Hewlett Packard Enterprise

Business white paper

How to evaluate data protection and recovery service providers

HPE Data Protection solutions

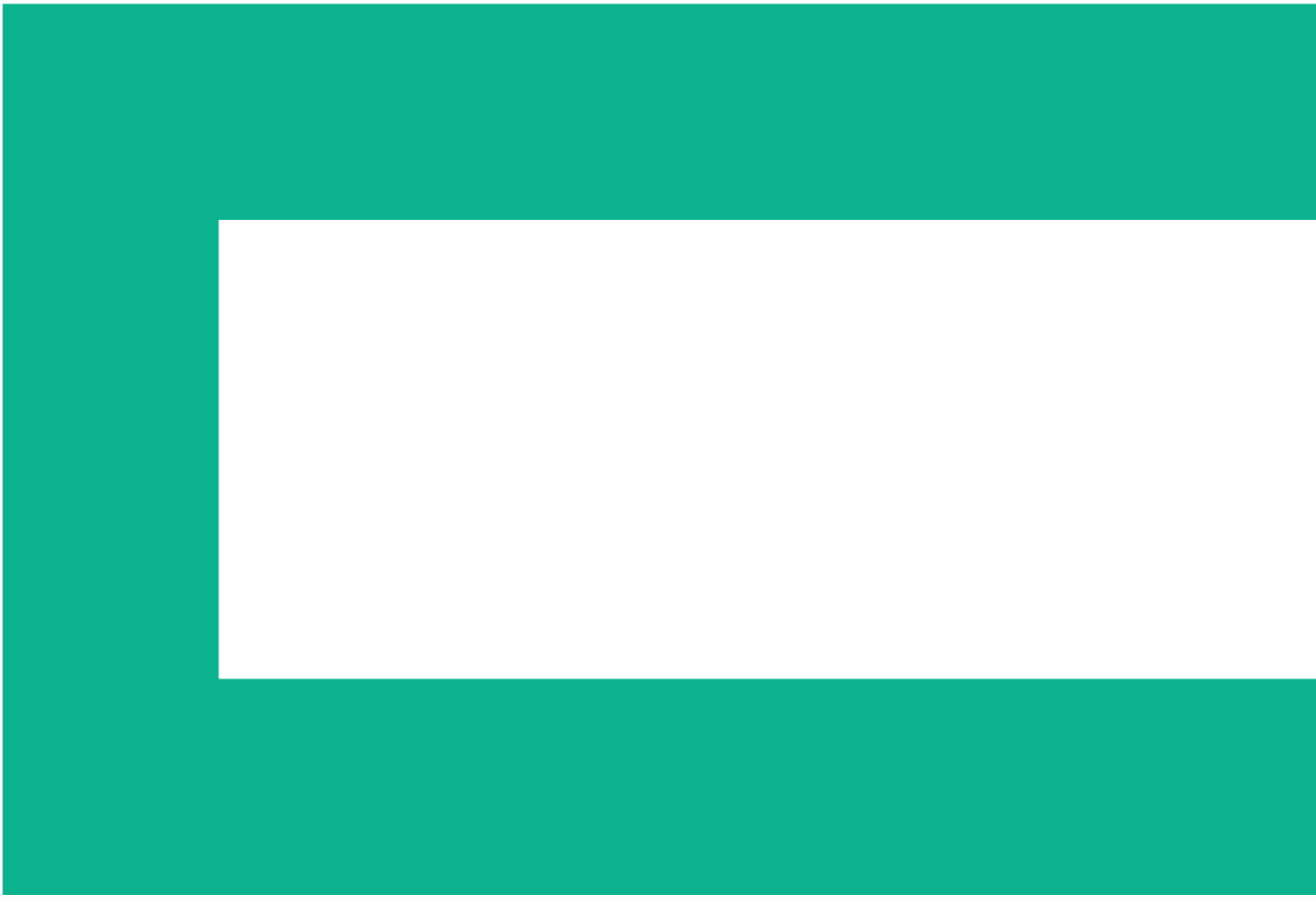

Table of contents

Understanding the strengths and weaknesses of different categories of service providers can help your business clarify its unique data protection and recovery requirements—and better align your selection criteria with productivity goals and strategic business initiatives. To achieve regulatory compliance, businesses are increasingly looking to data protection services. Such services can help you cost-effectively back up and recover terabytes of data distributed throughout your business on endpoint devices, while allowing users to search for, view, and access documents on their mobile devices.

According to IDC, in a distributed and mobile workforce, an average of 66% of employees at large firms work predominantly outside corporate headquarters, which makes them ever more reliant on decentralized data and puts greater pressure on IT to keep current data available and technology up and running.[1] This creates the challenge of how to provide this growing and distributed workforce with 24/7 access to reliable, secure data without adding capital expenses or increasing the support burden.

Three key categories of providers

Data Protection service providers have emerged from different market spaces and offer varied product focuses and business drivers. These providers can be grouped into three categories:

- Service providers leveraging existing core business resources to expand into adjacent markets
- Service providers concentrating on backup in niche markets
- Service providers whose backup and recovery offerings form an integral part of a spectrum of information management services

This white paper helps you to distinguish between the three categories of service providers. We characterize the scope, strengths, and weaknesses of each type of provider with respect to the current and forward-looking requirements of companies that seek to protect distributed data. Summary tables provide checklists of the essentials for successful data protection, and include an overview of how each category of provider addresses these requirements. A special section considers the role that service providers play in supporting strategic IT projects and programs for meeting corporate compliance objectives.

Understanding the strengths and weaknesses of different categories of service providers can help you meet your strategic goals while assuring that critical data is protected and secure.

[1] "Solving Today's Distributed Big Data Backup Challenges Yields Information Advantage", IDC, July 2013.

Protecting critical business information beyond the data center

More and more, the information required to run a business resides on the hard drives of desktops, laptops, and mobile devices—no longer just on servers in data centers. This information can be prioritized by its impact on business operations:

- Mission critical (revenue producing or customer facing)
- Business critical (supporting cross-organization functions)
- Operationally critical (important to individual departments)

The goal of data protection is to make sure that a company can recover from varying degrees of failure—from individual file loss to an entire system—in the optimum timeframe, or Recovery Time Objective (RTO), as well as to recover to a version of the data that results in minimal loss of productivity, or Recovery Point Objective (RPO).

IT professionals are increasingly looking to data protection services for distributed data protection. The major factors driving their search for these services are:

- The need to support a more distributed workforce and its dependency on 24/7 access to business data—while continuing to drive more strategic IT initiatives
- The attractive price and predictability of a Software as a Service (SaaS) subscription model versus solutions for distributed locations involving capital expense ongoing support and maintenance
- The increasing challenges of meeting compliance requirements by securely and consistently protecting increasing volumes of information distributed across a global enterprise

There are a large number of service providers with distinct approaches to data protection for distributed environments. Regardless of their category, all service providers must address the unique requirements that characterize data protection in a distributed environment. Data protection of desktops and laptops spread across the enterprise is distinctly different from server backup and recovery, and there truly is no "one size fits all" in distributed data protection. Unlike server backup and recovery, data protection for desktops and laptops must:

- Support intermittent connection and a greater range of connectivity, given the range of technology used in global enterprises (from dial-up to broadband)
- Protect against significantly greater risk of theft and security breach
- Efficiently manage backup and recovery of data from resource-intensive applications like email stored on individual desktops and laptops
- Address the greater vulnerability of desktops and laptops to system failure, requiring fast migration of user data, applications and custom user settings from old systems to new ones
- Accommodate high-volume requests for recovery from individuals and remote offices in a growing, distributed environment

The data protection service industry has matured to the point where customers can expect service providers in all three categories to provide certain fundamental features for distributed data protection. Beyond these fundamentals, there are specific features that are essential for data protection in distributed environments. Table 1 distinguishes between these two levels of functionality, which should be addressed by any service provider making it to a company's "short list."

Table 1: Data Protection and Recovery Service features for Distributed Environments

DATA PROTECTION	
Fundamentals	**Essentials**
• Automatic backups according to a pre-set schedule	• Two capture choices—file or system level—to allow not only faster restoration of failed systems but to support the migration of old systems to new ones
• Open file backup • Database support (e.g., Outlook®, Lotus Notes®)	• Built-in protection (native support) for open file and database support (rather than optional add-ons or plug-ins that may not be integral to the fundamental software)
• Online recovery of individual files or data folders as requested • Web-based retrieval by end users of lost or damaged files without helpdesk support—but with permissions set by IT	• In addition to data restores, full system restoration-heal to repair damaged or corrupted applications, configurations and files on any desktop or laptop
• Retention of daily backup sets on a weekly basis for at least 30 days	• Retention of up to 10 versions of any file, with deleted files retained for up to 3 months • Options to migrate older versions of files to archives
DATA PROTECTION ADMINISTRATION AND SUPPORT	
Fundamentals	**Essentials**
• Features supporting compliance programs: • Silent installation for consistent policies for backup to enable eDiscovery • Demonstrable, consistent best practices in regional data protection across the global enterprise	• Recovery of data across all repositories on demand through an eDiscovery service
• 24x7 monitoring and technical support	• Professional services for data protection best practices • Service Level Agreements available based on a SaaS offering • Staff experienced in "advanced topics" in data protection (e.g., the restoration of applications and systems as well as files) • For even greater IT control, software can be licensed and run from the data center by the customer or through a remote managed service
• Administrative console for monitoring backup jobs • Check-point restart if backup or restore jobs are interrupted	• Web-based administrator portal for centralized control of processes, status, inventories and reporting
• Support of Windows® platforms • Scalable from just a few to several thousand of desktops and laptops on a network	• Support of non-Windows® platforms (e.g., Mac®) • Optional backup of Windows file and print servers • Scalability to hundreds of thousands of desktops and laptops on a network
• Support of dial-up and low bandwidth connections • Adjustable bandwidth throttling with flexible scheduling • Data reduction technologies	• Email-specific data reduction and de-duping technology for faster backup and recovery
• Encryption in transit and in storage • Secure data centers	• Mirrored, redundant backup to a secondary data center • Data storage maintained by service provider with proven track record in security • Data centers located globally to accommodate regional privacy regulations • Certification appropriate to data stored (e.g., PCI compliance, SysTrust assurance)

Category 1: Service providers that leverage investments in core business resources

The first category of service providers includes those who leverage pre-existing investments in core business resources in what may appear to be an extension of their core competencies. These include:

- Business continuity and disaster recovery vendors
- Telecommunications vendors

Business continuity and disaster recovery providers
Hosted business continuity/availability providers typically provide:

- Cold sites—Data center space to house a customer's own equipment and backup tapes
- Warm sites and hot sites—An operationally ready data center
- Data archival, restoration capabilities, and managed services

These providers make sizeable investments in their sites and services, which can also include alternative mobile recovery data centers deploying large tractor-trailers equipped with electrical power, satellite communications, PCs, faxes, and other equipment that can be made available anywhere in the country to recover customer service operations or other mission-critical enterprise functions.

To take advantage of their investment in this infrastructure, which was designed originally for larger enterprises, some business continuity and disaster recovery providers have begun offering data protection services to smaller customers. But in reality, over 90% of data loss occurs as a result of more common events—human error, accidental deletion and overwriting, data entry errors, and so on. This is especially true of data protection in a distributed environment, which requires the faster, more service-focused, day-to-day recovery of individual systems, rather than recovery of an organization's entire data center.

Not surprisingly, these providers typically use third-party software on which to base their services, rather than developing their own service line. They share this practice with telecommunications providers, discussed in more detail below.

Telecommunications providers
Similar to business continuity and disaster recovery providers, some telecommunications providers also offer data protection services as an adjunct to other diverse lines of business. These backup and recovery services are also provided to leverage their infrastructure, which is designed to serve a huge installed base of consumers as well as businesses.

Telecommunication providers, like disaster recovery service providers, frequently license third-party technology to support their data protection services. Evaluating these services is a two-pronged process:

1. Determining the strength and quality of the provider's support, infrastructure, and security
2. Reviewing the third-party software used as the base platform for distributed data protection

Adopting a SaaS strategy, however, does include risk. The technology used by the service provider may be acquired by a larger company that changes the direction of its future development, or worse, discontinues support. Alternatively, a smaller and newer third-party developer may fail, and unless the technology is placed in escrow, those relying on it will be ultimately left without support.

Category 2: Point-product and niche-market service providers

Service providers in this category tend to be smaller companies, and are often newcomers to the data protection marketplace. They include:

- "Point solution" service providers who base services on software they have developed that addresses only data protection, rather than a broader spectrum of information management and protection solutions
- Niche-market service providers who attempt to focus exclusively on a particular vertical or geographic region

When considering service providers in this category, it is important to evaluate their capability for long-term viability and continued uninterrupted service. Will they be able to grow with their customers, adding data protection and adjunct capabilities along the information lifecycle? Will they experience growing pains, resulting in poor service, lack of focus on new features, and outages with new data centers?

Smaller service providers in this category frequently lease storage facilities owned and operated by another company, which may offer only standard security features. Finally, limited staff may curtail the types of Service Level Agreements (SLAs) that these smaller companies can commit to, and staff familiar with a niche market may not have the depth or breadth of experience required.

"Point-solution" providers for backup and recovery
Pure-play" providers are those who "concentrate primarily on online data protection for consumers, home offices, and SMBs. These point solutions do not offer adjunct services such as those that allow you to leverage or mine the backup information resources for archiving and eDiscovery. Unlike the providers considered thus far, these service providers typically develop and maintain their own software.

As the data protection and recovery market has matured, the barriers to entry have forced new providers to match the technical feature sets already standard in the industry, if they can. They must focus resources on fundamental data protection (see Table 1) and may require more time to develop essentials for protecting data in a distributed environment—for instance, technology designed to optimize email backup and recovery with data reduction techniques that affect efficiency and scalability.

An even greater challenge is developing the capability to back up and restore or migrate full systems, not just the data that resides on them. This is a key feature not offered by most point solution providers newer to the marketplace; in fact, it is missing from the feature sets of many larger and more mature service providers.

Although this limitation in service offerings is quickly flagged by the IT professional who is routinely called upon to restore or migrate the full systems of many users, it may not be clear to individuals in a distributed enterprise. If there is no corporate policy and/or online service in place that is easily accessible, there is a danger that individual users may choose a more consumer-oriented backup service only to discover that their data is not backed up to allow full system recovery, or that their back up network drives are shared by users on a LAN in a remote office. They may also find that less sophisticated filtering mechanisms force them to rearrange the file structure supporting their normal workflow to ensure classes of files are included in, or excluded from, automated backup—or that recovered files are, in fact, not restored to their original locations.

Ironically, if the provider's point solution is unique enough to challenge a larger competitor, they find themselves a prime target for acquisition. If the technology is not unique, it can be challenging to differentiate themselves from other data protection software developers who do not themselves offer service at all—but who exclusively license their solutions to service providers such as the third-party software providers previously mentioned.

Niche-market service providers

In contrast to the specialized providers who limit their services to data protection, there are a small number of providers who differentiate themselves as serving specific verticals such as healthcare or financial services, or limit their services to specific geographic regions; usually those in which they reside. In this case, companies with global footprints would need to contract with multiple regional service providers to protect data across their entire enterprise.

Probably because of the investment required to develop data protection services, most of these niche market providers license third-party software that is not specifically designed as a vertical-market data protection solution. An interesting case in point, a generalist data protection service was acquired by a larger corporation focused on healthcare and subsequently became the de facto solution for that market, although the service provider nor the third-party software used was designed specifically for healthcare data protection.

Some niche market service providers go further and "piggyback" on another service provider's data protection service or use a variety of licensed software solutions; sometimes by design, but often as add-ons to the legacy systems they are abandoning. As the complexity of managing multiple technologies grows, so does the risk due to the fact that the service provider does not control the destiny of any of the technologies.

Category 3: Broad-spectrum service providers

The final category of online service providers offers data protection as an integral part of a broader spectrum of information management and data protection services that may include PC backup, server backup, disaster recovery support, email continuity, and online records management. The established service providers in this category offer all the required, fundamental features for protection of distributed data and typically include many of the essential features listed in Table 1.

There are, however, key questions you should ask when evaluating these services:

- Are the essentials for distributed data included in the price of the service and integral to the software used—or are they extra cost add-ons or plug-ins?
- Is full system backup and recovery supported?
- Was the software originally designed for data protection of untethered desktops and laptops—or as a client to a server-based backup and recovery solution that may require the purchase of the server package to operate?
- Was the software originally developed for online backup—or is it an adaptation of software developed for other backup solutions, like tape backup?
- Is it a service that merely stores the backup sets of onsite software in offsite storage facilities? (This approach does not offload the burden of verifying the success of the backup or restore.)

Even within the "broad-spectrum" category of service providers, there are different core competencies and business directions, usually derived from the parent company and reflected in the primary product lines funded by the company. Some are actually storage manufacturers, offering data protection services as an added-value utility for the information hosted by their own devices. Others may be in the security business with data protection as an adjunct to tools that protect desktops, laptops, and mobile devices from viruses, malware, and other kinds of breaches.

When data protection services reflect a transition in the provider's basic business model, there is an element of risk for customers in how true the service provider will remain to the mission of distributed data protection. It is key to note what percentage of the company's revenue is derived from data protection. Will the service provider continue to invest in technologies and facilities critical to customers depending on them for data protection?

Comparing service provider categories across the essentials

Table 2 below compares each of the categories of service providers in terms of the essentials for successful data protection, highlighting key issues that should be considered in choosing providers.

Table 2. Summary comparison of service provider categories

	Business Continuity/Disaster Recovery and Telecommunications service providers	Point Solution developers and Niche service providers	Broad Spectrum Data service providers
Ability to deliver on essentials for Data Protection in Distributed Environments (detailed in Table 1)	• Typically are limited in their offerings for retention of specific types of data— and the ease with which historical versions can be retrieved	• Developers must stretch limited resources to develop both fundamental features as well as essentials, like multiple recovery points, full system backup, and range of retention periods	• Service providers typically offer most of the essential features • Verify that service charges include features like backup of email applications • Verify that both data backup and recovery and full system backup are supported
	• Use one or more 3rd party software as the basis for data protection services—do not control its viability or future development • Customers need to examine 3rd party software closely to ensure essential		
Ability to deliver on essentials for Data Protection Administration and Support in Distributed Environments (detailed in Table 1)	• Main focus of professional services is on primary lines of business, not best practices and compliance issues of backup and recovery	• May not have resources or expertise to offer in-depth professional services for data protection and compliance best practices • Unlikely to offer a managed service • New developers may not have had time to create multiple platform support	• Professional services may focus on products outside backup and recovery (storage hardware, IT tools) • Some SaaS platforms have a shorter track record than others • Some do not offer option of licensing software or managed services
	• Level of security of storage facilities varies widely—as does redundant, mirrored backup • Customers wishing to move from SaaS to licensed software must contract with 3rd party developer		

Cloud-based data protection service providers and compliance programs

IT professionals are taking on a greater role in designing and implementing regulatory compliance procedures and systems that protect sensitive data and help ensure business continuity. One of the primary measures of compliance is consistency across an organization. And while compliant data protection procedures must be demonstrably consistent in all locations, they are difficult enough to accomplish within a centralized operation and even more difficult in a physically distributed environment.

Online data protection, when applied consistently across a distributed workforce with no requirement for end user interaction, can go a long way toward meeting enterprise information governance requirements. How quickly data can be moved offsite to a secure location, and the level of ease of data retrieval, can also make RTOs/RPOs far more achievable.

Regulatory compliance
In the US alone, the Better Business Bureau has generated a list of 34 Federal and State privacy rules and regulations. Some of the more familiar ones are:

Gramm-Leach-Bliley (GLB) Act—requiring financial institutions to protect customers' non-public personal information

SEC Rule 17a—laws for broker-dealers storing electronic records

FACTA—protecting consumer information from misuse across industries

Sarbanes-Oxley Act (SOX)—regulation of financial reporting

FRCP Rules 26—governing discovery and disclosures of information relevant to civil lawsuits

HIPAA—supporting the protection of personally identifiable health information

Certifications
Some important data security related cloud-based data protection certifications include:

PCI DSS—The **Payment Card Industry Data Security Standard (PCI DSS)** is an information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. Validation of compliance is done annually—by an external organizations handling large volumes of transactions, or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes.

ISO 27001—**ISO/IEC 27001** is an information security management system standard by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO/IEC 27001 formally specifies a management system that brings information security under explicit management control. Organizations with ISO 27001 certified can therefore be formally audited and certified compliant with the standard

If a laptop is lost or stolen, centralized backup is essential to help an enterprise judge the scope of potential information exposure. In addition, an enterprise's centralized, up-to-date backup of distributed data can help uncover areas of legal exposure. Integrating their laptop backup with legal discovery and review tools can help reduce legal discovery costs, and the time it takes to perform early case assessments.

Of the categories of service providers examined in this paper, only two routinely provide significant support for compliance programs. Disaster Recovery service providers obviously address business continuity requirements, but do not typically provide electronic discovery tools to mine their storage of backup and recovery information. They also do not feature endpoint security solutions integrated with their online services.

Broad-spectrum service providers, at least the more mature ones, offer solutions that ensure business continuity and disaster recovery and offer technology that protects data privacy through encryption both in transmission and in storage. Some also offer email continuity services.

One differentiating factor that is often overlooked is the security level of the data centers of these service providers. For instance, do they own and operate their data storage facilities?

For global enterprises, it is important to verify backup data is stored in globally distributed data centers, though some operate only in North America and do not support business practices for customers in other regions.

Before choosing your provider

Before you select a data protection and recovery provider to work with, it's important to recognize the different categories of providers, as well as the origin and evolution of their SaaS offerings. By understanding basic distinctions in their business drivers, potential resources, and core competencies, you will be able to fully assess the capabilities of their offerings to meet distributed data protection requirements. By evaluating providers for specific features/requirements for data protection in terms of how those align to your overall business objectives, you can better focus on selecting the appropriate long-term provider.

Learn more at
hpe.com/software/informationmanagement

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA5-8249ENN, November 2015, Rev. 1