AberdeenGroup

Rethinking Data Protection Strategies

An Executive White Paper

February 2002

Aberdeen Group, Inc.
One Boston Place
Boston, Massachusetts 02108 USA
Telephone: 617 723 7890
Fax: 617 723 7897
www.aberdeen.com

Rethinking Data Protection Strategies

Preface

The safety of critical business data is an ongoing concern for responsible enterprises. They are challenged by myriad threats to that data: hackers, data corruption, power outages, natural disasters, and even the most unthinkable. At the same time, the dynamics of data are also working against the enterprise: Internet strategies are opening more access points and therefore exposing more data to these threats; the volume of data is rapidly mounting; and data is more vital to the business. As a result, enterprises are recognizing that core intellectual assets are vulnerable, and effective data protection is critical to business success.

Rational enterprises acknowledge these trends and are rethinking data protection architectures and business continuance plans. A wide selection of technologies, services, and architectural alternatives — each providing unique benefits, but each limited in data protection capabilities — is being considered. IT ecosystems are under analysis to identify the weakest links, where any exposures can nullify all other protective measures. Security policies are continually updated. Enterprises are reviewing contingency plans and understanding their effectiveness.

Technologies and services exist to protect an enterprise's mission-critical data. Unfortunately, the costs of protection often restrict the adoption of conservative data strategies. Instead, enterprises must be pragmatic in their planning, understanding the likelihood of data faults, the implications of those events on the business, as well as the costs of preventive measures. Enterprises must carefully manage these variables to minimize risk as if it were a statistical exercise. Outsourced data protection services have proven to be a practical alternative — when providers offer more secure solutions at lower costs — to those provided internally.

In this *Executive White Paper*, Aberdeen examines the fundamental variables — i.e., security and reliability — of data protection and outlines enterprise strategies. Aberdeen also provides a framework for enterprises to rethink their data protection architectures and offers insight into practical outsourcing alternatives.

Data Protection Fundamentals

Business privacy and continuity are the goals of corporate data protection efforts. Enterprises can ensure the safety of critical data sets and the stability of the business by building protective measures throughout the data architecture. The fundamental variables of security and reliability must be inherent in these strategies. Both are multi-faceted components of protection, but each requires specific expertise and resources to implement:

- Security: Providing protection for corporate data requires strict security policies on two fronts: physical access to the data and its supporting infrastructure and virtual access to that data through the network;
- Reliability: Data must be easily accessible to users or business continuity is sacrificed. The consistent availability of data means that all IT compo-

nents — network, equipment, management, and processes — are running smoothly. Redundancy across the IT delivery chain can ensure reliable access to data.

Given these fundamentals, enterprises face two exposures: data loss and data corruption. Aberdeen offers the following distinction:

- *Data loss* does not necessarily mean that digital assets cease to exist; rather, the data survives but is no longer accessible to the user. Data loss is commonly the result of hardware failures or human error but can be mitigated through redundant architectures and systematic processes. Less frequent, however, is the prospect of a disaster, either natural or produced where data is potentially eliminated. Distributed architectures and frequent data backups can minimize this exposure.
- *Data corruption*, on the other hand, means that the data is available but has lost its integrity. Viruses, software defects, hackers, and process errors are often the cause of data corruption. Tight security measures and consistent operational management can help maintain data integrity.

Data Protection Architectures

Clearly, enterprises can mitigate their data loss and corruption risks by building reliable and secure corporate networks. A range of protective technologies, processes, and infrastructure options should be considered. The deployment of these measures, however, must be consistent across the network in which data travels, within the storage repositories where data resides, and in the operational environment where data is hosted. Data protection schemes are only as strong as the weakest point of failure. The most effective strategies recognize network interdependencies and integrate the correlating protection measures throughout the data environment.

The most effective strategies recognize network interdependencies and integrate the protection measures throughout the data architecture.

Figure 1 categorizes the relevant data protection measures of hosting, storage, and backup and illustrates their interdependencies within the enterprise network. Aberdeen further explores these technologies and processes in subsequent sections, identifying key data protection attributes within the hosting, storage, and network elements of the data architecture.

Protective Elements of Hosting

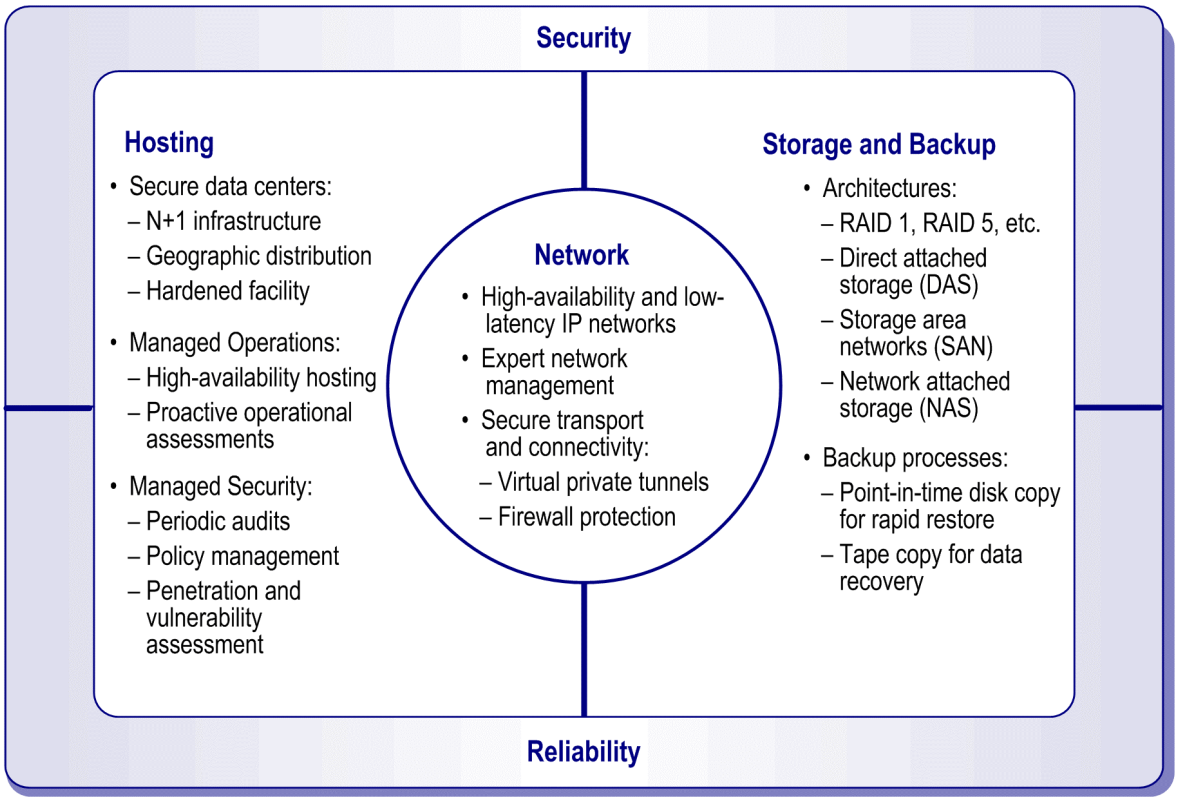
The stability of the hosted environment requires reliable infrastructure and seamless management to guarantee data availability. Aberdeen recognizes specific hosting attributes that improve data protection measures:

Telephone: 617 723 7890
One Boston Place
Fax: 617 723 7897
Boston, Massachusetts 02108
www.aberdeen.com

Secure Data Centers: Housing network elements in onsite, unsecured computer rooms is common. But enterprises are risking their data when opting for low-cost onsite hosting over high-quality co-location alternatives. Many onsite data centers are a Petri dish of security and reliability risks. One advantage of co-locating is the reliability of a highly redundant environment. Hosting centers emphasize N+1 planning in all aspects of the operation: networking gear, power sources, bandwidth sources, staff members, fire detection and suppression, and even temperature and humidity control elements like cooling towers. There is no single point of failure. The physical design of these structures emphasizes strength to provide reliability against disaster and invasion with biometrics and bulletproof glass. Strict security processes — armed guards, 24×7 monitoring, employee background checks — prevent any unauthorized personnel from getting close to the network operation.

Managed Operations: Infrastructure downtime is seldom the result of multiple failures to redundant equipment; rather, it is frequently the result of human

Figure 1: Data Protection in the Enterprise Network



Source: Aberdeen Group, January 2002

One Boston Place
Boston, Massachusetts 02108
Telephone: 617 723 7890
Fax: 617 723 7897
www.aberdeen.com

intervention. The ever-changing topology of networks introduces the potential for human error in infrastructure management. The smoothest operations, however, maximize data availability through concise execution of management tasks to reduce error rates and the resulting downtime. In addition, finely tuned operations management will include proactive testing of the operation's stress and load capabilities, as well as its scalability to data bursts to predict potential risks. These efforts allow managers of IT operations to promise reliability standards through service level agreements.

Managed Security: While infrastructure reliability is a function of a stable operation, data security requires distinct expertise and technologies. The maintenance of security policies and the deployment of security technologies like firewalls to prevent unauthorized access into the network, and intrusion detection software to identify breaches are essential to data protection. The continuous updating of these security policies and technologies is achieved through processes like security audits and vulnerability assessments that provide a proactive review of a data network's weakest links. Maintaining a static security policy in today's unstable world allows hackers, both internal and external, to catch the enterprise resting on its laurels and exposes the vulnerability of corporate data.

Concise operational processes allow for improved reliability and better service levels.

Protective Elements of Storage

As enterprises adopt data-intensive applications, such as Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), and Web-enabled business-to-business applications, the vast amount of data generated requires storage architectures to easily maintain, access, and manage the data. These architectures must also prove reliable and secure to ensure against data loss or corruption. With respect to protection, Aberdeen identifies three key storage architectures and processes:

Direct Attached Storage (DAS) — has an enormous installed base in enterprise networks. The networking of DAS allows greater utilization of existing storage resources and thereby reduces costs. But networking DAS creates a single point of failure — if the server fails, the networking lateral also fails and leaves the data stranded within the local server. While DAS offers convincing advantages, enterprises should recognize this potential data availability issue.

Storage Area Networks (SANs) — offers enterprises the advantages of decreased latency and centralized management. SANs also fortify data protection strategies. They allow geographically distributed users to access data and provide switch fabrics with no single point of failure. As a separate, special-purpose network of storage devices — typically linked by Fibre Channel to allow high-speed access to a centralized pool of data — SANs use redundant components through the parallel

Telephone: 617 723 7890
One Boston Place
Fax: 617 723 7897
Boston, Massachusetts 02108
www.aberdeen.com

storage network to improve reliability. SANs also offer unique management benefits of storage consolidation, performance, and scalability over DAS alternatives. For multi-tenant SAN environments, SANs allow logical zoning so data can "belong" to specific servers. Zoning protects customer data sets by establishing virtual storage paths to segregate customer access and servers within the SAN.

Network Attached Storage (NAS) — offers convincing advantages to enterprises: heterogeneous file access, easy installation and management, and low-end pricing. As NAS offers management and cost advantages in part due to its heterogeneity, it is subject to latency during the protocol sharing — something to which database applications are particularly sensitive. Enterprises must closely monitor NAS bandwidth to avoid these data bottlenecks, which can hinder performance and reliability.

While primary storage allows enterprises to access, maintain, and manage data, enterprises must also ensure against data failure. As a result, enterprises conduct data backups to maintain a "snapshot" of their data in case it needs to be restored from loss or corruption. Data backups are periodically scheduled by the enterprise and kept within an online disk and/or an offline tape. Each medium offers its own data protection advantages. Point-in-time copies made to disk allow for the quick restoration of data because of their online accessibility, while tape copies provide the advantages of portability to ensure against localized accidents that could destroy disk-based back ups. The complementary relationship between tape's disaster-recovery capabilities and the business continuance benefits of online disk copies results in both disk and tape backups run in addition to, not in place of, one another.

Enterprises typically store data across a ***redundant array of independent disks (RAID)*** to eliminate single points of failure and to promote reliability. Different configurations allow for varying levels of reliability. Two common configurations are:

RAID 1 — the entire duplication of synchronous data by a redundant disk. It is often recommended for real-time dynamic data sets and is valuable for continuing data availability in the case of a component failure on the primary disk array.

RAID 5 — stripes data across multiple disks, sharing the redundancy load across the disk array. In the event of a disk failure, the other disks can rebuild the data on a replacement disk.

Protective Elements of the Network

As enterprises move to distributed hosting and storage architectures, the security and reliability of the wide area network (WAN) becomes critical. Private intranets, or extranets on private IP networks, are understandable approaches, but prices are high and availability is low compared to the public Internet. IP networks with any-to-any WAN connectivity are an alternative, but their performance must accommodate low network latency and congestion, and high availability.

IP networks today are known for their "best effort" reliability. But, the redundancy of network elements can guarantee 99.999%, and sometimes 100%, availability,

while over-provisioning bandwidth has typically been the solution to performance limitations. In addition, combinations of technologies and expert network management can help optimize network latency and congestion.

With data repositories available from across a network, enterprises must be cautious of their networks' security. Virtual private network (VPN) tunnels must be configured and managed to provide secure WAN connectivity. The Internet Protocol security (IPsec) standard for tunneling, with Data Encryption Standard (DES) or the more powerful Triple-DES (3DES) for privacy, is common and effective. Firewall policies must be established for packet inspection, denial of service (DoS) protection, and intrusion detection — all required to protect data from unauthorized users. Network-based firewalls, it should be noted, offer greater DoS protection, defending against data surges that may overwhelm customer-premises-based firewall devices. The ongoing management of these security services by experienced technicians is essential. A controlled network penetration scan against a database of known vulnerabilities and system weaknesses must be performed annually. Similarly, intrusion detection services can conduct the real-time identification of suspicious traffic patterns.

Practical Decisions

Though each of the described technologies, architectures, and services are readily available to offer protection benefits, enterprises remain bound by fiscal restraints. Data protection strategies span a diverse landscape of expertise and infrastructure requirements. Many of these capabilities are simply too cost prohibitive or specialized to be maintained by an enterprise's internal IT organization. Outsourcing presents a logical opportunity for practical decision-makers. The advantages of outsourcing are generally well understood by enterprises, but some are particularly relevant to data protection and should be identified:

- *Cost-effective access to the most effective resources:* Outsourcing provides enterprises with access to best-of-breed technologies and expertise, resulting in better service, a stronger management, and better insight into the data risks;
- *Mitigation of technology risk:* Service providers offer the latest and greatest technology so the enterprise customers do not have to worry about having outdated data protection equipment or tools that leave them open to exposure; and
- *Mitigation of growth risk:* Predicting business and data growth is a volatile game. Outsourcers offer enterprises scalable operating environments so data remains protected regardless of the growth or contraction rate. Utility pricing models let enterprises pay for only the services used, allowing a "grow as you go" plan where operational upgrades do not involve a forklift upgrade.

Telephone: 617 723 7890
One Boston Place *Fax: 617 723 7897*
Boston, Massachusetts 02108 *www.aberdeen.com*

Service and Infrastructure Migration

For enterprises leveraging outsourced data protection services, the migration from the existing solution to a third-party data center should be a seamless transition of accountability. Successful providers will offer service migration strategies that permit the customer to remain in control, while realizing the benefits of network and IT resources that plan and execute the migration into an outsourced data center. The process should include data experts and security specialists to ensure integrity. The handoff of management and monitoring services, notification polices of data breaches, and identification and activation of resolution plans should be well documented. Experienced service providers should also recognize existing enterprise resources and seek ways to integrate or complement those capabilities with other data protection services. Efforts to leverage sunken technology investments can lessen migration costs and the humility of the original buyer.

Successful providers will offer migration services that ensure a seamless transition of accountability.

A Practical Alternative: Qwest Communications

Qwest Communications International Inc. is an established provider of reliable, scalable, and secure broadband data and voice services for businesses and consumers. The company's offering includes a comprehensive portfolio of data protection services for the enterprise. Qwest's global network, its extensive managed hosting solutions, and its storage and backup services combine to enable complete data protection strategies that emphasize both security and reliability.

Qwest's delivery approach of these services supports enterprises in the planning, provisioning, and management stages of data protection strategy implementation. Qwest works with each enterprise to identify data protection requirements and establish effective strategies. In addition, Qwest's migration services aim to minimize the risks and alleviate the stress of transitioning from existing environments to Qwest managed solutions. To ensure a seamless transition of assets and management accountability, Qwest features four comprehensive components: system/network architecture assessment, migration project management, temporary environment services, and infrastructure relocation services.

Core Data Protection Services

The Qwest data protection services portfolio extends across the operational landscape (Figure 2) to include hosting, storage, and network capabilities — each built to ensure reliability and security.

At the core of this offering is the Qwest OC-192c fiber network. Designed for 100% reliability, this IP network spans more than 113,000 miles globally. The network leverages multi-protocol label switching (MPLS) technologies to re-route broken signals in milliseconds, making downtime a virtual non-reality. Qwest

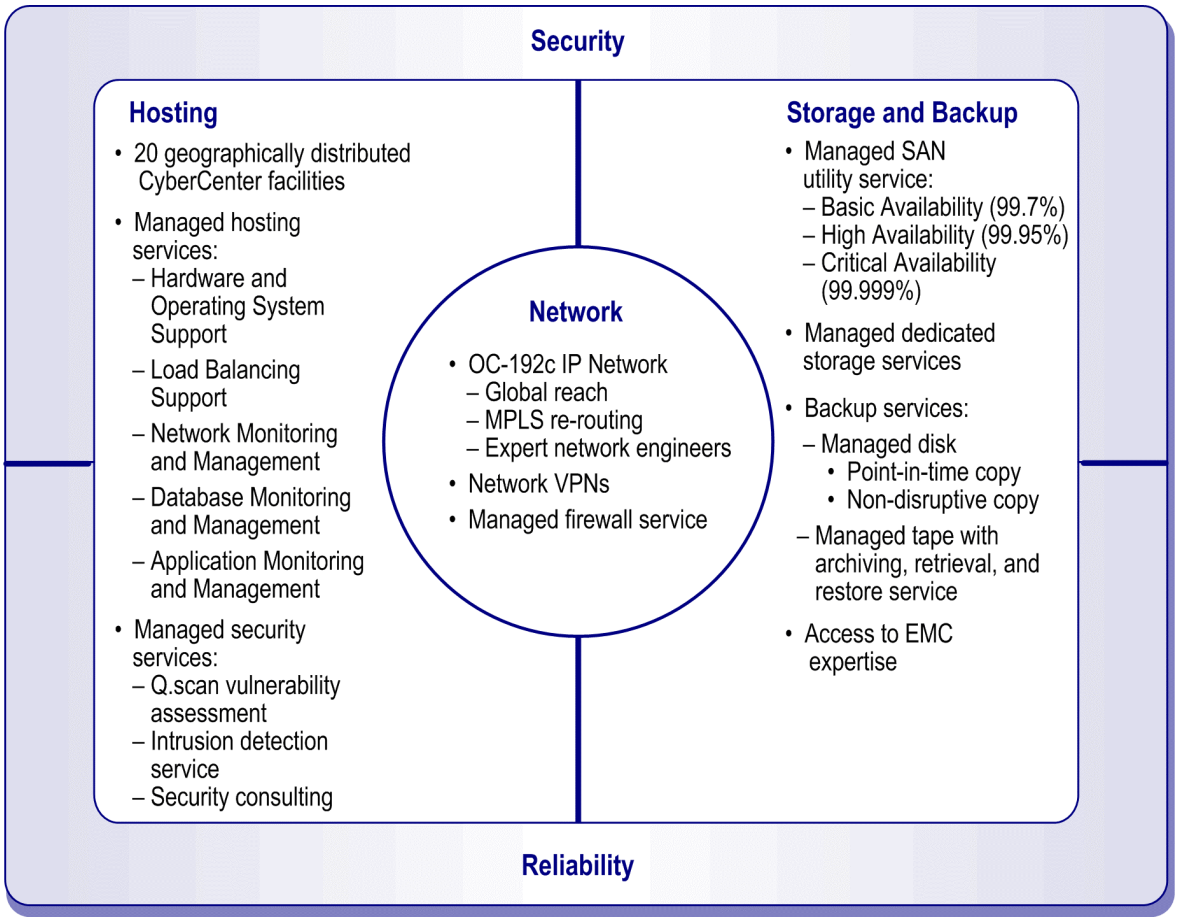
Telephone: 617 723 7890
One Boston Place *Fax: 617 723 7897*
Boston, Massachusetts 02108 *www.aberdeen.com*

network engineers also proactively monitor availability, packet loss, and latency metrics to identify any performance degradation.

Qwest's fiber network interconnects with the company's 20 globally distributed CyberCenter facilities, so customers needing redundant data centers for geographic mirroring can be served adequately. Qwest's CyberCenters are secure, reliable data centers, designed to provide state-of-the-art hosting for mission-critical data. CyberCenters are staffed 24×7 with highly trained technical engineers. Two tiers of support personnel are accountable for integrated event, problem, and change management, and all customer contact, notification, escalation, and quality/service metric reporting.

Within these CyberCenters, Qwest applies its honed expertise and disciplined processes to offer its managed hosting, storage, and security offerings.

Figure 2: Qwest Data Protection Service Portfolio



Source: Aberdeen Group, February 2002

Managed Hosting Services
Qwest offers enterprises a complete spectrum of hosting services to accommodate their infrastructure, monitoring, and management requirements. Qwest offers several solutions to provide co-location, systems monitoring, server management, OS management, managed backups, and administration services. Qwest also provides custom hosting solutions that leverage the expertise of Qwest's professional services organization. Furthermore, Qwest shares a partnership with Loudcloud to serve customers interested in management services through the application.

Qwest's hosting services accommodate several tiers of reliability and performance, enhanced backup services, service level agreement (SLA) commitments, and error alert/fix capabilities options. All hosted elements reside in a secure Qwest Cyber-Center and access the Qwest fiber network. The company's operational management expertise, defined processes, and infrastructure resources allow a successful integration of the hosted environment with the data architecture.

Managed Security Services
Qwest offers a broad set of managed security options for enterprises. All relate to data protection strategies and can complement the company's hosting, network, and storage offerings.

- A Network VPN service that connects all access ports to a carrier-grade, network-enabled firewall engine ensures secure, high-speed throughput. This architecture provides secure networking using IP-sec, packet inspection, anti-spoofing, URL blocking, DoS protection, and it allows network administrators to set access privileges for individual users.
- A Managed Firewall VPN service is a turnkey, premises-based firewall service using a Nokia appliance running Firewall-1 software from Checkpoint. Qwest provides 24×7 administration, monitoring, management and reporting.
- Qwest's vulnerability assessment service, Q.Scan, provides an analysis of network security and proactively locates vulnerabilities. The subscription-based service allows for the evaluation of security perimeters, databases, and applications to identify possible configuration weaknesses.
- Qwest's Intrusion Detection Service (IDS) includes all necessary hardware and software, 24×7 monitoring, and real-time alerting and reporting. Customer-specific IDS sensors listen passively to all traffic and alert security managers of any suspicious activity. The IDS sensor can be set at different levels of sensitivity to provide several tiers of service. Qwest provides this subscription-based service in alliance with security provider, Veritect.

Telephone: 617 723 7890
One Boston Place
Fax: 617 723 7897
Boston, Massachusetts 02108
www.aberdeen.com

Managed Storage and Backup Services

Qwest offers a portfolio of storage and backup services — tape and disk backup, multiple utility storage offerings, and managed dedicated storage services.

Qwest utility storage services are RAID 1-protected over a SAN infrastructure using multiple disk arrays, Fiber Channel fabric, and switch architecture services in three tiers:

1. *Basic Availability* service is targeted at non-mission-critical applications, like e-mail, to provide 99.7% availability through RAID 1 configurations;
2. *High Availability* service is for fast growing, robust data sets that require 99.95% availability, utilizing RAID 1, as well as dual separate paths in the SAN; and
3. *Critical Availability* service is for constantly changing, real-time data for which only a 99.999% availability guarantee will suffice. This service utilizes RAID 1 storage, has dual separate paths in the SAN, and includes one point-in-time copy.

Each service includes network operations center (NOC) management, equipment maintenance, SLA monitoring, and a 24×7 support desk. The services are billed on a GB-per-month basis.

Qwest's storage portfolio also includes Managed Dedicated Storage Services. Qwest will manage storage systems for customers who wish to purchase their own dedicated equipment. In addition, Qwest's portfolio includes remote management capabilities applied to its Managed Dedicated Storage service, providing storage management and backup services to the enterprise premises.

Backup services are available to Qwest's hosted customers that have also contracted for utility storage services. The backup services include:

- *Point-in-Time Copy* provides up to eight online copies of enterprise data, available for rapid restore capabilities in business continuance situations and to prevent any performance degradation during data queries, warehousing, batch processing, etc.;
- *Non-Disruptive Backup* creates tape backups of point-in-time copies and does not affect databases during the backup window; and
- *Managed Tape Backup* copies live data from server to tape.

Qwest supplements both tape backup services with additional services such as archiving, retrieval, and restore.

The culmination of Qwest's broad range of network, hosting, storage, and security services is a complete data protection solution for the enterprise. Qwest's multi-tiered offering can address each enterprise's requirements of reliability, security, and cost throughout their growth cycles. With vast resources, multi-tiered offer-

Telephone: 617 723 7890
One Boston Place *Fax: 617 723 7897*
Boston, Massachusetts 02108 *www.aberdeen.com*

ings, and international reach, Qwest can offer integrated data protection solutions with the advantages of a single point of contact, responsibility, and accountability.

Aberdeen Conclusions

As data grows more vital to business success, enterprises must be more cautious of those factors that threaten it. As a result, enterprises need to consider the effectiveness of their data protection strategies. Existing data architectures must be examined for reliability and security across the hosting, storage, and network elements of the IT environment. Enterprises must eliminate points of weakness by integrating protection technologies and processes with the data architecture. The effectiveness of these protection schemes will determine the vulnerability of an enterprise's privacy and continuity.

The implementation of uniform protection strategies throughout the data architecture can be an overwhelming task. The required expertise and resources are difficult to acquire and often cost prohibitive. However, outsourced services, however, offer an alternative means of obtaining the most effective data protection measures.

Qwest Communications' suite of data protection services allows the enterprise to establish a reliable and secure data architecture. The company's services minimize the risk of outages, failures, and security breaches, while establishing an effective business continuance plan in the event of a disaster. Qwest's extensive hosting, storage, network, and security capabilities enable comprehensive services that span the entire data architecture. Moreover, as a single source provider, Qwest can integrate its service components into an effective data protection solution.

Telephone: 617 723 7890
One Boston Place
Fax: 617 723 7897
Boston, Massachusetts 02108
www.aberdeen.com

To provide us with your feedback on this research, please go to www.aberdeen.com/feedback.

Aberdeen Group, Inc.
One Boston Place
Boston, Massachusetts
02108
USA

Telephone: 617 723 7890
Fax: 617 723 7897
www.aberdeen.com

February 2002

Aberdeen Group is a computer and communications research and consulting organization closely monitoring enterprise-user needs, technological changes and market developments.

Based on a comprehensive analytical framework, Aberdeen provides fresh insights into the future of computing and networking and the implications for users and the industry.

Aberdeen Group performs specific projects for a select group of domestic and international clients requiring strategic and tactical advice and hard answers on how to manage computer and communications technology.