

WHITE PAPER

The Data Protection Imperative in the Enterprise Remote Office

Sponsored by: Symantec Corporation

Laura DuBois
June 2006

EXECUTIVE SUMMARY

Enterprise IT departments are facing a corporate imperative for the secure protection, availability, and recovery of enterprise remote office operations and data. Paramount to a firm's ongoing utility is how to securely and centrally control, manage, and restore, if required, data that resides in many disparate, resource-limited enterprise remote offices. Critical data — such as medical records, images, account information, invoices, inventory data, sales histories and contracts, and client communications — that resides in enterprise remote offices but outside of IT datacenter control must be protected. Absent effective data recovery and availability, firms face operational risk, which can compromise their enterprise remote office productivity; impact time to market, supply chain efficiency, and customer satisfaction; or bring about cost penalties, fines, or negative publicity.

Firms without an enterprise remote office data protection strategy are developing corporate datacenter-managed initiatives. Firms with resource-limited, costly, or unreliable locally based tape backup are shifting to a centrally managed and controlled WAN-based data protection approach to satisfy business requirements and meet the demands of increasingly stringent business unit service-level agreements (SLAs). In response to the increasing need for cost-effective, centralized control for enterprise remote office data availability, recovery, and administration, capacity-optimized, disk-based enterprise remote office data protection solutions are emerging to address the historical enterprise remote office data protection challenges, which include:

- ☒ No technical staff available at enterprise remote offices to manage backups, pull tapes, troubleshoot software or hardware errors, initiate restores or recoveries, or ensure that backups occur
- ☒ Security or regulatory compromise to sensitive corporate data on removable tape media resident in the enterprise remote office location that can be subject to loss or theft
- ☒ No assurance that enterprise remote office backups are scheduled or completed successfully, impacting recoverability as well as new systems and data within the enterprise remote office (i.e., they are not assigned a backup policy)

- ☒ Expensive, redundant backup processes at each remote office location, creating islands of disparate hardware, software, data, and resources that are managed separately and outside the control of a centralized IT policy
- ☒ Growing and redundant backup data at the remote office that exceeds WAN network bandwidth, bringing WAN communications and processing to a crawl and impacting productivity
- ☒ WAN network latency and disruptions causing a remote office to become disconnected and impacting remote office backup performance or causing backup job failures
- ☒ Inability to meet remote office recovery time or recovery point objectives from recovery off tape media, impacting business continuity and operations
- ☒ Need for backup, local to the remote office, for easy user-level file restore, but also still sent to a centralized datacenter for disaster recovery
- ☒ Today's enterprise remote office landscape

Firms of varying sizes, in many different industries, are facing the need to centrally connect with and manage an increasing number of remote or branch office locations. The growth of advanced networking has brought about increased WAN connectivity and the recentralization of IT resources, while technologies such as intranets, email, instant messaging, online applications, and integrated voice and data networks have increased communications between corporate headquarters and remote or branch locations. As firms increase their dependence upon technology such as email, instant messaging, Web/online commerce, applications for supply chain integration, RFID and wireless technology, these services are being used for critical business and operational processes, customer transactions, and client communications.

However, the pervasiveness of technology is not the only factor driving the emergence of remote or branch offices. Competitive factors such as expanding operations, mergers and acquisitions, offshoring of business processes such as software development or manufacturing, supply chain integration, globalization of new markets, and an increase in the mobile worker population have brought about an increased focus on data and operational availability at remote or branch office locations. Data consistency, protection, and recovery between central datacenters and remote or branch office locations are paramount for operational recovery. Operational recovery allows the operations of the business to resume so that orders can be processed, inventory can be tracked, products can be delivered, policies can be settled, patients can be treated, and new accounts can be opened. This level of operational recovery allows for business continuity and risk mitigation.

Enterprise Remote Office Characteristics

An enterprise remote office can be characterized as a corporate office, branch, or remote site that is associated with a large firm or organization and that is connected to the corporate network. Enterprise remote offices can be characterized by the following:

- ☒ Multiple sites, either domestic or cross-border, connected to a corporation via LAN or WAN technologies, either in a dedicated or switched-network model, where connectivity can range from ATM, frame relay, T1, and T3 to higher-bandwidth optical network connections such as OC-1, OC-2, and OC-3
- ☒ Sites with some level of IT infrastructure at their locations (one or more servers to provide remote or branch office users with computing services such as file, print, application, and Web services to serve enterprise remote office productivity)
- ☒ Environments where remote office staff have near-real-time access to the same information and applications as they would in the main office or headquarters and can access common, shared data

IDC estimates that approximately 99,260 medium-sized and large firms in the United States have remote or branch office locations, representing 85% of the total population of 116,600 medium-sized and large firms in the United States. Almost all large firms (1,000 or more employees) have multiple locations, as do six out of seven medium-sized firms (100–999 employees). Depending on their core technology environments, many of these companies with multiple sites require enterprise remote office solutions. However, availability of remote office technology resources is typically more limited or even nonexistent compared with IT resources found at the headquarters and in corporate datacenters.

As firms grow in size, the average number of remote or branch offices also grows. Medium-sized firms have an average of eight remote or branch locations, while large firms have an average of 65 remote or branch locations. IDC expects the number of remote or branch office locations to continue to expand over the next five years, fueled by advancements in technology, expanding operations, mergers and acquisitions, offshoring of business processes, supply chain integration, globalization of new markets, and an increase in the mobile worker population.

Table 1 quantifies the average number of branch office locations by company size.

TABLE 1				
U.S. Branch Office Profile by Company Size, 2005				
	Total Number of Companies	Companies with Branches	Average Number of Branches	Total Branches
Medium-sized firms				
100–249 employees	73,500	60,850	6.9	420,474
250–499 employees	24,500	20,940	10.5	220,035
500–999 employees	9,600	8,770	16.8	147,363
Subtotal	107,600	90,560	8.7	787,872
Large firms				
1,000–2,499 employees	5,000	4,790	25.4	121,654
2,500–4,999 employees	3,000	2,916	65.2	190,123
5,000 employees or more	1,000	994	257.9	255,837
Subtotal	9,000	8,700	65.2	567,614
Total	116,600	99,260		1,355,486

Source: IDC's *U.S. Enterprise Remote Office/Branch Office Opportunity*, 2005

In addition to company size, the vertical industry in which a firm operates can impact the scope of its remote or branch office volume. The following vertical industries have a high propensity for multiple remote sites:

- Healthcare.** Healthcare providers with regional healthcare clinics, local hospitals, and affiliated physician offices
- Life sciences.** Biotechnology and pharmaceutical firms with regional plants, labs, and distributed mobile sales teams
- Travel and entertainment.** Gambling and hospitality industries with multiple hotels, entertainment facilities, and distributed reservation centers
- Financial services.** Banking institutions and insurance firms with regional banks and insurance branches

- ☒ **Public sector.** Regional or state-run healthcare agencies and public schools and universities
- ☒ **Telecommunications.** Telecommunications service providers that need to quickly connect company-owned retail stores, independent retailers, and point-of-sale (POS) terminals to centralized datacenters
- ☒ **Manufacturing.** Industrial manufacturing firms with regional plants, warehouses, and service depots
- ☒ **Remote engineering.** Firms with remote software development teams and/or remote scientific teams, such as those in the oil and gas industry

Geographic Considerations

In addition to company size and vertical-industry considerations, geographic considerations should be taken into account. Multinational firms and firms with international business operations, manufacturing, development or strategic partnerships, or joint ventures already have needs for communication between corporate headquarters and remote or branch office locations. European firms with headquarters in EMEA frequently have as many as 16 regional or enterprise remote offices in operation for each country in which they do business. For international or multinational firms, considerations in selecting a solution of remote office data protection include:

- ☒ **Networking infrastructure.** For international companies that operate in developing regions and need to connect remote offices to the corporate network, securing strong connections to a corporate WAN over an outdated and fragmented public network infrastructure can be a challenge. The types of networks, differing capacities, and reliability or response time of the networks can vary on a country-by-country basis.
- ☒ **Data security.** Corporate, cross-border WAN traffic may face security requirements based on regional government regulations. These regulations may prohibit the transmission of data beyond specific encryption strengths due to espionage concerns.
- ☒ **International compliance.** Regulatory compliance is mandated on a country-by-country basis, with international regulations in the United Kingdom, Germany, and Japan receiving increasing focus from governmental bodies.
- ☒ **Localization.** Firms should evaluate products that are localized or internationalized to their specific language and character set. Something as simple as storing data in the appropriate time and date range can impact usability and operations.

Enterprise Remote Office Data Types

As companies grow, either organically or through mergers and acquisitions, and add remote or branch offices, access to central IT resources and technology that support collaboration among workers becomes critical. By far, the busiest application workloads at the enterprise remote office are standard file, print, and networking services such as email and instant messaging. However, access to online HR applications, remote sales/order entry, and other corporate data repositories is becoming increasingly critical. Additionally, the convergence of voice services and IP-based WAN data services allows employees to communicate and share large amounts of data effectively outside the LAN.

PROTECTION OF ENTERPRISE REMOTE OFFICE DATA

Given the large number of enterprise remote offices, the growth of operations, and the offshoring of business processes, companies need to protect data that resides in the remote or branch office. The drive to protect remote office data is accelerated not only by factors such as continuity of business operations in response to different error conditions but also by compliance with regulatory mandates. Firms must respond to error conditions such as physical, logical, and site-level failures or disasters, thus eliminating the risks of compromise to enterprise remote office productivity that can impact time to market, supply chain efficiency, and customer satisfaction or bring about cost penalties. They must also increase their focus on IT governance, regulatory compliance, and SLA standards relating to data security, recovery, and availability and ensure that sensitive corporate information such as financial data and intellectual property is not compromised.

Solutions to the Pains of Enterprise Remote Office Data Protection

In response to the increasing need for cost-effective, centralized control for enterprise remote office data availability, recovery, and administration, capacity-optimized, disk-based remote office data protection solutions are emerging to address remote office data protection challenges. IDC has detailed some of the major problems associated with remote office data protection and potential solutions:

Problem. No technical staff available at the enterprise remote office location

Solution. Firms must look for backup technologies that allow backups to be scheduled, monitored for successful completion, and managed from a central datacenter or location where technical resources exist. Solutions that make use of centralized, scalable disk repositories as a backup target will eliminate the need for office managers or part-time IT consultants to pull tapes and therefore eliminate the risk of failed backup jobs, recoveries, or corrupted or damaged media.

Problem. Compromising sensitive data on tape media at the remote office

Solution. Eliminating the use of removable tape media at the remote office and placing data on disk systems that can be both physically and logically consolidated and secured addresses potential security compromises or tape media. Solutions that extend and ensure data recovery from a disaster recovery site provide more recovery points and greater flexibility.

Problem. Expensive, redundant, and commonly different backup processes and islands at each enterprise remote office

Solution. Consolidating the management of data backup in many remote offices under a single, centralized IT resource and standardizing on a single hardware and software solution reduces capital costs, reduces IT administration time and cost, and places critical data protection processes under centralized IT policy.

Problem. Growing and redundant backup data exceeding WAN network bandwidth and impacting remote office productivity

Solution. Solutions that can detect which data has already been backed up and eliminate the backup of that data again optimize the use of network bandwidth during enterprise remote office backup and free network bandwidth for remote office primary processing. Also, solutions that send data over the WAN should do so in an encrypted fashion.

Problem. WAN network latency and disruptions that impact backup job completion

Solution. Solutions that reduce the amount of remote office file data being sent over the WAN, by sending only new data, will cause less network latency and improve backup reliability. Solutions should also provide the ability to restart remote office backups from a point just prior to a network disruption as opposed to restarting the backup from the beginning.

Problem. Inability to meet enterprise remote office recovery time from recovery off tape

Solution. Local, user-level file restores from disk repositories that reside either locally or within the datacenter provide fast response to user errors and deletions. Additionally, solutions that can provide file system–level recovery from a centralized datacenter reduce the time required to support restore requests and eliminate the need for IT personnel to make onsite visits to the remote office.

Problem. Regulatory bodies requiring data protection and disaster recovery, regardless of whether the data resides in remote offices or datacenters

Solution. Satisfy industry-specific regulation requirements around IT processes, including disaster recovery and requirements on business continuity, by ensuring that backups are done and improving enterprise remote office recovery times from disk.

Problem. Response to different outages including unplanned outages such as physical disasters, logical failures, or attacks and user error

Solution. Firms should evaluate remote office backup solutions that can provide different levels of recovery. Solutions should provide not only recovery from disasters (e.g., fires, floods, hurricanes, tornadoes, terrorist attacks) but also recovery from logical attacks due to security vulnerabilities and user error such as tripping over the power plug to the server.

TRADITIONAL APPROACHES TO ENTERPRISE REMOTE OFFICE DATA PROTECTION

IDC conducted in-depth interviews with over 42 storage and IT managers in early 2006 about their current approaches to protecting and backing up data in their enterprise remote offices. The overwhelming percentage of respondents outlined one of two approaches. The first approach was either a local tape backup with offsite tape storage at a third-party location or a tape backup of local data to a central datacenter over the corporate WAN. The second approach was a disk-based replication of data on a scheduled or periodic basis over the corporate WAN. During the course of the interviews, many respondents expressed challenges, concerns, or dissatisfaction with their current approaches and had plans to modify their strategies over the course of the next 12 to 24 months. The following list includes some comments made by the storage and IT managers who were interviewed:

- ☒ "We have done a consolidation of our servers, but to achieve a centralized tape backup scheme, we needed to add greater bandwidth to the enterprise remote offices."
- ☒ "Our longer-term, strategic goal is the use of remote, disk-based data protection, instead of local backups being stored in a third-party facility, so we maintain control."
- ☒ "Most of the offices do daily incremental backups and fulls on the weekend. All have in-house tape units for their backups, but we lack any centralized management."
- ☒ "Our enterprise remote offices are two development centers, so there are IT skill sets available. However, we are focusing on creating localized data protection infrastructure solutions that can be remotely managed with emphasis on an appliance approach and disk-to-disk, with minimal, if any, tape media unless the data needs to be stored offsite. In those instances, electronic remote vaulting is being considered."

Challenges with a Tape Approach in the Enterprise Remote Office

A traditional tape backup approach to enterprise remote office data protection places applications, databases, or files in a consistent state for either a local, server-attached tape backup or a remote WAN or LAN tape backup to a central datacenter. When a failure occurs, recovery points are based on the last known good backup, and any data stored following the last backup is potentially lost. Recovery times were impacted by many variables, including the tape media location, the size of the restore, the type of the restore, and backup configuration attributes such as multiplexing and backup levels. Other challenges with a traditional tape backup and recovery approach include:

- Poor remote office operational recovery due to longer restore times and limited IT resources available in remote offices to conduct a restore
- High IT overhead and administration associated with tape handling, media management, backup and recovery verification, tape automation management, and lack of reliable tape media in specific conditions
- No available IT resources to manage the backup process and tape rotation and troubleshoot backup software or hardware problems
- High total cost of ownership related to redundant backup processes and data where the same data was periodically backed up again and again, increasing backup volumes, network traffic, and media costs
- Increased security risks associated with sensitive corporate information on lost, compromised, or offsite tapes
- Limited network bandwidth to back up local enterprise remote office over a WAN to a central datacenter
- Lack of control and increased risk associated with a distributed and nonstandardized approach to control data protection at enterprise remote offices

Challenges with a Replication Approach in the Enterprise Remote Office

Some enterprise remote offices have deployed a replication, snapshot, or cloning approach to replicate application or file data resident on disk at a enterprise remote office to a centralized datacenter, either asynchronously or in a point-in-time manner. Replication can be done bidirectionally or more frequently in a many-to-one fashion from multiple enterprise remote offices to a central datacenter. Replicating data from an enterprise remote office to another location using either host-based or array-based replication has presented several challenges, such as:

- Inability to identify redundant or duplicate data, either within each enterprise remote office or globally across all enterprise remote offices (As a result, the replication target continues to grow as redundant data gets copied.)

- ☒ Increased network bandwidth usage as the same data is replicated again and again (Thus, as the data grows, the network bandwidth usage increases.)
- ☒ Lack of local IT resources to manage the replication process, troubleshoot replication software or hardware problems, or conduct the restore or recovery process
- ☒ Lack of user-level or file-level recovery, depending on the replication approach (Thus, recovery is done in an "all-or-nothing" fashion.)

Challenges with a Wide Area File Services Approach in the Enterprise Remote Office

An alternative approach to local tape backup or replication is the use of wide area file services (WAFS) to address enterprise remote office IT services and data protection administration. WAFS products enable remote offices to access and share files over the corporate WAN, making file open performance appear as if it were local to the enterprise remote office, handling file locking while maintaining a single version of the file. WAFS solutions allow for the consolidation of storage in the corporate datacenter, thus eliminating the need for data backup at the remote office location. However, one challenge of a WAFS approach is that it does not completely obviate the need for remote office data protection. The WAFS server and or software itself must be maintained and protected; WAFS handles only file operations and file services, and most remote offices have semistructured or structured data that needs to be protected. Other challenges associated with a WAFS approach include:

- ☒ Slower speeds and the higher latency of WANs have challenged the implementation of WAFS and resulted in server deployment in remote offices.
- ☒ WAFS are application-specific products that only optimize file services or provide file system-based distributed applications.
- ☒ A WAFS approach does not address the challenge of limited IT resources in the remote office. Most WAFS products require client PCs to be reconfigured, which can be a significant burden, and the WAFS appliance requires administration.
- ☒ Most remote offices have application data such as email, Web-based applications, databases, ERP systems, and homegrown applications moving to remote sites which require IT infrastructure which must be protected.
- ☒ Data encryption can impede the effectiveness of WAFS and WAN optimization approaches because encrypted data cannot be compressed.
- ☒ WAFS requires a complete rearchitecture of an enterprise's remote office IT and application management strategy, a process that may not be feasible due to political and management boundaries within an organization.
- ☒ Many applications are run locally in remote offices because of a unique need for performance, availability, or autonomy at a given remote site. In these instances, centralization via WAFS may not provide the compute experience necessary at the remote office.

Firms considering the implementation of a WAFS approach should do so carefully because it is a significant storage and administration change for the enterprise remote office as well as the corporate datacenter.

KEY CONSIDERATIONS IN ENTERPRISE REMOTE OFFICE DATA PROTECTION

Firms are reevaluating their approaches to enterprise remote office data protection, given the business drivers not only to improve business unit SLAs, recovery times, and levels of availability but also to satisfy regulatory compliance requirements and mitigate security and privacy risks associated with corporate information. In the next 12 months, firms investigating or evaluating new approaches to remote office data protection should consider the following:

- ☒ **Data reduction.** The ability to identify unique data that has already been backed up, both locally within one remote office and globally across many enterprise remote offices, and eliminate the redundant process of backing it up again results in lower hardware costs and network consumption as well as less administration.
- ☒ **Flexible deployments.** A solution that provides backup application integration, with support for both internal high-capacity, cost-effective ATA disk storage and modular or enterprise storage arrays. Flexible data protection configuration options allows a firm to deploy configurations based on in-house expertise and skills, leverage existing supplier discounts, and protect investments in existing hardware.
- ☒ **Scalability** of a solution must be reviewed to ensure that as the environment grows (in terms of numbers of enterprise remote offices, servers, and files), the product can scale with the growth.
- ☒ **Disk-based protection.** A disk-based approach enables improved backup performance and enhanced restore times and eliminates the challenges of tape management or reliability. The use of disk as a target eliminates manual tape handling, collection, and administration at the remote office.
- ☒ **Ease of restore/recovery.** Ability for remote sites to restore files directly from the disk-based data store without involving IT personnel. The model for this should be based on a familiar user interface such as a Web-based file explorer interface and also provide search capability to locate files based on specific user permissions and access controls.
- ☒ **Data encryption,** both in transit and at rest, ensures that data and sensitive content within data cannot be compromised. Other considerations relative to encryption should be the encryption key strength, how key management is done to minimize administration, and the need for encryption of specific data based on regulatory pressures in key industries such as healthcare, financial services, and credit card processing.

- ☒ **Remote replication** of data from one or many enterprise remote offices for disaster recovery and an offsite option that eliminates tape. Network bandwidth constraints mean a solution should minimize the amount of data being moved over the WAN to increase performance and reduce overhead. Additionally, as data travels over the network, it should be encrypted to minimize security risks over WANs.
- ☒ **Centralized administration** can be achieved, eliminating the need to involve nontechnical enterprise remote office personnel in the backup process. Remote management should be done via a secure connection such as SSL so that IT staff in a remote location or datacenter can centrally manage all instances of enterprise remote office data protection. Additionally, if data can be restored by users at the remote location, then the need for IT in the frequent and high-overhead file recovery process is eliminated.
- ☒ **Synergy with datacenter protection strategy** where firms can use a solution that leverages as much of the hardware and manpower training investment in their datacenter protection environments, looking to extend it to the remote office instead of treating the remote office like a silo environment.

SYMANTEC'S VERITAS NETBACKUP PUREDISK REMOTE OFFICE EDITION

In April, Symantec Corporation announced the availability of a new product in the NetBackup line. Veritas NetBackup 6.0 PureDisk Remote Office Edition is targeted at solving management, reliability, and availability challenges associated with remote or branch office data protection and recovery. This new product offering provides both existing and new Veritas NetBackup customers with an integrated enterprise remote office data protection solution that:

- ☒ Eliminates the challenges associated with traditional tape and replication approaches to enterprise remote office data protection
- ☒ Integrates with existing NetBackup configurations in a central datacenter and complements an existing centralized tape backup process, if required
- ☒ Provides a centralized point of control and management for multiple enterprise remote office locations while ensuring enterprise remote office availability
- ☒ Addresses the Windows, Solaris, HP-UX, IBM AIX, and Linux file system data in the enterprise remote office location and can expand to additional platform and application coverage

Symantec's Veritas NetBackup PureDisk Remote Office Edition

Veritas NetBackup PureDisk Remote Office Edition offers storage and bandwidth-optimized data protection for remote offices. The product uses disk-based backup technology to enable companies to eliminate the risk and cost of tape from enterprise remote offices. It also incorporates disk-based backup with a unique data reduction process to identify unique data segments in files, both locally and across different offices. Veritas NetBackup PureDisk Remote Office Edition software identifies these unique file segments and keeps track of what has been previously backed up, and it will not move or copy data that has already been stored. This feature not only eliminates overhead in the storage of redundant data but also optimizes the use of the WAN bandwidth by transmitting only unique file segments and reduces storage and network consumption by a factor ranging from 10 to 50.

The management of the enterprise remote office data protection process is done centrally through a Web-based interface, addressing the challenge of limited IT resources at remote locations. Additional features in Veritas NetBackup PureDisk Remote Office Edition enable enterprise IT groups to effectively address the challenges of enterprise remote office data protection and include:

- ☒ **Fast, disk-based recovery.** Data can be recovered from a local server, a datacenter, or another remote site.
- ☒ **User-level file restores.** Users can quickly search for and recover files.
- ☒ **Remote replication.** Bandwidth-efficient asynchronous replication provides for offsite or disaster recovery protection replicating data to a datacenter, a disaster recovery site, or another enterprise remote office.
- ☒ **Centralized management.** Backup configurations, retention policies, and regular administration tasks can be performed via a secure, Web-based console.
- ☒ **Data encryption.** The use of 256-bit encryption of data both at rest and in transit over LANs or WANs ensures that data cannot be compromised due to security threats and eliminates the risk of loss or theft of removable media.
- ☒ **Standard, file system interface.** Administrators can quickly restore backup data that is filtered by file metadata, such as file type, date, and source, using a standard CIFS file system interface.
- ☒ **Storage scalability.** Administrators can add NetBackup PureDisk storage modules to scale the disk storage capacity. Because all available storage is virtualized in logical storage pools, scaling happens online without having to reconfigure backup and replication policies or clients.

Veritas NetBackup PureDisk Remote Office Edition is the first in a series of disk-based data protection approaches that Symantec will release with its unique data reduction capabilities, addressing the historical challenge of protecting the same data again and again during the backup process.

Execution Challenges

Symantec is an industry leader in data protection products and solutions for backup and recovery of data and systems, optimizing storage resource utilization, simplifying administration of heterogeneous environments, and providing continuous availability for critical applications and data.

Symantec's data protection solutions are designed to protect, back up, archive, and restore data across a broad range of computing environments, from large corporate datacenters, to departments and enterprise remote offices, to desktops and laptop computers. These products integrate to provide solutions to manage data through its life cycle, from creation to onsite and offsite disposal, across all levels of storage hierarchy, including disk, tape, and optical storage media. Symantec's legacy of data protection products includes the Veritas NetBackup product line. Given Symantec's strong history in the data protection space, the company is well-positioned to help firms address the enterprise remote office data protection challenge. However, Symantec must also address the following issues to maximize its opportunity:

- ☒ **The continued role of tape.** Some environments face regulatory mandates that prescribe that offsite or disaster recovery locations meet specific physical requirements. In some cases, a firm's remote datacenter or disaster recovery facility does not meet these physical requirements. As a result, the use of third-party offsite storage facilities where removable tape media is archived is commonplace. For these situations, it is important that the Veritas NetBackup PureDisk Remote Office Edition solution provide the ability to send backups to tape for the purposes of offsite storage. Although tape and tape drive spending may decline over time as the role of disk in the data protection process increases, tape is a medium that will remain in use, and new, disk-based solutions must seek to complement existing backup processes.
- ☒ **Application integration.** In parallel with tape support, disk-based data protection approaches must interoperate with existing backup applications. Large and very large firms frequently have as many as three to four different backup applications in place, and the ability of a disk-based data protection solution to work across these applications is paramount to supporting both existing and future data protection environments. Symantec must provide interoperability between Veritas NetBackup PureDisk Remote Office Edition and leading applications such as Legato NetWorker and Tivoli Storage Manager (TSM).
- ☒ **Product coverage.** The type of data that resides within enterprise remote offices includes more than just file data and runs on platforms other than Windows-based systems. Symantec must provide further enhancements to the product over the course of 2006, including additional platform coverage and application agents such as Microsoft Exchange and Microsoft SQL Server.

CONCLUSION

Enterprise remote offices must address the imperative to protect and provide higher levels of availability and recovery of critical data. If superior levels of bandwidth utilization, administration, security, and recovery are not met with a data protection strategy, then a firm's ongoing utility and enterprise remote office productivity and financial position can be compromised, especially in the remote office.

The Veritas NetBackup PureDisk Remote Office Edition solution provides firms with a disk-based data protection approach to achieve higher levels of recovery and eliminate the historical challenges associated with enterprise remote office backup. The product helps firms meet critical business goals while improving availability and recovery SLAs, reducing costs, optimizing storage and network bandwidth, and reducing IT administration and overhead of enterprise remote office data protection.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2006 IDC. Reproduction without written permission is completely forbidden.