Market Roundup

March 16, 2007

Iron Mountain Physical Storage and New Archiving Service for Email Good Combination

Seagate Now Shipping Hardware-Encrypted Notebook Drives

SPI Dynamics Web UI Adds Needed Perspective

HP Meets New ENERGY STAR Regulations

:sageza:

Iron Mountain Physical Storage and New Archiving Service for Email Good Combination

By Lawrence D. Dietz

Iron Mountain Incorporated this week introduced its Active Archiving Service for Email, a comprehensive solution for managing email storage, retention, and legal discovery. The new archiving service allows businesses to cost-effectively reduce their email storage burdens, apply granular email retention policies, securely archive email, and enable efficient ediscovery of messages while providing end users with easy access. It completes Iron Mountain's Total Email Management Suite that aims to provide email storage management, discovery, continuity, and disaster recovery and security services in a single, integrated, solution. The Active Archiving Service for Email, which is delivered through a partnership with MessageOne, is available on its own or as part of Iron Mountain's Total Email Management suite. The full suite includes Continuity Service for Email, a managed service that can be rapidly activated following a network interruption, facilities outage, or other event that disables an organization's primary email system; and Security Service for Email, a managed service that automatically eliminates spam, viruses, and unwanted content from the email environment. Additional features of the Active Archiving Service for Email include flexible storage management, auditing of email retention policies with support for litigation holds; ediscovery to make it easy for legal counsel and authorized users to search selected mailboxes and export results to legal review tools; and integration with Microsoft Outlook to allow end users to work in their familiar email environment. The Active Arching Service for Email, along with the Total Email Management Suite, is immediately available in the U.S, UK, Germany, and France, with plans to introduce to other countries over the coming months. In the U.S., the Total Email Management Suite pricing starts at $6 per user per month.

Just as it is impossible to separate people, process, and technology, sometimes it's equally difficult to separate the physical from the virtual. When it comes to the information and document life cycles, Sageza believes that organizations need to protect information based on its value, not its form. In the Defense world classified information is classified whether hard copy, electronic, or verbal. Consequently the protection mechanisms that are applied in national security matters are based on the classification of the information, not where it's found. Best practices call for an integrated and holistic approach to information protection. Furthermore, we have noticed a trend by larger organizations to try and reduce their cost of purchasing operations by reducing the number of vendors they deal with.

Given the need to protect information and data across the organization and regardless of format, it would appear that Iron Mountain may be positioned to take advantage of technology trends by varying their way of delivering services and offer end-user organizations a way to reduce their cost of acquisition.

Seagate Now Shipping Hardware-Encrypted Notebook Drives

By Clay Ryder

Seagate Technology has announced that it is now shipping its Momentus 5400 FDE.2, an encrypting 2.5-inch notebook PC hard drive for notebooks, to ASI Computer Technologies. The Momentus 5400 FDE.2 (Full Disc

Encryption) hard drive offers up to 160GB of capacity, Serial ATA interface, and hardware-based AES encryption. The encrypting hard drive is also positioned as a means by which organizations can easily repurpose or retire laptops without compromising sensitive information and comply with data privacy laws. ASI Computer Technologies plans to offer the drive in its new ASI C8015 system, which will also feature a biometric fingerprint reader for stronger user authentication. The laptop will target healthcare, legal, finance, government, and other industries requiring strong protection of information stored on laptop PCs. The C8015 will feature Wave Systems Embassy Security Center's Trusted Drive Manager, software that simplifies setup and configuration of Momentus 5400 FDE.2 drives. Trusted Drive Manager also makes it easy for administrators and users to create and backup passwords, and for administrators to control hard-drive policies and security settings. The software also leverages Seagate's DriveTrust Technology to allow administrators to instantly and easily erase all data cryptographically so the drive can be safely redeployed or discarded.

With all the fuss about security, data theft, compliance, and whatnot, the market has seen many vendors ply their data security solutions ware with an increasing zeal. Software-based encryption for files or hard drives is not new; however, the interest in it has grown considerably in light of recent embarrassing, if not illegal, data leaks or losses reported by various organizations. One of the challenges with software encryption is that it is generally not well understood by the technical layperson, and implementations often tend to be limited or specific in nature, e.g., encrypting email or certain files associated with a given application. By incorporating encryption at the hardware level, its use can be largely invisible to the user, which can remove a large obstacle to an effective deployment.

While many may view encryption of mobile devices such as notebooks solely as a means to block access to sensitive data in case of loss or theft, it can also prove advantageous to IT professionals. Depending upon the practices of an organization, sometimes a notebook may be "reassigned" to a new user, without IT's knowledge. It probably will not have been recovered to its factory-shipped configuration and the drive may still contain sensitive information even if it was deleted. With configuration software such as the Trusted Drive Manager, IT can intercept such a transfer at the preboot authentication phase by having the system not grant access if the user is not recognized as part of the preboot authentication, which is under the control of IT. The system would then flow back through IT, which can then take whatever preventative actions necessary to ensure the safety of sensitive information before repurposing the notebook to its new user.

Hardware-based encryption for notebook hard drive is new, and obviously it will be some time before it is commonplace. Nevertheless, we believe the security and best practices afforded by their use in highly regulated industries is a no-brainer and expect to see such deployments grow, especially as Seagate signs up more and larger notebook vendors to include the Momentus 5400 FDE.2 and similar solutions into their product offerings.

SPI Dynamics Web UI Adds Needed Perspective

By *Lawrence D. Dietz*

S.P.I. Dynamics, Inc. has announced its latest version of the Assessment Management Platform (AMP), version 3, that includes a Web-based interface for multi-user lifecycle collaboration and control of application security risk throughout the enterprise in a consolidated global view. AMP 3 includes a new Web user interface to give security professionals, executives, line managers, developers, and quality assurance teams anytime/anywhere access to AMP functionality. Core application security experts can now extend their team by giving developer and QA professionals the ability to quickly execute application security tests or access information about application security quickly without the effort associated with software installation, configuration, and maintenance. The Web interface provides users the ability to configure their interface, data, and dashboards exactly as they need them. Organizations are able to reduce costs by using AMP throughout the application development lifecycle for collaboration on finding and fixing application-level security defects early prior to production. AMP 3 also includes a new risk management component, application weighting, which allows users to prioritize and sort applications within their organization by a combined risk score that is based on vulnerabilities found and the importance of the application to the business. This enables organizations to identify and focus on the riskiest sites without having to manually score all of the sites; AMP prioritizes all sites based on their risk score giving security professionals the information they need to plan and manage remediation programs.

Today, security professionals in all industries are dealing with an ever increasing and overwhelming number of applications, vulnerabilities, and technical experts around the world. They must identify critical applications, maintain a holistic risk management view, and give numerous stakeholders visibility into the state of application security across the enterprise. While doing this, they must scale their assessment processes across the enterprise and throughout the lifecycle to developers, quality assurance teams, other security professionals, and even line-of-business managers who own the applications. Organizations are striving for proactive application security programs that find vulnerabilities early in the lifecycle, to avoid excessive costs associated with fixing defects in production applications. To do so, all of the stakeholders and participants require easy access to robust application security testing tools that do not require security expertise. AMP 3 is powered by SPI Dynamics' new Phoenix product architecture, which is able to analyze complex Web 2.0 applications to reveal previously undetectable vulnerabilities.

While many have talked about the US SOX regulation, few have delved into some of the less obvious ramifications of the requirement to validate the integrity of the organization's IT systems. The Software Development Life Cycle (SDLC) is generally something that is not top-of-mind to auditors and even security professionals. However, for organizations that are developing their own software, validation of the security of that development and continual evaluation of application security are ongoing requirements. While commercially purchased software may claim various levels of application security, the astute organization will trust no one and validate everything.

Sageza believes that the SDLC is becoming more complex for a number of reasons. First of all most large organizations have distributed development teams. In addition, key stakeholders such as information security, risk assessment, governance management, and so forth are distributed as well. We are of the opinion that a secure, Web-based infrastructure seems to be the most logical way to address the security issues inherent in the SDLC and the SPI Dynamics architecture appears to be a step in that direction.

HP Meets New ENERGY STAR Regulations

By *Susan Dietz*

On July 20, 2007, ENERGY STAR 4.0 regulations go into effect, and HP claims it is ready. Recently, HP announced its first business PCs that are configurable to the new EPA standards. The HP Compaq dc5700, dc5750, and dc7700 desktop PCs are designed to meet business customers' growing requirements for more efficient power management and cooling. HP has designed the new PCs to include increased system reliability and reduced system maintenance costs, as well as decreased air conditioning costs—all due to less heat generation, which can also extend the life of the system. Select HP Compaq dc5700 and dc7700 business desktop PCs meeting the ENERGY STAR 4.0 hardware specifications are available now and feature Intel Core 2 Duo processors, Microsoft Windows XP Pro, 80GB hard drives, 1GB of memory and DVD/CD-RW combo drives, starting at $899 and $959, respectively. ENERGY STAR 4.0 configurations are also available for the HP Compaq dc5750 business desktop with AMD Athlon processors, Microsoft Windows XP Pro, 80GB hard drives, 512MB of memory and DVD/CD-RW combo drives, starting at $609.

We imagine that even though the target market is business, consumers will also be early adaptors of the technology, in part because it is less risky to buy one PC than 1,000, and the economies of scale would dictate that HP will eventually roll these capabilities across a broad portion of its product portfolio. However, businesses are always looking for ways to reduce overhead; if they can help out the environment along the way, so much the better. We believe that the energy cost savings from HP's new desktops will help make them attractive and it represents another step in the right direction, as every little bit helps. One of the big problems is still the huge amount of waste from old PCs and laptops not being recycled or properly disposed of. This is something that HP and its market challenger Dell as well as Fujitsu Siemens in Europe have recognized for some time. On the other hand, not all PC manufacturers have been touting their strategies for making their machines more energy-efficient. An environmentally friendly solution that saves end users money is likely to be more rapidly adopted by the marketplace, even if certain regulatory initiatives issues seeking to address the issue are in the offing.

Green is the new black. However, everyone is paying lip service but few are following up. The companies that are making steps forward in that direction, no matter what size steps they are, deserve accolades and awards. The

---

report that Greenpeace puts out periodically is one way to track progress; a monetary incentive would be even better: a sort of Nobel for the tech world, say. However, as end users battle higher energy costs, appliances that use less electricity are become more attractive and thus generate more sales. That in itself may be enough of a financial incentive for more green innovations from a larger sampling of companies. If the U.S. Congress believes in saving energy to the extent that it flagrantly messes about with Daylight Savings Time, then it won't be long before it turns its attention to other aspects of our lives. HP seems to be ahead of the curve and at least three steps ahead of the U.S. government. We applaud their efforts.