druva

White Paper

How a Modern Approach to Online Backup Can Address CIO Challenges

CIO

Strategic Marketing Services

Within IT organizations, online backup of endpoints is moving up the value chain to address top CIO concerns.

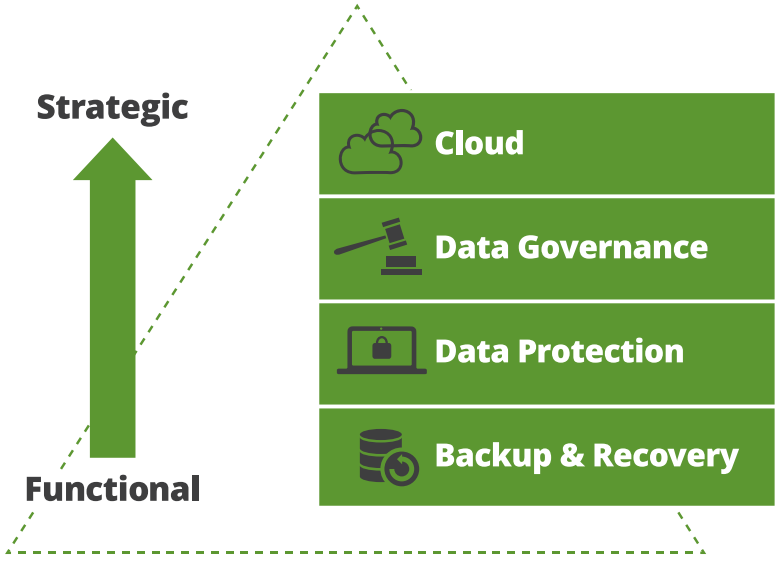
Historically, large swathes of IT have been seen as cost centers, below the radar of a CIO. Nothing represents this better than laptop and mobile device backup as an IT function. Viewed as a kind of insurance policy for avoiding end-user data loss, online backup of endpoints is usually managed by front-line IT staff and focused narrowly on data recovery and data loss prevention (DLP). However, with today's broader workforce and mobility trends, endpoint backup is moving out of the shadows and becoming a more strategic initiative to help IT leaders manage the explosion of data protection, privacy, and compliance needs.

For IT leaders looking to increase overall agility and ROI, online backup software is offering more than just efficient backup and restore of data on laptops and mobile devices. Backing up data on corporate endpoints can be a first strategic step toward a more nimble approach to disaster recovery and archiving. In addition, with the right leadership, online endpoint backup can address CIO-level challenges like data governance and eDiscovery, and the overall shift to managing critical business workflows in the cloud.

At the same time, information security is rising to the top of the list of CIO concerns. According to a survey of 112 CIOs by brokerage firm Piper Jaffray, 75% of respondents expect to increase security spending this year, up from 59% last year.[1] What used to be an easy-to-control environment, with all data stored behind the corporate firewall, is no longer. Shadow IT, mobile computing, consumer IT, and cloud computing are among the top trends transforming enterprise IT today. Workers using unsecured networks and devices without encryption are also a concern, as data breaches cost millions in fines, data loss, investigations, and customer backlash. While most CIOs agree that working against the business by instituting a traditional command-and-control environment is no longer viable, they've also realized that new governance models are necessary to manage risk.

Traditionally a concern only among IT leaders in highly regulated industries like healthcare and pharmaceuticals, the need for greater data governance is on the rise among IT professionals. In a recent survey of IT and legal professionals by Forrester Research, 53% of participants expect to have a centralized model for information governance within two years, up from 25% who have one now.[2] The top priority for companies is compliance with laws and regulations pertaining to end-user devices and data, say 87% of respondents. Technology is viewed as a viable approach to enforcing and executing data governance, according to 84% of organizations. Online endpoint backup solves for managing the threats of company data residing outside the data center, fragmented across myriad devices and locations.

Endpoint Data Protection Moves Up The IT Value Chain



1. *Wall Street Journal/CIO Journal*, "Piper Jaffray: Security Again the Top CIO Spending Priority"
2. Forrester Consulting and Druva, *Governance Takes a Central Role as Enterprises Shift to Mobile*

Getting More from One Solution

With a modern backup solution, companies not only achieve data loss prevention, but disaster recovery and more intelligent storage of data over time for archiving. On the disaster recovery front, that means instant access to backup data at any time, since the backups are continuous — updated every few minutes. When endpoint devices fail or are misplaced, IT can deliver real-time recovery and access to data for employees from another machine. As well, intelligent archiving helps improve visibility and data navigation for legal and regulatory compliance needs. In the past, decentralized and disconnected backup systems meant that significant gaps could exist for data that resided on mobile devices in far-flung locations.

Data governance initiatives require an environment that supports streamlined audits and rapid access to data for eDiscovery needs, a growing pressure on CIOs and other executives. According to Forrester's Forrsights Security Survey of Q2 2013, nearly half of organizations (46%) said that eDiscovery was a critical priority over the next year — up sharply from 20% in 2012. Modern online endpoint backup systems can integrate with eDiscovery tools to streamline the search and consolidation for data in response to pending litigation or investigation. Just as critically, changing privacy requirements across industries and world regions requires a granular, flexible approach to storing and backing up data. Finally, moving backup systems to the cloud helps control costs to support this more strategic and broad-based initiative for backups and archives.

The Necessity of Complying with Data Regulations

With regulatory compliance, companies in industries such as insurance, financial services, and healthcare must abide by specific laws on how data is used, stored, and handled. For instance, in healthcare, HIPAA requires specific protections of personally identifiable health data to protect patient privacy. Noncompliance can result in multimillion dollar fines, not to mention the loss of customer and shareholder confidence. All industries should protect against data breaches, even though there are no U.S. laws yet governing this. Organizations need a proactive understanding of where corporate data is at all times and confidence that data is not in the hands of unauthorized users. Here are a few ways that unified endpoint backup solutions can help IT organizations manage corporate compliance:

- **Auditing, monitoring, and tracking:** Modern endpoint backup solutions can supply visibility through centralized management and also deliver complete audit trails and tools such as federated search. Organizations can classify data for monitoring and data access permissions based on location, device, or user. IT can also receive alerts when an important document — such as an earnings release — is on an employee's laptop instead of on an encrypted server.
- **Compliance:** Always knowing where data is stored across the user base is critical for complying with regulations such as HIPAA, SOX, and CCAR, and for managing long-term archives.
- **Governance:** Today's enterprise data governance requirements can be a burden for IT and business leaders. The ability to create policies, monitor activity, manage legal holds, and provide data access for eDiscovery, all without impacting productivity, is critical. Also critical: the ability to assess whether compliance guidelines are being met by allowing IT to monitor and analyze data usage.

- **Data-based protection:** Backup solutions should incorporate industrial-strength security, as firewalls and server-based security are no longer enough for protecting sensitive corporate and customer data. Optimally, the system should store data separately from metadata in small, independent blocks, scrambling the data and making it difficult to reassemble the file in case of a breach. The system should also automatically encrypt all data and store encryption keys in such a way that nobody — not even the service provider under court order — can provide access to the keys or the unencrypted data.

CIOs Need to Get Ready for eDiscovery

In the past few years, courts have responded quickly to the electronic age. All types of electronic data are now accepted as legal evidence, and automated eDiscovery methods have won the hearts and minds of lawyers needing to cut costs on research. Yet supporting the eDiscovery practice is still stressful in most organizations, as IT scrambles to locate the requested data and collect it from various sites and machines. In fact, only 51% of companies are confident they can preserve data on mobile devices for eDiscovery, according to research conducted by Deloitte.[3]

Deploying a centralized endpoint backup system can improve eDiscovery processes on a number of fronts:

- Companies can search their backup systems, whether on-premise or in the cloud, to quickly find required data based on keywords such as employee name or product name.
- With centralized, continuous data protection, there's no risk of the data being lost, never discovered, or not preserved.
- The technology tracks administrator access, providing proof that the data has not been altered prior to release.
- Such systems can create a link to send data directly from the backup repository to the eDiscovery platform, saving time.
- Companies surveyed by Forrester were able to decrease time and effort spent on data collection. The composite organization saved $213,073 worth of manpower over three years by using a centralized endpoint backup system to support eDiscovery.

This was the case with Shire Pharmaceuticals, which used Druva inSync to connect its legal teams to endpoint backup data. Shire cut out additional data archival, recovery, and support services. "We recovered our software investment in just nine months," said a Shire representative. "There were real savings of money, cost, and time. We have reduced and rechanneled IT resources to do more productive work. This is a compelling value proposition."

Data Privacy is Becoming an IT Imperative

Protecting personal data has come to the forefront of IT priorities; the relentless pace of large-scale attacks on global companies hasn't abated. Companies are reevaluating security systems and deploying additional layers of protection across networks and at the data layer. CIOs and CTOs should work closely with software and infrastructure vendors to understand their level of protection — and backup systems are no exception here.

Modern endpoint backup systems should include industry-standard, data-level encryption, but also granular control over how stored data is handled. This requirement becomes critical for global companies, given the vast differences in privacy laws from country to country. Centralized backup systems should allow companies to segregate data within country borders to comply with regulations, and to apply country-specific policies, such as whether IT administrators can access personal data and how. By giving companies full control over privacy policy management, CIOs can help ensure trust with the business that IT is doing the right thing by its customers.

3. Druva blog, "40 Scary Stats About Endpoint Data at Risk"

Cloud Backup: More Workloads to the Cloud = More Agility, Savings, Innovation

Cloud computing has become a powerful driver of both innovation and increasing efficiencies in companies. Businesses are expecting IT leadership to use the cloud to help drive sales, build better relationships with customers, and support internal productivity and collaboration. By including endpoint backup in the cloud strategy, companies can move data and applications to the cloud securely and within the broader IT governance framework. Doing so allows IT to leapfrog legacy solutions that are not architected to meet the backup and archiving needs of today's enterprise. As data moves out of legacy platforms beyond the firewall, it still needs to be protected, and new cloud-based endpoint backup solutions enable this data protection across devices and networks.

An online backup solution gives companies flexibility to scale storage resources up and down as needed, and without having to assign IT staff to manage servers or incurring additional costs to store and protect an ever-growing volume of backup data within internal data center facilities. For companies that are already migrating operations systems to the cloud, adding backup systems to the cloud strategy eliminates data silos at branch offices and other remote sites and simplifies infrastructure management.

Online endpoint backup offers a way for companies to overcome doubts about and cross the hurdle to cloud, reaping the rewards of:

- Cost savings
- Better security (yes, better than legacy architecture)
- SaaS adoption for CAPEX and agility

Cloud backup systems are a sound strategy for maintaining companywide business continuity. Consider a customer service center that is knocked out for 24 hours due to a major storm. With endpoint backup in the cloud, employees can access all files and data from a computer, tablet, or smartphone while working from home or a temporary location. They can do their jobs as if no disaster had happened — and customers notice that kind of world-class service.

Generally speaking, the always-on benefit of a modern, cloud-based backup platform is what employees expect today. There's no saving of data to a Web storage app or performing manual syncs to ensure that someone can access a file when they're away from the office. A user's files are always there, always the latest version, and quickly shareable with colleagues without involving email attachments or other potentially unsafe file-sharing methods. Major cloud providers continue to drive innovation with enterprise-class technologies such as autoscaling, hybrid cloud, data-level encryption, multifactor authentication, redundant storage, and elastic load balancing.

Those features are making it viable for large companies to consider the cloud for storing even their most sensitive data assets. Building performance into the cloud is also important for the business, in terms of fast and reliable data access. Those characteristics pay off quickly in the event of an outage, audit, or eDiscovery requirement.

Finally, CIOs can emphasize the financial benefits of moving to the cloud with C-level colleagues. By reducing on-premise infrastructure purchases (CAPEX) and moving to on-demand subscription fees, companies can free up precious capital for high-priority business initiatives and get more bang for their buck in the long term through the efficiencies of the cloud. With this approach, CIOs can move the conversation of cloud-based systems beyond the financial discussion to the bigger picture: time-to-market.

IT departments are evolving from infrastructure providers to agile business technology partners responsible for developing innovative operational and customer-basic services. Cloud-based endpoint backup is a winning strategy to help companies move workloads to SaaS and modernize IT for better ROI, security, and the next generation of enterprise data governance and intelligence.

Link to druva.com to know more.

About Druva

Druva is the leader in converged data protection, bringing data-center class availability and governance to the mobile workforce. With a single dashboard for backup, availability and governance, Druva's award-winning solutions minimize network impact and are transparent to users. As the industry's fastest growing data protection provider, Druva is trusted by over 3,000 global organizations on over 3 million devices. Learn more at www.druva.com and join the conversation at twitter.com/druvainc.

Druva, Inc.
Americas: +1 888-248-4976
Europe: +44(0)20.3750.9440
APJ: +919886120215
sales@druva.com
www.druva.com