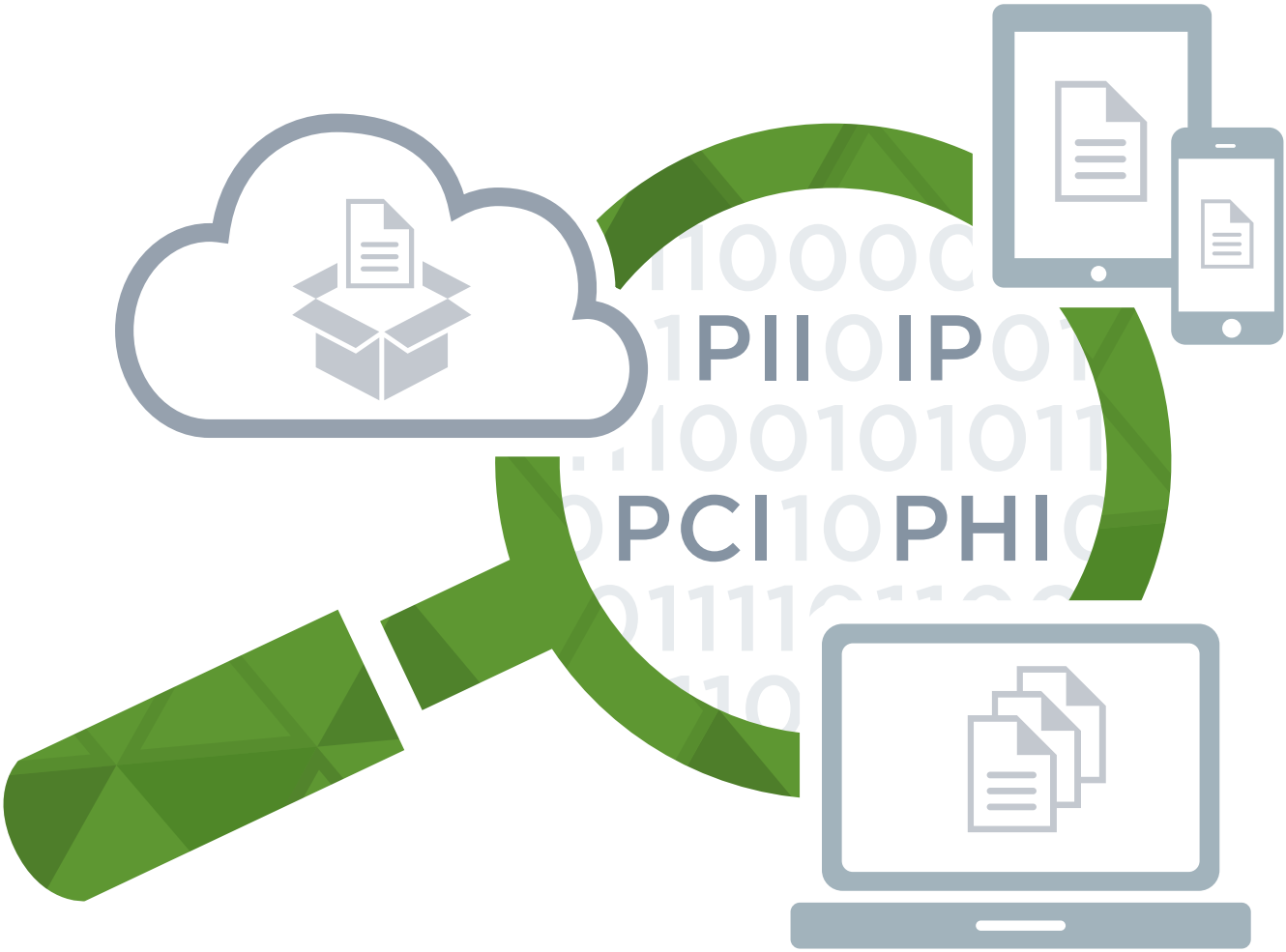
druva

Executive Brief

Addressing User Data Risks In A Distributed Data World



This paper is for IT and security executives addressing increasingly complex issues related to data compliance, privacy and security policies and regulations in large organizations with mobile workforces.

Background

With the significant increase of data sprawl brought on by the mobile workforce and cloud services (Office365, Box, Google apps, Salesforce, Dropbox, and so on), enforcing data governance policies has become increasingly more complicated. Certainly, mobile and cloud support has added to the business burden with the need for locating, tracking, monitoring, securing, and properly preserving sensitive data. In fact, Gartner reports that 75% of cloud security, compliance and risk resources will be spent on managing these services. IT and security executives agree that working against these business needs and instituting a traditional command-and-control environment is no longer viable. They have also realized that new governance models are necessary to manage this risk.

Requirements for Governance in Distributed Environments

At its most basic, *governance* is about applying policies related to service use. Every business has to define the organizing principles and rules that determine how it (and its employees or representatives) should behave. Some of these policies are internally-generated, but many of them are mandated by outside agencies: government regulations, court rulings, and industry standards.

And, as with all business rules, the IT department instantiates the policies in computing terms by building them into the company's computing functions (whether in-house or in the cloud) as well as including those policies data and human workflow. Thus, data governance includes the techniques and policies that measure and control how systems are managed. It ensures that IT assets are implemented according to agreed-upon policies and procedures, makes sure they're properly controlled and maintained, and ideally does its best to affirm that the assets provide value to the organization by supporting the organization's business goals.

Data governance has become integral to the modern enterprise. To successfully gain competitive advantage, businesses need to manage the complex technology that is pervasive throughout the organization, in order to respond quickly and safely to business needs.

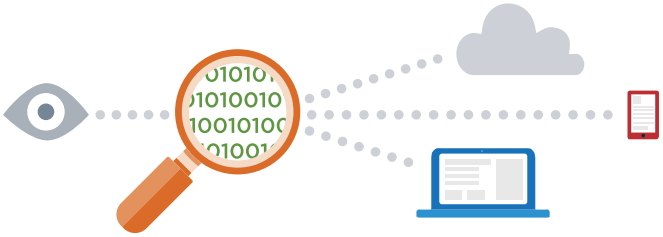
But safely has gotten a bit harder, in the past few years. Today, data is "everywhere and anywhere," across devices and cloud services, and Gartner predicts that by 2020 over 50% of all corporate data will reside outside the data center. This means that IT and security teams need to work harder—or at least differently—to ensure data security, compliance with regulations, and business continuity.

Each of those challenges are made more urgent as information spreads. For example, the complexity of data privacy regulations adds a new burden to IT staff who have to figure out obfuscated legal language and to respond to the complicated and sometimes-contradictory rulings. For example, the newly introduced General Data Protection Regulation (GDPR) in the E.U. provides guidelines for protecting citizen data and very stiff fines in the case of breach, which impacts any organization doing business with the E.U. With many new privacy regulations like GDPR, it's less apparent as to what specific controls IT must implement to align properly. As well, new content types will increasingly need to be collected for legal and compliance purposes – up to 90% of organizations will preserve messaging data by 2020 – putting further burden on organizations to understand what data they have and where it resides and implement controls to ensure alignment with policies.

Given the rising need for a holistic approach to data governance, what are some of the considerations unique to distributed environments? Among them:

- Access and visibility to data everywhere it is, across cloud services and mobile devices, which may be anywhere in the world
- Corporate and IT's ability to respond to compliance inquiries, internal investigation, and other legal department requests
- Addressing regional data handling and privacy regulations
- Identifying and taking action on identified data risks
- Rock-solid security

...as just a start.



A New Approach to Data Governance

The management and protection of corporate data can be seen with a somewhat wider lens by extending the notion of "command and control" to where end-user data resides. The goal is a better one than forcing data centralization and controls (which hamper end-user productivity and creates more side-stepping of policy by end-users).

With this approach, businesses need to:

- Centralize organizational visibility into business data dispersed across laptops, desktops, mobile devices, and cloud application services (such as Microsoft Office 365, Google Docs, or Box).
- Manage data governance over end-user data for compliance auditing, investigation and eDiscovery needs.
- Automate compliance monitoring for proactive identification of potential data risks across disparate data sources, devices, and users.

Druva inSync addresses this need by bringing together the core business requirement of data protection and availability with rich data governance capabilities. Doing so restores visibility and control to dispersed data, without impacting end-user productivity. In other words: End-users won't have any additional reasons to resent IT. They'll have fewer reasons to grouse, in fact, because their jobs will be easier (and so will IT's).

Druva's core technology efficiently and transparently collects data and audits information off of devices and cloud services. It provides a unified view of dispersed data for legal, compliance, information security, and IT teams to achieve their goals in both governance and end-user data recovery.

With Druva inSync, enterprises achieve:

- **End user data federation:** Druva inSync aggregates user data across devices and services to provide a single composite view of information. This enables organizations to identify files on devices by user as well as to access audit trails for understanding data activities and patterns.
- **Minimize data loss:** By efficiently collecting and storing time-indexed end-user data, Druva ensures that the data can be immediately recovered by end-users or IT if data is accidentally deleted, a device is lost, or a system failure occurs. We minimize the moments where users or IT have to say, "Oh no!" (and then lose another weekend in the attempt to retrieve information).
- **Security and privacy support:** Druva's extensive security and privacy controls address data on mobile devices (remote wipe, enforced encryption, geo-location of device). These features also provide controls for segmenting access and storing data regionally in order to meet local data regulations.

- **Unified policy management:** Centralize data source policy management and enforcement without end user involvement. Administrators can access, understand, and manage user data while ensuring business continuity with self-restore, data access and secure file sharing. Druva's approach streamlines data administration and assessment.

Facilitating Data Governance for Legal and Compliance Requirements

By extending the capabilities of what can be accomplished with data protection tools, businesses can achieve greater data governance, particularly in the area of supporting legal needs and compliance. Doing so enables control of data for legal requests; it also provides auditable and verifiable system logs on administrative and end-user data interactions to meet compliance inquiries.

Druva isn't just bolting on this functionality as an afterthought. It's a consequence of inSync's architectural design. The core technology that enables us to extend data protection features into governance, compliance, and legal requirements is the result of Druva's zero-latency, time-indexed file system model. As the software is implemented, information that is collected from devices is instantly retrievable and referable across any collection point stored in the system. For example, a company can instantly jump back to the state of its data (in the small or large sense) from six months back. In addition to storing retention policies, to meet various data regulations and legal requirements, Druva inSync also permits terminating employee data to be held as long as necessary (as part of a system legal hold, or necessary for archiving purposes).

Elements of data governance capabilities include:

- **Legal hold management:** End-user data increasingly is becoming the subject of legal inquiries for investigations or litigation purposes. IT and InfoSec teams can work in partnership to provide legal teams access to manage legal holds on aggregated end-user (custodian) data that is held in-place for the period of the legal matter.
- **Detailed auditing:** The system keeps full audit trails of user data and administrator actions. It integrates logging information from cloud-based services to provide a composite of user data interactions.
- **Federated search:** Organizations can search across multiple meta-data fields and parameters to identify information across the content base. This helps organizations identify potential risks when facilitating investigation or compliance requests.
- **eDiscovery connectivity:** For data placed on legal hold, Druva inSync provides secure, direct connectivity with third-party eDiscovery platforms to ingest the data without having to move the data to an intermediary server first. This reduces the risk of data spoliation.

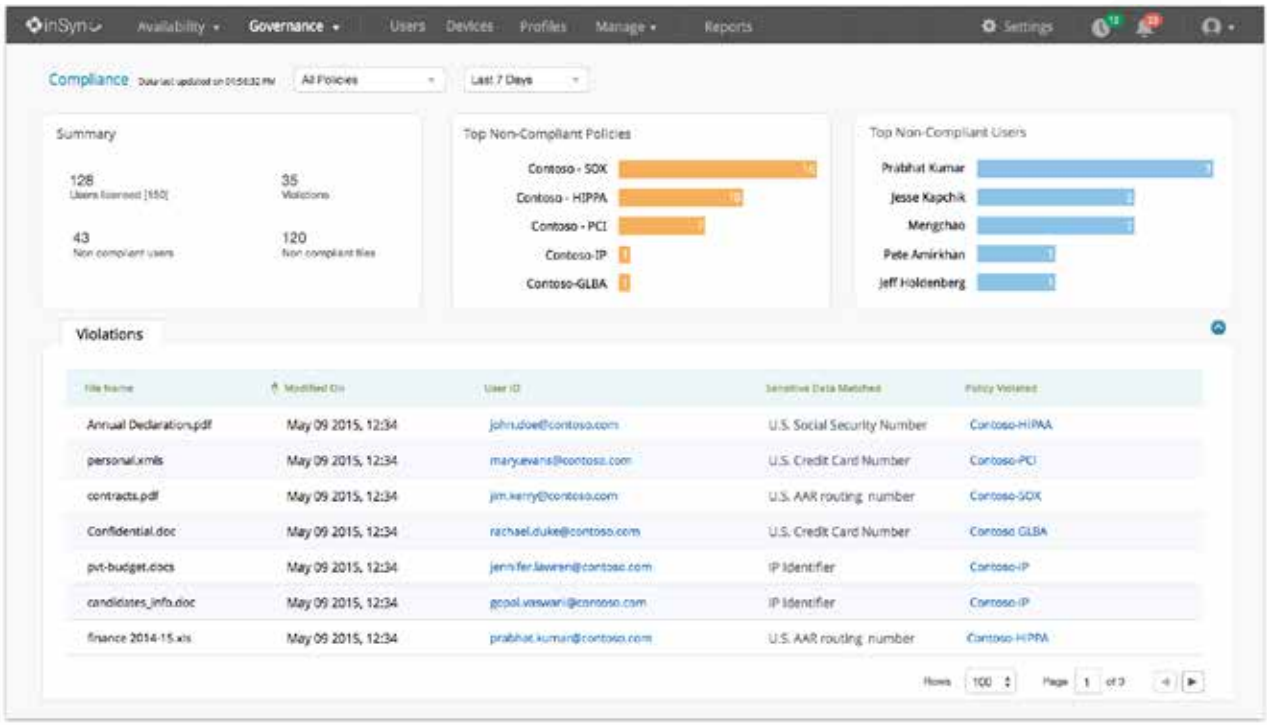
Proactive Compliance: Automated Data Monitoring

Many enterprises address data governance in a reactive manner, after legal or compliance teams inquire after an "uh-oh" event or some other data loss incident occurs. To address these challenges, Druva solves this problem with *proactive compliance,* enabling organizations to avoid data risks by gaining insights into the information flowing around end-user devices and cloud services.

Traditional data loss prevention (DLP) technologies monitor in-transit streams. Instead, proactive compliance assesses data at-rest, where it resides on devices or services. Most of today's data risks are less in-flight than on-device or -service.

With proactive compliance, organizations benefit from deeper analysis and notification capabilities, including:

- **Full-text data indexing:** Organizations can look deeper into their data, beyond meta-data, and dive into the business's investigative needs. You can identify files that contain intellectual property (IP), personal health information (PHI), personally-identifiable information (PII), or other data buried within unstructured data sources that you don't want escaping into the wild.



Druva Compliance Management Dashboard

- **Automated compliance monitoring:** The system, based on templates, can automatically scan aggregated data and alert the organization as necessary.
- **Predefined Compliance Templates:** Organizations' administrators can select from pre-configured templates for common regulatory definitions (such as HIPAA or GLBA) The system applies these business rules when scanning the federated data set, making automatic a once-arduous, time-consuming effort to build customized query expressions for standard regulatory policies.
- **Federated visibility of compliance risks:** Compliance, legal, and IT teams see a single dashboard displaying the potential data risks by service, by user, and by device. Administrators can drill-down levels of detail as necessary to better assess and remediate those risks.

Conclusion

IT and security leaders can address the growing challenges in data tracking and monitoring to meet regulatory and legal requirements on dispersed data with the extensive data governance capabilities of Druva inSync. Proactive compliance better equips enterprises to stay on top of their data, with awareness of where the data is located and how it's handled, while at the same time ensuring the integrity of that information for data availability needs.

About Druva

Druva is the leader in cloud data protection and information management, leveraging the public cloud to offer a single pane of glass to protect, preserve and discover information – dramatically increasing the availability and visibility of business critical information, while reducing the risk, cost and complexity of managing and protecting it.

Druva's award-winning solutions intelligently collect data, and unify backup, disaster recovery, archival and governance capabilities onto a single, optimized data set. As the industry's fastest growing data protection provider, Druva is trusted by over 4,000 global organizations and protects over 25 PB of data. Learn more at **www.druva.com** and join the conversation at **twitter.com/druvainc**.

Q217-CON-10606

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