Technology Brief...

June, 2021

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

"….With a wide array of security and safety focused products, BlackBerry is well positioned to become a major enabler of privacy and security services for both enterprise needs as well as IoT solutions… recent moves to provide more platforms and services enable them to expand their markets and moving to a cloud enabled as a service platform makes them much easier to become integrated into a wide array of organizations. Enterprises should evaluate the services that BlackBerry has recently added to its portfolio....."

BlackBerry Ramps up its Security

The BlackBerry has been making a number of announcements recently about extending their security products to a variety of markets. Indeed, they recently created two business units to better address two key market focus areas – Cyber security focused on enterprise needs with their UEM and UES products as well as professional services, and IOT to include their many products for autonomous vehicles and other industrial products (e.g., BlackBerry IVY, QNX). The business unit separation means that they can better address the marketing needs of these segments, while also continuing to leverage their major investment in core security products and processes they have been building for many years (e.g., Cylance AI powered security, zero trust, XDR, QNX hypervisor/virtualization).

At its recent BlackBerry Security Summit, which this year was held virtually, BlackBerry highlighted a number of key products and initiatives, including:

BlackBerry IVY platform – Through a partnership with AWS, this cloud-native solution consists of an on-vehicle component (IVY EDGE), a cloud-based IVY Console, and an IVY Development Environment. The platform enables the rapid creation and updating of services and applications resident in the vehicle, as well as obtaining valuable data from onboard sensors and analysis of that telemetry. This is especially important as so many add-on premium subscription services will be created for vehicles both by car makers and third parties. With an already massive installed base of QNX, and a leading position in the new electric vehicle market, this positions BlackBerry to be a major force in enabling the new vehicle ecosystem for major auto makers, as well as aftermarket services.

Security as a Service – BlackBerry Guard. BlackBerry has established a not-so-well-known capability as a full service security management company, including working with clients to detect threats, hunting for new emerging threats, managing any security incidents, providing threat intelligence, and increasingly providing response and mitigation services. With its decades of focus on security, and its major research in this area, BlackBerry provides a credible security as a service provider, especially to its large base of highly regulated industries. This is a growing industry and enables BlackBerry to leverage the information it provides in its products and provide feedback to its own engineering efforts.

Critical Event Management - BlackBerry Alert – Although seen as a one-off capability when it acquired AtHoc several years ago, BlackBerry is now focused on making critical event management part of a regular management function at organizations in many verticals needing business continuity, critical IT and security

communications and time-critical situational response. The ability to quickly and deterministically provide critical communications over a multitude of channels (e.g., email, text, collaboration suites, etc.) and especially in the context of the current pandemic needs makes this another key component of BlackBerry's expansion into security related mission-critical business areas. Critical event management is an important component of being able to quickly respond and control any security related situation, and providing it as a service allows BlackBerry to overcome many of the hurdles that made organizations hesitant to deploy internally-based systems.

Bottom line: With a wide array of security and safety focused products, BlackBerry is well positioned to become a major enabler of privacy and security services for both enterprise needs as well as IoT solutions. Although they are in a highly competitive market, recent moves by BlackBerry to provide more platforms and services enable them to expand their markets and moving to a cloud enabled as a service platform makes them much easier to become integrated into a wide array of organizations. Enterprises should evaluate the services that BlackBerry has recently added to its portfolio.

VMware Takes Workspaces Anywhere

Recently, VMware extended its workspace offering by announcing VMware Anywhere Workspace. This integrated product set consisting of VMware Workspace ONE multi-device workspace, VMware Carbon Black security suite and VMware SASE secured access is targeted at organizations that need to enable work from any device, on any connection and with maximum security and manageability. This is especially important in a distributed workplace environment that most companies will have in place for the foreseeable future. And while Workspace Anywhere is an integrated product set, customers can mix and match components to get started without committing to a full implementation. This is critical as many organizations do not want the expense or need the complexity that a full combined suite would require. It also creates an easy entry point for those companies already having some of the VMware components in place, and enabling VMware to have an up-sell opportunity. The complete solution allows enterprise to manage the multi-device and multi-modal experience by enabling work on virtually any device both on-prem or in the cloud, and adds intelligent device management, compliance, workflow, and creates a Zero Trust capability with situational intelligence and control points.

"…Anywhere Workspace will be especially attractive to those organizations already deploying VMware Workspace ONE or Horizon products. While the Anywhere suite provides a more complete integration of the tools needed for workforce optimization, especially for knowledge workers, it still is not a complete solution…. Still, with so many apps now being deployed in the cloud as a service, Anywhere Workspace is an attractive suite for those organizations with a distributed workforce…"

While this is a major step forward for VMware, it can be viewed as a response to its most direct workspace and VDI competitor, Citrix. Citrix has been moving down this path for some time, and with its new capabilities in data integration and directed task flows (through its acquisitions of Sapho and Wrike), has pioneered the integrated workspace and task management approach. VMware also has other competitors moving towards a more integrated workspace suite (e.g., Microsoft, Google, Cisco) that are attempting to create a fully secured and integrated workspace for users, although the above vendors are coming at it from a different direction by extending their collaboration tools to encompass collaborative work. However, VMware, with its inherent work on any device and unified endpoint management capabilities has an advantage in multi-modal situations.

VMware has two major advantages when it comes to integrated workspaces. First, its Carbon Black security suite is among the best at keeping endpoints safe with its AI-based functionality. Carbon Black and Workspace One share information to implement zero trust security in an automated fashion. Second, its capabilities in virtualization and SD-WAN enables a zero trust situation to deliver a cloud-native

security posture for either on-premise or remote use that can be natively deployed or delivered through localized points of presence with partners, and includes a partnership with Zscaler for cloud based protection. Further, VMware connects to all major cloud platforms, including AWS, Azure, GCP and Salesforce, although that's fairly standard practice for solution providers.

But to enable true workspace management and not just remote VDI, enterprises are increasingly looking at complex cross app workflows. To enable the integration of enterprise apps, VMware is providing a workflow engine with integration to Dell Boomi. This allows many pre-configured out-of-the-box workflows but also allows customers to create their own workflows across multiple apps. One example is employee onboarding workflow that can leverage multiples apps as a business delivers an onboarding experience to the new employee. However, adding Boomi requires an additional product outside of the suite that some organizations may not find attractive.

Bottom Line: Anywhere Workspace will be especially attractive to those organizations already deploying VMware Workspace ONE or Horizon products. While the Anywhere suite provides a more complete integration of the tools needed for workforce optimization, especially for knowledge workers, it still is not a complete solution in the sense that enterprises will still have to insure the required mission critical apps are available and integrated into the product. And it does not feature some of the workflow and microapp functionality that competitors offer. Still, with so many apps now being deployed in the cloud as a service, Anywhere Workspace is an attractive suite for those organizations with a distributed workforce.

HP Enhances PC Security

"…HP is delivering the highest level of security and services of any PC vendor, although there is certainly competition, primarily from DELL with its partnerships with VMware and Carbon Black. Nevertheless, with its move to creating the HP Wolf Security platform and service tiers, we believe that HP PCs are more security-capable and deliver a compelling product that enterprises interested in providing the most secure platform to their growing diverse workforces should strongly consider....."

All of the major PC vendors have made Security a prime objective in marketing their products, particularly when it comes to business-class Windows-powered machines. Apple has also been highly engaged in securing its PC offerings, but our focus for this report is in the Windows PC segment. While the key processor vendors (e.g., Intel, AMD) and the primary OS vendor (e.g. Microsoft Windows) have contributed to an increasingly secure PC environment, there is much that needs to be done by the device makers to build upon the base processor and operating system security-oriented functions, as well as a need to offer enhanced security services beyond the machine itself.

Recently, HP announced that it is moving all of its various security capabilities into a new branded platform called HP Wolf Security. This concentrated emphasis on a wide ranging security platform provides HP with a focus that its disparate offerings didn't have previously, and places it in a leadership position for a unified endpoint security capability with both on-device enhancements and as a service offerings that run the gamut from minimal consumer-level on-device offerings to large scale enterprise-class managed services. And like so many other products that are transitioning away from fixed onboard capability, HP's ultimate goal is to make security "as a service" a primary offering to enterprises.

It all starts at the endpoint

75% of end point infections are due to user actions – whether they know it or not. Deflecting such attack surfaces threats are a key driver for nearly all security initiatives and requires both hardware and software components to accomplish. Its previous Bromium acquisition gave HP the virtualization, containerization and AI based tools needed to extend security beyond its hardware components and into the realm of software by enabling an isolated session for each browser and/or application instance.

This is particularly important in the cloud-enabled world that's dependent on secured browser capabilities, and one plagued by various malware and ransomware attacks.

HP is the only PC company that supplements its device security with its own Endpoint Security Controller ASIC that enhances the inherent security features of the main processor and OS, but also allows HP to maintain the same level of security across different manufacturer's processors (e.g., Intel, AMD), each of which has its own unique capabilities. This is a major advantage that HP has created to maintain a consistent and extended security platform for all of its products. There are still some processor differences, as when deploying a "Pro grade" processor (e.g., Intel vPro) since it has unique built in security features. But generally speaking, HP's own hardware enhancements add security beyond what the processors themselves make available. Add to that the enhanced software capabilities like Bromium and AI based capabilities and HP maintains a higher degree of security functionality and malware avoidance than its competitors.

HP Wolf Security tiers

In its move to offer both below and above the OS security, HP has provisioned 3 tiers of security capabilities.

- HP Wolf Security for business – this is foundational and available in every business class device as a built-in standalone capability
- HP Wolf Pro Security – multi-level enterprise class security targeting SMB and enterprise by adding bundled and/or prepackaged services beyond what's inherent in the device. This is a configured service available that customers can select from a menu of functions.
- HP Wolf Enterprise Security – large enterprise focused with managed services for threat intelligence and threat remediation. This is the highest level of security capability offered and HP has built its internal expertise by offering similar services for some time to select customers. This is a direct competitor to some third party security service providers from whom HP wants to capture business.

Add to this all of the services HP provides in guarantying the full supply chain integrity of its products (an increasingly complex and difficult task), pre-configured and image installation services for customers, and after the fact services, all of which makes HP a premium supplier of secured devices and services.

Bottom line: HP is delivering the highest level of security and services of any PC vendor, although there is certainly competition, primarily from DELL with its partnerships with VMware and Carbon Black. Nevertheless, with its move to creating the HP Wolf Security platform and service tiers, we believe that HP PCs are more security-capable and deliver a compelling product that enterprises interested in providing the most secure platform to their growing diverse workforces should strongly consider.

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.