Market Roundup

February 16, 2007

New OpenSolaris Distribution for Developers

By Clay Ryder

Sun Microsystems has announced a new set of products and services targeting developers, startups, and Internet companies seeking to build and deploy their Web infrastructure on Solaris 10. The three offerings are Solaris Express, Developer Edition, Solaris + AMP (Apache/MySQL/PERL or PHP), and an expanded Sun Startup Essentials program. Solaris Express, Developer Edition is the first distribution based on the OpenSolaris project and provides developers an integrated environment for the development of applications for Solaris, Java technology, and Web 2.0 while supporting a variety of common x86-based desktop and laptop hardware with a simplified installation experience. This release includes an improved GNOME-based desktop, Sun Studio 11, NetBeans IDE 5.5, as well as 150+ open source applications. Solaris + AMP offers popular open source applications that have been optimized for Solaris, including the Apache web server, MySQL, PostgreSQL, PERL, PHP, and Python, as well as other developer and open source technologies. Sun is also posting "recipes for success" that feature systematic instructions as well as multiple levels of Sun Services. The company also expanded its Startup Essentials program to offer an improved buying experience through streamlined, online access to Sun hardware, including Sun Fire x64 servers and Sun Fire servers with CoolThreads technology running the Solaris 10 OS or other operating systems. Sun has now added Sun StorageTek modular disk arrays, NAS, and tape storage products to the program at deeply discounted prices. Lastly, Sun also announced Developer Services that provide specialized advice for programming issues relating to Solaris Express, Developer Edition on a per incident basis with guaranteed response times through Sun Developer Expert Assistance Service. The service is available to all developers with a cost of $49 per incident or unlimited requests for an annual subscription of $249. Developer Expert Assistance Service will be available for Solaris + AMP stack at the end of February 2007 with full production support on Solaris available early this summer.

As Sun continues to reinvent itself, it is not surprising to see programs targeting constituencies that may not automatically consider themselves as part of the Sun faithful. Smaller, Web 2.0-oriented firms sound like the natural playing field for Linux, low-cost industry server, and the open source movement: something that by perception would not seem to be in the bailiwick of Sun Microsystems… or is it? Judging by its actions, Sun's affinity for the volume server marketplace only seems to be growing. Its strategic relationship with AMD, and now Intel, illustrates a desire to reach the volume hardware platform in the marketplace. With its embrace of Open Source, especially with respect to Solaris, Sun has fundamentally changed its position in the lower echelon of the computing marketplace. However, simply rediscovering the x86 architecture is not enough, and Sun, to our way of thinking, has wisely taken many steps to make itself relevant again in this marketplace.

Startups and leading-edge companies, which encompasses most anything labeled Web 2.0, all live in a world of limitations, be they financial-, human-, market-, or time-based. By packaging Solaris-proven versions of the most popular Open Source applications and tools, offering recipes for success, and backing it all up with a modestly priced support package, Sun has made itself germane to this market segment. Combined with the newly enhanced

Startup Essentials program, Sun has taken this a step further and, most importantly, made its offerings affordable and financed in a way that matches the reality of the potential customer base.

While for many, Open Source may be all about the source code, the reality is that the binaries distributed are what are truly important. Solaris Express is not a listing of source code, it is a tested and support distribution of that source code that Sun is backing up with support. The Sun + AMP stack reinforces the value proposition by delivering Solaris-tested and -certified binaries of popular Open Source application. While all of the source can be freely viewed, the value proposition is that off the shelf, the code works, and customers can focus on developing their intellectual property, not fuss about testing the open communities' product.

Driving the ecosystem around any platform is essential, as this ecosystem provides the lifeblood of the platform. In this instance, the ecosystem may seem to be a collection of freely available software issued for the betterment of society. However, Sun correctly sees that without the solid commercial backing of a heavy hitter in the industry, this community will not thrive to its potential. For the target market, we believe Sun has done a fine job of making itself pertinent again to a market segment that a few scant years past would have likely dismissed the notion of Solaris and Sun altogether. While there is much work and outreach to be done, we are impressed with the tenacity that the Copernican company has illustrated under its new executive management and its repositioning of itself as a player to be considered by organizations who do not find themselves at the top end of the computing marketplace.

NeoScale and Symantec: Symbiosis in Action

By Lawrence D. Dietz

NeoScale Systems Inc., an enterprise storage security solutions vendor, has announced that its CryptoStor Tape security appliance has been qualified by Symantec Corp. and HP within their respective testing programs, the Symantec Technology Enabled Program (STEP) and the HP Tape Automation Compatibility (TAC) Partner Program. These qualifications provide Symantec and HP customers with the assurance that NeoScale data security solutions integrate with their preferred backup technologies. NeoScale CryptoStor security appliances are deployed on the storage network and deliver wire-speed encryption, compression, and cryptographic authentication of data on tape. They integrate with NeoScale CryptoStor KeyVault appliances, which provide centralized key management across heterogeneous devices for rapid information recovery from authorized locations. NeoScale's CryptoStor Tape has been validated for interoperability with Veritas NetBackup from Symantec. As part of the HP TAC Partner Program, CryptoStor has been tested for compatibility with HP tape libraries and is now included on the HP StorageWorks Enterprise Backup Solution (EBS) Compatibility Matrix. The latest round of integration recognition demonstrates the commitment from leading backup vendors to support NeoScale 's encryption technology to secure customers' sensitive data.

The NeoScale solution is also now included on the HP StorageWorks EBS Compatibility Matrix, a public document that provides information for designing data protection solutions, including backup/restore and archiving, that scale from entry-level workgroups to enterprise-level datacenters. By HP StorageWorks tape libraries with the NeoScale CryptoStor Tape security appliance HP customers can employ data encryption if they so chose.

Symbiosis in nature is a relationship between two different species of animals where at least one of them derives some benefit. Among the more interesting pairs are the Egyptian plover bird and the crocodile. The bird helps the croc by eating parasites on his body and mouth while the croc offers protection to the bird. While we are certainly not comparing either vendor to an animal, never the less large vendors need an ecosystem of smaller, generally specialist vendors to reinforce the market position of the large vendor. For its part, Symantec with its heavy reliance on NetBackup as an anchor to its product line has recognized that there are advantages to linking backup and security services. Having exited the appliance business, Symantec recognizes that some appliances have their place. Encryption appliances in particular may be a viable option for organizations who want to have secure, yet easily recoverable data.

Sageza believes these relationships are good ones. NeoScale, the smaller firm, benefits through association with the larger, more well resourced vendor and VARs may be the ultimate beneficiary by offering the consulting and support services necessary to implement and support the combination. The concept of “secure yet available” data is likely to take on more value partially because the new U.S. Rules of Civil Procedure require an early meeting between the parties to agree on initial electronic discovery procedures and production. The contentious nature of litigation and the court’s history of generally refusing to take a technological excuse for lack of availability may also help stimulate this product combination.

HP Unveils Latest HP-UX 11i

By Clay Ryder

HP has introduced the latest version of the HP-UX 11i operating system and new HP Integrity servers. The latest release, HP-UX 11i v3, focuses on making virtualization easier to deploy while delivering mission-critical virtualization for applications such as business intelligence and data warehousing, and providing mainframe-class availability. HP-UX 11i v3 can address up to 100 million zettabytes (100 billion TB) of storage and features new hot-swap and online patching capabilities that aim to reduce downtime. Binary compatibility with past releases ensures that applications will run unchanged on HP-UX 11i v3 with the company-noted benefit of executing an average of 30% faster. The company also announced a new rack-optimized unit, the Integrity rx2660 entry-class server, as well as the HP Integrity BL860c Server Blade, the first Integrity model for the HP BladeSystem c-Class. The HP Integrity rx2660 targets application-tier workloads and is positioned as a versatile solution for porting, application serving, testing, and development. Although the new server targets smaller deployments, it offers business-critical computing, and HP-UX features including VSE, HP Serviceguard, and HP Systems Insight Manager. The new HP Integrity BL860c Server Blade targets database-intensive applications and scientific computing environments and offers a powerful virtualization engine for application consolidation, which can help drive down total cost of ownership. HP also noted the availability of four new Virtual Server Environment (VSE) Reference Architectures, including Oracle, SAP software, and shared services based on HP’s own application server and database implementations. A base configuration of the HP Integrity BL860c Server Blade is priced at $3,827 and is expected to ship in March. A base configuration of the HP Integrity rx2660 has a starting price of $4,931 and is available now. The HP-UX 11i v3 operating system is now shipping at lower prices for OS and some of its supporting software.

UNIX, much like the Mainframe, is the platform that has been pronounced stale, in decline, or even outright dead, but which simply refuses to die. In the world of mission-critical back-office computing, or super-high-performance installations, UNIX continues to deliver value to organizations across industries and the globe. True to form, we see HP’s penchant for engineering illustrated in this release. The company’s notion that virtualization is a key technology is well supported by its continued investment in the VSE and the latest reference architectures. Although most larger organizations have a cadre of IT professionals inhouse, there are often few spare human resources available to weave from whole cloth a well thought out architecture and deployment plan for new technology installations. Knowing the right thing to do and having the time or resources to do it are two very different things. This is where the value of VSE Reference Architectures is readily apparent. By bringing tried and tested approaches to the table, HP has removed one of the barriers that may be impeding organizations’ greater deployment of virtualized solutions, especially with respect to primary back-office or business-critical applications.

For those who have made a strategic commitment to the blade architecture, we believe the availability of the Integrity BL860c will be well received. As this is the first Integrity blade for the new c-Class BladeSystem enclosure, organizations that have been actively migrating and consolidating their x86-based applications now have the opportunity to expand their efforts to include their Integrity workloads. This achievement is more than simply adding another kind of blade to the mix, but rather bringing together HP’s two main processor families within the IT unifying framework of the blade architecture. Organizations can now much more easily make the strategic decision to unify the bulk, or in some cases all, of their IT infrastructure within the blade environs, servers, storage, and the like. For shops with mixed HP environments, this could prove tantalizing.

Overall, we are pleased to see that HP continues to value its HP-UX heritage while at the same time looking to increase the flexibility and options afforded its customers that base so much of their business well-being on HP’s UNIX platform. With Sun’s recent focus on driving Solaris into new and interesting places through attention to

Open Source and OpenSolaris in particular, it is interesting to note HP's reduced pricing for HP-UX. However, price alone does not make an operating system, and neither solely does being open source. It is the value proposition afforded by its use that is determinant. HP maintains a strong ecosystem of partners and third-party technology providers that support its platforms, which is essential for its long-term success. All said, it seems that February is a good month for the UNIX marketplace.

Sophos Mobile Security: Shooting ahead of the Target

By *Lawrence D. Dietz*

Sophos this week announced the availability of Sophos Mobile Security to protect organizations against the growing number of malware attacks aimed at Windows Mobile. Sophos Mobile Security provides realtime protection for Windows Mobile 5.0-based devices against mobile viruses and spyware threats and enables IT administrators to implement and lock down security policies for PDAs and cell phones. The vendor stated that the mobile malware threat has been steadily increasing over the last few years and more businesses are now looking to secure confidential data against potential attacks at all endpoints. In a recent Sophos web poll, 81% of business IT administrators expressed concern that malware and spyware targeting mobile devices will become a significant threat in the future. However, 64% also said they currently have no solution in place to secure company smartphones and PDAs. Sophos Mobile Security protects devices against malware infection via MMS, SMS, email, instant messaging, WiFi, and Bluetooth, ensuring business communications are kept secure. It offers on-access, on-demand or scheduled scanning and detects and quarantines any mobile viruses or spyware with minimal impact on device performance. Central policies can be created and deployed to ensure consistent company-wide security. Sophos Mobile Security is bolstered by Sophos Behavioral Genotype Protection technology, which proactively blocks new and unknown mobile threats before they execute. Network administrators are alerted with realtime notification of malware incidents, ensuring threat activity is monitored and neutralized, reducing the impact on employee productivity. Sophos Mobile Security supports Windows Mobile 5.0 for Pocket PC Edition and Windows Mobile 5.0 for Pocket PC Phone Edition. This version will also protect devices using Windows Mobile 6.0 which Microsoft plans to launch later in 2007.

Sophos is not the first to offer a product aimed at protecting mobile devices from malware. Both McAfee and Symantec have products in this space. So if it's not new and the dominant players in the market already have similar products in the field, then why bother writing about it?

Simply stated, the threat of malware on mobile devices represents a classic security conundrum. On one hand organizations will readily concede that they are highly dependent on these new endpoints and that the use of the devices is growing at all levels within the organization exacerbated by the fact that the technology continues to advance providing yet more bells and whistles. On the other hand, the threat has not yielded any horror stories of successful attacks and there are many other demands on IT budgets in general and on allocations for security in particular.

Sageza believes that attacks on mobile devices will gradually increase as targeting becomes more sophisticated and focused. There is a growing body of evidence that indicates that cybercrooks are following Willie Sutton's apocryphal advice to rob banks because that's where the money is. As more criminal and hostile elements (read "nations and terrorists") become more sophisticated and blend social and technological attacks they will exercise more specificity with respect to devices and malware of all types will become more prevalent. The trick for end users however is to close the door before the horse gets out and employ the mobile protection before they become target rather than after.

Can KeepYouSafe Keep You Safe?

By *Susan Dietz*

Information Survival LLC has developed a service called KeepYouSafe Online Safe Deposit Box. This is an encrypted storage service that utilizes a 256-bit AES encryption key aimed at enabling users to send and receive sensitive email files securely. The online service also works as a virtual safe-deposit box, also encrypted, available to the person with the key at any time, anywhere in the world where the Internet is accessible. The key is only available to users; the company does not carry a spare and employees reportedly do not have access to any information. In fact, the company website urges that users write down their password as a failsafe. Traditionally, encryption services are difficult and technical, making them tricky for the typical end user to fully utilize. KeepYouSafe's goal is to enable average end users to easily encrypt sensitive documents without slowing down the email to do so.

Encryption of email used to be only the concern of big companies and governments; what need had Joe Q. Public to encrypt an email to his mother? However, as more business is conducted online, SMBs and individuals in sensitive jobs such as physicians and attorneys, and in particular medical and legal offices, may be drawn to the service. Emails sent to patients and clients containing sensitive information probably should be encrypted; some professions, such as the law, require confidentiality on the part of their practitioners. However, in the real world how much expectation of privacy do people really have once they send their information out into the Net? "Not much," is the answer that Sageza picked up at the recent RSA show.

Historically there have been some issues about providing hard-to-break cryptography for general use. The founders of KeepYouSafe are both members of the United States Secret Service New York Electronic Crimes Task Force, so it seems counterintuitive that they would develop a service that would help break the law. On top of their own security measures, they have contracted with another company to run a daily check of their perimeter, plus they have the option of running two-factor authentication for users. Will the public trust that the keepers of the vault won't be entertaining themselves, or worse, selling the contents of the vaults? We have been assured that as all contents are encrypted, and that the key itself is encrypted, there is no way that employees could view the contents of either the emails or the boxes.

While the U.S. Congress has been kicking around various ideas of legislation, protection legislation is generally technology-neutral. We have seen California lawyers advised to protect confidential email and it would appear that this service may be a relatively painless way to protect their clients. ISPs may become early adopters of this technology as a way to differentiate themselves in this highly competitive field and as a way to field a premium service at a premium price.

Given that much commerce is electronic today, some SMBs, especially those dealing with sensitive data or trade secrets, will most likely provide encryption service as a "must-have" rather than a "nice extra." Those not inclined to trust anyone will probably then have to choose which will seem the least likely target for hackers, a giant ISP storage vault or a heavily-fortified encryption service. One might want to sign up early at the encryption office.