Market Roundup

December 7, 2007

Fujitsu Siemens Computers New CentricStor Storage Solution

By Clay Ryder

Fujitsu Siemens Computers (FSC) has announced a new version of its CentricStor Virtual Tape Appliance. Version 4 features dual-target save, which provides end users the choice of backing up data to either the VTA's disk-based cache or to tape as well as thin provisioning through flexible allocation of storage resources. The latest version also expands service and maintenance functions, provides the basis for deduplication functionality, and targets the three major pain points that data protection managers face today including continued growth in data volume, increased data retention periods, and the need to support secondary data centers for enhanced disaster tolerance. Version 4 features a substantial VTL cache (up to 1PB) with support for 1,500,000 logical volumes as well as intelligent data protection whereby end users specify which information should be automatically retained on disk and which should be saved to tape according to desired service level. In addition to existing maintenance services, FSC also offers enhanced proactive services such as Live Monitoring and Health Check which can include FSC monitoring of CentricStor systems with rules-based actions that can be taken automatically in the case of an error along with regular testing and pro active risk assessment. Customers are also offered service management for their complete data protection solution including servers and tape libraries. Pricing information was not disclosed.

The mantra of "tape is dead" continues to be heard throughout the marketplace; however, the reality of simple economics combined with a new "green" twist on tape illustrates how tape continues to enjoy a viable position in many organizations. With all the focus on eco-friendly IT, tape is able to rightly claim that when idle, its storage cartridges consume no energy whereas idle disks (unless powered off) consume some amount of power. While there are many advances in current disk technologies that have substantially reduced power consumption, for archival purposes tape can presently make the greener claim. Given the astronomical rise in data volumes being stored, this is potentially a non-trivial savings especially for organizations that do not require frequent or instantaneous access to archived data. At the same time, the support for automatic backup of data whether to disk or tape based upon policy addresses a common need in organizations of most any size. This in conjunction with a larger ILM initiative can offer flexibility and overall efficiency gains with respect to data storage.

With this latest release of its CentriStor platform, FSC is demonstrating not only that it sees continued need for virtualized tape solutions, but that the capacity needed is growing as well. 1 petabyte of data is a lot, even if the organization is a Global 1000 enterprise. For the more modest of organizations commonly dubbed as SMBs this degree should meet or exceed their operational storage requirements handily. As such, FSC has a very large addressable market for this offering that, combined with the flexibility in storage approaches offered by CentriStor, places FSC in a desirable, if not enviable, marketplace position.

Madrid-Based Panda Enters U.S. Malware Fray

By Lawrence Dietz

Panda Security has announced the availability of Panda Security for Business version 4.02SP1, a multi-layered protection from malware attacks for corporate users. Panda Security for Business allows customers access to its online, on-demand audit service, Malware Radar, for detecting and disinfecting malware and other security problems that slip past the permanent protection systems installed at most companies. Panda's approach

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

automates and enhances the malware collection, classification, and vaccination process by gathering malware information from the Internet community at large, rather than locally. Panda Security for Business integrates Malware Radar to bring companies periodic non-intrusive malware audits, providing maximum security against targeted attacks, botnets, and other threats that manage to bypass traditional protection. Each discovered threat forms part of Panda Security's planetary database, which now includes more than two million samples of malware. And as an online service, this security model minimizes resource consumption on local systems.

Panda Security for Business provides several features to benefit users. Web 2.0 Protection fights Malware 2.0 by collecting information from the Internet community; complete process automation fully automates sample collection, analysis, and vaccine generation processes; proactive protection blocks unknown threats; periodic auditing reveals threats not recognized by existing security solutions; layered protection provides users with access to all network points through protection at different infrastructure layers including the desktop, server, and gateway; and remote updates enable users to update signature files directly from PandaLabs through a WiFi network. Panda Security for Business integrates three types of protection—antivirus, anti-malware, and proactive technologies—with a fourth technology Panda calls Collective Intelligence. Collective Intelligence is based on exhaustive remote, centralized, and realtime knowledge about malware and non-malicious applications maintained through the automatic processing of all scanned elements from "the cloud." This approach provides the ability to maximize malware detection capabilities, while at the same time minimizing the resource and bandwidth consumption of protected systems.

The marketplace has told security vendors that ease of use and problem elimination are the principle buying criterion. Combinations of goods and services that prevent harm to networks and the IT infrastructure they serve are usually regarded positively. The combination of antivirus, anti-malware, and proactive technologies with periodic audits and assessing the results against a global intelligence data base therefore makes a great deal of sense. We tend to believe that end users, particularly SMB, are unlikely to keep adding specialty security products to deal with the threat du jour, but are more willing to pay vendors to deal with all the details and deliver protection in the form of network reliability uninhibited by attacks, regardless of their source.

From a marketing perspective, since the U.S. is the largest security market in the world, it was only a matter of time before non-U.S. vendors stepped up their activities to grab for a piece of the pie. Madrid HQ Panda joins Moscow HQ Kapersky and UK HQ Sophos in attacking leaders Symantec and McAfee on their domestic home turf. However, long-time experience in the security market has shown us that the spoils do not necessarily belong to the best product; they belong to the product with the best sales and distribution. It remains to be seen if any of these offshore competitors can cause a blip on the U.S. security radar screen.

OpenSolaris and the System z

By Clay Ryder

Sun Microsystems and Sine Nomine Associates have demonstrated the OpenSolaris code base running on an IBM System z mainframe. The demonstration follows Sine Nomine's announcement last year of an independent project to do the port and August's announcement that IBM and Sun would investigate a project to port OpenSolaris to the System z mainframe. Sine Nomine Associates is a research and engineering firm based in Ashburn, Virginia. In the demonstration, OpenSolaris ran within the System z's z/VM, IBM's mainframe virtualization technology that enables more than 1,000 virtual images on a single hypervisor. z/VM already provides the foundation for running Linux on the mainframe. The Solaris demonstration included support for powerful Solaris features including Solaris ZFS, and Solaris Dynamic Tracing (DTrace), which help customers improve uptime, cut costs, and speed time to market.

The IT marketplace is never a dull place. The successful demonstration of OpenSolaris on a System z is another example of where a good dose of New Think at Sun is creating new opportunities for the company while also potentially stemming some of the abandonment of Solaris for Linux on alternative hardware platforms. The mainframe has continuously re-proven its abilities as a virtualized consolidation platform for a variety of nontraditional workloads including those based on Java and Linux. Solaris has a rich ecosystem of applications, but many of them have been deployed on servers that today would qualify as being long in tooth, and ready for refresh. The combination of Solaris and the mainframe offers benefits not only to IBM and Sun, but to the end-

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

user organizations as well. For Sun, maintaining the vibrancy of Solaris is essential to curry ISV and developer support. For IBM, mainframe sales offer margins and value-added solutions and services on a scale that is hard to duplicate in the industry. But most importantly, organizations can benefit from the substantially enhanced efficiency of a mainframe that requires fewer watts to deliver results than a collection of aging RISC machines. At the same time, organizations can continue to leverage their existing skill sets and software investments related to Solaris, as well as consolidate Java, Linux, and other workloads within a single physical server deployment that should significantly reduce administration and support costs.

This announcement just goes to show that there is always something percolating under the surface of the marketplace. The hardened battle position taken by Sun Microsystems in the early 21st century painted a view of the company where any solution would be welcomed provided that its was based on Solaris and ran on SPARC. If five years ago one were to suggest that in the future Sun would embrace industry-standard processors, open source its operating system, and work towards the day where Solaris would run on the mainframe, the Copernican Company would be the first to disparage such tomfoolery as the obvious antics of a deranged industry malcontent. Well, all hyperbole aside, over the past couple of years Sun has done many things that were once unthinkable. To our way of thinking, this is Sun operating at its brightest and best.

Website Vulnerability Scanning Software from WhiteHat Addresses Several Market Needs

By Lawrence Dietz

WhiteHat Security has introduced Sentinel Standard Edition as the latest addition to the WhiteHat Sentinel Service family. Sentinel SE is a service delivering an enterprise-class, ongoing Website vulnerability scanning service with 100% verified, actionable results, shifting the focus from finding vulnerabilities to fixing them. Sentinel SE, built on WhiteHat's SaaS technology platform, tests for the thirteen technical Website vulnerabilities (including SQL Injection and Cross-site Scripting) as defined by the Web Application Security Consortium. The product is broadly targeted to Fortune 500 companies with hundreds of Websites to small startups with only a few. Sentinel SE is designed for less complex, lower-risk websites, where code changes are relatively infrequent. Sentinel SE also provides compliance with section 6.6 of the PCI Data Security Standard, which mandates that all merchants and service providers that store, process, or transmit cardholder data institute a review of Website code by an organization that specializes in application security, or provide an application-layer firewall by June 30, 2008. Sentinel SE and Sentinel Professional Edition offer customers unlimited scanning during the annual subscription period. WhiteHat Sentinel SE provides baseline website security with full API access and email support from the WhiteHat Security Operations Team, and is currently available for an annual subscription of $9,950 per Web application. WhiteHat Sentinel Premium Edition is also currently available for $24,000 per Web application per year. In addition to the features available with SE, Sentinel PE includes custom business logic testing, an operations team, and proof of concept testing for vulnerabilities to demonstrate exploitability.

Website attackers will likely continue to adapt their efforts to take advantage of soft targets. Websites, unlike many networks, are designed to be open and inviting. Furthermore, Websites have become the most common online sales vehicle, and consequently are likely to be high on the target list of digital criminals. It also appears that Payment Card Industry standards have induced more purchases of security-related products than have laws and regulations. Consequently this announcement by WhiteHat appears to be on target in terms of its intended markets.

Having said all this, we are always a bit skeptical of products that are targeted at both large enterprises and small businesses. We don't subscribe to the one-size-fits-all theory. Clearly PCI standards apply to small businesses as well as to large ones; however, a $10K nut is pretty steep for a small business. Over time we might expect vendors like WhiteHat to approach the SMB market employing a software-as-a-service model wherein the customer pays a monthly fee based on usage and where there might be no commitment to long-term contracts. In any event we expect to see competition increase in the Web application security space with service providers perhaps offering this service as a means to differentiate themselves, charge premium prices, and oh yes, be of service to their customers.

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