imperva

CAPABILITY BRIEF

Data Risk Analytics

Stop data breaches before damage happens

Digital business relies on the opportunities enabled by data, yet the scale and scope of data-related financial risks also increase. With exponential growth of data, there are more legitimate data accesses than ever, making it more difficult to determine whether a data access is acceptable. Moreover, security teams are often overwhelmed with a huge amount of alerts, let alone false-positives. Inappropriate data access and ignored incidents can lead to a catastrophic data breach because the risk associated with it is significant- penalties of non- compliant, loss in market share and stock price, reputation damage and more.

To mitigate data risk, advanced security analytics is required to identify risky data activity and bad practices, gain actionable insights into data usage, and to accelerate detection and investigation of potential breaches.

KEY CAPABILITIES

- Detects critical incidents among billions of audit events using machine-learning
- Peer group analysis that uncovers suspicious user data access
- Provides actionable insights in plain language
- Executive dashboard that helps accelerate threat investigation and response
- Out-of-the-box analytics with minimal tuning required

Data risk analytics

As a key feature in Imperva Data Security, data risk analytics provides security insights that can be immediately acted on. Unlike user behavior analytics tools, Imperva data risk analytics creates a contextual behavior baseline by analyzing both user behavior and data access activities. By learning and correlating data details like what sensitive data has been touched, by whom and when, and how data is used and accessed, Imperva data risk analytics can accurately identify critical threats to the data that matters. It cuts through the noise and prioritizes only the few high-risk incidents that require immediate investigation. This feature allows security team to uncover and contain a potential breach more effectively and gives CISOs and CIOs more confidence in preventing data breaches.

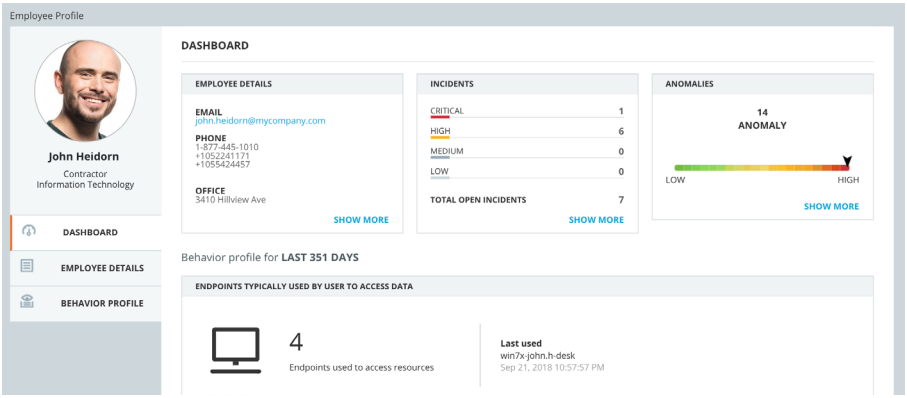

Figure 1: The dashboard provides the visibility security team needs to investigate suspicious user data access that could indicate a data breach.

Identify risky data activity and get actionable insights

Pinpoint true risk to your data

To mitigate the risk of a data breach, you need to be able to detect and pinpoint actual threats to your data. Data risk analytics utilizes machine learning and behavior analytics to uncover suspicious data access and bad practices. It automates the processing of massive amounts of database and file activity logs and correlates them to surface meaningful incidents. By analyzing both the user and data access context and continuously learning the details of who the users are, how they typically access database and use enterprise data, the analytics engine creates a contextual behavior baseline to help discern behaviors that are normal from "normal but not right".

Prioritize what matters most

Data risk analytics prioritizes critical incidents by applying grouping and scoring algorithms. Each incident is assigned a risk score based on a sophisticated algorithm that factors in various variables, such as amount of sensitive data, privileged account, prevalence and more. If the incidents are related (e.g. they are all associated with the same user account or multiple users are abusing the same service account), they will be grouped into one issue. As a result, only few high-risk incidents are bubbled up and far less alerts get sent to your SIEM.

Accelerate and streamline incident response

Investigating data threats often requires deep database knowledge to know if any sensitive data has been misused or if users are accessing data inappropriately. Data risk analytics interprets security incidents in plain language and provides actionable insights and risk context, so security professionals can quickly understand what happened to the data environment and respond to threats even with little to no database knowledge. While the dashboard is intuitive and easy-to-consume, it contains all the information and visibility a security professional needs to carry out an investigation.

Summary

Data risk analytics is a key component of Imperva Data Security. It helps security team detect and pinpoint critical threats to your data, prioritizes what matters most, and provides actionable insights and risk context, allowing you to accelerate threat investigation and response. You can start seeing the benefits and changes in weeks, not months. Mitigate data breach risks more effectively before damage happens.

IMPERVA DATA SECURITY

Data Risk Analytics is a key component of Imperva Data Security, which reduces breach risk while enabling digital transformation. The solution safeguards data on-premises and in the cloud by:

- Discovering sensitive data
- Monitoring all data activity
- Stopping unauthorized access and activity
- Uncovering risky users and suspicious actions
- Providing actionable security insights
- Masking data for non-production use

Learn more about Imperva Data Security at www.imperva.com.