Market Roundup

April 6, 2007

IBM Move to Lower-Cost IPS an Inevitable Step for ROBO Security

uXcomm To Acquire Virtugo Software

Postini Positive Position Pushed by New Features

Power.org to Host Software Summit

:sageza:

IBM Move to Lower-Cost IPS an Inevitable Step for ROBO Security

By Lawrence D. Dietz

IBM has announced it will extend its Internet Security Systems (ISS) intrusion prevention technology to remote segments of the network by adding a new, lower-cost product to the IBM Proventia Network Intrusion Prevention System (IPS) family. Through the addition of Proventia Network IPS GX3002, IBM will offer comprehensive, ahead-of-the-threat protection for a new layer of the enterprise network. The GX3002 is designed to protect a single network segment at up to 10MBps of throughput, and its desktop form factor features integrated zero-power bypass functionality to help ensure high network availability. Proventia Network IPS GX3002 brings IBM's IPS protection to remote segments of the network such as small branch offices and critical end points, including ATMs, points-of-sale, and self-help kiosks, which are increasingly becoming popular targets for Internet attacks. Until now, companies needing to protect these points have had only limited-feature IPS offerings available to them. This product provides the same robust security features found in other Proventia Network IPS products, while still meeting the lower cost requirements for remote segments.

It is not unusual for technology to evolve in a top-down manner. Large sites mean larger orders so it's only natural for vendors to start at the top of the enterprise food chain and move down. However, security practitioners and those charged with Governance, Compliance, and Risk Mitigation have known for some time that the weakest link is often the Remote Office or Branch Office (ROBO). These organizational outposts often have little or no tech support, yet offer an inviting entry point for would-be attackers. Consequently it makes a great deal of sense to offer the same kind of security across an organization, regardless of the size of the location.

The announcement also includes some indications that IBM has had the foresight to extend security into specialty devices. Many of these devices such as kiosks, fuel pumps at gas stations, and others are powered by variations of embedded operating systems. The ability to safeguard these systems with their almost limitless variety in configurations requires a significant investment in testing security products in specific environments.

Sageza believes this particular announcement demonstrates that IBM has done its homework in forging a strategy across the disparate elements of large organizations to include their outposts and specialty devices. In the future we would expect to see additional focused targeting from IBM. In particular we would expect to see a push into power, energy, water, sewerage, and oil/gas applications be expanding the technology used in the critical end points noted in the announcement to the Supervisory Control and Data Acquisition (SCADA) devices found in these target verticals. It also appears to Sageza that IBM is one of the few organizations to actually take the U.S. Strategy to Secure Cyberspace seriously and we applaud these efforts.

uXcomm To Acquire Virtugo Software

By Clay Ryder

uXcomm, a provider of monitoring, control, and optimization software for virtual and physical servers, announced this week that it has acquired the assets of Virtugo Software, a performance and service-level management tools vendor for virtual environments. Under terms of the agreement, uXcomm is purchasing all of Virtugo's

---

VirtualSuite product line, including Perform and PerformLite, Capacity, Optimize, Meter, and Connect, as well as the company's tested software architecture. The company is assuming responsibility for all sales and support contracts and has retained several key members of the Virtugo staff. uXcomm provides standards-based systems management solutions aimed at helping customers manage disparate network devices from almost any management framework. The addition of Virtugo's VirtualSuite will extend the management scope so IT professionals will be able to monitor and control 1,000s of virtual machines and hosts while optimizing performance to meet SLAa and ensuring sufficient capacity to maintain high availability. The company states that the combination of uXcomm's XManage platform, which supports XenSource's core virtualization technologies, and Virtugo's VirtualSuite, which supports VMWare, provides the first integrated management solution for heterogeneous physical and virtual environments.

Consolidation and virtualization have been hot-button topics for the past few years, and for good reason. There are plenty of opportunities to optimize the efficiency of the data center and IT deployments in general. As more powerful and cost-effective servers have come to market, the opportunity to refresh aging equipment, reduce datacenter footprints, and raise overall efficiency and simplicity has become a welcome arrow in the quiver of any IT professional or CIO. However, with the acceptance of virtualization schemes, there are new management issues raised that sometimes may be trickier than managing one or two workloads on a physical server. Managing multiple virtual machines, with various operating systems and distributed application workloads, requires being able to assess the state of the physical and virtual environment simultaneously within a single context.

Past and present virtualization schemes for the most part have focused upon enabling virtualization, i.e., carving up a larger physical server into smaller virtual servers to support workloads that in the past were often mapped one per physical machine. This is a great first step in improving efficiency as the number of machines, cables, and power consumption all decrease and organizations can do more with less. However, there are other capabilities that are just as important such as measurement, management, and reporting. As time progresses and workload needs grow, the size of the virtual machine deployed to support a workload can become insufficient. This is where measurement management comes into play. To garner the next level of efficiency gains requires being able to reallocate unused resources temporarily to other virtual machines to order to meet peaks in workload without permanently allocating resources that will go unused in non-peak scenarios.

Perhaps the most interesting aspect of this new technology marriage is that uXcomm will be able to provide solutions that not only monitor physical and virtual environments but will be able to do so from within a single management framework. The ability to identify and loan resources temporarily from virtual machines addresses some of the inflexibility of some virtualization schemes in place. Further by supporting both Xen and VMware platforms, the company is relevant to the lion's share of virtualized servers in the market today. By taking a holistic view of resources, both physical and virtual, organizations would be in a better position to optimize their infrastructure, and therefore raise utilization/efficiency even further. From both an IT and corporate operations perspective, this potential should be well received.

We have long articulated that the totality of virtualization will be realized when we think of all IT resources as simply being a function or capability available on the network when we request it. Where services physically reside is irrelevant from a functional perspective; the physical attributes only come into play when assessing SLA and choosing the appropriate resources to meet that need. We are heartened by the potential this marriage of uXcomm and Virtugo's Virtual Suite offers to organizations that are serious about achieving the maximum efficiency and competitive advantage from their IT and datacenter investments.

Postini Positive Position Pushed by New Features

By Lawrence D. Dietz

Postini has detailed major new innovations and enhancements to its family of Software as a Service solutions. Postini's solutions are designed to protect businesses worldwide from threats to their electronic communications, enforce business policies, secure intellectual property, assure privacy, and enable compliance with legal and industry requirements for the retention and discovery of email and IM data. Postini has enhanced its security offerings to protect clients from the increasing threats to their electronic communications. New innovations

include adaptive heuristics, improved PTIN intelligence, and compressed file scanning. Heuristics (behavior sensing and recognition capabilities) have been enhanced with rapid filter updates and new algorithms that block emerging sophisticated zero-hour spam, virus outbreaks, and image spam attacks. PTIN intelligence refers to the Postini Threat Identification Network (PTIN), a realtime data collection of malicious and infected IP addresses that propagate attacks across the internet. PTIN data is based on the collective data observed by Postini across the billions of connections processed daily across Postini's global data centers. PTIN has been further enhanced to provide protection against distributed bot-net attacks. Compressed file scanning helps facilitate detection of malicious executables hidden inside compressed or archived attachments. Combined with Postini's security architecture, which is designed to ensure the most effective protection, these new innovations to Postini Email Security strengthen the value delivered to Postini clients by maximizing catch rates of unwanted communications and minimizing false positives.

Other innovations and enhancements to Postini Web Security and Postini Web Compliance include pre-scanned search results, network effect for URL scanning, mobile and remote user support, and intelligent Web protection. The pre-scan innovation provides an "early warning system" for search results from popular search engines including Google, Yahoo! and MSN. The network effect for URL scanning ensures that threat data is learned and shared across all users in order to improve security posture, improve operational integrity, and reduce load on IT staff. This new self-learning system continuously monitors Web activity and adapts to threats in real-time. Mobile and remote user support ensures that access and usage policies are enforced regardless of the location from which users access the Web and protect the corporate systems. Intelligent Web protection filters out portions of Web sites that contain malware or malicious links while providing access to the safe parts of the site. The company also announced new archiving features such as investigation management, email storage management with personal archive access, and a new Postini toolbar. Other enhancements were noted for encryption and the platform.

Sageza believes that these new features address a host of issues. We have stressed that attackers will become more innovative and targeted. This means that organizations will need to harness a variety of intelligence sources to ensure they have a knowledge base sufficiently broad enough to challenge conventional security planning. Attention to distributed bot-net attacks is particularly important as this capability is not only harmful in itself, but can be an ongoing attack vector for other nefarious activities. It s also incumbent on organizations to share intelligence and defensive actions across the organization as noted with the URL scanning noted above. We are also strongly supportive of the notion that access and usage policies must be enforced uniformly across an organization.

Postini's new announcements offer quite a bit of food for thought. Sageza believes each of these is significant not only for individual characteristics but in the approach to the totality of the security and integrity challenge they represent in total. It's also important to point out the inextricable link among information security, governance, compliance, and risk mitigation.

Power.org to Host Software Summit

By Clay Ryder

Power.org has announced that it will host the first Power Architecture Software Summit, a conference for software developers and development managers to provide input and help refine Power.org's software strategy. The summit will focus on identifying solutions to challenges associated with software development on Power Architecture. Discussions will revolve around presentations that address a wide range of topics including Power.org itself, PlayStation 3 as a development workstation, the business case for software on Power, and IDEs and Eclipse, among others. The summit will be held in Austin, Texas, April 19 and will also be available through an Internet conference.

Since Power.org was founded a little over two years ago, the organization has grown and garnered the interest and participation of many of those playing in the broad ecosystem that surrounds this unique architecture. Much of the emphasis of Power.org has been to promote the hardware architecture and get as many participants on board as possible. However, any hardware is only as useful as the software that it drives. So, the Power Architecture Software Summit is a logical exercise in bolstering interest in the platform.

Given the highly varied uses of the Power Architecture, Power.org is really the only venue in which a non-vendor-specific call for input and discussion would take place. Obviously, IBM's software vision for Power differs from that of Freescale, Ericsson, or any of the dozens of other Power architecture-based solution providers. There is where the notion of collaborative innovation manifests itself, as many players with very different places in and approaches to the marketplace come together to promote development of intellectual property that benefits the greater community. Top-notch software and software development practices are essential for the growth of any platform and communities of developers offer a unique insight into the strength and challenges inherent in any platform. As such, we are pleased to see the Power.org cast a wide net in soliciting the feedback from its varied developer community, but also in its desire to enable development on the architecture in existing markets as well as helping seed development potential in new solutions as well.