Informatica

Solution Brief

Case Study: Behavioral Analytics for Enterprise SaaS

Key Benefits

- Enable business processes with rapid and agile access management
- Increase assurance how sensitive data was accessed and by whom
- Remove uncertainty surrounding insider threat and credential compromise
- Focus response and governance efforts on responding to actual threats

Enable business agility and speed while increasing assurance.

In today's competitive market place, speed, agility, access to information, and reliable data to enable a quick decision can mean the difference between a successful enterprise or one that succumbs to the competition. The traditional security engagement model focuses on implementing secure systems that meet business requirements. The rapid iterations of market demand after a go-live, however, stretch even the most agile security teams and create tension between security and the business.

How, then, can a security team successfully keep pace with natural business change while maintaining alignment with the principle of least privilege and objective of role-based access control (RBAC)?

With Informatica Secure@Source User Behavioral Analytics (UBA) capability, access compliance models long-used by IT administrators can be applied and will provide data owners with insights and assurance on how their data is being used and by whom. Combined with alerts and response, UBA enables data managers and owners to manage and mitigate the inherent risk from credential compromise and privilege abuse.

Because of its use of models familiar to audit and compliance teams, UBA lets even highly regulated environments benefit from rapid access to the information needed to remain competitive without a negative impact on assurance posture.

Precisely quantify your risk from authorized users

Situation and opportunity

When business change is rapid, security and access concerns can slow down the rate of change and impede business enablement. This can drive the business to adopt workarounds and conduct data management/analytics activities outside of the primary control system.

The resulting access control sprawl is very difficult to manage, impedes insight into who has access to which data sets, and renders misuse/abuse detection impossible. Understanding of how business processes use and expose data is fundamental to improving controls without interrupting business transactions.

The confluence of the business's requirements for speed and agility, regulatory requirements for certainty around data access, and compliance drivers' need for a conservative position creates an opportunity for capabilities that can provide assurance around not only which data users have access to, but what users are doing with the data.

Approach and solution

We found that UBA provides required assurance around data access while maintaining business speed and flexibility. In our in-house example, we first examined a few key business processes and followed the data set as it moved from authoritative source downstream through the analytics and reporting stack. Evaluating activity across the data domain rather than exclusively in one application provides broader context on data set activities and greater assurance on the usage boundaries of the data. We did not define user access scenarios in advance. Instead, we maintained assurance and accountability through oversight of user actions facilitated by anomaly detection and reporting capabilities.

Detection and alerts alone cannot reduce risk without rapid action from users, data owners, and management. You need to bring data owners and team managers into the loop early. They need to take ownership of the risk outcomes for access to their data, an outcome best-achieved by demonstrating the risk (or potential risk) from a data perspective. In most cases, data owners and managers do not have easy-to-consume insights into data access and usage patterns. A feedback loop involving users, management, and data owners underscores usage patterns and acceptable behaviors and encourages the adoption of responsible patterns.

There are many similarities between this model and the "break glass" access model typically used by administrators of sensitive systems who need to violate segregation of duties controls during maintenance and troubleshooting. The administrator has adequate permissions to complete the functions of the role. Elevated access triggers a review to ensure all actions were authorized. The use of machine learning allows this model, recognized by auditors as adequate, to scale and cover the organization.

A successful program should focus first on optimizing the action-oriented response model to respond to user behaviors and anomalies. Next, expand to cover critical business processes that require speed/agility or present significant risk to the organization's objectives.

Conclusion

Secure@Source's machine learning capabilities provide a level of assurance unattainable through manual review or, and the result is a tighter alignment between access grants and data usage.

UBA naturally integrates with data ownership models to establish a formal driver and encourage owners to manage and protect their data. Through awareness programs, targeted training, and process remediation, UBA can drive process improvements and changes to keep the organization in line with compliance objectives during rapid growth.

Because UBA is not tied to a specific application or platform, it can be used across applications to protect an entire data ecosystem instead of focusing solely on a source system and leaving reporting systems uncovered.

Informatica's Secure@Source UBA supports business speed and agility as well as security and compliance objectives by involving the data owner and management in the response process.

About Informatica

Digital transformation is changing our world. As the leader in enterprise cloud data management, we're prepared to help you intelligently lead the way. To provide you with the foresight to become more agile, realize new growth opportunities or even invent new things. We invite you to explore all that Informatica has to offer—and unleash the power of data to drive your next intelligent disruption. Not just once, but again and again.

Informatica

Worldwide Headquarters, 2100 Seaport Blvd, Redwood City, CA 94063, USA Phone: 650.385.5000 Fax: 650.385.5500
Toll-free in the US: 1.800.653.3871 informatica.com linkedin.com/company/informatica twitter.com/Informatica

© Copyright Informatica LLC 2017. Informatica, the Informatica logo, and Secure@Source are trademarks or registered trademarks of Informatica LLC in the United States and many jurisdictions throughout the world. A current list of Informatica trademarks is available on the web at https://www.informatica.com/trademarks.html. Other company and product names may be trade names or trademarks of their respective owners. The information in this documentation is subject to change without notice and provided "AS IS" without warranty of any kind, express or implied.