CUSTOMER TYPE

Global Media & Telecom Partner

CHALLENGE

Extending the value of DLP data, creating automated remediation workflows, and maximizing available security expertise.

SOLUTION

Bay Dynamics Risk Fabric

BENEFITS

- Added detailed contextual user data to DLP investigations to prioritize response
- Reduced the number of false positive alerts handled by security analysts
- Automated mitigation of large volumes of low-risk data policy violations
- Created a standard source of insider risk metrics across the larger organization

Automated 80%

of DLP remediated with video-based employee learning

Symantec ICA

Global Media & Telecom Leader Automates DLP Remediation with User and Entity Behavior Analytics

Based in the United States, this worldwide media and telecom conglomerate is one of the largest broadcasting and cable television companies in the world, both in terms of sheer revenue and number of customer accounts. With massive television, film, and digital holdings, along with an array of adjacent entertainment businesses, the company has significant data security concerns, along with complex compliance requirements.

The Challenge: Next Steps in Optimizing DLP Program

Spurred by a change in IT security leadership under a newly appointed CISO, the payment processing giant sought to enlist a more advanced approach to management of insider threats and related IT risk. To establish a cohesive solutions architecture supporting this initiative, the executive and his team moved to implement the market-leading Symantec Data Loss Prevention (DLP) platform, along with a source of dedicated analytics that could provide detailed visibility into user behavior.

By leveraging this additional layer of analysis in concert with its DLP implementation, the telecommunications company identified the opportunity to both increase the overall volume of incidents analyzed by its teams, and more effectively prioritize those events that required manual or automated remediation. Another key element of the strategy was to accomplish these goals without committing additional headcount. Employing dedicated analytics and machine learning to determine the severity of DLP policy violations and risk to sensitive assets would allow the company to embrace this model.

The Solution: Enlist Symantec Information Centric Analytics and UEBA

Having implemented the robust, market-leading Symantec DLP platform, the CISO's team undertook a close review of available User and Entity Behavior Analytics (UEBA) technologies that could provide detailed contextual awareness to advance management of insider risk.

“Instead of spending their time analyzing DLP event data, our teams use ICA to increase risk visibility and work together to take actions that directly impact the business.

— **CISO**
Media & Telecom Giant

While many UEBA solutions offer detection of behavior anomalies using a variety of analytics, the company was specifically focused on enlisting a system that would directly integrate with its existing DLP architecture to boost efficiency in handling related incidents. In addition to reducing so-called “alert fatigue” by cutting through the volume of potential results, including false positives and normal business activities, the company sought a platform that would eliminate the need to log into multiple solutions to address the individuals, data, and systems involved in each reported event.

With the overarching requirement to deepen visibility into insider threats and prioritize high priority risks, the CISO and his team quickly moved to implement Bay Dynamics Risk Fabric based on its ability to meet all the organization’s immediate goals.

Choosing Symantec ICA

Ultimately, for this company, Symantec Information Centric Analytics (ICA) represented a far more strategic approach to insider risks for numerous factors, including:

1. Direct integration with Symantec DLP to allow for user-based analysis, reporting, and escalation of policy violations that indicated high levels of risk to sensitive assets and data
2. Bulk analysis of large volumes of DLP alerts, across existing classes of users, data, and systems, to pinpoint identification of problematic issues and refine existing policies
3. Triggering of automated remediation workflows including self-paced video end user security training for employees that repeatedly violate low-level DLP policy thresholds
4. Customizable dashboards designed for communication of relevant metrics and results with numerous stakeholders, from security analysts to line of business executives

Results: Escalating Real-World Risks

Once the company deployed Symantec ICA alongside its existing Symantec DLP implementation, it saw an immediate increase in the volume of incidents analyzed, along with a sharp decrease in those issues requiring manual investigation.

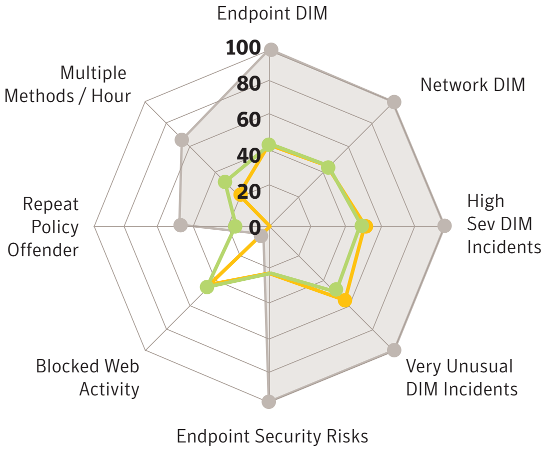
By employing advanced analytics at the front of its data security systems, leveraging user behavior detection and machine learning to more effectively separate actual threats from inefficient policies and unintentional violations, internal stakeholders were able to focus manual remediation efforts on critical risks. All of this was accomplished while reducing the overall number of analysts focused on DLP, freeing them for new strategic projects.

How Symantec ICA Works

Symantec ICA provides a proprietary cyber risk data model, with User and Entity Behavior (UEBA) and value at risk analytics, along with an ad hoc analysis user interface and customizable dashboards, driving more effective cyber risk management.

By providing a cohesive, contextually enriched view of insider threats and vulnerability across enterprise security and IT risk management data, at both an executive and operational level, Risk Fabric delivers a consistent view of changing posture across executives, line-of-business owners and security professionals alike.

Risk Rating Vectors



With ICA integrated into its security architecture, the CISO and his team achieved a wide range of measurable benefits, including:

- Increased visibility into DLP incidents that represented serious policy transgressions, kicking off subsequent investigation and targeted high-priority, focused mitigation
- Ongoing refinement of troublesome policies that resulted in frequent DLP alerts but did not represent significant risks to the organization or its data
- Reallocation of staff and resources previously focused on insider threat investigations to new strategic matters of analysis and IT risk reduction
- Centralized monitoring and communication of insider risks across the larger organization, including subsidiaries that also embraced the Risk Fabric approach to assessment

Looking Ahead: Building on Risk Fabric Success

Looking ahead, as the media and telecom provider continues to mature its approach to insider risk through broader use of Symantec ICA, officials are planning to incorporate related data from an even broader array of technologies–including endpoint protection, web application monitoring, user authentication, and threat intelligence tools.

By expanding the volume of data and the inherent reach of its program, company officials plan to use ICA as a more-centralized source of insider threat and IT risk management information, allowing for improved analysis and response across the entire organization.

Importantly, by moving to adopt ICA's integrated asset value ranking capabilities, the company plans to increasingly utilize the solution to measure the financial impact and risk to the business of specific applications, systems, and users.

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