Market Roundup

March 30, 2007

EMC/Microsoft Give Operations Manager Some Smarts

By *Clay Ryder*

EMC and Microsoft have announced a technology licensing agreement and a broader technology collaboration aimed at enhancing network-aware, end-to-end service management. As part of the agreement, Microsoft is licensing EMC Smarts network discovery and monitoring technology for use in future releases of Microsoft System Center Operations Manager. In addition, EMC will develop network management and root-cause analysis management packs to be deployed in current and future releases of System Center Operations Manager. EMC also announced the EMC Smarts Connector for Microsoft System Center Operations Manager 2007. This two-way connector enables Smarts to share network discovery, topology, and root-cause events with Operations Manager and for Operations Manager to synchronize alert status and resolution back to EMC Smarts technology. The two companies also stated that they are collaborating on the co-development of a cross-domain behavioral model within the context of Operations Manager to improve IT operations management across disparate devices and systems. Operations Manager customers will be able to determine the root cause of service issues across the modeled infrastructure whose definition can be supplemented by other Operations Manager partners to broaden visibility and control to other new devices, services, and applications. The EMC Smarts Connector for Microsoft System Center Operations Manager 2007 connector will be generally available in May 2007.

EMC has started positioning itself as a Storage Infrastructure provider, and this announcement is illustrative of this positioning if not perhaps even broadening the scope of what might be considered storage infrastructure. Trends in the marketplace are blurring the lines between what discretely constitutes storage or server technology. One can quibble over whether an NAS head is different from a server, but it largely doesn't matter since it is the function of providing storage that users and applications are ultimately concerned with. The uninterrupted flow and movement of information, whether it is application- or data-derived, is fundamental to business operations. In a distributed/virtualized storage environment, it is essential to understand all the interactions and current state of operation for each component, regardless of whether it is a spindle, networking component, application, or whatnot in order to deliver a cost-effective, SLA-compliant storage solution. In order to achieve this, one must be able to model the infrastructure, and be very open to new definitions of the components one might find in the infrastructure today or in the future.

We see this agreement and resulting product offerings as particularly well suited for SMBs, whose IT point-of-reference is most likely to be Microsoft-centric, but whose degree of specialization in its human resources is typically limited and facing an increasingly complex IT infrastructure and network topology. One of Microsoft's strengths is that its GUI interfaces are typically well understood by the IT generalist. By delivering a modeling scheme driven by add-ins to its management solution, MS and now its partner EMC are offering the potential for a larger number of organizations to gain a better understanding and control of their infrastructure while also potentially broadening the scope of the components being monitored. The add-in approach implies an incremental path to deployment as opposed to the more rigid comprehensive definition of the infrastructure required in other approaches. The two-way communication between Smarts and Operations Manager is much akin to having a second set of eyes looking out for the network, and reporting what it sees. Enhancing the discovery of objects on the networks that are then incorporated into Operations Manager and then fed back to Smarts would provide an enhanced understanding of the terrain and its management. This should help organizations become more efficient and thus be able to do more with their infrastructure, which strategically would help both vendors, as it will free up resources to ponder new tasks that could ultimately drive more usage of the infrastructure and lead to demand for additional investment.

Overall, we see this as good for vendors as well as the SMBs who are the likely target for the solution. MS gets to enhance its systems management solution with improved discovery and look more heterogeneous in scope, EMC bolsters its position in the SMB space and furthers the notion that it is more than just a traditional storage provider, and SMBs gain access to a richer, more comprehensive set of tools that is in alignment with their skill set. In an increasingly virtualized world, management of resources is more important than ever. We are encouraged by the strategic thinking apparent by EMC and MS as they collectively look to solve the challenges of managing this brave new IT world, while keeping deployment complexity and pain within the threshold of IT ability available in a large portion of the marketplace.

Trust Digital Addresses Smartphone Security Issues

By Lawrence D. Dietz

Trust Digital, a provider of enterprise smartphone security management software, has released the latest version of its software. The company is selling the product through its direct sales force and channel partners such as Verizon Wireless. Trust Digital's Web-based console centralizes management and automates enforcement of on-device security and network access. Primary software features include On-Device Security, realtime enforcement of device/configuration settings and user authentication; realtime, on-the-fly data encryption of policy-specified files, databases, and removable media (e.g., SD cards); and FIPS 140-2 certified encryption (AES128/196/256 and Triple DES). Device and Application Management features include self-service, over-the-air (OTA) device registration and provisioning, and configuration and application access as well as a patent-pending "Trusted Application" architecture that the firm claims prevents viruses, Trojan horses, etc., from accessing protected data. There is also a feature set for Exchange ActiveSync Network Access Control which allows Microsoft Exchange synchronization with only registered, approved, and compliant devices and a silent, OTA remediation of devices that do not meet current security policy requirements. There is a Personal Firewall, which restricts the use of multimedia resources including camera and voice recording, prevents the use of and/or encrypts SD cards and other removable media and control communications services including WiFi, Bluetooth, and IR. Lastly the Web-based Enterprise Console provides for policy, systems, and administrative management, a Help Desk for decommissioning, remote unlock, and remote wipe and reporting of device compliance status.

In today’s connected world large organizations are continually looking for new ways to connect with their out-of-office employees and eke out additional work from them. Sageza believes that the majority of knowledge and service workers will have personal communications devices helping them manage calendar, contacts, and email. Additionally many of these devices will be modified to perform specialized tasks in line with the individuals’ work. It stands to reason that important and perhaps sensitive data will be stored on these devices and that they may be unwitting entry points for attacks by adversaries. It appears to us that the smartphone and PDA would be key elements of this device population.

The security management suite offered by Trust Digital contains a number of key features that we believe will be essential to manage risk on this new generation of devices. Authentication, on-the-fly data encryption (especially certified to well recognized standards such as FIPS-140-2 or AES) will be important ingredients to safeguard sensitive data and minimize the risks of adversaries entering the IT infrastructure. We also believe that a central management console is necessary for control and provisioning and that remote capabilities for provisioning, adjusting, remote wipe, and compliance insurance will also be de rigueur in future remote security management schemes. We applaud efforts of vendors like Trust Digital who are addressing today’s and tomorrow’s security needs as the technology itself is implemented.

Finjan Offers New Approach to Address Unforeseen Nature of Future Threats

By Lawrence D. Dietz

Finjan, a Web security product vendor, has announced that its patented realtime code inspection technology is the only Web security product that detected malicious code on a potentially destructive Web page propagated by a malicious Russian Website earlier this month. Finjan subsequently communicated its discovery of the malicious code to an independent online security industry benchmark website, VirusTotal.com, which benchmarked the code against thirty-two well known Web security products. Upon completion of the benchmark, VirusTotal established that the entire list of products failed to detect the code as malicious and as a result did not block it. Finjan's Vital Security Web Appliance was the only security solution that managed to detect and block the code in realtime, without any product update or signature. The malicious code detected is discussed in detail in Malicious Page under Benchmark, a report from Finjan's Malicious Code Research Center (MCRC). The malicious code exploits various browser vulnerabilities and uses AJAX technology to download and execute malicious code from a remote server. Simply by visiting this page, without taking any action, the visitor's machine is infected.

It should be noted that an important aspect of the benchmarked page was its use of dynamic code obfuscation to hide the malicious code. The company claimed that "this technique is increasingly popular among hackers as a way to create malware that eludes traditional signature-based solutions like antivirus and URL filtering. “

Sageza believes that, as Richard Clarke once said “The future will not be like the past.” Over time adversaries will employ more sophisticated means to attack their chosen targets. We concur with other industry leaders who believe that targeting is becoming more sophisticated and that financial gain is by far the most significant motivator at this time. An interesting characteristic of the hacker world is that it continually attempts to develop tools that lower the amount of technical expertise and resources needed to wage a successful attack.

As we’ve stated in the past, merely detecting a problem or warning an end user about a potentially dangerous condition is not adequate protection. Finjan’s technology appears to add a new dimension in Web security by detecting and blocking obfuscated malicious code in realtime. While we haven’t tested the product, Sageza believes that an ounce of prevention is worth more than a pound of cure, and in the case of safeguarding your Web technology it may be worth tons. Large organizations in particular need to opt for technology that prevents problems rather than merely reporting them.

New 160GBps Optical Chipset Research from IBM

By Clay Ryder

IBM scientists have unveiled a prototype optical transceiver chipset capable of reaching speeds at least eight times faster than optical components available today. The announcement, which took place at the 2007 Optical Fiber Conference, highlighted the potential to move information at 160GBps, fast enough to provide a one-second download time for a typical high-definition movie. The company stated that shrinking and integrating the components into one package, and building them with standard low-cost, high-volume chip manufacturing techniques, will allow it to make this optical connectivity viable for widespread use. One scenario offered that the technology could be integrated onto printed circuit boards to allow the components within a PC or set-top box to communicate much faster, thus dramatically enhancing performance. To achieve this level of chipset integration, researchers built an optical transceiver with driver and receiver integrated circuits with CMOS technology, the same high-volume technology used for most chips today, and then coupled it with other optical components made from exotic materials, such as indium phosphide (InP) and gallium arsenide (GaAs), into an integrated package measuring 3.25 by 5.25 mm. This compact design provides a high number of communications channels as well as very high speeds per channel, resulting in what the company states is the highest amount of information transmitted per unit area of card space ever.

Sometimes geeks have all the fun. Blazing fast is always cool, whether it is for automobiles, processors, or connectivity. While this technology is obviously just beginning its movement towards commercialization and eventual productization, the implications of its sheer throughput are enormous. When one thinks about blazing fast network connectivity today, 4GBps is a decent benchmark with 10GBps more-or-less acting as a generally available upper limit, although there are the rarefied few options that speed even faster along. This chipset offers an order of magnitude plus improvement over commonly available technology in a package the size of a small pencil-tip eraser. Visions of George Jetson and personal jet packs start coming to mind.

But in all seriousness, let's consider the ramifications of this level of communication speed on IT infrastructure. Assume that all network fabric becomes optical-based and supports this speed, what happens to other electrically and mechanically based components? What would have to happen to make storage technology be able to fill or empty a pipe this size? The striping and RAID techniques available today pale by comparison in their ability to sustain information throughput. Processor cores are faster than ever, but even with blazing instruction execution, the state of backplane chips are about advanced as a dirt trail is compared with an Autobahn. We will forgo the moot discussion of how affordable WAN connectivity to the end user would consume this bandwidth.

The press release states this prototype offers a glimpse of a new era of high-speed connectivity that will transform communications, computing, and entertainment. Although some would point to this announcement as proof that the DVD and CD are dead, as everything will download to the media-center set-top box in a second, we are quick to point out there are many other factors to be overcome before this scenario would be realized. Nevertheless, the potential of this level of optical communication speed could severely alter how we view the rest of data center, and ultimately where the industry next invests in solving the IT bottleneck. We are excited and enthused, but also patient; nevertheless, we will be watching for the future announcement of the first commercial use of this technology.

GFI's Latest and Greatest LANguard N.S.S.

By Susan Dietz

Recently GFI announced the newest version of its LANguard Network Security Scanner (N.S.S.), version 8. This latest version addresses the three pillars of vulnerability management: security scanning, patch management, and network auditing, combined into one integrated solution. GFI LANguard N.S.S. 8 is a cost-effective solution for businesses to safeguard their systems and networks from hacker attacks and security breaches. LANguard N.S.S. 8 scans the entire network for over 15,000 vulnerabilities, identifies all most-likely security issues and provides administrators with the tools they need to detect, assess, report, and remediate any threats before hackers do. It has over 2,000 new vulnerability checks— using SANS top twenty and Open Vulnerabilities Assessment Language (OVAL) security definitions—over and above the vulnerabilities which are discovered through its inbuilt vulnerability assessment functionality. OVAL is an international information security community standard, and this is the first time that this technology is being made available to SMBs as OVAL is mainly offered in enterprise level solutions. Apart from more extensive vulnerability scanning capabilities, LANguard N.S.S. also has a performance-enhanced scanning engine, additional patch management functionality, and an intuitive graphical threat level indicator. The latest version has received a variety of patch management improvements including added support to rollback Microsoft patches as well as technology to automatically download new Microsoft security patches when made available. It also supports scanning for vulnerabilities on Windows Vista-based systems. As part of the launch, LANguard N.S.S. 8 also includes a ReportPack add-on with over thirty customizable reports, which automatically generate graphical IT and management-level reports based on data collected during security scans.

Traditionally, companies have taken the approach of building for the enterprise, then scaling back the product to try and sell to the SMB market. But over time some companies have figured out that simply decreasing the dimensions of a product doesn't necessarily make it fit, and so are beginning to build specifically for the SMB market in the first place. GFI seems to have taken the reverse approach. Their focus has traditionally been the SMB market with the ability to scale to enterprise. However, it seems a good guess that the modified fit would be just as wonky. Building for the market you are targeting is generally the best approach. Granted, some companies, with their exit strategy developed right along with their business plan, are only concerned with the short term. GFI seems to be cut from a different cloth than some companies, however, and appears to have its gaze focused on the horizon.

Another trend that GFI is riding is making the security package configurable to the current OS system of the client. Giving customers a la carte choice rather than a package deal puts the control of the company where it should be: in the customer's hands rather than in the computer company's. We believe the days of buying every last IT need from one gianormous WeSaySo Corporation are numbered, even though developing a product then selling that product to WeSaySo Corporation will always be one way of doing business. But more boutique companies are starting to recognize that due to litigation and lawmakers, world domination from one or two large companies is most likely going the way of the dinosaur and that perhaps hanging onto their company and building more market share is going to be the smart option in the long run.