White Paper

Symantec
A Division of Broadcom

Optimizing DLP with Symantec® ICA

Organizations Seeking to Accelerate, Triage, and Mitigate User-Driven Data Security Risks

Introduction

Today's Data Loss Prevention (DLP) platforms offer unparalleled capabilities for organizations to significantly harden information protection, empowering numerous stakeholders to ensure the 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 an 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 a market-leading Symantec DLP solution and the integrated analytics provided by Symantec Information Centric Analytics (ICA) 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 and triage DLP incidents based on user risk, inform and automate remediation processes, augment policies, and track metrics for business and policy 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.

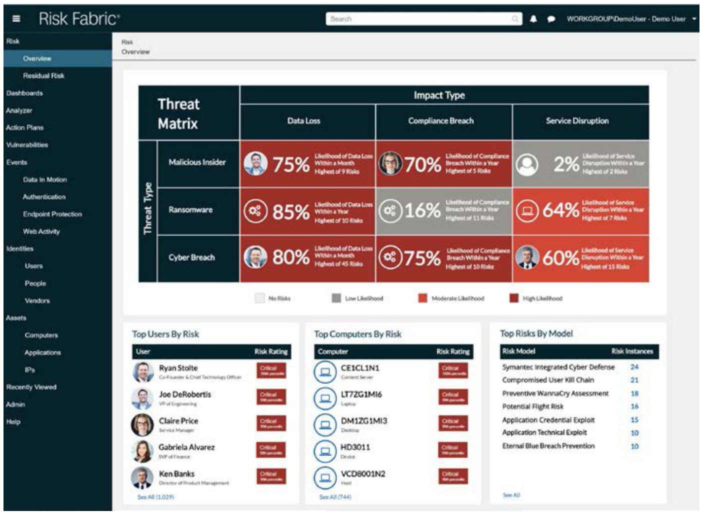
Another distinct capability of applying UEBA analytics for DLP Optimization is leveraging supervised machine learning to learn from human analysts' actions over time related to investigation, triage and remediation response. If certain types of events are consistently escalated for hands-on review or 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

Figure 1: ICA Provides Detailed Visibility into Those DLP Incidents that Command Immediate Response



Threat Matrix		Impact Type		
		Data Loss	Compliance Breach	Service Disruption
Threat Type	Malicious Insider	75% Likelihood of Data Loss Within a Month Highest of 9 Risks	70% Likelihood of Compliance Breach Within a Year Highest of 5 Risks	2% Likelihood of Service Disruption Within a Year Highest of 2 Risks
	Ransomware	85% Likelihood of Data Loss Within a Year Highest of 10 Risks	16% Likelihood of Compliance Breach Within a Year Highest of 11 Risks	64% Likelihood of Service Disruption Within a Year Highest of 7 Risks
	Cyber Breach	80% Likelihood of Data Loss Within a Month Highest of 45 Risks	75% Likelihood of Compliance Breach Within a Year Highest of 10 Risks	60% Likelihood of Service Disruption Within a Year Highest of 15 Risks

□ No Risks ▨ Low Likelihood 🟥 Moderate Likelihood 🟥 High Likelihood

Top Users By Risk

User	Risk Rating
Ryan Stolte Co-Founder & Chief Technology Officer	Critical
Joe DeRobertis VP of Engineering	Critical
Claire Price Service Manager	Critical
Gabriela Alvarez SVP of Finance	Critical
Ken Banks Director of Product Management	Critical

See All (1,029)

Top Computers By Risk

Computer	Risk Rating
CE1CL1N1 Content Server	Critical
LT7ZG1MI6 Laptop	Critical
DM1ZG1MI3 Desktop	Critical
HD3011 Device	Critical
VCD8001N2 Host	Critical

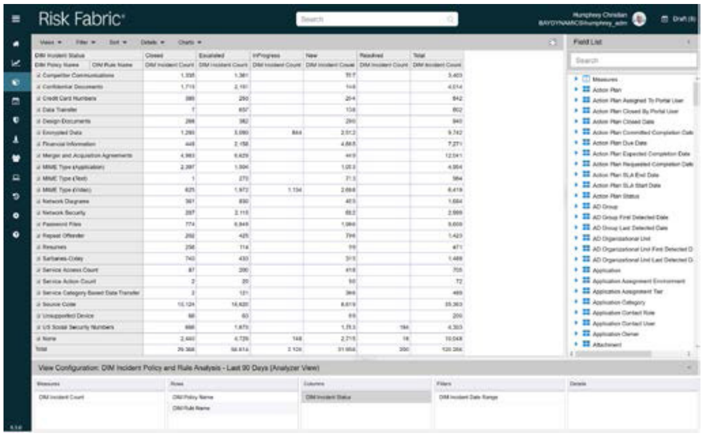
See All (744)

Top Risks By Model

Risk Model	Risk Instances
Symantec Integrated Cyber Defense	24
Compromised User Kill Chain	21
Preventive WannaCry Assessment	18
Potential Flight Risk	16
Application Credential Exploit	15
Application Technical Exploit	10
Eternal Blue Breach Prevention	10

See All

Figure 2: ICA Provides Detailed Insight into DLP Policies to Enable Accelerated Response

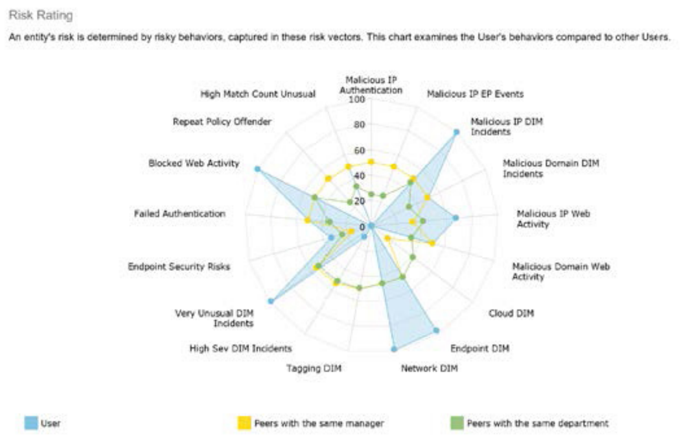


DIM Incident Status		Closed	Escalated	InProgress	New	Resolved	Total
DIM Policy Name	DIM Rule Name	DIM Incident Count	DIM Incident Count	DIM Incident Count	DIM Incident Count	DIM Incident Count	DIM Incident Count
Competitor Communications		1,335	1,381		687		3,403
Confidential Documents		1,715	2,151		148		4,014
Credit Card Numbers		388	250		204		842
Data Transfer		7	657		138		802
Design Documents		268	382		290		940
Encrypted Data		1,290	5,080	844	2,512		9,742
Financial Information		448	2,158		4,665		7,271
Merger and Acquisition Agreements		4,983	6,629		449		12,061
MIME Type (Application)		2,397	1,504		1,053		4,954
MIME Type (Text)		1	275		718		994
MIME Type (Video)		625	1,972	1,134	2,688		6,419
Network Diagrams		361	830		473		1,664
Network Security		287	2,115		682		2,999
Password Files		774	6,849		1,986		9,609
Repeat Offender		202	425		796		1,423
Resumes		258	114		99		471
Sarbanes-Oxley		742	433		313		1,488
Service Access Count		87	200		418		705
Service Action Count		2	20		50		72
Service Category Based Data Transfer		2	121		366		489
Source Code		10,124	16,620		8,619		35,363
Unsupported Device		68	63		69		200
US Social Security Numbers		698	1,673		1,738	194	4,303
None		2,440	4,729	148	2,715	18	10,048
Total		29,368	58,614	2,126	31,958	200	120,266

View Configuration: DIM Incident Policy and Rule Analysis - Last 90 Days (Analyzer View)

Measures	Rows	Columns	Filters	Details
DIM Incident Count	DIM Policy Name DIM Rule Name	DIM Incident Status	DIM Incident Date Range	

Figure 3: ICA Machine Learning Empowers Detailed User Behavior Analysis Across DLP Channels and Policies



Risk Rating

An entity's risk is determined by risky behaviors, captured in these risk vectors. This chart examines the User's behaviors compared to other Users.

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.

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.

Immediate Impact: Use Cases and ROI

In real world environments, this marriage of Symantec DLP and Symantec ICA 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 top-line 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 ICA UEBA capabilities alongside its Symantec 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 Symantec ICA and Symantec 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.

Broadcom Delivers Integrated Symantec DLP Optimization

Every organization enlisting an information protection strategy stands to benefit from DLP Optimization. Symantec ICA, combined with every manner of Symantec DLP, 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, ICA escalates those issues that might otherwise go unnoticed or demand complex manual analysis. With automated remediation recommendations, ICA 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, ICA 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.

To find out more about how Broadcom can help your organization, visit broadcom.com/products/cyber-security/information-protection/data-loss-prevention.

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com