WHITE PAPER

The Critical Need for Edge Data Protection

Sponsored by: CommVault

Eric Burgener
October 2014

IDC OPINION

The 3rd Platform of computing, based around the four pillars of mobile computing, social media, big data and analytics, and cloud, is redefining what IT infrastructure needs to provide. More and more content is being created, edited, and shared at the edge on mobile devices such as laptops, tablets, and smartphones, raising accessibility, security, and protection concerns. Much of this data is confidential or otherwise sensitive corporate information. As a result, data protection requirements are rapidly evolving to include endpoint protection as a must-have.

Endpoint solutions must meet not only traditional data protection requirements such as flexible data capture, multiple recovery options, efficient and secure data transfer and storage, and comprehensive coverage but also a new set of requirements driven by the explosion in mobile computing. As end users blend their work and personal lives using an ever-increasing array of handheld options, they often create shadow IT operations such as Internet-based file sync and share (FSS) to meet their agility requirements. Fragmented data stores that contain sensitive corporate data make it very difficult for IT to manage corporate information assets to meet security, recoverability, compliance, and regulatory requirements. The challenge for IT has been meeting corporate guidelines for data management while providing the agility, ease of use, and unfettered access to which end users have become accustomed.

CommVault, the originator of the unified data management concept, just introduced an enterprise-class FSS service into its CommVault Edge endpoint data protection solution. The platform, called Simpana, provides a single, centrally managed repository for data that has made it easy to consistently, comprehensively, and efficiently back up, recover, archive, search, access, share, and manage sensitive corporate information. With the introduction of its FSS service, CommVault promises to meet collaboration requirements with a scalable, easy-to-use platform that intelligently expands the definition of unified data management to include collaboration. Organizations that deploy the entire CommVault offering have a comprehensive way to identify, protect, and manage all sensitive data across the business, regardless of how that data is created and used.

IN THIS WHITE PAPER

This IDC white paper explores the customer challenges associated with safeguarding data residing on various endpoint devices, including laptops, tablets, and smartphones, at the edge of an organization's IT infrastructure. IDC then reviews the CommVault Edge endpoint data protection solution, discussing how this centrally managed platform can be used to simultaneously address data protection, collaboration, regulatory, and eDiscovery requirements in a secure manner.

SITUATION OVERVIEW

The 3rd Platform computing era is here. Driven by the needs of mobile computing, social media, big data and analytics, and cloud, IT infrastructure is quickly evolving to provide much more agility, scalability, and availability. As businesses move more to a data-driven "always on" model, IT must adapt to the need for higher availability, burgeoning heterogeneity (particularly in the areas of mobile devices), and increasing collaboration among employees and nonemployees. As shadow IT operations that leverage easy-to-use Internet-based services become more popular with end users, IT is struggling to manage data protection, recovery, compliance, and regulatory risks.

Data Protection Requirements Are Becoming Increasingly Stringent

End users expect to be able to access their data from a variety of different locations and endpoint device types 24 hours a day. This is driving not only the need for infrastructure that is continuously available but also the evolution of recovery objectives. Over the past five years, recovery point objectives (RPOs) and recovery time objectives (RTOs) have become increasingly stringent. Recent IDC research shows that 82.3% of small enterprises (1,000–4,999 employees) and 87.5% of large enterprises (10,000+ employees) have an RPO of under 1 hour. 73.4% of small enterprises and 77.6% of large enterprises have RTOs of under 4 hours. RPO defines the amount of data loss acceptable in the event of a failure, while RTO defines the time it takes to bring a failed application service back into normal operation. That same research indicates that the cost of downtime at a company level for mission-critical applications ranges from $224,952 for small enterprises to $1,659,482 for large enterprises.

While most organizations have implemented good data protection strategies for their servers, edge protection can be haphazard or even nonexistent. Because end users are increasingly capturing, creating, and/or using critical business data on laptops and mobile devices, this represents a significant risk. While it's rare to "lose" a server in the datacenter, this is a common occurrence with endpoints. Lost laptops and mobile devices put corporate data as well as productivity at risk. Lost endpoints at best will impact employee productivity until data can be recovered to a new endpoint (if it can be) and at worst can provide improper access to confidential corporate information to potential bad actors.

As the value of this edge data becomes more and more apparent to IT organizations, the need for a more comprehensive data protection strategy that covers endpoints becomes clear. End users like the agility that mobile devices provide, and the use of these devices will only increase. To provide the best protection for corporate data, IT needs to come up with a comprehensive data protection solution for all critical corporate data that meets the needs of both end users and IT management.

Collaboration: The New Way to Work

Corporate work is increasingly being done by virtual teams that are composed not only of employees but also contractors, business service providers, partners, and customers. Virtual group workflows for tasks such as document creation and editing cross corporate boundaries, and all of these workers need to share folders and documents. Historically, IT-based services have limited networked corporate resource access to employees, providing a more secure approach but not making it easy to quickly collaborate with nonemployees. Cloud-based FSS products such as Dropbox, Google Drive, and Microsoft OneDrive make it easy to bypass traditional IT, dynamically sharing documents on demand that can be accessed from anywhere in the world across the Internet. End users can be much more productive sharing folders and documents with others using these services instead of just using email, thumb drives, and other unprotected mechanisms. Unfortunately, because end users are primarily focused only on their immediate rather than their strategic IT needs, they typically do not see the downside of conventional FSS products or do not prioritize addressing the risks.

As a project scales over time, challenges with FSS begin to appear. File deletions are the biggest issue. Depending on how permissions have been defined in an FSS service, a file or folder that is deleted by one user will be deleted for everyone authorized to share it. Deletions may also include accidental overwrites. Although many FSS services provide an "undelete" option, collaborator deletion is not necessarily obvious to the virtual team sharing the content, and the deleted content may not be missed until it is too late to retrieve it. An additional issue is that virtual team members may join or leave the team or the company in midproject, and designating new owners or denying access to individuals who have left the company can be problematic. Access to critical corporate data can be lost. Both of these issues can impact productivity and, at worst, require certain project work to be redone.

If the data in FSS services is important corporate information, it should be secure and protected. IT has no visibility into how this data is being shared, who has access to the data, and if (or how) this data is being protected. Data protection capabilities in FSS services are often rudimentary and may not be able to meet corporate RPO/RTO requirements for critical data.

In addition, the ad hoc use of FSS services can considerably complicate search. Finding content can be difficult and time consuming, particularly when multiple FSS services are in use. There is no ability to search across disparate repositories. No two people have the same tree structure for their content, so locating desired files or folders in even a single repository can be challenging. This can complicate not only collaboration work but recovery activities as well.

Meeting Regulatory and eDiscovery Requirements

End users don't think about the operational details of meeting eDiscovery requests or regulatory compliance requirements; they focus on how to make their jobs easier. For many, this means making it easier to share documents with virtual workgroup members. IT departments are left to deal with the fallout. How do they efficiently search multiple cloud-based repositories? How do they make the most efficient use of expensive storage capacity? How do they meet time-sensitive eDiscovery requests and enforce legal holds? How do they prove that they're meeting compliance requirements for the retention and protection of sensitive data in regulated industries such as healthcare (HIPAA), retail (PCI DSS), financial services (SOX), and government (FIPS)? These are all critical operations for many organizations that shadow IT can put at considerable risk.

Even if organizations use a comprehensive endpoint backup solution, it can still present eDiscovery challenges if it is not integrated with other key data protection platforms. Separate data silos require separate eDiscovery workflows, introducing additional complexity that already overworked administrators do not need.

Evolving Endpoint Data Protection Requirements

Shadow IT operations have sprouted up at many organizations because IT has had difficulty creating an infrastructure that allows end users to work as they would like to. Centralized IT and end-user requirements aren't necessarily incompatible, but they certainly demand a set of much more agile 3rd Platform-based services. A primary responsibility of organizations is to adequately protect sensitive data while meeting compliance requirements. But if IT expects to centrally manage all data protection operations, it needs to provide services that give end users the flexibility and ease of use to which they've become accustomed with Internet-based FSS and other consumer-oriented applications. IT needs to protect confidential information while accommodating the trend toward virtual workgroup collaboration with nonemployees. As enterprises investigate how to best meet these requirements, they should consider the following:

- Because of the increasing amount of critical corporate data that is created and edited on laptops and other mobile devices, all organizations that work with sensitive data need to implement comprehensive endpoint data protection strategies that feature transparent secure backup (encryption), efficient data transfer (deduplication), self-service access and recovery (role-based access control), and remote wipe.
- IT needs to implement its own FSS services that meet not only end-user requirements for agility, worldwide access, and ease of use in supporting virtual workgroup collaboration with both employees and nonemployees but also IT's requirements for security, manageability, and compliance.
- Given exploding data growth rates (44% CAGR through 2018), solutions must be scalable and leverage a full complement of storage efficiency technologies, including flexible, incremental data capture with synthetic full backup creation; multiple recovery options to support short RTOs, efficient data transfer, and dissimilar platforms; and snapshot backups that leverage changed block tracking, compression, and deduplication.
- Heterogeneity is the watchword in 3rd Platform computing environments, and data protection solutions should cover a variety of server types, operating systems (Windows, Mac, and Linux), hypervisor platforms, endpoint device types, and data types (structured, semistructured, and unstructured) as well as datacenter- and cloud-based data; support both disk and tape; offer both on-premises and off-premises choices; and provide options for both local and remote recovery.
- Data protection schedules for all corporate data (both server and endpoint based) should be centrally managed to meet corporate RPO/RTO requirements.

The trend toward unified data protection platforms bodes well for enterprises looking to create a single, centrally managed service that comprehensively covers secondary storage requirements such as backup, disaster recovery, archive, and eDiscovery for server, desktop, laptop, and mobile devices.

CommVault Edge: Endpoint Data Protection for the Original Unified Data Management Platform

Traditionally, secondary storage operations such as server backup, disaster recovery, and archive were handled separately with multiple platforms. Mobile devices didn't exist, and desktops and laptops generally weren't being backed up by IT. There is a lot of commonality between the data used for backup, disaster recovery, archive, and search, although the use cases are different. Seeing an opportunity, CommVault was the first data management solutions vendor to introduce the concept of a single, centrally managed platform that unified these secondary storage operations with the release of Simpana in 2007. The unified data management concept brought considerable efficiencies and cost savings to the administration of storage.

With the rise of mobile computing, sensitive corporate data is increasingly being created, edited, and/or accessed at the edge with laptops and mobile devices. In 2012, CommVault expanded the Simpana platform with the introduction of CommVault Edge technology for endpoint data protection, providing a way for that data to be protected according to IT guidelines. Evolving collaboration strategies are yet another discipline that can benefit from the protection and security of centralized management, provided end users' agility and ease-of-use needs are met. In 2014, CommVault enhanced Simpana 10 with an FSS service that provides end users with a scalable collaboration platform that can securely yet easily share content with employees and nonemployees alike on a worldwide basis while meeting IT's more strategic protection, recovery, and compliance requirements.

This strategic expansion of the unified data management concept takes advantage of the commonality in the data sets that need to be shared, backed up, recovered, archived, and searched to deliver a scalable, secure, recoverable, and cost-effective repository called the ContentStore. The ContentStore is the single repository for all this data, allowing it to be centrally managed with datacenter expertise and to meet corporate IT guidelines.

CommVault Edge software's rich feature set includes:

- **Efficient data capture,** leveraging source-side deduplication, opportunistic scheduling, and bandwidth throttling for transparent endpoint data protection
- **Multiple recovery options,** including administrator-driven and user self-service file-level and system-level recovery options via a mobile app, Windows Explorer integration, or a Web console
- **Secure data transfer** without a VPN connection using secure, encrypted backup streams over SSL
- **Prevention of unauthorized access** with file-level encryption, remote wipe, and geolocation capability
- **Virtually anywhere, anytime access** for users to view, search, download, and edit protected data for increased productivity
- **Secure file sharing and collaboration** with sync across laptops and the ability to share information within an organization and with external partners and customers

- **Centralized management of all data** in the ContentStore, a scalable single repository that supports up to tens of thousands of mixed Windows, Mac, and Linux clients; enables backup, recovery, archive, search, and eDiscovery (with legal hold definitions) to work seamlessly across any platform; includes integrated indexing; and offers reporting and analytics to quickly identify client status
- **Flexible acquisition options** that include capacity licensing per terabyte or per-user pricing with an annual term and flexible deployment methods that include on-premises, cloud, and hybrid options as well as offerings designed especially for service provider partners

CommVault also recently introduced new solution set packaging options that allow customers to purchase solution sets such as endpoint data protection, virtualization, email archive, or IntelliSnap integrated snapshot backup as standalone products. Organizations can start with the functionality and solution set they need and ultimately expand to the full Simpana feature set by adding capabilities as needed. This significantly lowers the entry price point to this unified data management platform, providing an attractive option for smaller customers.

FUTURE OUTLOOK

The data protection market is rapidly evolving to accommodate the new requirements of the 3rd Platform of computing. This evolution is impacting historically adjacent markets, such as endpoint protection, disaster recovery, and archive, as well as other markets where the availability of a single repository for corporate data can help IT organizations more effectively safeguard these precious assets. CommVault's integration of an easy-to-use FSS service that meets end-user requirements for collaboration but leverages the ContentStore repository is a unique approach that brings significant benefits to both IT and end users.

Infrastructure consolidation to improve efficiency is a time-tested datacenter trend. By integrating backup, disaster recovery, and archive into the initial release of Simpana, CommVault is largely responsible for the secondary storage consolidation trend in the open systems market that has now taken hold with all the major enterprise software vendors (Symantec, IBM, EMC). Server consolidation using virtual infrastructure is the underpinning of the 3rd Platform of computing, both enabling and defining the way computing is done today and will be done in the future. As flash continues to permeate the enterprise, it will fuel widely available storage arrays that will deliver millions of IOPS and drive a new trend in primary storage consolidation as organizations retire legacy storage arrays. Consolidation results in a better-managed, lower-risk business environment.

Collaboration in virtual workgroups that span employees and nonemployees as well as different geographies is the new way to work, and expanding the definition of the unified data management platform to include FSS makes perfect sense. This is another example of consolidation that improves overall datacenter efficiency and is a step toward the convergence of the backup and FSS markets. As IT evolves to become a much more agile provider of needed services, end users will have less need to create shadow IT operations. It is difficult to imagine that pure-play FSS providers will be able to enhance their products rapidly enough to fully meet the scalability, security, manageability, compliance, and protection requirements of business users before the major data protection vendors follow CommVault's lead and integrate an FSS capability into their platforms.

CHALLENGES/OPPORTUNITIES

Agility and ease of use have been the two driving forces behind the development of shadow IT to date. Integrating FSS, a service that has been a big driver of shadow IT, into its unified data management platform is a sensible move by CommVault. The service, however, must meet the requirements of end users in terms of ease of use and ability to share content with nonemployees for it to reduce the risks currently associated with virtual workgroups and endpoint data sharing. Otherwise, it will be just another IT offering that end users bypass because it is too hard to use.

Recent IDC research indicates that most end users (81%) adopt Internet-based FSS services without any training. The challenge of using these services is not in learning how to share content with collaborators but in learning how to *securely* share content, manage access appropriately, and protect the data cost effectively. Training end users in these procedures is one challenge that may stand in the way of broad adoption of what is an excellent consolidation strategy on CommVault's part. Just-in-time training strategies that make short tutorials (two to four minutes) about critical tasks (e.g., setting and managing permissions) available on demand online may be one way to make a more professional approach to file sharing easy. Providing transparent data protection, a feature already included in CommVault Edge software, is another example of how the needs of both IT and end users can be easily met.

As critical corporate data continues to be created, shared, and edited on laptops and mobile devices, end users need to be aware of the risks. CommVault is already seen as a leader in unified data management and has a good opportunity to take the lead around an expanded definition of that concept that will ultimately make things easier for end users while meeting IT requirements for scalability, security, recoverability, and compliance.

CONCLUSION

With the rise of mobile computing, more and more sensitive corporate data exists at the edge. New collaboration strategies based around virtual workgroups are making this data more accessible than ever, increasing worker productivity but also increasing risk to corporate information assets. It is incumbent upon IT to find ways to adequately safeguard all sensitive corporate data, and it is clear that this now includes endpoint data. Endpoint data protection must move from an ad hoc approach to a professionally managed discipline that takes into account strategic considerations such as comprehensive coverage, recoverability in line with corporate RPOs/RTOs, compliance and regulatory requirements, and eDiscovery.

By integrating FSS services into an already strong unified data management solution, CommVault has potentially found a way to serve end users with a scalable, easy-to-use collaboration platform while addressing IT requirements for security, recoverability, and compliance. Interestingly, Internet-based FSS vendors are trying to extend their platforms to provide many of the features that have already proven themselves in enterprise use across thousands of customers with Simpana. As the consolidation trend continues to permeate the datacenter, CommVault's support of a truly enterprise-class FSS service makes the company's business case that much stronger. And it may well extend how all unified data management vendors define their platforms in the future.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com

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.