Bay Dynamics®

DATA SHEET

Risk Fabric®

Identify and Act on Cyber Risks

At a glance

- Integrated behavioral analytics capable of analyzing alerts and telemetry from diverse security sources, including DLP – connecting the dots between violations, users, accounts and assets
- Detection of risky user behaviors and identification of malicious insiders and outsiders via comparative risk scoring
- Advanced investigation capabilities and response workflows delivered via clear dashboards and a intuitive user interface

Today's organizations face countless obstacles in seeking to protect their critical data from numerous risks, including malicious insiders, negligent workers, compromised accounts, and advanced persistent threats.

In 2017, over 90 percent of targeted threats sought to identify and steal organizations' sensitive information, with the vast majority of those efforts focused on hijacking the privileges of specific individuals, according to Symantec's "2018 Internet Security Threat Report." Combined with internal attacks, employee errors and inadequate policies, security practitioners remain acutely challenged to pinpoint those user and entity behaviors that represent material risks.

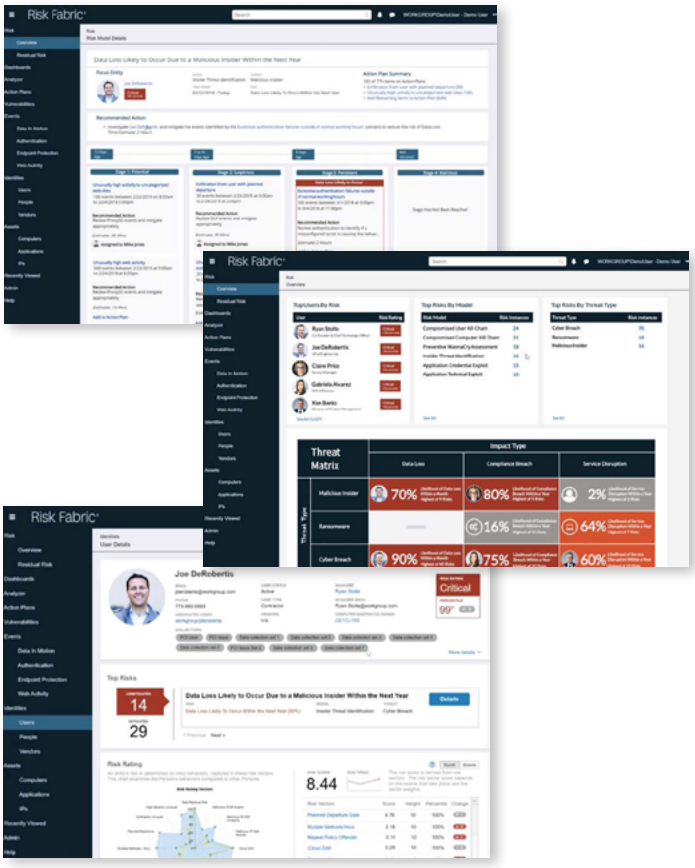
Manual sorting and prioritization of security incidents often fails to escalate crucial alerts until it's too late. To improve threat detection and mitigation, your organization needs advanced automation to help rapidly prioritize risky behaviors and identify malicious users on a continuous basis

.

Solution overview

Bay Dynamics Risk Fabric is a User and Entity Behavior Analytics (UEBA) platform that provides an integrated, contextually enriched view of cyber risks in your enterprise. It collects, correlates and analyzes large amounts of security event data from across diverse sources, including all data exfiltration channels (data telemetry), user access (identity telemetry), corporate asset data, and alerts from other security systems (threat telemetry). Backed by patented machine learning, Risk Fabric delivers rapid identification and prioritization of user and entity based risks.

Data Loss Prevention provides detailed information about violations of sensitive corporate data, including the responsible source. Data telemetry sources also include data tagging, cloud security and encryption platforms. Identity telemetry is provided via solutions like Microsoft® Active Directory®, while threat telemetry sources include endpoint security, web security and threat intelligence platforms. When sorted, correlated, and analyzed together, this vast amount of data gives invaluable insight into user behaviors.



Risk Fabric's adaptive risk models, customizable dashboards and point and click interface allow analysts to address the specific users and risks that matter most to your organization.

Thanks to a flexible and intuitive user interface, Risk Fabric allows analysts to rapidly differentiate between malicious and otherwise risky activities. Risk Fabric is able to pinpoint both real threats and prevalent issues created by broken business processes, and automatically generate remediation recommendations that measurably accelerate response.

Risk Fabric delivers an advanced datacentric UEBA approach providing centralized integration and analysis of large, complex data sets to create clear visibility into those behaviors that demand immediate investigation. Risk Fabric does the heavy lifting for you: by enabling rapid prioritization of alerts that represent emerging risks across multiple platforms, along with categorizing those incidents tied to misaligned policies or user mistakes, Risk Fabric allows analysts to optimize their time and effort, making the most of related resources.

Additionally, Risk Fabric's unsupervised and supervised machine learning capabilities automatically create baselines for comparative analysis, while constantly observing and informing future investigation based on analyst input. Through automated generation of recommended remediation workflows Risk Fabric empowers cross-functional teams to partner easily to execute, track and validate risk mitigation through a unified, closed loop process.

Finally, Risk Fabric offers dedicated analysis related to leading security compliance measures such as the EU's General Data Protection Regulations (GDPR), providing critical insight into user and entity-based interactions with affected data sets and applications.

Key benefits

- Centralized analysis and reporting of cross-platform, cross-policy data security risks
- Continuous assessment and prioritization of emerging threats
- Optimization of resources, analyst work cycles, security tooling and policies
- Reduced risk of regulatory noncompliance including GDPR

Data-Centric Analytics

Today's organizations require a data-driven approach to information protection and Bay Dynamics Risk Fabric offers the ability to leverage powerful user and entity behavior analytics precisely in this manner. Every organization must incorporate its unique data handling considerations across numerous security platforms spanning data loss prevention, endpoint defenses, cloud security systems and data encryption, among others. By integrating dedicated UEBA analytics with these critical sources, along with HR systems and other user repositories, practitioners are enabled to combine the most important factors related to information protection for centralized analysis, visualization and response.

Utilizing this approach, organizations can ensure that their protected information is being properly handled, while adapting to changing business requirements and continuously validating the effectiveness of existing defenses. This data and user-centric approach to information protection optimizes resources, increases return on investment and unlocks business agility through more adaptive and intuitive threat detection and prevention.

To learn more about Risk Fabric

System requirements

Primary architectural components

- Server operating system: Microsoft Windows® Server 2012 R2
- Application and web server: Internet Information Server
- Primary database store: SQL Server® 2016 cu5 or above
- Multidimensional database: SQL Server Analysis Services

Typical production database server specifications

- 128 GB RAM, 8–12 cores
- 250 GB minimum disk space

About Bay Dynamics

Bay Dynamics enables enterprise organizations to identify, prioritize and mitigate their most critical cyber risks based on a strategic array of real-world conditions. Our flagship User and Entity Behavior Analytics (UEBA) and risk analytics software solution, Risk Fabric, integrates and analyzes security data across the full breadth of existing security infrastructure to pinpoint emerging threats and enable rapid remediation. For more information visit www.baydynamics.com or connect with us on Twitter and LinkedIn.

Bay Dynamics® 99 Hudson St 6th Floor, New York, NY 10013 USA | 1+ (646) 757 8075 | www.baydynamics.com

 092718_DS_RF