Market Roundup

February 17, 2006

IBM Launches Identity Management Services

By Clay Ryder

IBM has announced the IBM Identity Management Services (IDMS), a portfolio of solutions covering the identity management lifecycle from identity proofing, to user provisioning, to access control. IDMS allows organizations to engage at any point in their identity management lifecycle and at every level of an organization, from business strategy, to applications, to IT infrastructure. IDMS offers a portfolio of complementary services that can be implemented as integrated solutions or individual components. Key elements of IDMS include briefings, assessments, and workshops; industry-specific identity management architectures and custom design services; and solution implementations and hosted services. IDMS incorporates identity management products and technologies from IBM Tivoli, ActivIdentity, ADT Security Services, Axalto, Cogent Systems, Encentuate, Exostar, GE Security, Lenovo, Passlogix, Verisign, and Viisage, among others. IDMS also utilizes IBM's Information Security Framework (ISF), which is designed to enable clients to review and assess their entire security landscape and develop a pragmatic roadmap to maintain an effective security program based on their needs. The ISF covers eight core areas with best practices for planning and deploying the necessary security measures related to governance, privacy, threat mitigation, transaction and data integrity, identity and access management, application security, physical security, and personnel security

Security remains a much talked about, if not hotly debated topic, which most would agree is very important. Yet there are many factors involved and more often than not no universal consensus exists on what constitutes secured vs. unsecured. For the budget-strained IT department already stretched thin simply keeping the infrastructure up and running, securing it, which generally requires making invasive changes to configuration and operational processes, is not something that most would look forward to doing. Nevertheless, the reality is that for external regulatory compliance, internal governance, or more strategic operational concerns, securing the IT environment is rapidly becoming a mandatory undertaking. Given the numerous threats, both external and internal, and the need to get matters under control and on a path to a given level of security, compliance, and good governance, there is a good argument to be made that this undertaking should be outsourced to a trusted third party. This is where the IDMS comes into play.

IBM has not only the breadth and depth of technologies, but perhaps more importantly, the scale of services and financing that would make it possible for it to undertake critical security assessments and develop plans to address shortcomings while not engaging in politicized finger-pointing within the organization. Further, as a trusted outsider, the recommendations can be brought, relatively unfiltered, to the senior management of the organization for strategic review. By ascertaining buy-in from the top, there is an opportunity for the organization to garner widespread support for needed changes not only to infrastructure but to business and personnel behavior as well. Rather than IT imposing its will, it is the organization as a whole defining its policy and safekeeping. This can be made in view of the strategic goals of the enterprise as opposed to more tactical goals of IT personnel protecting their personal fiefdoms. That said, effectively auditing security, developing a security plan, and executing upon it remains a non-trivial matter. Bringing a combination of technology expertise, an overarching framework, and considerable business expertise to bear should help cultivate a sense of confidence, if not relief, for potential customers. IBM is well positioned to bring this to the market as a service and we look forward to see if the market agrees.

CA Integration

By *Susan Dietz*

CA announced this week that it is integrating its SiteMinder with its Single Sign-On (SSO) products as a part of the Identity and Access Management Suite. This incorporation of two separate product solutions seeks to enable seamless authentication between resources that are protected by either solution by deploying a combination of authentication schemes, with additional authentication or re-authentication available for more sensitive areas. Aimed at enterprises, the integration will allow multi-factor authentication while reducing the complexities of multiple passwords for end users. Single Sign-On, when combined with SiteMinder, should not compromise security and compliance for an enterprise's different applications. The integrated products support multiple platforms, different organizations, and several generations within the same enterprise.

Forget the Chinese Year of the Dog; this is the computer industry's Year of Compliance. If a product offered by a company does not help their customers meet their compliance needs, then the product is quickly washed out of the market place. Luckily, CA has taken that into consideration when combining the different SiteMinder applications with the SSO solution. When end users have to remember multiple sign-on names and passwords, then they are less productive employees due to the frustration level and time lost looking for, searching their memories for, and finally just guessing at what their password is for the particular application they are trying to access. Single sign-on solutions are great for end users, but may seem to be more of a headache for some security administrators, in part due to their level of creativity and thinking. SiteMinder products attempt to alleviate that particular headache by providing a centralized security infrastructure for managing user authentication and access across both internal and external sites, while at the same time ensuring that applications are up-to-the-minute compliant. Combining the two applications into a seamless integration just makes sense. When done correctly, it allows all enterprise employees to quit futzing about with passwords and authentication and compliance issues and just get back to the business of making money.

IBM Boldly Goes Where No One Has Gone Before

By *Joyce Tompsett Becknell*

IBM has announced a new company-wide initiative combining its software and consulting experience to provide clients with access to accurate, reliable, and trustworthy business information. On the software side, IBM will invest $1 billion over the next three years to expand its information management software development. On the services side, it will expand its consulting base by 65% over the next three years. In addition, IBM is announcing six new solution portfolios and new software products to help clients transform their business including step-by-step assessment tools and new centers of excellence to help clients assess and solve their individual information requirements. The centers of excellence will provide clients with a quantitative summary of their current needs with prescriptive guidance on how to proceed. The centers will have solution architects, information architects, and researchers from IBM Business Consulting Services (BCS), IBM Software Group, and IBM Research. The solutions are designed to help customers manage information as a service. They help clients exploit existing information assets as well as emerging information sources for risk and compliance, business analysis and discovery, business performance and process management, master data management, process innovation and workforce productivity. IBM believes that after people, information is a company's most important asset and that it needs to be effectively managed and delivered to people, business applications, and processes. IBM believes that existing products focus on parts of the problem, but that it will take a holistic approach to solve the total problem.

When IBM announced On Demand, it seemed like just another high-tech company slogan emerging in the market place and designed to cover whatever the vendor was planning. However, IBM had the right instinct and spent a lot of time working out what it actually meant, starting from an understanding that business and technology did need to work together better and then working out from there the implications to its business. Because of its BCS experience, IBM understood how much work was really involved and that it involved a lot more than product integration services. The missing link was the data connection. After all, what technology and business processes have in common is the data that becomes information in the proper context. Once IBS worked that out and incorporated it into its approach, the next steps became clearer. Like On Demand before it, the Information on Demand message may be overflowing with buzz words and sound a bit large and vague at first glance, but if anyone can pull this off, it would be IBM. It is the only vendor with a credible services business. It wouldn't be stretching to say that Information on Demand will lay to rest forever the question of whether IBM did the right thing in purchasing PWC.

That said, IBM still has a long way to go. As we've mentioned before, management software is an area that ranks high for many technology firms and there are no shortage of candidates available to influence that space, none of which have truly comprehensive capabilities in their current incarnation. Furthermore, success doesn't require a vision of corporate nirvana. Winning the largest installed base is a good enough start. What IBM can do with Information on Demand at this point is applicable to only a small stratum of companies with the bandwidth and resources either to be a guinea pig or to help drive information on demand to its logical conclusion. However, one of our benchmarks on the maturity of an IBM vision is when it can deliver to a mass market. Information on Demand is certainly not there; in fact it is barely out of embryonic mode and it will be a couple of years before it can be distilled into products and services that benefit the vast majority of companies. Despite this, IBM does have a head start on anyone else as it is one of the few companies with both vertical industry excellence and business process capabilities. The challenge for IBM will be to develop the internal processes that allows it to distill the progress it makes to its other communities: the product groups within IBM, the partner communities, communities its has established in places such as health care and education, and other communities that will inevitably arise as it continues down this path. Management software developments will surely be one of the primary gauges for measuring progress overall as what it designs will surely move first into that and other IBM middleware before anything else. The challenge then will be to IBM's ability to distill a galactic vision into succinct bits for appropriate segments. We look forward to watching the progress and observing how it drives IT development forward.

Symantec Has Ambitious Name for Ambitious Product

By Susan Dietz

Symantec has announced that it will be releasing the Network Access Control Enforcer Appliance Series in late April. This suite of products is preconfigured to help companies ensure that multiple units, including networks, branch offices, telecommuters, and mobile workers, are both protected and compliant with the company's security policies. This is a hardened, rack-mountable appliance and before granting network access to a user, it will block or remediate non-compliant, infected, or compromised devices. The appliance scales to support tens of thousands of concurrent sessions. Automatic software and patch updates also figure into the Symantec solution, and it supports an array of network equipment, access methods, and protocols. All enterprise IT systems will reportedly be insulated from information theft, violation, and disruption. The Network Access Control Enforcer Appliance Series integrates with the Sygate Enterprise Protection 5.1 client software, which offers security protection against known and unknown attacks by combining host intrusion prevention, desktop firewall, and peripheral device control. The new products also integrate with On Demand Protection 2.6, which together will enable compliance-on-contact for unmanaged devices. By supplying endpoint security before a user is granted access to the network, Symantec hopes to mitigate threats before they happen. No pricing information was released.

Again, compliance is a key marketing strategy this year. Internal threats are often the most successful and insidious, and companies are taking note. With the Network Access Control Enforcer Appliance Series, Symantec is attempting to mitigate most, if not all, of those internal threats. Making sure an employee's electronic device is compliant is a critical factor in any total security solution. By dealing with those internal threats before they manage to insinuate themselves into the network, endpoint security is a proactive solution, and we like companies being proactive rather than reactive. In the world of computer security, reactions to threats, no matter how fast those reactions, are still way, way too late to make a difference.

Building security solutions that work across the enterprise on every level that enterprise operates on is a challenging undertaking, but one that we think Symantec is well positioned for. Its recent spate of acquisitions has brought quite a bit of dynamic talent to a company that was beginning to get a bit of a reputation for being—shall we say—a little less than vibrant. This new offering offers some new shine for the company's image, showing an aggressive stance against computer crime. The world of computer security should make one feel secure about their computers. We believe that Symantec's efforts in this regard will help brings us all closer to that goal.