IDC OPINION

Many firms are acutely aware of the costs and risks associated with lost or unrecoverable data on employee devices, including desktops, laptops, and mobile devices. Data loss frequently results in reduced productivity and revenue generation. In addition, the loss of sensitive company information or the inability to discover it for a legal event can damage a corporate brand, shake shareholder confidence, and increase customer and/or employee concerns about data privacy.

Given the high costs and risks, it is surprising to learn that many companies do not have the infrastructure, IT staff, budget, or corporate mandate to adequately protect the data at the edge of their organization. Fortunately, the rapid growth of employee-generated data and the increased reliance on mobile/remote workforces are driving firms to assign higher priority to protecting and recovering data sitting outside the walls of their datacenter.

Today, mobility initiatives, including bring your own device (BYOD), are gaining popularity as businesses look to provide portability of data through a “personal data cloud.” Explosive growth in the use of mobile devices, such as phones and tablets, opens up new opportunities for anywhere access to information, but it has also impeded IT’s ability to protect and control sensitive corporate data. End users have high expectations that their data will always be available, with consistent versions of their work files across laptops and tablets. Corporate policies for managing and safeguarding user data have not been able to keep pace with the proliferation of tablets and mobile devices as a result of the BYOD trend.

Many organizations are in a quandary, faced with the prospect of using point-oriented solutions that do not efficiently scale to meet future data growth, do not provide the access capabilities they seek, or do not integrate well with existing data protection and search processes. Often, they turn a blind eye toward employees who seek to protect data on their own. This raises the possibility that sensitive data will be stored offsite or sent over the wire where it may not be secure, easily retrieved, or discovered. Making matters worse, deploying point or relegated data protection solutions for edge protection often introduces complexity, inefficiency, and higher administrative costs because the solutions may not enable protection, recovery, access, and discovery simultaneously (or with only one solution).

Our research indicates that many companies have a critical need not only to protect data at the edge of their organization with easy-to-use and scalable solutions that have low impact on client performance but also to open up secure access to that data.
for self-service use whenever and wherever it is needed. Ideally, any edge data protection solution would minimize the impact on help desk staff and IT resources, be transparent to the end user, and simultaneously deliver user-initiated restoration of folders, files, or data on demand. Furthermore, solutions for data at the edge should tie into existing infrastructure and processes and provide recovery, retention, access, eDiscovery and compliance, and analytics without the complexity and cost of additional products and data silos.

CommVault Simpana software provides a comprehensive and flexible data protection, recovery, management, and access solution that allows organizations to extend beyond their physical and virtual environments in the datacenter, ultimately safeguarding the edge of their environments. Simpana software’s flexible, modular architecture allows customers to protect, find, and use their business-critical information from the datacenter out to the fringes of their organization. Since its inception, Simpana software has utilized a single code platform that provides backup, recovery, archive, deduplication, replication, and search. This IDC White Paper explores the challenges associated with safeguarding data and opening up universal access for distributed desktop and laptop systems residing at the edge of an organization’s IT infrastructure. IDC examines CommVault’s Edge solution in the context of CommVault’s data protection, management, and access framework and reporting capabilities — managed from a single console. CommVault, leveraging its core data protection and recovery architecture, extends Simpana software functionality to protect edge environments.

**IN THIS WHITE PAPER**

This IDC White Paper explores the challenges associated with safeguarding data and opening up universal access for distributed desktop and laptop systems residing at the edge of an organization’s IT infrastructure. IDC examines CommVault’s Edge solution in the context of CommVault’s data protection, management, and access framework.

**SITUATION OVERVIEW**

**The Challenges of Safeguarding Data at the Edge and Delivering Self-Service Access from Anywhere**

IDC has discovered that many firms do not have adequate protection and recovery policies or tools in place to manage their ever-increasing volumes of data. Worse still, backups for data on desktops and laptops can be very problematic or even nonexistent in some organizations. The era of BYOD is here to stay as end users now have true mobility and demand anytime, anywhere access to their files, email, and other content. This has had enormous implications for corporate IT managers who are charged with safeguarding data that in the past has resided outside their control and corporate mandates. The mobility revolution and BYOD have allowed end users the luxury of increased productivity and creativity; however, they have done so at the expense of data security and control in the eyes of IT.
The prevailing tools that have been embraced by groups focused on mobility for sync, collaboration, and file sharing have acute shortcomings. Security and encryption are nonexistent. It has also been demonstrated that these tools allow nonauthorized employees access to files or folders. Regulatory concerns have skyrocketed because certain files or data cannot be related to a specific location. In short, these tools do not provide any search, authentication, auditing, or authorization of critical distributed corporate data. More important, although these tools provide sync, collaboration, and file sharing functionality, they provide no data or file replication services and, therefore, no disaster recovery framework for restoration of data. Furthermore, these tools do not have any in-house IT administration or central point from which policies can be enforced to restrict access to certain files from a tablet or mobile phone. The major focus of the prevailing sync, collaboration, and file sharing solutions has been users' need for an easy way to share information and collaborate, along with support for multiple devices, including mobile devices, tablets, laptops, and desktops, with no thought toward security or disaster recovery.

Additionally, traditional backup and recovery approaches to tape and disk are not well suited to protecting and recovering sensitive data on client devices, particularly over a WAN connection; instead, they require IT departments to perform recovery operations for users, which ultimately strains resources. Organizations of all sizes are grappling with expanding IT infrastructure as a result of growth, corporate acquisitions, telecommuting, and the distributed nature of sales personnel. This proliferation of decentralized business operations has created the need for a more centralized approach to managing and understanding data. It also introduces new challenges for enabling global discovery, financing costly VPN licenses, and collecting and finding data, without excessive bandwidth consumption that impacts end users.

Conventional backup and recovery methodologies do not adequately protect the burgeoning requirements of virtual and mobile environments, and they do not have the ability to scale as user requirements change and data volumes continue to grow. Traditionally, the backup of data on client devices has been the responsibility of end users, who typically save their data to removable media or to cloud service providers. They also define the files and folders to be backed up. This methodology does not provide adequate safeguards or protocols that many IT administrators demand in today's risk-averse environments. Additionally, some cloud storage providers have had notoriously short life spans, exposing critical user data to the possibility of loss, co-opting, or accessibility by virtually anyone.

Users are charged per gigabyte to protect unique copies of business-critical data, which may not be cost-effective on a broad scale. Such types of inconsistent backup practices jeopardize sensitive corporate data. Consequently, firms are exploring new technologies that enable more efficient and cost-effective data protection solutions that take advantage of storage optimization capabilities, such as data deduplication, remote replication, and content indexing, which extend security, search, and backup protection to desktops and laptops.

Increasingly, the protection of data residing on desktop or laptop devices has become a critical component of a much broader business mandate to centrally manage, secure, and control data on distributed assets. In addition to centralized backup and recovery solutions, many firms are applying additional controls, such as disk and
file encryption, data loss prevention measures, security auditing, and governance, risk, and compliance (GRC) initiatives. Firms are also protecting sensitive data using auto-erase applications that can be activated if a remote or mobile device is lost or stolen, and they're creating and enforcing policies that specify how individuals should move, copy, or share sensitive corporate data.

Furthermore, the need for corporate IT visibility into distributed information assets is critical to mitigate risk. In the event that a laptop is lost or stolen, a centralized backup store is imperative to help a firm understand the scope of potential information exposure. Moreover, firms can use a centralized, up-to-date backup store of distributed data to understand legal exposures. Integration of desktop and laptop backup with legal discovery and review tools can help firms reduce custodian discovery costs and plan for early case assessments.

Recent developments in cloud services have created more dynamic data protection, recovery, and backup environments that are capable of extending these services to laptops and mobile devices. However, the challenge with cloud services is the ability to globally identify or discover data, both cost-effectively and in a timely manner. This is particularly problematic if end users have commissioned their own backup service outside the control of IT. A data protection and management solution built on a singular platform provides the benefits of content indexing for recovery, retention, file access and file sharing, eDiscovery and compliance, and reporting and analytics.

IT administrators need greater assurance that mobile client data is protected and discoverable with less complexity and cost. The combination of opportunistic scheduling, bandwidth throttling, granular policy settings, and client-side deduplication technologies supports faster, more efficient backup and restoration capabilities — particularly for remote and mobile users — without detrimentally impacting user productivity. These products deliver markedly improved bandwidth and storage utilization compared with traditional backup and recovery methods. Furthermore, they give firms a way to resolve the growing challenges of managing their distributed business and budget requirements.

The CommVault Edge Advantage

CommVault has made significant investments in its Simpana technology over the past decade to provide a singular, integrated data and information management platform. CommVault's Simpana architecture delivers backup, recovery, archive, replication, reporting, and search capabilities built on a single, modular, common code platform. The Simpana software architecture shares a single set of back-end services, which ensures granular, release-independent application recovery and services. This capability allows CommVault customers to accelerate new installations and upgrades or add additional data management operations.

Among Simpana's latest features is the CommVault Edge solution, which is designed to meet the burgeoning data protection and access needs of customers with an easy-to-deploy, scalable, and efficient way to safeguard distributed laptop and desktop devices. It supports all the latest Windows, Mac, and Linux systems with the same solution. CommVault's Edge software reduces the complexity of protecting those systems with a single solution; new client systems are automatically discovered, and
administrators can centrally determine user policies, access rights, and security. For the end user, the experience is seamless — backups run automatically in accordance with a set of predefined criteria, which include network and resource parameters configured to maintain an uninterrupted computing experience. Users no longer need to be cognizant of network speeds, VPN access, or time of day. Single sign-on integration with Active Directory provides users with transparent access to their protected data, without consuming administrators’ time.

A backup monitor runs locally for a quick snapshot of current or recent activity, with a link to the browser-based Web console, which includes an intuitive set of controls that allows end users to customize their own data protection and restore experience. The controls are fluid across all platforms for a unified experience and are extended to tablets and smartphones, empowering end users with access to data from virtually any location and any device with an Internet connection to the Web console. Data captured from edge devices is supported by CommVault's Content Indexing capabilities and does not require an additional touch to the device. Users can search through their own backup data and see HTML previews of documents before executing a restore, and the organization can perform discovery across the entire data set.

CommVault provides customers with a familiar and comprehensive solution that facilitates an end-user "self-service" approach to accessing, protecting, and recovering data at the edge of the organization. The mix of functions helps reduce management burdens on the IT department, thereby lowering the capital and operational expenses of deploying separate products that are considerably more complex and time consuming for IT to oversee. Customers can deploy CommVault Edge wholly on-premises or by leveraging the cloud resources of their choosing and can select a licensing model based on traditional agents and options methodology or a capacity-based model according to the amount of data being protected. This allows for a simple, straightforward acquisition model applicable to multiple configurations and use cases.

Enhancements to the CommVault Edge Data Protection Solution

CommVault Edge launched more than a year ago and features key enhancements to increase its functionality, including:

- Doubling the number of clients protected by a single CommCell to 10,000 from 5,000 in the initial release
- Enhanced intelligence that minimizes impact on resources and shrinks protection windows by checking to see if a file has changed before executing a backup job
- Expanded support for operating systems and mobile devices, including Windows 8 systems and a Windows 8 RT mobile app, respectively
- Enhancements to CommVault Edge mobile app and the Internet-based console for better usability and to provide users with mobile access to their laptop/desktop data and their Simpana software-protected Exchange data
New flexible, low-impact and automated rollout capabilities such as smart content definition, registration workflow, client ownership, and firewall and port controls that make it quick and easy to deploy and maintain laptop/desktop protection.

Adding the capability to protect the local Dropbox folder on a system so that IT can understand usage and ensure this information is also protected and searchable.

CommVault Edge is based on Simpana’s fast, efficient collection of data; flexible, cost-effective deployment; efficient management and resource usage; and pricing model. The Simpana architecture can enable new use cases for organizations by allowing them to leverage data that is stored in a single virtual repository — ContentStore. Customers can utilize their data more efficiently and increase their productivity and mitigate risk of loss.

CHALLENGES/OPPORTUNITIES

The biggest challenge for the CommVault Edge solution will be replacing existing or relegated remote data protection products that are already deployed in customer environments. We expect that CommVault will have great success in selling its Edge solution to existing Simpana customer accounts that do not have any endpoint protection. CommVault will need to continue to demonstrate its customer value and the utility of its scalable, modular Simpana software, especially to prospects that are considering migration to a different vendor. CommVault’s scalable, easy-to-deploy data protection architecture will provide measurable customer value for organizations that need, or want, to make a change in their protection and recovery practices.

CONCLUSION

IDC believes the need to protect sensitive data residing on desktops, laptops, and mobile devices is more critical than ever. Furthermore, users are demanding self-service access from any device, anywhere. As a result, corporate IT control and monitoring of, as well as processes related to, remote and mobile IT assets are growing concerns across many enterprises, especially as more companies adopt mobility initiatives. The BYOD model has been embraced by companies of all sizes, and centralized management tools to safeguard their data are sorely lacking.

This challenge is largely driven by the growing amount of data and content created and managed on edge devices. The proliferation of devices, combined with the distributed nature of today’s workforce and more stringent regulatory requirements, makes edge data protection a critical necessity. Furthermore, companies simply cannot overlook the risk or consequences of public exposure that would likely result if sensitive data, stored outside the datacenter, is lost, stolen, or compromised or cannot be discovered when required. We expect the market for this type of data protection, backup and recovery, access, and discovery solution for desktops, laptops, and mobile devices to continue to grow in importance.
CommVault, building on the success of its flagship Simpana software, will continue to grow existing customer accounts with the CommVault Edge solution and will generate new customers looking to deploy a lightweight, easy-to-use, scalable, and comprehensive solution for endpoint protection, access, search, and recovery. The introduction of the CommVault Edge solution demonstrates the company's commitment to continued investment and innovation in the data protection market. Simpana software is an extendable data protection and recovery framework that allows customers to safeguard their data, from the datacenter to mobile devices sitting outside IT control.

CommVault Edge delivers a solution that is secure and allows users to access their data anywhere and at any time, enhancing productivity. Moreover, Simpana software provides customers with a holistic approach to truly modernize their data protection infrastructure by leveraging the common code platform, content indexing, search, and discovery. Simpana software offers customers efficient and flexible recovery options for on-premises or edge clients from disk, tape, or cloud.

CommVault's theme of "modernized data management" will resonate well with the company's current Simpana software customers as well as those customers looking to bridge their data protection solutions from physical to virtual to cloud and from the datacenter to the edge. Simpana's technology enhancements, such as ContentStore, allow customers to add more value and eliminate silos by allowing greater access to data already collected and stored in a virtual repository. Customers can now more efficiently and intelligently utilize their data through content indexing, data reduction, tiering of storage resources, reporting, and improved management. CommVault Edge will provide Simpana software customers with greater access to and greater control and protection of data residing on mobile devices, outside the confines of their corporate IT infrastructure.

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 2013 IDC. Reproduction without written permission is completely forbidden.