Factsheet

Boost DLP/CASB/SASE Effectiveness with Precise Data Classification and Contextual Insights

Tackling Today's Data Security Challenges

In today's digital landscape, the emphasis on data governance, security, and compliance is greater than ever. As organizations handle increasing volumes of data—particularly **unstructured data**—the challenges surrounding data leakage, improper classification, and compliance failures also escalate. These risks become even more pronounced as sensitive data traverses multiple cloud environments and is accessed by various stakeholders.

While Data Loss Prevention tools (DLP) play a vital role in safeguarding data, there are areas where they may face limitations, especially when dealing with the complexities of modern enterprise data.

Data Visibility Limitations

Sensitive data often resides in SaaS applications like Salesforce, Zendesk, and Snowflake. Without adequate context and content visibility, DLP tools may struggle to create accurate data protection policies.

Adaptive Classification Needs

As data constantly updates across files and emails, the need for flexible, adaptive classification policies becomes critical. Traditional DLP tools may find it challenging to define policies that account for consent, sharing, and data residency requirements on an individual file or email basis.

Comprehensive Data Inventory

Achieving a single-pane view of enterprise data is essential for effective data protection. Relying solely on app logins and data movements, DLP tools may find it difficult to provide a holistic view, which is crucial for developing robust data protection strategies.

Managing Global Policies and Exceptions

Applying policies and managing exceptions at a granular level can be complex and error-prone. A more streamlined approach may be needed to reduce noise and ensure effective policy enforcement.

Inventory, Classify and Link Enterprise Data with Secuvy's DLP/CASB/SASE Connector

Revolutionary Data Classification

Discover, identify and categorize data across data sources and applications with Secuvy's cutting edge unsupervised AI. This sophisticated method illuminates the context, intent, and sensitivity lifecycle, thereby refining the scope and effectiveness of DLP/CASB policies for your customers.

Classify Dark Data

There's a significant risk that crucial data might slip through the cracks due to broad or insufficient classification systems. Such oversights can potentially lead to serious compliance and security challenges.

Adaptive DLP Policies per Data Context

Secuvy offers the capability to inventory and categorize your sensitive data based on various factors such as age, access privileges, relevance, data sprawl, and more. This allows you to craft dynamic DLP policies that adapt to your data's evolving landscape. Drastically reduce alert fatigue.

Comprehensive Data Inventory

Imagine having a single, unified view of all your data—whether it's structured, unstructured, or semi-structured. Secuvy enables you to establish global data policies at scale, seamlessly managing data across on-premises, SaaS applications, cloud resources, and hybrid infrastructures.

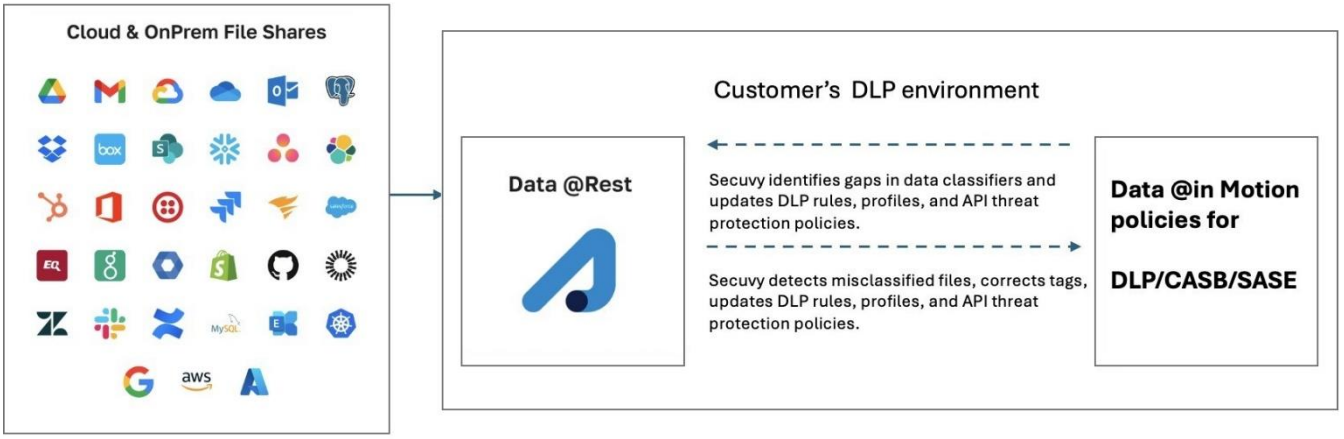
Seamless Metadata Updates Across Cloud Providers

Keeping up with data changes can be daunting. Secuvy simplifies this by automatically updating metadata in classification sources like MPIP, Box, Google, Dropbox, and other data cataloging platforms. This proactive approach prevents data leaks and oversharing, all while ensuring compliance with your policies.

How Secuvy Integrates with DLP/CASB/SASE tools

The collaboration between Secuvy and DLP/CASB/SASE is crafted for maximum efficiency and simplicity. Secuvy conducts a thorough analysis of data at rest, cataloging essential information and augmenting DLP/CASB/SASE detection capabilities by providing additional insights. This synergy ensures that DLP/CASB/SASE activity monitoring and data protection efforts are guided by the most precise and current data classifications available.

As a result, this integration greatly minimizes the need for manual intervention, enhances the accuracy of DLP alerts, and strengthens compliance with data security regulations



Key Advantages of the Secuvy DLP Integration

Reduce False Negatives

Elevate the effectiveness and return on investment of your DLP/CASB solutions by minimizing false negatives

Detect Misclassified Records

Improve accuracy by addressing misclassified data at rest and updating classifiers, which sharpens the precision of your DLP/CASB policies.

Mitigate Data Leak Risks

Reduce the chances of data leaks and exfiltration, particularly of sensitive personal and organizational information, by ensuring that classification labels and policies on files are accurate and not intentionally misconfigured.

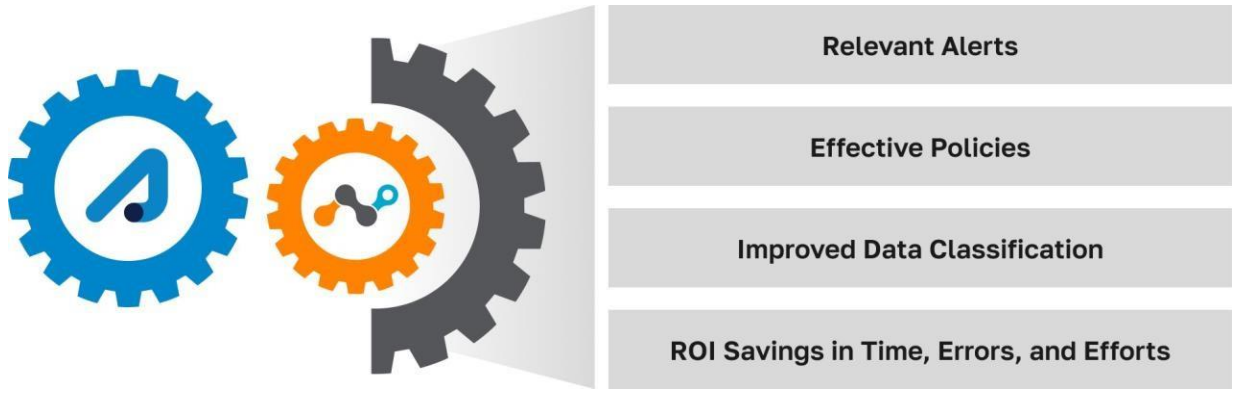
Align and Enrich Identifiers

Ensure that identifiers and DLP profiles are consistent and comprehensive between data at rest and in motion, particularly for operations that are unique to your industry and environment. Develop and refine DLP/CASB policies to accommodate custom data types and unique identifiers

Validate Permissions and Activity

Cross-reference user permissions for data at rest with their activity when data is in motion. This helps in identifying unauthorized data access and sharing violations

Secuvy and DLP integrated offering



Use Cases

Industries that are highly regulated and are technically specialized such as Life Sciences, Biotechnology, Pharmaceutical, Defense, IT & Engineering, Healthcare, and Finance demand completeness and precision in its ability to detect and identify data categories which are unique to its operations. Unexpected changes in the data environment can degrade the ability of rules-based DLP and CASB tools to effectively detect and enforce data security controls for data in motion.

- Enable an organization to keep up with changes in the data and ensure consistent enforcement of security policies between highly sensitive data at-rest in cloud storage and content collaboration platforms and when it is shared between users within and across the organization's domain.
  - Secuvy will detect and identify gaps in critical data classifiers and initiate the relevant remediation to update the DLP rules, DLP Profiles and API Threat protection policies.
- Ensure that DLP policies and API threat protection rules, which rely on a storage or content platform's sensitivity labels, are keeping up with changes in a file's classification
  - Secuvy has the ability to read the classification or sensitivity tags applied to file, detect for misclassification, initiate remediation actions to correctly reclassify the file and update the relevant DLP rules, DLP Profiles, and API threat protection policies.Applicable industries: Defense and Critical infrastructure, Pharma and bio-life sciences, Healthcare, Technology.

Strengthen Your DLP and CASB Integration Ready to take your data security to the next level?

Contact us today to schedule a demo.

Discover how Secuvy can enhance your DLP/CASB/SASE investment and safeguard your critical data.

About Secuvy

Secuvy makes data protection easy, efficient, and trusted with a next-generation privacy, data security, and AI data governance platform. The self-learning AI automates the inventory of any type of data, in any format, in any environment, at record speed and highest accuracy in the market. The era of AI governance is here.

secuvyai

39 California Ave, Pleasanton, CA 94566

secuvy.ai

Learn more about Secuvy

www.secuvy.ai

Schedule a demo