Market Roundup

July 13, 2007

IBM's Next-Generation Tape for Mainframes

By Clay Ryder

IBM has announced its next-generation tape solutions for mainframe customers along with enhancements to the IBM Virtualization Engine TS7740, a mainframe virtual-tape solution designed to support business continuity, improved tape processing, and energy efficiency through Grid connectivity and automated replication. The enhanced offering supports automatic duplication of tape data with its Three Site GRID Configuration, which enables a Virtual Tape Grid computing environment with global awareness functionality, allowing data residing on TS7740s at three different sites to be easily tracked and accessed. Other new features of the TS7740 include tailored performance and cache capacity increments, a 1TB single-cache drawer configuration for businesses that require less capacity, a Copy Export function that supports exporting of data from a standalone or GRID TS7740 for disaster recovery, and improved management capabilities. The enhanced Virtualization Engine TS7740 features will be available on August 31, 2007 except for the 1TB cache configuration and Copy Export for GRID configurations, which will be available on November 23, 2007.

IBM also announced an enhanced TS1120 Tape Controller that permits the TS3400 Tape Library to be attached to mainframes. The TS3400 features the functionality of an enterprise drive in a two-drive library that delivers drive-based encryption capabilities in a small-footprint eighteen-cartridge library with up to 37.8TB of compressed data, and optional WORM storage. The enhanced TS1120 Tape Controller will be available on August 31, 2007. The company also introduced the TS2230 Tape Drive Express Model H3S LTO 3 Half Height, a model that targets midsized organizations, and incorporates the new LTO IBM Ultrium 3 SAS Half-High Tape Drive featuring a 3GBps single port SAS interface. The TS2230 Tape Drive Express Model H3S LTO 3 Half High will be available on August 3, 2007.

Proven technology has a habit of hanging around long after the pundits and crystal ball gazers have declared it obsolete, if not dead, on more than one occasion. These announcements are more evidence of this propensity as two venerable technologies, namely the mainframe and tape-based storage, are once again the focus of next-generation advancements in features and capabilities. While IBM made it clear a few years back with the release of the System z9 that the mainframe would remain a vital and future focused technology, the past several months have witnessed a rekindling of interest in tape-based storage from multiple vendors including IBM, HP, and Sun, among others. Two themes that we continue to see revolve around tape-based encryption and LTO Ultrium-based drives with an eye-popping capacity upwards of 800GB. Clearly, the use of tape is far from dead.

At one level, it only makes sense that tape retains such interest in the marketplace. Given the well established growth in data being stored by organizations, despite the ever decreasing price of disk storage, the ability to cost-effectively store large quantities of historic data for the duration of the many compliance and/or best practices mandates in effect tends to favor tape-based solutions. Granted, some environments will still demand a disk-based approach in order to meet SLAs or other best practices; however, for a substantial number tape remains a balanced approach that meets the price/performance needs.

We are also intrigued by the expansion of the Virtual Tape GRID to support three sites. Short of galactic mayhem, two sites are sufficient for business continuity; however, the support for a third site tends to illustrate a more

The Sageza Group, Inc.
32108 Alvarado Blvd #354
Union City, CA 94587
510·675·0700 fax 650·649·2302

pragmatic consideration, i.e., distributing tape backup and recovery windows across more geography. For global enterprises, many of which are coincidentally mainframe customers, business is a 24-hour activity. By supporting a third geographically dispersed location in their tape GRID, organizations can engage in backups at most any time of day. But more importantly, should retrieval of a certain data set be required, the task can be initiated during the local work day, even if the request initiates across the globe.

Overall, these announcements illustrate the ongoing interest in long-established technologies and the lengths to which Big Blue is willing to go to continue enhancing the mainframe and tape-based storage. As with many of its market approaches the company is seeking not only to maintain its existing customer base, but to grow new customer opportunities through enhanced technological capabilities and performance that illustrate the relevance of these time-honored approaches to meeting organizations' IT needs.

Google Acquisition of Postini Recognizes Fundamental Truths

By Lawrence D. Dietz

Google Inc. announced this week that it has signed a definitive agreement to acquire Postini, a vendor of on-demand communications security and compliance solutions serving more than 35,000 businesses and 10 million users worldwide. Postini's services, which include message security, archiving, encryption, and policy enforcement, can be used to protect a company's email, instant messaging, and other Web-based communications. Under the terms of the agreement, Google will acquire Postini as a wholly-owned subsidiary for $625 million in cash, subject to working capital and other adjustments. The agreement is expected to close by the end of the third quarter 2007.

Hosted services, like Google Apps and Postini solutions, provide organizations with communications tools without the expense and hassle of traditional on-premise solutions. Google Apps, which includes Gmail, Calendar, Talk, Docs & Spreadsheets, and Personal Start Page, has been adopted by more than 100,000 businesses already. Postini solutions include Email Security, IM Security, Web Security, Message Archiving, Message Encryption, and Policy-enforced TLS. Google will continue to support Postini customers and invest in Postini products. The Google Enterprise group makes popular Google technology available to businesses of all sizes, from small, two-person startups to some of the largest companies in the world. Google Enterprise products help businesses find, see, and share information through products such as Google Search Appliance, Google Mini, Google Earth, Google Maps, and the Google Apps suite of hosted applications.

It would be quite tempting to jump to the simplistic conclusion that Google's acquisition of Postini was motivated by its desire to break out of the consumer mold and become a more attractive technology option for businesses. A strong argument could be postulated that Google felt it needed to beef up the security aspects of its mail services and that this move was made to assuage businesses' concerns about security and assurance. It could also be stated that by embedding Postini capabilities into Google applications the company has ensured a higher level of security and compliance for its customers because of the built in nature of the security and the end user's inability to circumvent these security measures. Both of these arguments would be good ones. However, we believe there is much more to the move.

It appears that Google correctly understands the fundamental shifts that are slowly evolving in the enterprise and government markets. Both these sets of large end users of IT want to implement security as a part of their infrastructure, but more importantly they recognize that end users want to be increasingly untethered and less concerned about the "form" of IT and more concerned about its utility. The wave of software-as-a-service will build until it reaches tsunami proportions. Users are now bouncing between desktops, laptops, and PDAs/Smartphones. They don't have brand loyalty to a particular software or hardware company and want to be able to connect and function when it's convenient regardless of where they are or what end-point device is at hand. Many governments in particular are looking for a way to reduce their Microsoft bill. Some such as Japan have looked at Open Source as a way to accomplish this, but this solution hasn't gone far enough. Consequently we congratulate Google on correctly moving to where technology is going rather than where it has been. We believe Google will continue to develop and/or acquire pieces that will help develop the virtual, secure workplace and that the Postini acquisition was only a first step on what promises to be a journey worthy of Harry Potter himself.

The Sageza Group, Inc.
32108 Alvarado Blvd #354
Union City, CA 94587
510·675·0700 fax 650·649·2302

Cisco + EMC + Microsoft + Others = SISA

By Clay Ryder

Cisco, EMC, Microsoft, and three others have announced the formation of the Secure Information Sharing Architecture (SISA) Alliance to develop IT architectures that permit only authorized personnel access to specific information while easing the management of shared, protected information across trusted communities. The SISA combines industry-leading applications, information infrastructure, and networking technologies to help protect customers' IT investments while enabling the sharing of sensitive information such as finance or HR, for example, more effectively among authorized communities. The three major companies are providing the core off-the-shelf technology that comprises SISA. Cisco will provide network protection, security-enhanced virtualized network links, and data protection features for sharing sensitive information across the network. EMC's storage systems, information management, and security software will provide the infrastructure for storing, managing, and protecting critical and sensitive data. Microsoft will provide identity management, client and network operating systems, and a collaboration framework that helps keep content in the hands of authorized users. In addition, there are three other alliance members: Liquid Machines, a content protection provider that extends Microsoft DRM technology; Swan Island Networks, which designs and operates sensitive information-sharing systems; and Titus Labs, a provider of labeling and classification solutions.

The alliance has agreed upon a partner-led go-to-market strategy, with a three-tier certification program to provide potential SISA customers a range of delivery partners offering a variety of strategy, technology, and business services. SISA delivery partners will receive training as part of the certification program that will validate the capabilities of SIs and other professional service firms to provide implementation, administration, and analysis support to SISA customers. The formalized business alliance will be managed by Addx Corp., which has established the SISA Joint Program Office to manage the solution architecture and SI certification process.

Industry Alliances and Consortia appear to come and go as often as the wind changes direction, but in this case we believe that SISA will probably have more staying power, and hence more impact in the marketplace, with its quest to drive awareness and deployment of information security and management solutions. The three large players in this alliance bring many of the requisite pieces to the table given their established credentials in managing users' access, storage, and network connectivity as well as having some degree of longer-term cooperative relationships amongst themselves. Although one could argue about where the true center of gravity lies in the SISA scheme, we tend to point to the data as the logical place, as without the data to protect and manage, the rest of the initiative is largely moot. This is where the light shines on EMC's expertise as illustrated by the many and varied software acquisitions the firm has made over the past several years, especially RSA. The extent of knowledge regarding the data being stored within EMC's solutions provides the underpinnings to support a policy- or business-processed focused point of view with respect to data, and—dare we say—information management.

The growing collaboration between EMC and Microsoft is evident in this alliance as are the relationships with Cisco, who over the past couple of years has stated its desire to be in the storage management (albeit with a somewhat different definition) space. As data must flow over the network, and Cisco is the network king, any successful security and management scheme must treat the network as a fundamental, if not inseparable, part of the information sharing, management, and storage solution. Likewise, the operating system, and user authentication/management schemes in conjunction with rights management, must share the same close relationship with the network and storage systems in order to achieve the sought-after level of control, reliability, and ease of legitimate use that SISA seeks.

We do note the absence in this industry tryst of Symantec, one vendor who, from a technology vantage point, would seem to have much to offer. However, Symantec figures prominently in the Cyber Security Industry Alliance (CSIA) that does count RSA, but not the rest of EMC, Microsoft, or Cisco amongst its ranks. Thus, CSIA as an alliance promotes one group of vendors, and SISA for the most part appears to be the marketplace counterpoint given its omission of Symantec, CA, PGP, and IBM amongst others. Vendor politics and corporate personalities can often effect alliance participation; nevertheless, as alliances mature, their membership roles

The Sageza Group, Inc.
32108 Alvarado Blvd #354
Union City, CA 94587
510·675·0700 fax 650·649·2302

often swell because of no one wanting to be left out of what may become a marketplace winner. However, an equal reticence to being first can also influence early participation.

Overall, we believe SISA has much to do for its vision to become reality. Among the challenges will be to educate and energize marketplace agreement that SISA meets a valuable need, one with which we are not in dispute, and to develop the broad spectrum of certified solutions providers to drive the solution into the market. An indication of the success of the Alliance would be visible activity by government buyers. Information sharing has been a bugaboo for some time, if SISA can deliver on the promise of secure information sharing and government agencies adopt it, it would certainly be a positive signal to the commercial sector. It would also be a potential omen to those vendors who are outside the exalted alliance circle. Given the systemic nature of what SISA offers, it would likely require a strategic assessment of an organizations infrastructure followed by creation of transitional path that would incorporate the essence of SISA into everyday operations and practices. As such, it would take time and resources to achieve, but we believe the potential dividends in sharing information across a wider community of participants while ensuring its protection and compliance with both internal and external policy mandates justifies the short-term investment for long-term payback.

Tablus and Vincera Combine For Two-Fisted Data Loss Prevention

By Lawrence D. Dietz

Tablus, a provider of content loss prevention solutions, and Vincera, Inc., a document security company, this week announced a strategic alliance to provide enterprises with a complete solution for monitoring and controlling sensitive information distributed both inside and outside of the managed network. Tablus Content Alarm NW monitors and prevents the unauthorized transmission of sensitive content off of enterprise networks via email, Webmail or file transfer. Content Alarm NW, a network monitoring and blocking solution, includes a comprehensive One-Click Policy Library, of benefit to organizations that need to ensure regulatory compliance and prevent the loss of sensitive corporate information. For businesses that require the distribution of sensitive documents outside of the managed network, the Vincera Intelligent Protection technology delivers behavioral intelligence, data loss prevention, and business rights management in one solution, enabling enterprises to protect and encrypt, monitor, measure, and manage that distribution. With automated conversion of over 300 file types to Adobe PDF, enterprise data is fingerprinted, digitally watermarked as a unique document thread, encrypted and associated to a security policy to ensure secure distribution and access for documents containing sensitive data that needs to be distributed beyond the managed network. The combination of the two solutions will enable enterprises to meet management, compliance, and audit requirements for securing sensitive information throughout the complete distribution cycle, while ensuring they are safeguarded from the repercussions of content loss.

Organizations faced with the challenge of protecting their sensitive information are being offered a growing array of technological solutions. Sensitive information is sensitive because of its content or value, not its location. Consequently, effective data loss prevention must recognize internal dangers as well as external threats. Heretofore technology vendors have tended to concentrate on either the end point, or the device holding the information, or the network that may be used to transport it. Users need to address the whole distribution cycle as a part of their due diligence.

Alliances of vendors with complementary products benefit sellers as well as buyers. Sellers can often combine their marketing efforts and reach more prospects effectively as a team than either can independently. Buyers benefit because a marketing alliance implies that the vendors have worked together behind the scenes to make their technologies dovetail, and perhaps more importantly, after-sales support is generally coordinated more effectively than if the vendors were acting independently with no established alliance or presumed ground rules. Given the impetus to data privacy and the growing mounds of sensitive data to include personally identifiable information (that information needed to assume another's identity or abscond with their assets), organizations large and small need to employ safeguard technology. Complementary alliances such as the Tablus/Vincera connection benefit the market and help ensure the longevity of the partners over time. We expect to see more such alliances and business combinations in the data loss prevention market over the next year and a half.

The Sageza Group, Inc.
32108 Alvarado Blvd #354
Union City, CA 94587
510·675·0700 fax 650·649·2302