to enable improved product deployment decisions and go to market strategies. We work with our clients to produce successful new product strategies and deployments through workshops and reviews, business and strategic plan coaching and reviews, assistance in product selection and vendor evaluations, needs analysis, competitive analysis, and ongoing expertise transfer.

J.Gold Associates provides its clients with insightful, meaningful and actionable analysis of trends in the computer and technology industries. We have acquired a broad based knowledge of the technology landscape and business deployment requirements, and bring that expertise to bear in our work. We cover the needs of business users in enterprise and SMB markets, plus focus on emerging consumer technologies that will quickly be re-purposed to business use.

We can provide your company with a trusted and expert resource to maximize your investments and minimize your risk. Please contact us to see how we can help you.