The Critical Need for Edge Data Protection

Sponsored by: CommVault

Robert Amatruda        Eric Sheppard
January 2012

IDC OPINION

Today, many firms are acutely aware of the risks associated with lost or unrecoverable data on employee devices such as desktops, laptops, and mobile devices. The loss of sensitive corporate information can damage a corporate brand, shake shareholder confidence, and increase customer and/or employee concerns about data privacy. The loss of corporate information also frequently results in reduced productivity and revenue generation. Given the high costs and risks associated with the loss of such information, it is surprising to learn that many companies do not have the infrastructure, IT staff, or budget to adequately protect the data at the edge of their organization. For this reason, many organizations have traditionally not mandated their IT department to protect against the loss of such information.

Fortunately, the rapid growth of employee-generated data and the increased reliance on mobile/remote workforces are driving firms to give a higher priority to protecting and recovering data sitting outside the walls of their datacenter. However, in many cases, organizations face the prospect of using point-oriented solutions that do not scale to meet future data growth or that don’t integrate well with existing data protection processes, or they rely on employees to protect data on their own. This opens up 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 and higher administration costs because it may not enable protection, recovery, access, and discovery simultaneously (or with one solution).

Our research indicates that many organizations have a critical need to protect data at the edge of their organization with easy-to-use and scalable solutions that have low impact on client performance. Ideally, any edge data protection (EDP) solution would minimize impact on the client and enable user-initiated restoration of folders, files, or data on the fly. Furthermore, edge data protection solutions should tie into existing infrastructure and data protection and recovery processes, not only for recovery of data but also to provide compliance and eDiscovery.

CommVault Simpana software provides customers with a comprehensive and flexible data protection and recovery solution that allows users to extend their data protection tools beyond their physical and virtual environments, ultimately safeguarding the edge of their IT organizations. A key enabling feature of Simpana software is network optimization, which comes from source-side data deduplication and bandwidth throttling for efficient data transfer. Simpana software’s flexible, modular architecture allows customers to protect, recover, access, and discover their business-critical information from the datacenter to the fringes of their organization.
Since its inception, Simpana software has utilized a single code platform that provides backup, recovery, archive, deduplication, replication, search, and resource management capabilities — managed from a single console. CommVault, levering its core data protection and recovery architecture, extends Simpana software to protect edge environments.

**IN THIS WHITE PAPER**

This IDC White Paper explores the customer challenges associated with safeguarding data on distributed desktop and laptop systems residing at the edge of an organization's IT infrastructure. IDC examines CommVault's Simpana Edge Data Protection (EDP) solution in the context of CommVault's data protection, recovery, and access framework.

**SITUATION OVERVIEW**

**The Challenges of Safeguarding Data on Laptops and Endpoints**

IDC has discovered that many firms do not have adequate protection and recovery policies or tools in place to manage the ever-increasing volume of data. Worse still, backups for protecting user data on desktops and laptops can be nonexistent for some organizations. Moreover, traditional backup and recovery methodologies to tape and disk are not well suited to protecting and recovering lost sensitive data on client devices, particularly over a WAN connection, and 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 a need for centralized management and understanding of data and introduces new challenges for collecting and finding data without excessive bandwidth consumption that impacts end users, enabling global discovery and requiring costly VPN licenses.

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 was left up to end users, who saved their data to removable media or to cloud service providers. Furthermore, users define the files and folders to be backed up. This methodology does not provide the adequate safeguards or protocols that many IT administrators demand in today's risk-averse environments. Some cloud storage providers have had notoriously short life spans, and critical user data could be lost, co-opted, or left accessible to virtually anyone. Also, 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 to take advantage of storage optimization capabilities such
as data deduplication, remote replication, and content indexing, extending security
and backup protection to desktops and laptops.

Increasingly, the protection of data residing on desktop or laptop systems 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. In addition, firms are protecting
sensitive data using auto-erase applications that can be activated if a remote or
mobile device is lost or stolen; they’re also creating and enforcing policies that specify
how individuals move, copy, or share sensitive corporate data.

Furthermore, the need for centralized 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 in helping 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 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 cost-effectively and in a timely manner. This is
particularly problematic if end users have enabled their own backup service outside
the control of IT. A data protection solution built on a single platform provides the
benefits of content indexing for eDiscovery and consistent recovery. Therefore, IT
administrators will have greater assurance that the mobile client data is protected and
findable with less complexity and cost. The combination of intelligent scheduling,
bandwidth throttling, granular policy settings, and client-side deduplication
technologies supports faster, more efficient backup and restoration capabilities —
particularly for remote or mobile users — without detrimentally impacting user
productivity. These products deliver markedly improved bandwidth and storage
utilization compared with the 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 Simpana Edge Data Protection 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,
storage resource management (SRM), 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 CommVault's latest features is Simpana EDP software, which is designed to meet the burgeoning remote data protection needs of customers with an easy-to-deploy, scalable, and efficient way to safeguard distributed mobile, tablet, and laptop devices. CommVault also supports the most recent Windows, Mac, and Linux systems with the same solution. With the proliferation of BYOD (bring your own device) policies in the workplace, EDP 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. With single sign-on integration with Active Directory, users also have 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 enables the end user to manage the data protection and restore experience. The controls are fluid across all platforms for a unified experience and are extended to tablets and smartphones, thus empowering the end user to access 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 the organization can perform discovery across the entire data set.

CommVault provides customers a familiar and comprehensive solution that enables 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, thus lowering the capital and operational expenses of deploying separate products that require considerable attention and complexity for IT. Customers can deploy EDP through a licensing model based on traditional agents and options methodology or on 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.

**CHALLENGES/OPPORTUNITIES**

The biggest challenge for CommVault's EDP solution will be displacing existing or relegated remote data protection products already deployed in customer environments. We expect that CommVault will have great success in selling its EDP solution into 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 those considering migrating to a different vendor. CommVault's scalable, easy-to-deploy data protection architecture will provide measurable customer value for those needing or wanting to make a change in their protection and recovery practices.
CONCLUSION

IDC believes that the need to protect sensitive data residing on desktops and mobile and remote workers' laptops, coupled with the need for more centralized control and understanding of remote IT assets, is a growing concern across the enterprise. This challenge is largely driven by the growing amount of data and content created and managed on edge devices. This 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 afford the consequences or public exposure that could result if there is no knowledge of the data stored outside the datacenter when the data is lost, stolen, or compromised. We expect the market for these types of data protection, backup and recovery, access, and discovery solutions for desktop, laptop, and mobile devices to grow in importance.

CommVault, building on the success of its flagship Simpana software, will continue to grow existing customer accounts with its EDP solution and will generate net-new customers looking to deploy a lightweight, easy-to-use, scalable, and comprehensive solution for endpoint protection and recovery. The introduction of CommVault's EDP solution demonstrates the company's commitment to continued investment and innovation in the data protection market. Simpana software is an extensible data protection and recovery framework that allows its customers to safeguard their data from the datacenter to the edge. Moreover, Simpana software provides customers 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 protection" will resonate well with CommVault's current installed base of Simpana software customers as well as those customers looking to bridge their data protection solutions from physical to virtual to cloud. Simpana technology enhancements fit very well into CommVault's cloud offering by utilizing content indexing, data reduction, tiering of storage resources, reporting, and improved management. These enhancements, coupled with CommVault's EDP offering, will enable Simpana software customers to migrate and archive data to lower-cost cloud-based storage. CommVault has set the foundation for its customers to protect their data from edge to core to cloud and beyond.

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 2012 IDC. Reproduction without written permission is completely forbidden.