SOLUTION BRIEF

Symantec Information Centric Analytics

Simplifying DLP Policy Management and Incident Remediation

Symantec™

Overview

Data Loss Prevention (DLP) is a strategic data protection solution that today's organizations can deploy to keep their confidential data safe and compliant. Symantec DLP provides tremendous visibility and the broadest protection across data loss channels: cloud, email, web, endpoints, and storage. When a violation of corporate data policy occurs, DLP also provides detailed information including the responsible source. But manual sorting and prioritization of large volumes of security alerts could be resource intensive for DLP administrators and analysts.

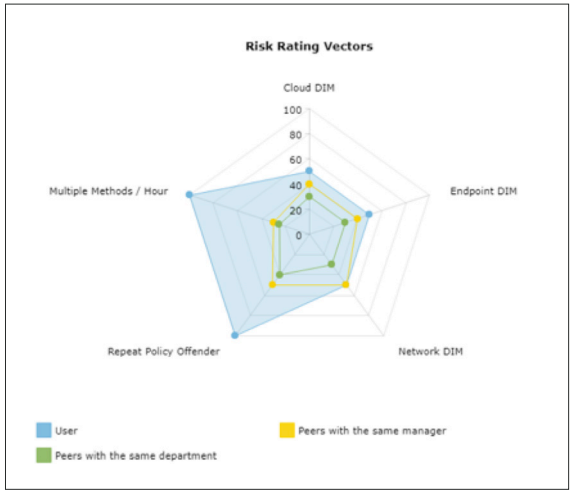
Symantec Information Centric Analytics (ICA) addresses this key challenge: with the myriad of DLP incidents reported every day, how can I identify and investigate the policy violations that represent my most significant risks?

ICA integrates directly with Symantec DLP to help security teams analyze large amounts of DLP security alerts and provides the analytics tools and context necessary to answer 3 specific questions:

- How can I enable effective DLP policies to best address my organization's normalized business processes and data risks, and how do I make sure if I cover every blind spot?
- How do I fine-tune my DLP policies and reduce the likelihood of false positives without impacting normal business processes?
- How do I ensure my DLP team and analysts are using their time efficiently by focusing on higher priorities?

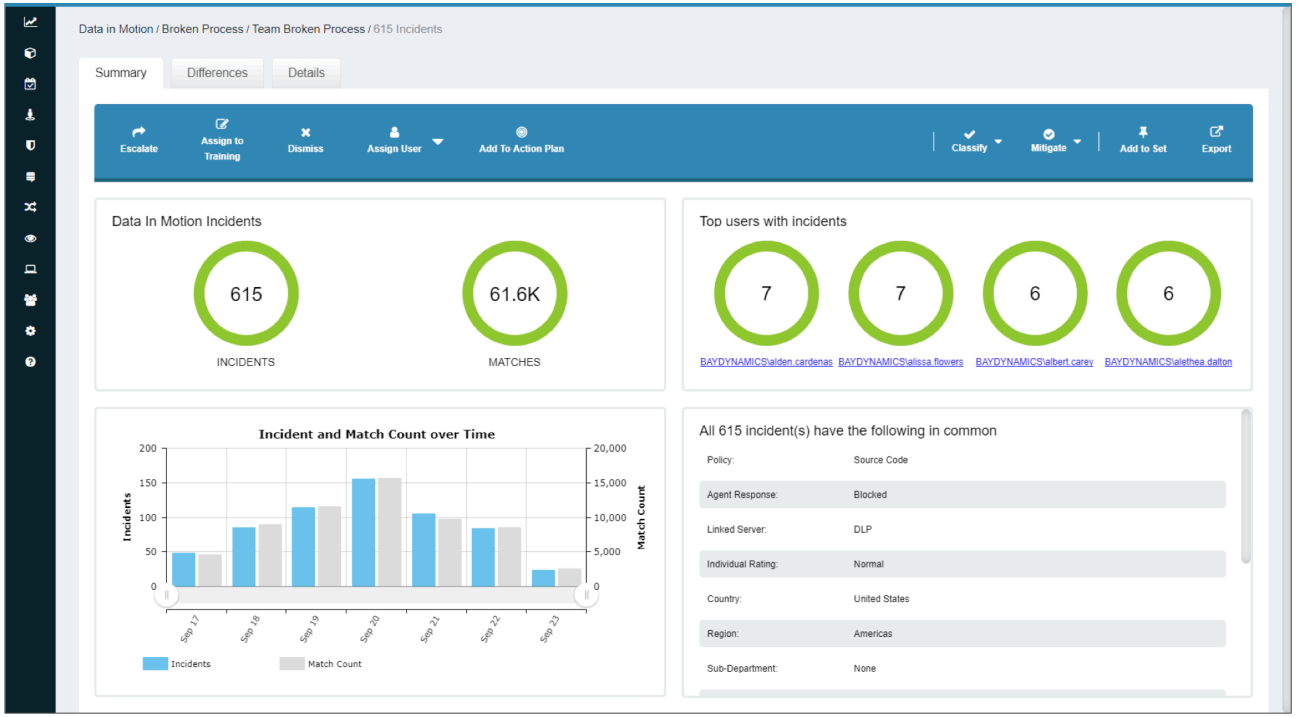
Symantec ICA is a user and entity behavior analytics (UEBA) tool that, integrated with Symantec DLP, helps to simplify DLP policy management and incident remediation. ICA can automatically isolate those scenarios that represent truly abnormal or risky behaviors. ICA thus helps shifting your DLP management from an event-driven to a risk-based strategy. This allows organizations to accelerate time-to-value with DLP systems, fine-tune policies with less false positives and achieve more efficient risk mitigation by using a broader set of truly effective DLP policies.

Examples: ICA would monitor changes to user behavior and, for instance, show an extensive pattern of incidents conducted by the same individual, who happen to be a recently dismissed worker and who is now attempting to copy or email sensitive files. In another scenario, if a widespread pattern of data violations where all conducted by individuals working in similar roles (for the same business units or managers), the risk vector would actually reveal a legitimate business process, not malicious behavior, therefore a false positive that needs DLP policy correction.



ICA analytics with machine learning detects and highlights abnormal behaviors within the context of the organization and its business processes.

Simplifying DLP Policy Management and Incident Remediation Through User and Entity Behavior Analytics (UEBA)



DLP Incident Analysis

Simplified DLP Policy Management

Practitioners face numerous challenges in authoring and tuning efficient DLP policies – those that identify true data incidents without overwhelming investigators with too many alerts. By integrating ICA at the outset of DLP implementation, Symantec customers will benefit from:

- Reduced time and efforts necessary to implement effective DLP policies
- Rapid time to value by enabling the use of out of the box DLP rule sets
- Deploying a broader set of DLP policies to cover more potential incidents

Specific DLP Implementation use cases include:

Broken Process Analysis – ICA quickly identifies existing policy violations that rather consist of normal business behaviors [ex. approved PII communications]. This reduces the number of false alerts yet enables policy refinement.

Detection of Abnormal Behavior– ICA can identify anomalous changes of users' behaviors from their normality in order to isolate the actual high risk data incident scenarios [ex. repeated attempts to copy sensitive data].

Simplified DLP Incident Remediation

When it comes down to DLP incident remediation, practitioners may be challenged to handle an avalanche of results generated by policies broadly applied across several data loss channels. By leveraging ICA to analyze DLP incidents, Symantec customers will benefit from:

- Increasing the volume of processed DLP alerts with a reduced time for investigations
- Comfortably expanding their DLP policies with the existing dedicated analysts
- Faster mitigation of DLP incidents via recommended remediation workflows

Specific DLP Remediation use cases include:

High Risk DLP Scenarios – ICA provides behavior-driven escalation of DLP incidents and a prioritized list of higher risk DLP incidents [ex. failed email exfiltration, followed by encrypted transmission] to inform of remediation actions.

Ad Hoc DLP Analysis – ICA extends the scope of the DLP analysis, by delivering rapid and flexible creation of visualizations and reports [ex. hunting specific, timely issues] to identify emerging threats.

Conclusion

Increasing the effectiveness of DLP to reduce the risk of a data breach is a key goal within security organizations. Symantec ICA offers immediate value in applying dedicated analytics and machine learning to simplify DLP policy management and incident remediation, regardless of the environment or the program maturity.

Whether your primary challenge lies in deploying the broadest set of DLP rules during initial implementation, filtering through numerous, varied DLP alerts to isolate risk, or anywhere in-between, Symantec ICA delivers measurable results.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec™

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

SYMC-SB-ICA-EN-V2A