

# [ UPLOAD ]

NEWS, REVIEWS, AND PERSPECTIVES



Stephen Trilling, Vice President  
Symantec Research Labs

## ■ SNEAK PEEK

# Symantec Research Labs

## SPACE SAVER

Organizations will soon be able to take better advantage of their virtual machine-based data centers, thanks to a new storage management technology being investigated by Symantec Research Labs (SRL).

Today's enterprises are increasingly moving to virtual machines (VMs) to save money on equipment and to reduce complexity. While migrating to a virtual machine-based environment confers benefits, it also creates challenges for administrators, especially with regard to storage management.

SRL's new technology, known internally as VM-Aware Storage, will reduce disk space by several orders of magnitude in data centers that employ large numbers of virtual machines. "Imagine you have 100 virtual machines in a data center. They're each running the same Apache Web Server. Suppose each of those virtual machines has 100 gigabytes of hard drive space associated with it," says SRL Vice President Stephen Trilling. "A traditional storage management solution would store 100 gigabytes for each



of the 100 virtual machines, equaling 10 terabytes of storage. However, we know all the VMs are running the same Web server software, meaning that each has a largely similar set of files. So we thought rather than storing all that data, let's eliminate duplicate files and save companies money."

With the new solution, just one copy of the base image of the Apache Web Server (100 GB) would be stored, plus any machine-specific differences (1 GB for each machine or 100 GB total). In this example, the total storage needed is 200 GB, which is 50 times less than the 10 terabytes required with traditional storage mechanisms.

Symantec researchers plan to extend the VM-Aware Storage system to improve efficiencies in patching, cloning, backup, and rollout of VM storage in the future. VM-Aware Storage will be built into Symantec's existing storage management solutions.

PHOTO: MARK ESPERT; PHOTO: GETTYIMAGES

## ■ NEWS

### >> Customers

[ Follow the Sun ]

Sun Microsystems is standardizing on Symantec's Veritas NetBackup throughout its enterprise. The move is part of Sun's Integrated Business Information Solution (IBIS) project, an

initiative to optimize its global environment by standardizing on key technologies and applications. "This will help us reduce the cost and complexity of our data center environment," says Gordon McGowan, IT operations director of Sun Microsystems.

### [ Missouri: This Time, No Compromise ]

Missouri has standardized on Symantec's desktop security solutions to improve the protection of the state's desktop environment. The state has implemented Symantec AntiVirus desktop protection for 50,000

seats across 14 departments, resulting in an estimated cost savings of US\$836,000 over three years. "Symantec allows us to offer our state a high level of protection at a great price-performance value," says Dan Ross, CIO of the state of Missouri's Information Technology Services

## ■ IT'S ALL GOOD

# Green: The New Black

Whether your motivation is social or economic, there's plenty of green (as in dollars) to be had in going green (environmentally conscientious).

Companies around the globe are starting to wear their environmentally friendly policies on their sleeves. Industry leaders such as Dell and HP have initiatives offering to recycle hardware and peripherals for free. As data centers grow—and along with them, the energy bills to keep them cool—CIOs are likewise giving 'eco-nomics' a closer look.

Implementing sustainable policies and processes is not only good for publicity, it's good for the bottom line. Here are some steps your organization can take to demonstrate a commitment to cleaner environments:

- Buy from local suppliers whenever possible. It cuts transit costs and lowers fuel consumption.
- Replace incandescent bulbs with compact fluorescent bulbs.
- Create and distribute a report that discloses energy usage by function (printing, faxing, running reports, queries, etc.) to make people conscious of the cost and environmental impact of their actions.
- Work with vendors who demonstrate a commitment to green business practices.
- Use videoconferencing instead of travel whenever possible.
- Create a committee within IT to explore ways your organization can become more energy efficient. Can you consolidate servers? Implement virtualization technologies?

## >> Identity Crisis

**60%** The percentage of U.S.-based businesses that believe they are unable to effectively assess or quantify "insider threat" risks.

**64%** The percentage of those same businesses that have deployed an access and identity solution, including access control, password management, provisioning, and role management.

[SOURCE: Survey on Identity Compliance, Ponemon Institute, and SailPoint Technologies]

Division. "Within two years, we expect a 100 percent payback from using Symantec technology and plan to reinvest those savings in other critical areas of the IT infrastructure."

[ **The Medium Is the Message** ]  
Media General, Inc. owns and operates three metropolitan newspapers, 25 daily newspapers,

150 weekly newspapers, 23 network-affiliated television stations, and an interactive media division that includes more than 75 online enterprises. The media giant is using Symantec software and Symantec Global Services to improve instant messaging (IM) security and to protect critical data. Symantec IM Manager helps prevent threats from penetrating

Media General's network. "Symantec IM Manager helps enable us to focus on delivering content to our readers and viewers rather than worry about network security and data protection issues that could hinder our ability to get a newspaper out the door or keep a station on the air," says Mike Miller, director of support services for Media General.

## >>Products

### [ **360 Degrees of Separation** ]

Norton 360—the all-in-one security service from Symantec that combines Norton's industry-leading technologies for antivirus, antispyware, firewall, intrusion protection, antiphishing, backup, and tuneup—was recently awarded the CNET Editors' Choice Award. Norton 360 comes with ➤

## >> Top 10 Mistaken Methods of Estimating Cyber Attack Costs

1. Adding up the cost of lost capacity
2. Neglecting costs of substitute procedures employed during cyber attacks
3. Assuming the sum of losses to individual companies equals the loss to the economy
4. Neglecting lost value experienced by customers
5. Focusing solely on lost revenues instead of overall costs of cyber attacks
6. Assigning standard productivity rates to IT equipment and calculating losses by downtime
7. Equating information value with the cost of creating it
8. Assuming losses of revenue from stolen products equals the total loss
9. Examining stock prices or capitalization
10. Improperly reconciling multiple business activity measurements

[Source: Scott Borg, Director and Chief Economist of the U.S. Cyber Consequences Unit]

# [UPLOAD]

## ■ TAMING TOOLS

### Moving Target

#### *Getting a handle on mobile devices*

Since new functionality and devices always add complexity, most—if not all—of IT is a double-edged sword. Mobile devices, which include everything from PDAs to portable storage devices, are one of the most important technological tools impacting the work environment today. The use of these tools puts pressure on IT organizations in myriad ways. Malware enters the IT environment via cell phones and PDAs; data is leaked, whether from a lost or stolen laptop or via information transferred to a portable storage drive; and support costs are increased as these devices are increasingly utilized away from the office.

Try these strategies to gain control over mobile devices:

**SIMPLIFY.** Study the available mobile solutions and settle on the one that's best for your organization. This way, you will

only have to maintain and support one standard.

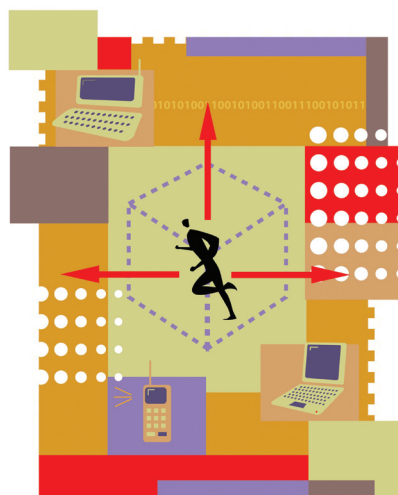
**PREDICT.** Try to stay ahead of users by developing a strategy for managing mobile devices. With a strat-

**40%** The percentage of large enterprises that do not have a mobile device management policy.

[SOURCE: BPM Forum]

egy in place, you—not users—will determine what standards to adhere to, which devices will be supported, and what types of usage are acceptable.

**CALCULATE.** Examine which users need mobile services, which services your users need, and the extent to which they really need them. Not every piece of information is needed in real-time, for example.



## ■ NEW TECH

### Seeing Savings

#### Optical storage comes into focus

The wave of regulatory compliance that has swept across the enterprise landscape over the past five years has spawned any number of technologies in response to new retention and reporting policies. Now, add one more technology to the list: ultra-density optical (UDO). With libraries capable of storing up to 19 terabytes of data and energy consumption costs decreased to a possible range of less than 10 percent of the cost of magnetic media, UDO is starting to see the light of day as an alternative and a complement (not a replacement) to more traditional storage media. The low-cost, high-capacity UDOS give storage execs another option in an alternate media to ensure that data is never lost.

an add-on pack of online tools that includes parental control and antispyware. Optional features include a tool that blocks private data from leaking onto the Internet.

#### [ Recovery Rules ]

Symantec recently released Symantec Backup Exec System Recovery 7.0, the latest version of its Microsoft Windows system

recovery solution. Enabling businesses to recover complete Windows systems in minutes, Backup Exec System Recovery also introduces enhanced Microsoft Exchange, virtual, and data recovery capabilities. The new version also includes centralized management to give IT administrators added flexibility and simplification when it comes to protecting IT assets.

#### [ Back Me Up, Scotty ]

Symantec has introduced the beta version of the Symantec Protection Network. Symantec's first software as a service (SaaS) platform, it is designed to deliver easy-to-use security and availability offerings to small and mid-sized businesses at a price they can afford. The Symantec Protection Network's first

offering is Online Backup Service, which enables cost-effective, reliable backup and restoration of business-critical data from the convenience of a Web browser. Full-scale services will be available later this year.

#### [ Going Mobile, Securely ]

Now available: Symantec Mobile Security Suite 5.0, a solution

## ■ SPEAR PHISHING

# Making Sure the Big One Gets Away

U.S. Department of Defense casting a wider net to deter spear phishing

**T**rolling for information is one thing; setting a trap is another. While neither is acceptable to agencies such as the United States' Department of Defense (DOD), the latter—known more commonly as spear phishing, where specific types of information are sought from specific individuals or agencies—is the more dangerous. To combat spear phishing, the agency, which oversees the U.S. military, is adding additional layers of security.

System users at the DOD must now log on to networks with a common access card (CAC) that verifies identity and provides a digital signature with the key contained on the card. Email messages must be in plain text to avoid malicious programming code that can plant viruses, key-stroke loggers, and other malware on computers.

## >> Missing In Action

**478** The number of laptops reported as lost or stolen by the United States Internal Revenue Service (the U.S. tax collector) between 2002 and 2006.

**112** The number of those lost or stolen laptops that were believed to contain sensitive data such as Social Security numbers.

[SOURCE: Attrition.org]

## >> Is Thin in Again, For Real This Time?

**T**hin client computing—effectively diskless desktop computers that rely on centrally located servers to perform most processing and administration tasks—has been around for years. But it wasn't until recently that the state of computing affairs reached a point where taking the thin approach makes sense on enough levels to implement it. Here are some reasons to consider slimming down:

> **SECURITY, SECURITY, SECURITY.** The recent high-profile breaches in computer security make thin clients—with their essentially empty data footprints—an unwelcome target for thieves.

> **VIRTUALIZATION.** The increased trend toward virtualization on the server side of operations meshes nicely with a thin client approach. Virtualization techniques, masking the physical location of IT resources from end users, make for a smoother user experience while lowering costs and maximizing resources.

> **SAVINGS TRACK RECORD.** Thin client computing has been around long enough for its savings to be documented. Fewer moving parts mean fewer touch points for repairs, upgrades, and maintenance. This translates to lower costs. Thin clients also reduce energy consumption more than PCs.

> **OPTIONS.** Recent entries into the thin client computer arena have led to more choices in machines and operating systems, effectively driving down their costs.

> **64-BITS.** As 64-bit computing gains ground in the enterprise, thin client computing becomes geometrically more attractive. A 32-bit server supports 72 concurrent users; a 64-bit server supports more than 500 users concurrently.

> **EASE.** Applications become ubiquitous for all authorized users no matter where they are. Users literally plug-and-play whichever applications they need, whenever and wherever they want.

designed to provide enterprise customers with the same security and data protection capabilities on their Microsoft Windows mobile smartphones and PDAs as they have on their laptops and other computing devices, is now available. Symantec Mobile Security Suite 5.0 includes antivirus, firewall, anti-SMS spam, and data encryption technologies that are easy to deploy, manage, and maintain.

[ **Discarding Dupes** ]  
By leveraging the data deduplication capability of PureDisk as part of their overall backup strategy, customers can dramatically reduce the amount of storage and bandwidth consumed from disk-based backups. New enhancements to NetBackup PureDisk enable the deduplication and allow enterprise customers to use

a single application—Veritas Backup Reporter—to consolidate reporting on the backup activities of PureDisk, NetBackup, and other major backup applications. Centralized backup reporting and the ability to plan growth based on the historical data of all backup types allows for better backup management and the customization of backup methods including tape

backups, snapshots, and data deduplication.

## >>Community [ All in the Digital Family ]

To minimize the generation gap between many parents and their cyber-savvy children, Symantec has introduced a nationwide initiative in the United States. The program includes the appointment of Marian Merritt as the company's Internet >

# [UPLOAD]

## ■ SENSE OF SECURITY

### Two-Minute Drill

Security technology expert Bruce Schneier reveals his views on IT security risks.



**B**ruce Schneier is known for his wit and ability to communicate complex security issues in accessible business language. The author of eight books, he also publishes *Crypto-Gram*, a monthly security technology newsletter, and is the founder and CTO for BT Counterpane, an authority on protecting corporations against emerging IT threats. His latest book, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*, addresses the problem of security from personal safety up to the corporate and national security levels. He has an M.S. degree in computer science from American University in Washington, DC, and a B.S. in physics from the University of Rochester in New York.

**Q: When did you first become interested in security?**

**A:** As a kid I would see security systems everywhere, and puzzle out how to get around them. My father created coded messages for me to break. Security is a mindset first, and a skill set second.

**Q: Can you narrow it down to a specific event, moment, or issue that caught your attention?**

**A:** I remember walking around department stores, and figuring out how to avoid the security systems. I remember my mother taking me with her to vote, and me telling her about security flaws. I'm lucky I was taught ethics.

**Q: You've said that security "is both a feeling and a reality. And they're not the same." Can you elaborate?**

**A:** As technologists, we concentrate on the reality of security: how secure people are. Equally important is how secure they feel. Even if we do a perfect job making people's Internet shopping experiences secure, for example, they're still not going to use the service if they don't feel secure.

**Q: What should people be most worried about online?**

**A:** Crime. Crime is the Internet's most serious problem. For the most part, everything else can be defended against by a good set of backups.

**Q: You've said that security is a question of making trade-offs. Can you give an example of this?**

**A:** We make security trade-offs every day. For example, this morning, when I decided not to put on a bulletproof vest and double-lock my front door. Every even slightly advanced species on the planet makes security trade-offs all the time.

**Q: Will new security risks emerge due to new technologies, or do you think it will be more of the same?**

**A:** There hasn't been a new security risk in a millennium. For example, identity theft is just fraud based on impersonation. What changes are particular tactics. Changes in technology make certain tactics or defenses cheaper or more expensive, and that changes the nature of the risks. As long as technology continues to change at its present pace, that kind of thing will continue.

—Alice LaPlante

STEVE WOOT

Safety Advocate and the launching of the Family Resource Web site ([www.norton.com/familyresource](http://www.norton.com/familyresource)), which is aimed at helping parents deal with topics such as social networking, cyber ethics, privacy, and online gaming.

#### [ Innovation Comes Home ]

In April, Symantec hosted a forum on innovation at its Cupertino,

California headquarters. The forum examined strategies and programs needed to increase the development of talent needed to strengthen innovation in the United States and help maintain its global competitiveness. The forum was held as part of the National Governors Association's (NGA) Innovation America initiative. Attendees included Dr. Robert

Dynes, president of the University of California collegiate system; Sean Walsh, special advisor to California Governor Arnold Schwarzenegger; Cathleen Barton, manager of U.S. Education, Intel Corp; and Tom Malloy, senior vice president and chief software architect, Advanced Technology Labs of Adobe. The event was chaired by NGA Chair and Arizona Governor

Janet Napolitano and Symantec Chairman and CEO John W. Thompson.

#### [ Scholarly Endeavors ]

Symantec Research Labs has awarded one-year fellowships covering 100 percent of tuition and fees, along with a research stipend, to David Brumley, Jack Lange, and Justin Ma. The

## ■ MIDYEAR MAINTENANCE

# It's Midway Through 2007. How Safe Is Your Data?

Securing enterprises—and the information assets inside them—has never been more challenging. New threats, old threats, and even old threats dressed up in new clothes put information at risk around the clock. Assess if you are doing all you can to mitigate risk by contemplating these strategies:

- **Discard unnecessary data.** What you don't need can hurt you. Data that lingers longer than regulations mandate can come back to haunt you.
- **Consider new ways to identify files.** Phone numbers, social security numbers, and other publicly identifiable means of sorting files exposes you and your customers to unnecessary risks. Create unique IDs that don't simultaneously create a lucrative target for thieves.
- **Be vigilant about passwords and password policies.** As the key that unlocks the digital entrance to the enterprise, the importance of strong passwords and

a policy that keeps criminals guessing about them goes a long way toward keeping data safe.

- **Shine a beacon on the situation.** Beacon software, which sends out a signal every time a PC is connected to the Internet, can help trace lost or stolen laptops.
- **Encrypt it.** Less than 40 percent of companies say they encrypt data at rest on tapes and disks. Encryption may slow business down, but not nearly as much as data falling into the wrong hands would.
- **Put up a perimeter.** Establish a policy as to which types of data can leave the company premises and which types can't. Then, enforce the policy.



## To Encrypt or Not to Encrypt? That's Not the Question

The need to add one more layer of protection by encrypting data is becoming increasingly apparent. What's not so easy to decipher is which method of encryption to use: source encryption, hardware encryption, or backup software encryption.

The tradeoffs are accessibility versus performance. The importance of the data itself—how secure it needs to be and how often it needs to be retrieved—may help you choose one method over another.

If you have highly sensitive data, you'll want source encryption. If you have data that only needs to be encrypted as it leaves one system on its way to be backed up, you need backup software encryption. Both of these methods have serious performance and capacity drawbacks—as much as 50 percent in some cases. If you don't want to figure out which data should be encrypted and which should not, consider hardware encryption.

TODD DAVIDSON

program also includes the option of a salaried summer internship, offering recipients direct on-site collaboration with leading scientists from Symantec Research Labs.

Brumley is a doctoral candidate in computer science at Carnegie Mellon University working on novel binary analysis techniques for computer security. Lange, a

doctoral candidate in electrical engineering and computer science at Northwestern University, is interested in high-performance distributed communication frameworks for optical networks. Ma is a doctoral candidate in computer science and engineering at the University of California, San Diego, whose primary work

revolves around malicious code analysis and defense.

### >>Corporate

[ **A New Configuration for Altiris** ] Symantec recently completed its acquisition of Altiris, the pioneering developer of service-oriented management solutions. The first offering will be Altiris CMDB Solution, which is natively built

on the Altiris service-oriented architecture to provide tight integration with Altiris execution tools for closed-loop IT service and configuration management. CMDB Solution provides an alternative means of automating configuration management and servicing an IT environment, going above and beyond basic information and relationship tracking.