IDC
Analyze the Future

IDC TECHNOLOGY SPOTLIGHT

Control Business Data Risks through End User Data Protection and Governance

February 2017

Adapted from *Increasingly Complex Regulatory Environment Brings Challenges to Business Leaders Trying to Manage Corporate Policies and Procedures* by Angela Gelnaw and Sean Pike, IDC #US41081916

Sponsored by Druva

Workforce mobility — and the data dispersion it engenders — has created the perfect storm for IT in regard to the management, security, and governance of enterprise data. IT departments are working in a new reality with the same old tools of the past. New solutions are required to help those trying to tame the data management chaos created by the evolution of the digital enterprise. This Technology Spotlight examines the need for increased visibility and control to better manage and mitigate the risk presented by a decentralized corporate data environment. This paper also discusses how Druva is helping solve these challenges with its inSync product offering.

Introduction: Market Overview and Trends

Between the consumerization of technology and the globalization of business, IT leaders are dealing with some major obstacles in the realm of data management. However, the dispersion of data — which can now be stored across millions of endpoints and cloud applications — is causing heightened concern within the enterprise. The decentralized nature of the modern enterprise is great for increased productivity among the workforce, but it has created a nightmare for business executives in terms of security and risk.

The rise of the mobile workforce, the greater acceptance of bring your own device (BYOD), and the increased adoption of nontraditional communication channels and cloud collaboration platforms have created an IT environment with limited visibility into and control over the data being created and stored across the enterprise. Such a decentralized data environment is already a pretty big management challenge. To make matters worse, regulations are on the rise in almost every geography, with increasing punishments for noncompliance. When one considers that ransomware is on the rise and thrives in chaotic conditions, the potential consequences of poor data management and governance strategies are clear.

Any organization operating in today's world with data blinders on is at high risk of experiencing any or all of the following:

- **Loss of business-critical information.** Ransomware is part of the new reality in which all businesses operate now. The question regarding a data breach is no longer "if" but "when." The result of such a breach may have a direct impact on an enterprise or an indirect impact via the breach of a supplier or trusted third party (i.e., Heartbleed). Data loss is not solely the result of security breaches. More often than not it is the result of accidental deletion or simply the inability to recover information from a laptop, mobile device, or cloud application. Organizations should design their information governance programs with data loss protection strategies in mind.

- **Penalties from noncompliance.** Business continues to be transacted on an increasingly global scale. However, the laws and regulations that govern different geographies, industries, and even certain departments vary in nature and are evolving at a much faster pace than at any other time in history. The rapid pace of change results in extremely difficult circumstances for creating and maintaining data policies from office to office on an ongoing basis. Of particular note, the General Data Protection Regulation (GDPR) is causing concern, as penalties for noncompliance with this law have been set extraordinarily high (penalties as high as 4% of total annual revenue for those out of compliance).

- **Costly corporate investigations.** Internal investigations are still largely performed on a manual basis. Without a centralized, auditable, and secure location available for search, discovery, and retrieval of information, corporate investigations can become extremely complex and costly as well as time consuming.

- **Ballooning storage-related costs.** The modern enterprise is responsible for more than half of all the data created around the world — a contribution of more than 2.3 zettabytes of information every year. This data explosion places a significant burden on enterprise IT teams and budgets. While storage costs have diminished significantly, the savings are offset by the sheer volume of data that has to be retained. Without a strong program for data retention and deletion, the costs related to maintaining the infrastructure of such a large data environment can quickly become unwieldy.

- **Data risk.** The opaque nature of this type of decentralized storage environment can lead to the buildup of "dark data." Because of the volume and dispersion of enterprise data, it is retained over time and never purged. As such, it is nearly impossible to exert the necessary policies for effective data retention and disposition. This poses a big risk to organizations from a governance and compliance perspective.

These conditions have caused a monumental shift in the way that data is created, stored, and used. As such, new methodologies and tools are required to adapt data governance and security strategies in this new reality.

Benefits

The markets for enterprise data management, data protection, and data governance solutions are large and fragmented — further complicating the situation for IT executives. However, these markets are beginning to converge, and there is significant value to be had by finding the right combination of solutions. Vendors that can incorporate these capabilities, as well as unlock access to specific data traits, into a truly holistic solution for unified information management will have a real market opportunity to capture share away from both emerging and legacy competitors.

Benefits that can be gleaned from a unified information management solution are fourfold, providing value to the enterprise IT team and the general corporate employee as well as the legal, risk, and compliance teams.

- **Increased visibility and control.** A unified information management platform provides centralized access to all endpoint and cloud application data. This feature allows IT administrators to easily apply role-based privacy and security rules for greater governance control and better protection against data loss. Search and discovery can easily take place within one platform for visibility across all enterprise data — helping inform data retention policies and understand the organization's state of compliance at any given time. Of course, one repository means there is no need for duplicate copies of files, thus minimizing storage bandwidth and costs.

- **Set it and forget it.** Gone are the days of weekly or monthly laptop backups for line-of-business employees. Employees no longer need to stop working in order to back up their files, nor do they need to worry about storing (or misplacing) those files. With a cloud-based platform, employees can be confident that their work is safely and securely backed up and available to them whenever they need it — even in the event of a breach. The benefits to the end user are realized through greater productivity and less risk of data loss.
- **Peace of mind for legal, risk, and compliance.** The ability to access all enterprise data from a single, secure, and compliant data repository enables defensible collection, preservation, and discovery of information for corporate investigations and litigation.
- **Confidence in the security and privacy of enterprise data.** Vendor partnerships that leverage public cloud service providers (such as AWS and Azure) as part of their technology offering enhance the value proposition to customers through greater data residency, security, and privacy on a global scale.

Considering Druva

Druva's inSync offering helps enterprise IT leaders simplify some of the complexity related to managing information dispersed across an organization's communication and collaboration platforms and devices. inSync is a cloud-native software platform for unified data protection and proactive governance.

The product enables users to view and access all endpoint and cloud application data through a single pane of glass. Druva's inSync helps facilitate the enforcement of security and compliance policies across the organization as well as enable litigation readiness and corporate ediscovery.

The company's partnerships with public cloud service providers AWS and Azure enable inSync to harness the native efficiencies and global reach of the cloud, including storage flexibility, data durability, and security. With more than 30 datacenters around the world, Druva is able to offer on-demand scale to meet any global organization's specific needs around data privacy, data security, and data residency compliance and storage requirements. inSync can deliver the following additional benefits:

- Complete view of enterprise data across endpoints and cloud applications from a single platform for greater data accessibility and discoverability (Druva integrates with leading enterprise productivity suites including Microsoft Office 365, G Suite [Google Enterprise Suite], and Box.)
- High-performance backup and recovery with global deduplication and bandwidth throttling/WAN optimization
- Minimal downtime during necessary business processes such as data restoration or data migrations
- Advanced customer controlled encryption and data sharding techniques that provide robust security, compliance, and data privacy protections (Druva's unique approach to storing enterprise data guarantees that Druva has zero access to customer data — a critical component of meeting today's stringent global data privacy regulations.)
- Automatic identification of potential data risks using industry-verified regulatory compliance templates
- Federated full-text search for fast, deep text search and identification of information across all endpoints and cloud applications, thus allowing faster response to legal and compliance information requests
- Forensic data collection with chain of custody reporting, extended metadata, and file fingerprinting to ensure authenticity and alignment with EDRM and Department of Justice requirements

- Corporate litigation readiness with the ability to automate legal holds for in-place preservation, set data retention policies, and view audit trails
- Integration with leading ediscovery software platforms so that data can be easily ingested for ediscovery

With the inSync offering, Druva is addressing some of the enterprise's biggest pain points related to information governance. These pain points include visibility and control, search and audit, compliance management, and ediscovery and litigation readiness.

Challenges

Data security, compliance, and discovery solutions, while related, each offer unique value in regard to managing data to meet enterprise security and compliance mandates. As such, each of these markets is at a slightly different place in its maturity life cycle. Many data compliance and governance solutions are relatively new to the market, but discovery applications are becoming fairly mature. However, all three areas are converging and evolving into "features" rather than individual "markets." As this trend takes hold, the competitive landscape will also adapt.

As such, the market in which Druva competes is highly fragmented and crowded — causing vendors in these adjacent markets to build out features with the goal of capturing additional revenue. Many discovery vendors have added archiving, data protection, and investigation tools. Likewise, archive vendors have added discovery and compliance capabilities to their offerings. The overlap in these features is creating even greater competition for vendors in all of these markets.

As a result of this adjacent market creep, the discovery software market has seen high levels of consolidation over the past couple of years. This could benefit Druva by opening up more opportunity in this market. However, the consolidation is causing major shifts and could potentially impact some of Druva's integration partners. It will be critical that Druva continue to keep an eye on the market and evolve its partnering strategy as these changes take place. Additionally, Druva should continue to provide open integration options that are platform agnostic in order to minimize the impact of any event that might negatively affect the company as a result of its existing partnerships.

Conclusion

The proliferation of endpoints and the increased adoption of both approved and shadow cloud applications have contributed to that fact that over half of all enterprise data no longer resides behind the corporate firewall. Enterprise information is now dispersed, sitting across numerous platforms and creating issues around visibility, security, and control. Given this trend as well as the rise in ransomware and the quickly evolving regulatory environment, business leaders are right to be concerned about the potential loss of business-critical information and the possibility of reputational damage.

IDC believes that corporate IT leaders will continue to struggle with the complexity of managing and protecting critical enterprise data assets. Solutions that simplify this process for IT administrators, provide greater confidence for compliance managers, and have minimal to no impact on employee productivity will continue to have significant growth opportunities. To the extent that Druva can address the challenges described in this paper, the company has a significant opportunity for success in the market for unified data governance and protection solutions.