Market Roundup

February 18, 2005

In a Good Place

IBM Chiphopper Automates x86 Linux Applications Ports to IBM Platforms

Ooops

Cisco Secures New Level of Network Protection

In a Good Place

By Jim Balderston

Novell made a series of announcements this week at LinuxWorld focused on the company's continuing efforts to advance its place in the Linux universe. The company announced it will deliver products to harden Linux for business-critical applications; it has new datacenter solutions based on its SUSE Linux including its PolyServe Clustering software; it is now offering Open Enterprise Server; with IBM, it has completed a new higher level of security certification for SUSE Linux; it is launching the Open Source Collaboration Server Initiative; it now offers perimeter security for Linux; and it has contributed more Linux code to the open source community. In these announcements Novell continued to stress the viability of Linux from the desktop all the way through to the data center.

Novell has done a very good job of recasting itself in the last eighteen months. Novell Netware —while still enjoying a substantial installed base — is not the first topic on everyone's lips these days. Once a major part of the IT world, Netware has slowly drifted out of the spotlight. Recognizing this, Novell scooped up SUSE Linux as part of a larger commitment to both Linux and open source development and has as a result put itself much more in the center of IT developments. Novell is relevant once again.

And in our mind, the company is in a good position to continue maintaining its relevance going forward. Not only are its investments in Linux paying off with more visibility and credibility in the markets, it is also building a sustainable revenue path going forward. It is not coincidental that we see in Novell's LinuxWorld press releases the presence of Big Blue, which has become an increasingly integral part of SUSE Linux and, therefore, Novell's fortunes. By hooking up with a dominant vendor like IBM, Novell has the opportunity to make its way into hundreds — if not thousands — of potential customer sites that it would have had little or no access to before. Perhaps there are a few NetWare sales within these customers, but no matter. With IBM's Linux on Power initiative moving ahead full speed, it would appear that Novell has found a niche in which it can leverage its existing brand value while remaking that brand going forward. Not a bad place to be at all.

IBM Chiphopper Automates x86 Linux Applications Ports to IBM Platforms

By Rob Kidd

This week IBM, with business partners Novell and Red Hat, introduced Chiphopper to encourage ISVs to port x86 Linux applications to the zSeries and POWER architectures, by automation of the porting process. Chiphopper, formally called IBM eServer Application Server Advantage for Linux, is a combination of testing tools, support services, port certification, sales and marketing assistance, and post-sales support. IBM is providing a Linux Standards Base application check tool and other technology to validate cross-platform applications. Once an application has passed the automated tests, IBM provides free access to IBM innovation centers where ISVs can do live final applications testing on IBM hardware. At completion IBM provides ISV application certification, demonstrating IBM backing and port validation. IBM then provides the ISV with industry-specific application sales and marketing assistance, and offers the ISV post-sales application support for up to two years. Chiphopper

The Sageza Group, Inc.
32108 Alvarado Blvd #354
Union City, CA 94587
650·390·0700 fax 650·649·2302
London +44 (0) 20·7900·2819
Milan +39 02·9544·1646

is available immediately worldwide at no charge to ISVs. IBM also announced the creation of special interest communities in conjunction with Chiphopper, to provide a one-stop help source to assist ISV customers in migrating from Solaris and Windows to Linux.

The number and quality of applications available for a hardware/software platform is an important factor in determining the platform's market success, and the wider the range of platforms that an application runs on, the higher the probability that the application will succeed. The Chiphopper offering allows ISVs to cost-effectively increase both their customer reach and revenue opportunities by enabling their Linux applications to operate across the entire IBM eServer product line, from entry-level x86-based servers to blades and clusters; from POWER-based servers to Linux on the mainframe. IBM is influential and has made a significant investment in open source which increases Linux market value and provides customers a high degree of ISV application assurance. IBM has approximately 6,000 applications that run on Linux x86, with plans to double the number by 2007. IBM expects a large number of these applications will be ported, significantly adding to the current thousand or so applications available on the Linux POWER architecture and zSeries. Such a scenario would benefit IBM, the ISV community, and the Linux and Open Source movement in general, and make Linux more of a key driver for the application services business.

It is IBM's hope that the special interest communities will help drive Linux adoption at the expense of Sun and Microsoft. Over the last several years Sun's ISV base has been eroding, and if the Solaris-to-Linux interest community fulfills IBM's hopes, it would accelerate the process. Windows Server customers now have an additional incentive and vehicle to aid in Linux migration, and with the delay of Longhorn this could prove more than just a minor irritation to Microsoft. IBM's focus is on the customer as the ultimate beneficiary of Chiphopper and the special interest communities. With the expanded Linux application portfolio on IBM platforms, it becomes less likely that lack of an application will be an impediment to Linux migration and adoption. Add to the equation the IBM value propositions such as mainframe Linux, value-added functionality such as virtualization and middleware, and the IBM reputation for mainstream, mission-critical datacenter computing, and IBM's vision of driving customers to Linux on IBM platforms becomes more probable.

Ooops

By Jim Balderston

A Georgia-based data collection company publicly acknowledged this week that more than 100,000 people nationwide had been exposed to identity theft when the company sold personal and financial information to scam artists who obtained the information on false pretenses. The company, ChoicePoint Inc., initially said it would notify the 35,000 Californians of the exposure of their data since they were required to by California law, but would not do so with the other 65,000 people since they were not required to by any state or federal laws. News reports indicate that some 700 people whose data was taken from ChoicePoint have already become victims of identity theft. The company decided later in the week to send letters to more than 110,000 people whose information may have been compromised, regardless of what state they lived in. California law enforcement officials indicate that the 110,000 figure may be too low and that in fact more than 500,000 people may be at risk due to the thefts. ChoicePoint has bought fifty data collection companies in the past few years and has substantial files on nearly every American citizen.

ChoicePoint's original refusal to notify all potential victims raises yet again the conflicts and changes being forced upon societies by communications networks that cross state, federal, and international borders. ChoicePoint's original position was in keeping with applicable laws, despite the fact that the company did business across state lines and that its failure to properly protect data affected people nationwide. California's law requiring notification to the affected parties makes complete sense for the residents of the Golden State but leaves non-Californians in the dark. Clearly laws like this one need to become more universal, so that a company less prone to bending under public pressure would be forced to notify all affected parties.

ChoicePoint officials said that they were not to blame for the theft; that the parties requesting the information appeared legitimate at first glance. These officials said they would take responsibility for the thefts but argued they

The Sageza Group, Inc.
32108 Alvarado Blvd #354
Union City, CA 94587
650·390·0700 fax 650·649·2302
London +44 (0) 20·7900·2819
Milan +39 02·9544·1646

were not to blame because the thieves were smarter than they were. Perhaps so, but the aggregation of personal and financial data on the scale ChoicePoint has achieved makes it an extremely tempting and potentially lucrative target for sophisticated identity thieves. In an age where information is both figuratively and literally money, safeguards against inadvertent release of such data should be protected in a way that few if any thieves could penetrate. We suspect that regulations and guidelines for such data will be forthcoming as more and more of these incidents occur. We believe regulation will be a plausible corrective for this kind of theft, given that it was human error, and not a breakdown of security technology that led to the exposure of the data. There is no technology to prevent that historically repetitive fault, but forcing people to obey laws that prevent them from making catastrophic errors is at least a start.

Cisco Secures New Level of Network Protection

By Joyce Tompsett Becknell

Cisco has announced the next step in strategic plans to advance security offerings for its networking products. Entitled Adaptive Threat Defense (ATD), the offering consists of new products, new features, and new services. According to Cisco, these new offerings deliver more proactive and broader protection from a wider variety of network and business-application threats. Cisco believes that these new products underscore the evolution of the Cisco Self-Defending Network security strategy. The ATD architecture increases security effectiveness through three components: Anti-X defenses, application security, and network control and containment. Anti-X defends against intrusion by invaders including virus, spyware, and other threats. Application security is provided by various products including VPN services, security policy frameworks, and user-to-application security. Network control and containment are provided by the Security Auditor and the Cisco Security Monitoring, Analysis, and Response System (CS-MARS). These products in total or in various combinations are designed to drive Cisco's vision of network security to fruition.

Taken individually, these products represent an alphabet soup of acronyms and new capabilities that can be overwhelming at first glance. In addition, CEO John Chambers made statements this week that Cisco will continue to aggressively partner, purchase, and build on its security portfolio. Cisco plans to drive more intelligence into the network at various levels and to coordinate the integration of these products with its partners' products to make adaptive, intelligent security a reality. Cisco has long dominated the networking market, and has moved into other areas such as VoIP and storage as a way to broaden their base. They are one of the vendors who have realized that to gain customers' trust and loyalty, they have to take products beyond base function and evolve them to the next level. Like IBM and EMC, Cisco has a far-reaching vision that spans the IT infrastructure, including the traditional voice components. Announcements like this one, their largest in security since they announced Network Admission Control in 2003, are proof of their ongoing commitment. They have also integrated their security vision with announcements across their other products, underlining their belief that security is not a standalone product but part and parcel of the entire infrastructure.

We believe this is good news for users because until now, security has more closely resembled a DIY kit project or hobbyist endeavor rather than something planned by professional architects and contractors. IT managers seeking greater security have had to approach multiple companies and products in a pieces-and-parts approach where solutions rarely work in conjunction with others or are merely reactive to existing threats. Cisco is large enough and pervasive enough in their reach that they can credibly discuss the network, its needs, and what they should be doing to achieve their vision. In fact, the greater challenge for Cisco, its channel, and its customers is to know where to begin, and with whom to start within the organization. Most companies do not have a comprehensive, global security program that handles physical, compute, and voice security but many certainly handle at least some part of these various concerns. That's to be expected as this is an evolutionary market, but it means that articulating the full implications of what Cisco has to offer could be more difficult than it first seems. We expect that most customers will continue to approach specific aspects of security and grow from there as they and Cisco evolve an understanding of their specific needs. Over time, smaller security companies will be relegated to niche products and specialties or will perhaps position themselves to be Cisco's next acquisition. Worse things could happen.

The Sageza Group, Inc.
32108 Alvarado Blvd #354
Union City, CA 94587
650·390·0700 fax 650·649·2302
London +44 (0) 20·7900·2819
Milan +39 02·9544·1646