Market Roundup

March 23, 2007

Novell Announces Thin Client Based on SLED

By Clay Ryder

Novell has introduced the SUSE Linux Enterprise Thin Client, a solution consisting of SUSE Linux Enterprise Desktop and an image-creation tool kit that channel partners will be able to use to provide a finished thin-client solution to customers. The offering is positioned for organizations that are seeking to transition from traditional desktops to thin-client devices in order to reduce costs, increase data security, and improve manageability. SUSE Linux Enterprise Thin Client includes both the desktop software and a tool kit to create, deploy, and maintain images for diverse thin-client environments, including call centers, manufacturing floor workstations, other fixed-function, and transactional settings. Images can be deployed on a variety of devices, such as re-purposed legacy PCs, new PCs, or specialized thin-client devices. SUSE Linux Enterprise Thin Client will be generally available later this year.

The thin client is another one of those technologies whose promoters state will take over the marketplace and whose detractors say is doomed due to ever decreasing acquisition costs of traditional desktops. Yet neither prediction has come to pass, as thin clients continue to play a vital if not growing role in certain computing scenarios while at the same time achieving an insignificant footprint in the consumer and smaller organization marketplace. Nevertheless, the value proposition of the thin client has much going for it, especially for mid-sized and larger organizations where there are many dedicated or fixed function access devices. While this announcement makes it clear that Novell is not getting into the thin client hardware business, the company is pulling together the requisite pieces so that others will be able to offer a SUSE Linux-based thin client. Based upon endorsements in the press release, at a minimum, we expect that thin-client purveyors such as Wyse Technologies and Ericom as well as others will be exploring how they can be part of this ecosystem.

Unlike some vendors' past forays into thin-client solutions, this announcement from Novell does not tie the user into a single form factor; rather it provides choice in how organizations choose to deploy a thin-client solution. In all new deployments or as part of an overarching technology refresh, thin-client terminals can be deployed; however, software-based thin clients installed on older generation desktops will be as option as well. Either way, organizations will gain another option in delivering Linux applications to the desktop, and Novell will gain a customer not only for Linux, but for the many value-added offerings the company wraps around its operation system.

In general, we are supporters of the thin-client architecture as it has a lot to offer from a management, operations, and financial perspective. Thin clients thrive in environments of homogenous scale. Given the ever rising popularity of Linux applications and substantial impediments to upgrade older Windows environments to Vista, this new offering may prove to be a welcome alternative for organizations that are looking to bring more Linux applications to the desktop, extend the life of the aging Windows desktop, or simply replace it with thin-client hardware.

Copyright © 2007 The Sageza Group, Inc.
May not be duplicated or retransmitted without written permission

The Sageza Group, Inc.
32108 Alvarado Blvd #354
Union City, CA 94587
510·675·0700 fax 650·649·2302
London +44 (0) 20·7900·2819

RSA Trojan Service

By Lawrence D. Dietz

RSA, The Security Division of EMC, has announced it will launch its new RSA FraudAction Anti-Trojan service, designed to help companies secure their organizations, brands, and customers from a new generation of crimeware attacks. The RSA FraudAction Anti-Trojan service is designed to provide a proactive, layered approach to dealing with financial crimeware and advanced attacks. The service is being developed based on RSA's experience in external threat protection services including anti-phishing and anti-pharming services. As engineered, the RSA FraudAction Anti-Trojan service will be an end-to-end solution covering the identification, analysis, blocking, and shutdown of attacks. RSA claims that their 24x7 Anti-Fraud Command Center has detected and shut down more than 32,000 unique phishing attacks, and has broad detection and blocking networks already in place with leading antivirus, anti-spam and ISP players. The main components and benefits offered by the RSA FraudAction Anti-Trojan service include Identification; Analysis which the aggregates RSA and antivirus partner data enabling financial institutions to see what crimeware is targeting their customers and understand how it works; Blocking to help financial institutions put up an immediate layer of protection, by blocking consumer access to known infection points on the Web; and Shutdown to help financial institutions to mitigate further against attacks via targeted infection and drop-site shutdown.

Fraudsters are increasingly deploying these attacks, including session-hijacking Trojans and keyloggers, in order to steal personal and financial information from consumers. Sageza believes that cyber attacks are becoming more targeted and that phishing/pharming attacks are among the most harmful because their "soft" nature, capitalizing on the user's confidence in the brand being used as a cover, makes them immune to many technological safeguards. Further, RSA states that phishers are particularly targeting financial institutions. This make sense since financial services brands are most often used to entice consumers into revealing confidential information or to defraud them. Given RSA's efforts with PassMark, notably the SiteKey used by Bank of America, we believe that RSA has made a positive move with this announcement.

The layered approach offered by RSA is one that Sageza believes is classically sound. This additional protection should help financial institutions to accelerate further their businesses online and increase consumer confidence in the channel. Security practitioners will often use the analogy of defending a castle with its cordon of defenses to explain the notion of layered defenses. It is also useful to point out that RSA is working with partners such as antivirus vendors to develop their database of potential threats. Organizations outside of the financial sector will also need to take steps to prune their email of phishing and pharming attacks. While RSA is not the first to offer anti-trojan protection we believe that it is a logical extension of its security business and may ultimately offer a connection with other EMC products as well.

Qlusters Expands Virtualization and Xen Support

By Clay Ryder

Qlusters, Inc. has announced an extension to its openQRM systems management platform that brings advanced virtualization and Xen management capabilities to assist in the deployment and management of Xen hosts and virtual machines. This new extension, combined with existing support for VMware, enhances openQRM's ability to provision, manage, and monitor both virtual and physical server environments. openQRM helps IT professionals adapt/repurpose their infrastructure by redeploying or migrating their operating system and application environments among various physical and virtual configurations as needed. The latest version of openQRM helps administrators increase or decrease the memory consumption of a Xen partition dynamically while enabling the addition, removal, and reassignment of virtual machines to specific physical units without necessitating a system restart. Additional new features include the ability to migrate an operating partition from a small Xen-host to a larger one; add/remove network cards for partitions and configure through which physical network card the Xen-host traffic should be routed; and extend a handed-over Logical Volume Manager device from the Xen-host to the partition without restart for on-the-fly increases to partitions on virtual hard disks. openQRM is available immediately with support for advanced virtualization and Xen capabilities. Qlusters

Copyright © 2007 The Sageza Group, Inc.
May not be duplicated or retransmitted without written permission

The Sageza Group, Inc.
32108 Alvarado Blvd #354
Union City, CA 94587
510·675·0700 fax 650·649·2302
London +44 (0) 20·7900·2819

provides enterprise-level subscriptions, which include Enterprise plug-ins and tools, updates, trouble ticketing, email-based technical support and full production support starting at $500 per managed physical server.

Virtualization and systems management remain hot topics, and for good reason. The potential for operational streamlining and cost reductions available through enhanced utilization of IT assets is simply too good to overlook. While the technology continues to advance in ability and ease of use, the fact remains that are multiple virtualization schemes in the marketplace with varying degrees of capability and the integration or cross management of these resources is often less than optimum. A key aspect of virtualization is the logical separation of resources from physical implementation, so accepting silos of virtualized resources under discrete management schemes just seems to come up short. This is where solutions such as openQRM come into play.

This new offering seeks to simplify the deployment and use of Xen virtualization to provision and manage virtual and physical environments to improve administrator and hardware efficiencies. Being able to manage disparate resources, despite differences in operating systems, as well as increase the automation of as many tasks as possible are concepts that often top the IT professional's wish list. Easing the management of virtualized environments is an important component in realizing the cost benefits of such environments. Being able to migrate from one virtualization environment to another, for example from Xen to VMWare ESX, from a central management console streamlines operations, and enhances the overall value of virtualization schemes. The multi-OS support (Solaris, FreeBSD, Windows, and Linux) positions openQRM as a relevant solution to a broad spectrum of the marketplace. The fact that openQRM is available as open source should help further cultivate a marketplace expectation that provisioning and management of virtualized environments should be as easy, if not easier, than physical ones. Overall, we are pleased with technological advancements being delivered through openQRM and will continue to watch with great interest as this technology and market need continues to grow and mature.

Leak Protection Market Gets Downright Soggy: Provilla Offers a BigFix

By Lawrence D. Dietz

Provilla, Inc., a provider of endpoint solutions for data leak prevention, has announced a new technology partnership agreement with BigFix Inc. The companies will provide customers with a highly scaleable, realtime-visibility and control-based data leak prevention (DLP) solution, for both desktop and mobile computers, online and offline, and on corporate or public networks. Using Provilla's patented DataDNA data leak prevention technology, the BigFix agent detects and stops leaks of sensitive data at rest, in motion, and in use by corporate desktops, branch offices, and mobile workers, and reports the results in realtime via the BigFix console. Unlike other solutions that only monitor email or removable media, this DLP solution can enforce security policies by effectively blocking all exits, including emails, as well as any type of attached device. The company claims that the combined BigFix/Provilla solution can enforce security on the endpoint globally whether the device is connected or disconnected from the corporate network. Provilla's DLP technology blocks the transfer of confidential data through any network or I/O port. Comprehensive forensics and on-demand scanning of all confidential data throughout the organization provide powerful tools for addressing compliance regulations such as PCI, CA SB-1386, GLBA and Sarbanes Oxley (SOX), enabling enterprises to determine if confidential, unencrypted data exists on laptops and desktops. The BigFix platform provides realtime visibility and control through its single agent, multi-function architecture. Its solution is in production at more than 600 companies, government agencies, and public sector institutions worldwide, and currently manages over 7,000,000 desktop and mobile clients, workstations, and servers.

During RSA 2007 one Sageza Analyst remarked "there's so much data leakage on the exhibit floor, someone needs to get out the Pampers." Clearly a growing number of vendors have turned to DLP as a major marketing thrust, rivaling compliance as a purported business driver. As it turns out, Sageza believes there is a real need to safeguard sensitive information. We have already gone on the record as saying that Privacy will eclipse compliance as a concern this year. We are positive on the combined approach offered by Big Fix and Provilla because it appears to address the security principle of protection information based on its value, not its location. The combination also has the advantage of not just monitoring and reporting a potential problem, but taking specified actions based on predetermined policies.

Copyright © 2007 The Sageza Group, Inc.
May not be duplicated or retransmitted without written permission

The Sageza Group, Inc.
32108 Alvarado Blvd #354
Union City, CA 94587
510·675·0700 fax 650·649·2302
London +44 (0) 20·7900·2819

We believe that combining detection, prevention, and remediation is a best practice for end-user organizations. However, this recommendation implies that end users have already gone through the exercises of classifying their information and establishing policies to safeguard each level of classification. This approach is necessary for good governance, which reduces operational risk and demonstrates compliance as a by product of planning ahead and employing technology to enforce policies.

Copyright © 2007 The Sageza Group, Inc.
May not be duplicated or retransmitted without written permission

The Sageza Group, Inc.
32108 Alvarado Blvd #354
Union City, CA 94587
510·675·0700 fax 650·649·2302
London +44 (0) 20·7900·2819