CUSTOMER TYPE

Global Electronic Payment Processing

CHALLENGE

Improve visibility into insider risk, expand the scope of DLP, and do so without adding headcount

SOLUTION

Bay Dynamics Risk Fabric

BENEFITS

- Advanced insider threat analysis enabled risk-driven (versus event-driven) response
- Reduced false positives and allowed for targeted remediation of existing risks
- Enabled stronger communication of risk across security and line of business officials
- Optimized available analyst work cycles to focus on the most significant insider threats

UEBA Finds 80%

of DLP incidents not malicious, can be auto-remediated, additional staff not needed

Bay Dynamics®

Bay Dynamics

Global Electronics Payment Leader Combines DLP and UEBA to Uncover Insider Risks

Based in the United States, this global electronic payment leader supports over 6 million merchants worldwide, including numerous retail market leaders, and handles nearly half of all US-based credit and debit transactions – processing an estimated $1 trillion in transactions annually. In addition to significant IT risk considerations, the company is also subject to multiple compliance mandates, including the PCI Data Security Standards.

The Challenge: Rapid Behavior Assessment and Policy Optimization

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 managing insider threats and related IT risks. 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, and the Risk Fabric behavior analytics platform from Bay Dynamics to provide detailed visibility into user behavior.

By leveraging the combined capabilities of DLP and User and Entity Behavior Analytics (UEBA), the company identified the opportunity to gain conclusive insight into, and control over, potential data loss, allowing its analysts to prioritize those activities that constituted real-world risks. Another key element of the strategy was to accomplish these goals without hiring additional security expertise. Employing an integrated package of advanced DLP capabilities and highly automated user behavior analytics empowered the payment processor to directly engage this challenge.

The Solution: Integrated DLP Analytics

Having implemented the same solutions at a previous employer–which reduced DLP incidents needing investigation so dramatically that 30 of 35 analysts were freed up to work in more strategic risk management roles–the CISO and his team quickly moved to implement both Symantec DLP and Risk Fabric, creating an advanced architecture for the classification, monitoring, and analysis of sensitive data and user activities.

> Risk Fabric allowed us to increase the number of issues analyzed, while driving down required remediation activities, resulting in more effective risk mitigation, without adding more security analysts.
>
> — **CISO**
> Electronic Payments Giant

While other UEBA solutions offer detection of behavior anomalies using a variety of analytics, the company was specifically focused on using a platform that offered deep contextual awareness of user behavior and policy adherence related to ongoing DLP investigations. By integrating directly with Symantec DLP, the Risk Fabric solution would quickly provide detailed identification of those incidents that actually represented problematic activities, while allowing for targeted remediation, most often in the form of end user security training.

Additionally, the use of such an integrated DLP analytics approach would allow for greatly improved communication across management and operational staff, including reporting of efforts to senior management, partners, and other stakeholders.

Choosing Bay Dynamics Risk Fabric

Ultimately, for this company, Bay Dynamics Risk Fabric was significantly differentiated from other solutions across a range of key capabilities, including:

1. Unique bidirectional integration with Symantec DLP to provide top-down and operational visibility into changing insider risk posture, with detailed metrics and trending
2. Detailed contextual user, incident, and asset value data to prioritize efforts based on organizational risk, including automated remediation
3. DLP incident matching with other data-critical sets to investigate high-impact scenarios and policy issues, while eliminating false positives
4. Automated data aggregation and bulk analysis across DLP and other security platforms, with customizable dashboards for use by numerous teams

Results: Escalating Real-World Risks

Once the payment giant elected to move forward with adoption of Bay Dynamics Risk Fabric, the company rapidly extended the value of data provided by its DLP platform, along with other adjacent security systems.

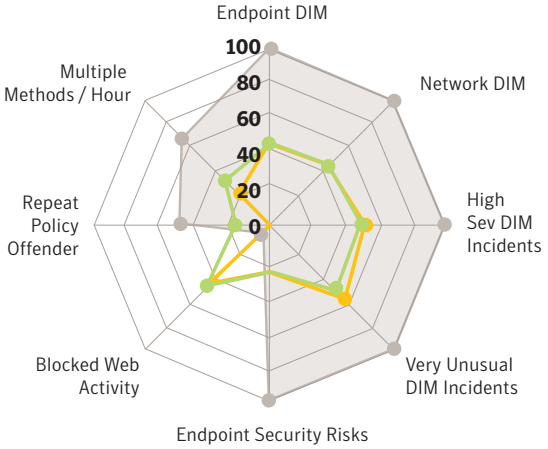
By gaining detailed visibility into DLP event details related directly to user behaviors – namely, where individuals reside in the organization and their normal patterns of activity – the insider threat team quickly realized the opportunity to identify problematic events. Moreover, this strategy allowed the organization to cover more ground related to IT risk mitigation, without requiring additional staff.

How Risk Fabric Works

Bay Dynamics Risk Fabric 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 Risk Fabric integrated with DLP and the company's existing security infrastructure, the CISO and his team achieved a wide range of measurable benefits, including:

- Conclusive improvement of insider threat metrics, driving significantly greater operational effciency across security and remediation teams, while handling more incident data
- Widened volume and scope of insider threat investigations, and resulting mitigation, while driving down workloads previously attributed to discovery and handling of false positives
- Ability to accelerate and refine remediation of truly at-risk assets, optimizing use of existing vulnerability assessment results to streamline workflows and improve risk posture
- Rapid identification and adaptation of problematic policies commonly triggering DLP alerts, allowing for increased user education and adaptation of the requirements themselves

Looking Ahead: Building on Risk Fabric Success

Moving forward, as the payment company continues to expand its insider threat management programs through broader use of Bay Dynamics Risk Fabric, offcials 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 inherent reach of its program, company offcials plan to use Risk Fabric 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 Risk Fabric'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

 SYMC_CS_BayDynamics_DLP-and-UEBA_EN_v1a