sageza

Market Roundup
September 20, 2002

IBM and Intel

By Joyce Tompsett Becknell

This week IBM and Intel announced their intention to jointly design and develop modular server solutions, also known as blade servers. The companies will focus on three aspects of development: system and chassis development, networking infrastructure, and systems management. The two companies aim to produce blade servers that provide scalable performance and reliability features at a lower total cost of ownership. IBM plans to soon launch blade servers that will incorporate Intel Xeon family processors as part of a solution, and Intel intends to provide blades to its OEM customers based on the Xeon architecture. The companies will be able to offer the portfolio of jointly developed products to their respective customer bases.

IBM states that blade servers are expected to reduce costs with improved systems management, simplified provisioning, and increased reliability. These goals are not particularly surprising, as most vendors are designing systems and architectures to solve these rather pertinent customer issues. What is interesting is the bit where IBM argues that they will not sacrifice performance for increased density. And indeed poor performance has been the bugbear that has limited customer adoption of blade systems so far. The first generation of blades has not been able to maintain attractive price/performance ratios. Customers performing comparison tests have frequently found that pizza box servers provided better performance for the price even with server density factored in.

IBM and Intel maintain that IBM's experience with architecture and systems design combined with Intel's expertise in building modular servers, chipsets, and software optimization will provide the best of both worlds and produce the new generation of blades that will genuinely provide the capabilities customers are looking for. Sageza believes that this is a win for both companies. For Intel, selling more blades means selling more processors. And creating an OEM system that beats vendor solutions gives Intel opportunities to sell greater volumes of higher-margin products. For IBM, this is the opportunity to replicate their success in the original PC market. Once again IBM can create a system that becomes the standard for the next generation of modular computing. Sageza also believes that the focus on improving performance is a win for customers. Without addressing this issue the blade market will be just another fad that fades when customers find alternate ways to address the problems that blades were meant to solve. By focusing on increasing performance as well as better manageability, reliability, and serviceability, the evolution of blade computing will affect the evolution of SMP and its role in modular computing as well.

The Sageza Group, Inc.
836 W El Camino Real
Mountain View, CA 94040-2512
650·390·0700 fax 650·649·2302
London +44 (0) 20·7900·2819
Munich +49 (0) 89·4201·7144
Amsterdam +31 (0) 35·588·1546

Microsoft Offers WiFi Hardware for the Home

By Jim Balderston

Microsoft has announced that next month it will begin selling Microsoft-branded home wireless networking hardware based on the 802.11b standard and use the Intersil PRISM WLAN products as its core technology. Among the items Microsoft will be selling are: a wireless base station ($149.95), a wireless USB adapter ($79.95), a wireless notebook PC card adapter ($79.95), and kits including both a base station and adapters for notebooks or USB connections ($219.95). The company will also offer wire 10/100 Ethernet gear as well, including a base station ($79.95), USB adapter ($29.95), a notebook adapter ($39.95), a PCI adapter ($24.95), and a 5-port switch ($39.95). The wireless hardware will include a 128-bit encryption that is turned on by default, a network address translation (NAT), and a built-in hardware firewall. The company also offers further security through its browser-based Base Station Management Tool, such as address filtering and parental controls.

Its déjà vu all over again. Microsoft, the world's largest software maker, has never shown any real interest in becoming a hardware vendor — a la Sun, HP, or IBM — but it has repeatedly dabbled on the periphery — or should we say peripherals? Branded keyboards, mice, joysticks have all shared a common strategy: to drive forward the value proposition of the PC, and of course drive sales of Windows software. This latest foray into branded hardware seems right on track with those earlier initiatives.

Windows XP has a significant amount of easy-to-use networking capability built into it. By offering its own branded WiFi hardware we believe Microsoft is trying to assure that these new capabilities are actually used, especially in homes and small businesses where the non-alpha-geek user would rather not participate in the head-scratching (and sometimes fist-pounding) rituals of trying to make multi-vendor products work together. Utilizing features like Internet Connection Sharing (ICS), not only will this initiative drive sales of XP, it will elevate the status of that PC to an Internet server. This will also make the proposition of wireless handhelds and multiple PC environments in the home a much more viable and attractive proposition, which of course means more software sales. Looking a bit farther down the road, establishment of the PC as the home/small business Internet server will open up a host of opportunities for connecting and managing non-PC devices that have IP capability. This will position Microsoft to own the software and networking environment that will be pivotal in establishing what Bill Gates has called the Internet Lifestyle. Entertainment systems, including TV's, audio systems, digital recording devices, and interactive gaming, as well as medical monitors, HVAC systems, security systems, and more will all become part of the network managed through a Windows PC. Looking forward to living like George Jetson? Let's just hope it doesn't turn into Fahrenheit 451.

IBM Upgrades Web Services Security

By Jim Balderston

IBM has announced new software to further secure Web services based on the WS-Security specification. The new software will allow IBM customers to secure transactions with partners regardless of what type of web services or security the partners are deploying. IBM's WebSphere Application Server Version 5 will support WS-Security in the fourth quarter of this year and the Tivoli Access Manager will do so early in 2003, according to IBM. The new capability in WebSphere and Tivoli Access manager will feature out-of-the-box support for the XML Key Management Specification, and, in the future, other identity standards including Security Assertions Markup Language, Kerberos, and XML Digital Signatures. The new software will also allow WebSphere customers to automate the process of created trusted relationships with partners, whether they are using Microsoft TrustBridge, Kerberos Tokens, PKI credentials, or other methods to be developed in the future. IBM also plans to offer higher granularity authorization for SOAP transactions within the Web service environment.

Essentially, IBM is enjoying the fruits of being Big Blue. For big systems vendors like IBM, with its well-entrenched place in the market, the company can avoid the risks smaller vendors must take when it comes to

The Sageza Group, Inc.
836 W El Camino Real
Mountain View, CA 94040-2512
650·390·0700 fax 650·649·2302
London +44 (0) 20·7900·2819
Munich +49 (0) 89·4201·7144
Amsterdam +31 (0) 35·588·1546

betting on a particular standard and its future market share. For smaller companies, such a bet is often fatal. Here, however, we see IBM rising about the fray of multiple computer security standards and offering its customers a product that does not bind them (or their suppliers) to single standard. Of course, it doesn't hurt if you are one of the co-authors — with Microsoft — of the WS-Security specification in the first place. That's a privilege reserved for big market dominators as well.

IBM's customers are the end beneficiaries as they are theoretically released from the cursed vendor lock-in when it comes to creating trusted relationships with partners and suppliers. To many companies, the ability to be able to reach beyond a supplier base artificially constricted by islands of non-interoperable security schemata could become a real boon. Creating and managing a series of trusted relationships with the broadest array of available suppliers offers a much more flexible — and market driven — supply chain, no doubt of keen interest to many companies fighting to hold on to margins in a tightening economy. Such margins and efficiencies will only provide greater benefit as general economic conditions pick up. In short, IBM rightfully sees no need — or benefit — to itself or its customers from picking a single security standard and asking everyone to fall in behind it. Why have an ice cream cone when you can have the whole store?

Feds to Drive IT Security?

By Jim Balderston

The White House and FBI released a 65-page draft report entitled "A National Strategy to Secure Cyberspace" outlining the federal government's plans to enhance national IT security in the public and private sectors. The plan as it is presently laid out is largely voluntary for the private sector, with government agencies more on the hook to meet deadlines and security standards, when finalized. As it is now, the plan asks industry to consider conducting a gap analysis on security research and development, and ideas surrounding more government-funded research. The report contains a number of charts showing the increase in attack incidents and responses in recent years, as well as details on the growth of Internet domains. The report includes a hypothetical scenario in which terrorists take over a variety of U.S. infrastructure IT networks, such as the air traffic control system, and shut them down. The document also outlines overall strategy and policy. Notable is the statement that formal regulation to enhance security will not be pursued. The plan lays out threats to the individual and enterprise environments, and calls for greater awareness of threats and the need for public-private partnerships.

While the war on terror continues to run its course, it come as little surprise that the Federal government would propose some sort of response to the risk of what has been dubbed a "digital Pearl Harbor." While this draft report indicates that at least some level of the federal government is focusing on the potential threats in cyberspace, the lack of substantive proposals indicates that much any real meat of a national strategy has yet to be formulated. In short, this document contains little more information or insight than most mid-level IT managers possess today.

The administration's insistence on avoiding any sort of federal regulations for the private sector comes as no surprise. However, the lack of meaningful, positive incentives for the private sector to up its evaluation of — and thereby its investment in — IT security would seem to leave much of the response to a digital sneak attack in the hands of budget-hamstrung IT administrators. In short, little will change. Perhaps the brightest note in the document is the possibility of government investment in IT security, whether through mandated minimum security requirements for federal agencies or ongoing research in the academic realm. The former will certainly pay dividends to the struggling IT sector in the near term; the latter may provide relief in the long term. Yet, as we review the sum and total of this proposal, we see it more as a fire drill, one in which the alarm is sounded by little actual fire-fighting takes place.

The Sageza Group, Inc.
836 W El Camino Real
Mountain View, CA 94040-2512
650·390·0700 fax 650·649·2302
London +44 (0) 20·7900·2819
Munich +49 (0) 89·4201·7144
Amsterdam +31 (0) 35·588·1546