SOLUTION BRIEF

# Symantec Information Centric Analytics

## Malicious Insider and Cyber Breach Monitoring

Symantec™

# Overview

As malicious insiders and targeted threats continue to result in countless high profile, high impact incidents, prevention of unauthorized activities that exfiltrate sensitive data remains a significant challenge. To identify those scenarios that represent real-world risks, today's IT security practitioners clearly require an analytics platform that aggregates user and event data across numerous sources to expose anomalies that indicate emerging cyber breaches.

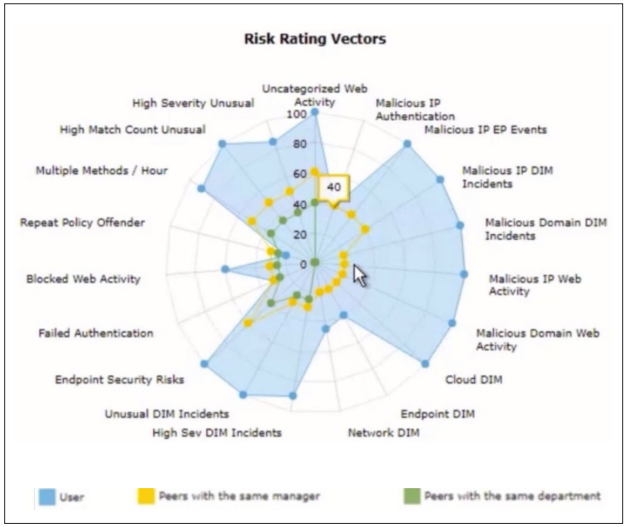
**Symantec Information Centric Analytics** (ICA) tackles this pervasive issue with the need to analyze relevant information from a wide variety of data sources and understand user behavior to mitigate risks.

ICA integrates directly with Symantec DLP, Symantec Endpoint Protection, Symantec CloudSOC Cloud Access Security Broker (CASB) and many other tools, including human resources systems, to help security teams identify malicious insiders and cyber breaches, and answer 3 specific questions:

- How do I synthesize critical data sets distributed across multiple platforms and policies to pinpoint anomalies that represent breaches or insider threats?
- How can I enable effective security policies that account for my organization's normalized data interactions and business processes to optimize enforcement?
- How do I ensure that security analysts are enabled to directly mitigate high-risk incidents and consolidate remediation of low-risk alerts?

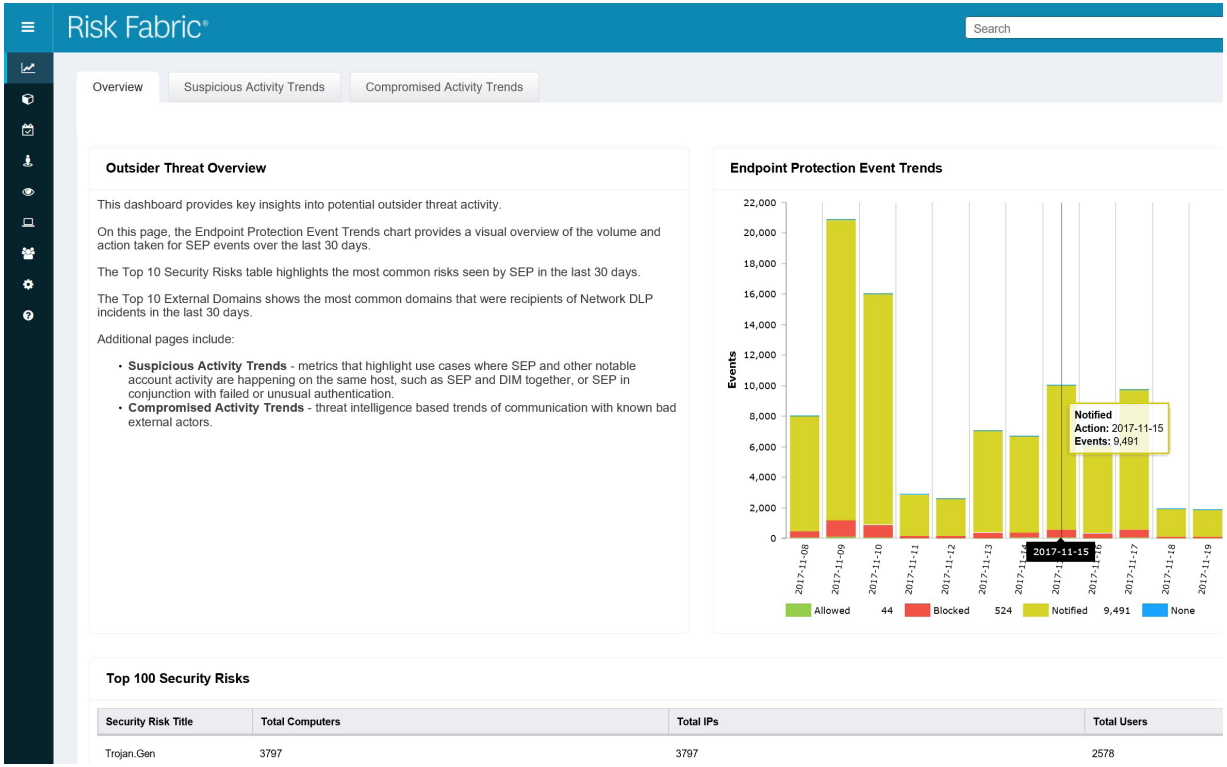
Symantec ICA is a User and Entity Behavior Analytics (UEBA) platform that, when integrated with Symantec DLP, Symantec SEP, Symantec CASB and many other solutions – including Active Directory and other human resources systems – enables rapid identification of insider threats and cyber breaches. Through centralized analytics, extensive dashboards and in-depth metrics, ICA escalates those issues that might otherwise go unnoticed or demand complex analysis. With automated remediation recommendations, ICA provides organizations with the visibility and workflows necessary to directly reduce exposure to sophisticated threats, greatly reducing manual effort.

Examples: ICA integrates assessment of policy violations across DLP, endpoint and cloud systems, along with application of user analytics, to create the full context around a data exfiltration scheme carried out by a disgruntled worker. In another example, if there is evidence of a compromised system or account resulting from malware infection, combined with a high-risk DLP policy incident, ICA synthesizes these factors to drive visualization and mitigation of an externally-driven attack.




*ICA integrates numerous data sources, leveraging user analytics to unveil insider threats and attempted cyber breaches.*

## Exposing Real-world Risks Through User and Entity Behavior Analytics (UEBA)




*Cross-vector incident investigation*

# Targeted Threat Analysis

Practitioners face acute challenges in rapidly focusing investigations on those alerts that represent high-profile or newly emergent risks. By integrating ICA with their DLP implementation, human resources systems and other sources, Symantec customers will benefit from:

- Increased precision in escalating high risk DLP policy violations
- Rapid investigation through drill down analysis and visualization
- Automatic de-prioritization of common or low risk user incidents

Specific malicous insider use cases include:

**Detection of Abnormal Behavior –** ICA can identify anomalous changes of users' behaviors from their normality, along with any changes in user privileges, to isolate actual high-risk incident scenarios [ex. repeated attempts to copy sensitive data in a short timeframe].

**Classifying Common Risk Factors –** ICA isolates common factors that result in DLP alerts [ex. unencrypted data transmission among peers] to calculate related prioritization and enable rapid risk reduction through established mitigation steps.

## 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.

# Cyber Breach Mitigation

The complex nature of today's data breach methods has made it extremely challenging for organizations to isolate and visualize multi-vector risks. By leveraging ICA to integrate, collect and correlate existing security data, Symantec customers will benefit from:

- Centralized analysis and behavior-based escalation of attacks
- Dedicated dashboards and detailed visualization of threats
- Trending of key threat investigation and remediation metrics

Specific Cyber Breach mitigation use cases include:

**Multi-Vector Investigation –** ICA ingests and analyzes evidence of abnormal behaviors and compromised activities across endpoints, networks and the cloud [ex. multi-stage malware attack] to paint the full picture of cross-channel breach attempts.

**Automated Action Plans –** ICA generates detailed Action Plans that determine and communicate required actions for every stakeholder and track end-to-end workflow resolution [ex. mitigation involves security and line-of-business officials].

# Integrated Risk Management

In addition to providing tactical ability to isolate and mitigate those incidents that represent an organization's leading instances of insider threats and breach exposure, ICA represents a powerful set of capabilities for overall improvement of related risk management. To that end, ICA provides numerous dashboards, scorecards and metrics that offer in-depth visualization and reporting of crucial data sets that highlight key management details including:

- Which elements of the organization are generating increased risk
- Where patterns are emerging across existing security infrastructure
- How effectively related tools are functioning and implemented

# Conclusion

Creating the ability to identify previously undetected threats and prevent resulting data theft remains a major challenge in IT security today.

Symantec ICA provides the centralized data integration and user behavior analytics necessary to visualize and prioritize those incidents that previously went unnoticed or proved too difficult to investigate across today's complex security infrastructure.

Whether you're attempting to uncover unseen attacks, accelerate investigation of known incidents, or improve overall security management, Symantec ICA delivers measurable results.

Symantec™

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



SYMC-SB_MALICIOUS INSIDER 211217