Optimizing DLP
with Bay Dynamics
Risk Fabric

Who should read this paper

Organizations seeking to accelerate, triage and mitigate
user-driven data security risks

WHITE PAPER

> **Bay Dynamics**®

Introduction

Today's Data Loss Prevention (DLP) platforms offer unparalleled capabilities for organizations to significantly harden information protection, empowering numerous stakeholders to ensure appropriate oversight of critical data assets.

At the same time, due to the unique requirements of every organization, DLP policies must be finely tuned to minimize false positives and adapted to suit business workflows with ever-changing security ramifications. To that end, practitioners increasingly require additional means of prioritizing DLP incidents to achieve effective incident remediation and threat investigation, while evolving policies to accommodate business specifications. Both business and security stakeholders also require up-to-date metrics and reports to measure the overall effectiveness of data protection.

These challenges have led many practitioners to adopt integrated behavioral analytics to optimize nearly every element of DLP strategy, enabling organizations to extend the value of their existing investments and provide even greater control over protected information.

Behavioral Analytics is Key to Optimizing DLP Programs

For over a decade, DLP systems have provided the backbone of information protection, allowing organizations to effectively catalogue and safeguard their most important data while employing highly diverse policies to monitor and control its handling. In recent years the continued explosion of cloud adoption and expansion of punitive compliance measures have driven even wider uptake of DLP.

At its core, DLP systems and policies help dictate the limits of acceptable data interaction and the occurrence of either improper or malicious activities, a hugely complex proposition given each organization's extremely nuanced business practices. Additionally, DLP platforms and policies have expanded to cover the myriad channels over which data is transmitted, including networks, endpoints, email, storage systems, Web gateways and the cloud.

The result of this increasingly strategic and distributed DLP ecosystem is a world where those practitioners responsible for managing policies and incident response find themselves faced with a sea of related intelligence. For many DLP teams the primary challenge has become translating the prodigious information generated by these systems to enable efficient response.

Driven by this goal, many practitioners have begun to enlist user and entity behavior analytics (UEBA) integrated directly with their DLP infrastructure to gain detailed visibility into their most pressing data

security matters. By delivering the detailed context necessary to understand which incidents represent emerging risks, how to remediate those issues, and where policies can be refined to account for accepted practices, these analytics greatly optimize DLP process.

The powerful combination of market-leading DLP solutions and the integrated analytics provided by Bay Dynamics Risk Fabric, offers the precise manner of DLP Optimization sought by today's experts.

How it Works: Defining DLP Optimization

DLP Optimization is a focused set of technical and process-driven capabilities that ensure organizations derive ideal results from their existing investments and available expertise. By leveraging analytics to prioritize DLP incidents, automate remediation processes, augment policies, and track metrics for business stakeholders, measurable improvements are realized.

Integrating behavioral analytics directly with the DLP platform allows for rapid isolation of truly abnormal incidents – such as individuals inappropriately seeking to access sensitive information or recently resigned employees attempting to copy protected data onto external systems. Importantly, numerous DLP policy violations that represent non-malicious activities can also be categorized quickly.

Backing this analytics-based approach are powerful unsupervised machine learning capabilities that enable in-depth and automated contextual analysis, along with supervised machine learning in the form of reinforcement training. Through processing huge volumes of DLP data to create behavioral baselines and continuously learn at the hands of human analysts, significant progress is made.

Prioritizing Investigation: Isolating Truly Risky Incidents

DLP analysts are faced with a daunting proposition each day; namely, identifying which incidents that have accrued overnight command their immediate attention, and then undertaking appropriate triage and remediation. Differentiating which issues represent problematic risks that must be investigated amongst a variety of incident logs, and deciding how to respond, may require hard-earned savvy; the larger the volume of incidents, the greater the challenge.

Leveraging DLP alert data alone, experts have traditionally labored to ensure that they focus on precisely those issues that matter most. One of the most persistent obstacles facing these analysts is how well internal stakeholders responsible for DLP policy creation have accurately accounted for accepted business practices. Policies that trigger large amounts of alerts that represent legitimate business workflows are a frequent and widespread challenge.

Applying behavioral analytics to DLP incident data creates the opportunity for new levels of precision in isolating specific data interactions that can be absolutely defined as problematic. Further, performing comparative analysis of DLP events against behaviors carried out by an individual's peers, such as workers with the same role reporting to the same manager, allows for ranking of DLP-centric risks based on correlation of the involved incidents.

Another distinct capability of applying UEBA analytics for DLP Optimization is leveraging supervised machine learning to learn from human analysts' actions over time related to investigation, triage and remediation response. If certain types of events are consistently escalated for hands-on review or assigned lower risk ratings, this insight can be used to automatically trigger future prioritization.

Adapting Policies: Tuning Parameters to Improve Effectiveness

One of the most challenging aspects of actively managing or deploying DLP relates to the accuracy and timeliness with which policies can be created. Changing data security requirements also dictate continuous refinement and tuning, heightening the importance of policy review workflows.

Leveraging integrated analytics to accelerate feedback loops for policy improvement significantly increases precision, driving massive savings of time and related resources. For instance, by utilizing analytics to determine which policies are triggering large amounts of DLP alerts based on legitimate business processes, such as internal stakeholders allowed to transmit sensitive customer data outside the organization, those policies can be adapted to reduce future alerts.

Moreover, adopting DLP Optimization techniques to aid in policy management allows technical experts including analysts and operational security teams to connect directly with business stakeholders. By creating end-to-end workflows that allow individuals responsible for oversight of sensitive data, such as R&D staff, to partner and communicate with DLP administrators and responders, the policy management lifecycle can be shortened significantly.
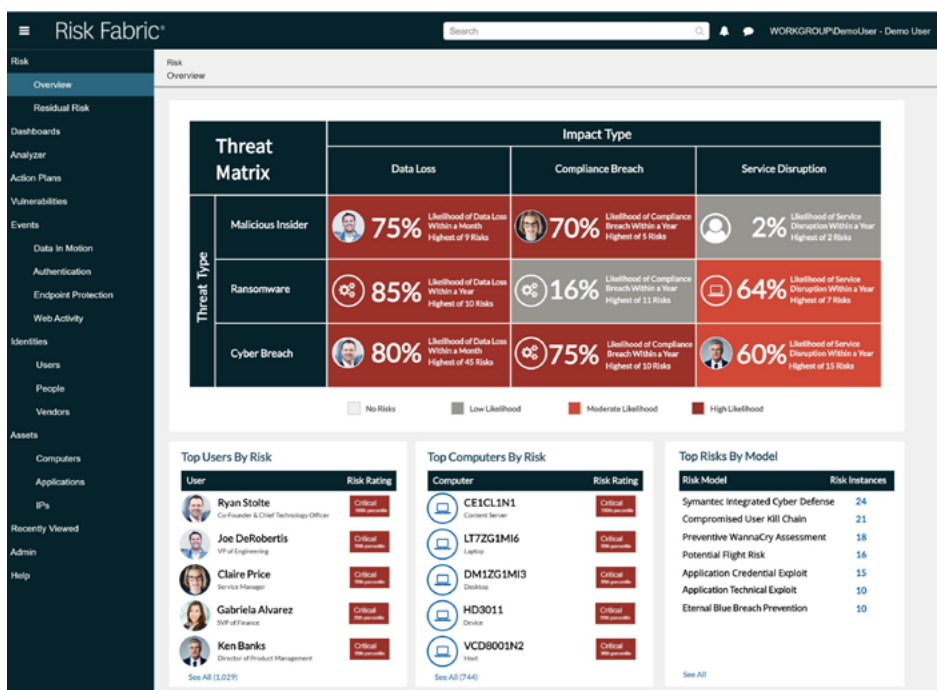
Risk Fabric provides detailed visibility into those DLP incidents that command immediate response.

Applying this approach over time fundamentally enables the organization to utilize DLP Optimization to approach the entire process in a more holistic manner. As various stakeholders from both security and business perspectives are brought closer together with common data, and policies are continuously improved to represent the real-world practices of the organization, critical metrics for business and policy stakeholders alike can be generated and tracked.

Risk Fabric provides detailed insight into DLP policies to enable accelerated response.

Immediate impact:
Use Cases and ROI

In real world environments, this marriage of DLP and Bay Dynamics Risk Fabric has produced impressive results. Deploying the two solutions in an integrated fashion, either to improve existing DLP implementations or accelerate new DLP platform deployments, has transformed related workflows including:

- **Analyst Response:** Allowing experts to dramatically reduce the time needed to triage incidents and enact informed remediation steps to address real-world risks.

- **Policy Tuning:** Accelerating feedback loops for policy improvement by connecting stakeholders to better tailor policies to address business processes and data handling practices.

- **Centralized Visualization:** Creating a visibility into DLP incidents and policies across all channels to develop useful metrics for both business and policy stakeholders.

These topline use cases encompass a huge variety of underlying benefits whose impact can be tied to measurable improvements and tangible return on investment figures.

For instance, in one case a global media and telecom provider that integrated Risk Fabric's UEBA capabilities alongside its DLP implementation was able to assign a full 80 percent of reported and ultimately non-malicious policy violations for rapid remediation – greatly increasing the efficiency of its analyst teams and improve the accuracy of future investigations.

In another example, a global electronic payments leader implemented Bay Dynamics Risk Fabric and DLP at the same time, leveraging the combined solutions' abilities to prioritize incident response and reduce its team of dedicated analysts from 35 to 5, re-assigning the staff to address other strategic activities.

Applying a simple ROI model to the latter example, and assuming a per analyst cost of $50 per hour, then extrapolating across the first 90 days of DLP Optimization, the organization saved roughly $28,000 in that timeframe, or $124,000 per analyst, annually. Prior to reducing its team from 35 analysts to 5 based on efficiency gains, this savings would amount to roughly $1 million in analyst work hours over the first three months, and over $4 million for the entire year.
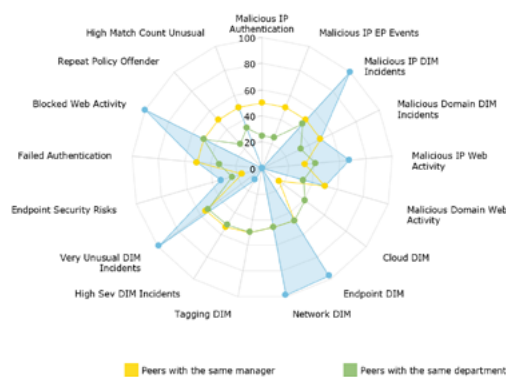
Risk Fabric's machine learning empowers detailed user behavior analysis across DLP channels and policies.

Risk Fabric Delivers Integrated DLP Optimization

Every organization enlisting an information protection strategy stands to benefit from DLP Optimization. Bay Dynamics Risk Fabric, combined with every manner of DLP platform, across networks, endpoints, email, storage, the Web and the cloud, represents the only fully integrated approach to DLP Optimization on the market today.

Through direct integration of DLP and UEBA platforms, backed by extensive dashboards and in-depth metrics, Risk Fabric escalates those issues that might otherwise go unnoticed or demand complex manual analysis. With automated remediation recommendations, Risk Fabric also provides organizations with the specific actions needed to immediately reduce risks, while connecting numerous stakeholders in closed loop communications that drive overall improvement of DLP polices and data protection.

Backed by patented unsupervised and supervised machine learning, Risk Fabric not only provides tactical capabilities to improve and accelerate nearly every DLP process, but also delivers a powerful set of visualizations and reporting for improvement of enterprise security management – allowing for continuous measurement and improvement of the overall reach and health of security infrastructure.

Bay Dynamics can help your organization Optimize DLP practices, visit:
https://baydynamics.com/optimize-data-loss-prevention/

About Bay Dynamics

Bay Dynamics enables enterprise organizations to identify, prioritize and mitigate their most critical cyber risks based on a strategic array of real-world conditions. Our flagship User and Entity Behavior Analytics (UEBA) and risk analytics software solution, Risk Fabric, integrates and analyzes security data across the full breadth of existing security infrastructure to pinpoint emerging threats and enable rapid remediation. For more information visit **www.baydynamics.com** or connect with us on **Twitter** and **LinkedIn**.

Bay Dynamics®   99 Hudson St 6th Floor, New York, NY 10013 USA | 1+ (646) 757 8075 | **www.baydynamics.com**