sageza

Market Roundup

July 3, 2003

EMC/BMC Ink Global Software Partnership

Linux Insecure? Or Just Immature?

Spam in the Can?

EMC/BMC Ink Global Software Partnership

By Charles King

EMC and BMC have announced a global sales, marketing, and technology partnership with a goal of delivering end-to-end enterprise storage management solutions. As part of the deal, EMC will acquire rights to BMC's PATROL Storage Manager software and BMC will resell EMC's ControlCenter products through its MarketZone program. The companies also plan to tightly integrate ControlCenter solutions with BMC's PATROL systems and performance management products. In addition, EMC will support BMC in providing maintenance, service and support to PATROL Storage Manager clients, and will assist customers in making the transition from Storage Manager to ControlCenter. To enhance this process, BMC will be able to offer PATROL Storage Manager customers equivalent EMC ControlCenter licenses to provide a migration or upgrade path.

Consolidation is an ongoing story in the IT industry, and examples range from outright mergers and acquisitions to partnership agreements such as the EMC/BMC deal. The real issue to consider about any partnership is what the individual partners give and receive in turn. In this particular case, BMC off-loads the storage management piece of its PATROL product family and gains access to EMC's more complete ControlCenter solution. By doing so, BMC eliminates some of its own development/upgrade costs, significantly enhances the storage management options it can provide its 5,000+ clients, and makes new friends with a significant roster of enterprise customers. For EMC's, the deal will require some effort in supporting the migration of BMC customers to ControlCenter, but more importantly, it also provides EMC major new channels and an enthusiastic partner for driving ControlCenter further into the storage marketplace.

What is perhaps most significant about this deal is that it is the first EMC ControlCenter partnership signed with an independent software vendor. Other ISVs like Veritas probably have too much time, money, and effort tied up in their own storage management solutions to consider such an agreement. However, as the storage market shifts ever more toward a service/software delivery model and systems vendors like HP, IBM, and Sun attempt to aim hardware customers toward their own discreet storage management solutions, many ISVs and storage specialists like EMC are coming under increasing pressure. In this situation, independents like Veritas will have to run faster to keep up, and maintain or enhance product development efforts to keep up a position of offering all things to all vendors' customers all the time. To our way of thinking, the EMC/BMC is a more intelligent approach that leverages each company's relative strengths, offers each a host of new opportunities, and does it all without significant cost or risk to the participants. That, we suggest, is what a strategic partnership is all about.

Linux Insecure? Or Just Immature?

By Jim Balderston

A recent study from the UK-based mi2g security consulting firm reported that between March and May of this year it had tracked 19,208 successful breaches of Linux-based web sites compared to 3,801 such attacks on Windows-based web sites during the same period. The reports comes after earlier similar tracking reports that show a steady increase of successful attacks on Linux-based systems over the past few years, including a dramatic rise in 2002 in which the first six months of that year saw the attacks rise almost 50% higher than the total for the entire year 2001.

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

While many pooh-pooh such reports from security firms as being attempts to sell more security products by spreading fear and uncertainty, we are not ready to write off this report as a mere marketing tool. Security firms traditionally have hyped digital threats, occasionally overstating a particular threat, but on the whole, and over the long haul, we see the increased need for security measures as an ongoing and ever-growing need. More valuable data, more business critical systems, and more global network interaction make securing an enterprise network a high-ranking priority. For these reasons, we are willing to take claims of over-hyping security FUD with a shrug and look at what this data really says about Linux and its increasing role in the marketplace.

This report should not be seen as disheartening for Linux advocates; instead, in our mind, it shows just how far Linux has penetrated the market. As far as any comparisons between Linux and Windows as it relates to security, we can only point to the relative youth of Linux and the relative inexperience of IT managers in managing the OS relative to the more mature and widely disseminated Windows platform. As IT administrators gain experience with Linux management, they will learn the specific settings and security measures and additional software that are needed to run this OS securely, just as many admins had to do with the Windows and UNIX environments over the past decade. After all, few admins will run any operating system on its default setting fresh off the CD, now would they? As Linux and the human beings managing Linux become more "mature" vis-à-vis security issues, we suspect the gap between Linux's vulnerabilities and those of more mature operating systems will close significantly. This is a familiar and inescapable process for any emerging platform as it moves into the marketplace. Security is largely a process of public vetting and testing; cryptosystems are a notable example of the public process that ensures — or debunks — claims of impenetrability of any security system. Linux is presently going through that very process, one that continues apace as well with all other major operating systems and one that will continue indefinitely into the future. As a result, the major Linux systems vendors need to continue to offer guidance and configurations that allow IT managers to climb the Linux security learning curve as quickly as possible, and in doing so have an opportunity to add one of the real values that IT needs to successfully deploy what is seen by many as a "free" product.

Spam in the Can?

By Jim Balderston

A recent summit in the UK concerning spam brought together a number of officials, many who expressed concern about spam and the fact that most of it is originating in the United States. As a result, opinions on pending U.S. legislation regulating spam were heated and diverse. One speaker at the conference, Steven Linford of the UK-based non-profit Spamhaus, argued that the U.S. legislation being considered in the Congress would lead to an explosion of spam as it is essentially an opt-out system that would force consumers to take action to not get spam and in turn would legalize — to a large degree — spamming and spammer activities. The Direct Marketing Association supports this opt-out methodology over a more stringent opt-in technique, where users would have to proactively request and approve the receipt of what heretofore had been unsolicited email.

Congress needs to take the issue of spam seriously and recognize that it is a problem for its constituents to such a degree that cosmetic and ineffectual legislation will not mollify an increasingly irate voting public. Spam not only is a nuisance to people and network administrators, it is seen increasingly as an unwanted and sometime vile intrusion into people's private and personal lives. While technology solutions continue to make some headway against Spam, it is the rare public email account that is not the repository of solicitations for a host of alleged maladies besieging the online public.

We suspect that any bill that is supported by the Direct Marketing Association will have little real effect on the consumer, who will continue to get unsolicited mail offering to enhance sexual prowess, end baldness, lower credit car payments, or engage in somewhat shady Nigerian banking transactions. Mr. Linford appears to be spot on, as legitimizing a widely abused business process will do little to protect the consumer in either the short or long run and only enhance the ability of spammers to operate with a larger legal shield. If Congress wants any indication of the true sentiments of American citizens vis-à-vis unsolicited marketing efforts they should quickly glimpse at the 10 million Americans that signed up this week for a national Do Not Call Registry aimed at stopping telemarketers' constant harassment during dinner. When one considers that many states with similar registries are already up and operating and well populated by consumers seeking a little relief, we see the idea of playing

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

footsie with the DMA while letting consumers stew would be bad politics indeed. Effective legislation is a key ingredient to reducing Spam, and half-measures will not cut it with the public on this particular issue.

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