IMPERVA

Reduce Your Data Breach Risk

Do you have any of these challenges?

- Undetected data breaches
- Insider threats
- Event overload and alert fatigue
- Lack of skilled security staff
- Regulatory compliance responsibilities

Imperva data security helps keep your company out of the data breach headlines while simplifying security operations. It helps organizations detect data breaches before damage happens, accelerate incident investigation and response, reduce your overall attack surface, and automate data audit and compliance efforts.

Overview

Whether caused by an insider threat or an external attack, data breaches have always been CISO's and CIO's top concern. They are worried about undetected data breaches that can cause significant financial and reputational harm to the organization. With the escalating threat landscape lacking enough skilled security professionals, security teams suffer from event overload and alert fatigue, which slows down their ability to identify the true risk and to respond to threats. To address these problems, you need a solution that improves breach detection effectiveness while simplifying the investigation work by automating laborious processes.

Imperva Data Security Solution

Imperva technology allows you to detect and stop potential data breaches before any damage happens. It addresses security teams' biggest concern by improving risk identification and breach detection effectiveness, without increasing labor costs. As outlined below, the Imperva data security solution offers valuable security capabilities to address the data security challenges organizations face today.

Key Features and Benefits:

- Threat detection and prioritization using behavior analytics and machine learning
- Identification of risky user data access – for all users including privileged users
- Database and file access monitoring to meet industry compliance requirements for PCI, HIPAA, GDPR and others.
- Real-time detection and alerting of policy violations
- Real-time user access blocking and quarantine to contain data breach
- Automated data discovery and classification
- Static data masking to reduce attack surface
- Vulnerability assessment to identify security gaps

Customer Benefits

- A financial services company was able to monitor 25X more databases and investigate 100% of alerts without adding more employees
- Allows a large healthcare company to reduce the amount of alerts from 1.2 billion to 30 per day
- Customers start seeing benefits within 2 weeks

Pinpoint true risk to your data

To mitigate the risk of a data breach, you need to be able to detect and prioritize actual threats to your critical data. Imperva data security solution utilizes machine learning and behavior analytics to uncover anomalies and any suspicious data access. It creates a contextual behavior baseline by analyzing user behavior, database and file activity information to help discern behaviors that are normal from "normal but not right".

The solution correlates millions of data access events captured and pinpoints high-risk incidents, helping security staff to easily identify the most critical issues. It then prioritizes these critical incidents by applying grouping and scoring algorithms. Each incident is assigned a risk score. And if the incidents are related in some way (e.g. they are all associated with the same user 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 and security analysts.

Imperva data security solution simplifies IT and security operations, allowing security professionals to focus on the incidents that matter the most. Once an inappropriate data access incident is identified, you can then block that access or any unauthorized activities as well as quarantine suspicious users.

Accelerate incident investigation and response

Another challenge facing security teams when investigating data threats is that it often requires deep database knowledge to know if any sensitive data has been misused or if users are accessing data inappropriately. Imperva data security solution interprets security incidents in plain language and provides actionable insights, so security professionals can quickly understand what happened to their data environment and respond to threats with little to no database knowledge (see Figure 1). The executive dashboard presents the top few high-risk incidents (see Figure 2). While the dashboard is intuitive and easy to consume, it contains all the information and visibility a security professional or incident responder needs to carry out an investigation (see Figure 3).

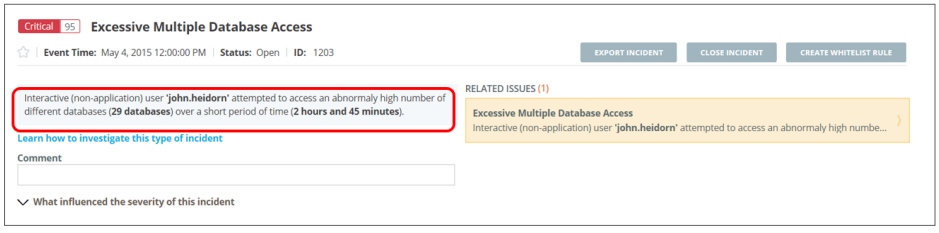

Figure 1: Imperva data security solution provides a short description of the incident, giving security professionals actionable insights to quickly respond.

"This makes our lives so much easier."

SECURITY ANALYST FROM A FORTUNE GLOBAL 500 COMPANY IN HEALTHCARE INDUSTRY

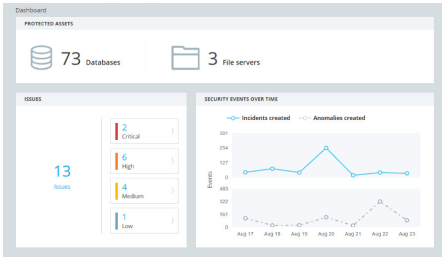

Figure 2: The executive dashboard is easy to read and allows security professionals to focus on few high-risk incidents.

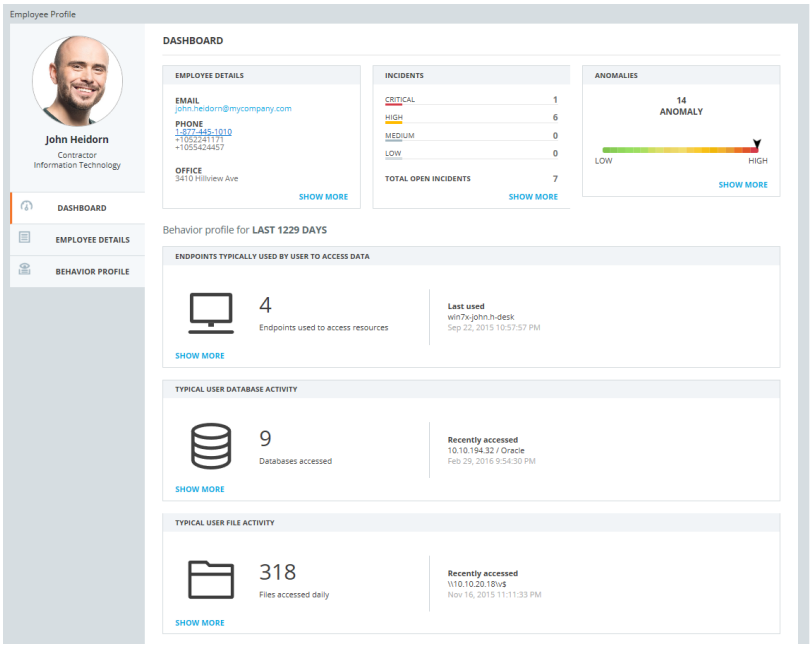

Figure 3: The user profile dashboard provides the visibility security professionals need to investigate suspicious user data access that could indicate a data breach.

"This is the next-gen solution in detecting anomalies. I can't imagine what would companies do without it."

IT DIRECTOR OF SECURITY FROM A LARGE RELIGIOUS ORGANIZATION

Mask non-production data to reduce attack surface

With the exponential growth of data and users, particularly in the non-production or DevOps environments, the risk and costs associated with a data breach are becoming even more significant. Imperva data security solution includes static data masking that de-identifies data such that the data can no longer directly identify the subject. It replaces real data that contains sensitive information with fictional yet high quality realistic data that is functionally and statistically accurate. For example, the original data contains a record of Amy Choo who is 60 years old, and her SSN is 123-44-5555. After the data is masked, it might become Jessica White, 56 years old, with a SSN of 747-88-9999. Data masking maintains data utility for non-production environments, such as app development, testing, and research, yet reduces the risk of data breach and limits the spread of sensitive data beyond "need-to-know".

Automate data audit and compliance

Imperva data security simplifies audit and compliance by continuously monitoring all database activity across your cloud and on-premises environments. Data discovery and classification find sensitive data that falls within scope of data privacy and protection regulations. Vulnerability assessments identify exposed databases by scanning for platform, software and configuration vulnerabilities. Detailed data activity, including privileged user access and service account activity, is captured automatically.
Data activity events are standardized across relational databases, big data environments, data warehouses and mainframes, providing you with a unified and consistent view. Imperva data security provides you with flexibility to customize your own security policies and allows you to alert or block inappropriate data access in real-time. Pre-defined reports and compliance policies makes it so much easier for you to fulfill audit and compliance requests.

Summary

In the era of exponential data growth, you need to assume open interaction between users and data to allow your business to grow. However, the increased risk of an innocent or malicious data breach also comes along with this growth. To prevent your organization from being the next breach headline without slowing down your business growth, you must take a different security approach – one that enables the business rather than locking down data by default. Imperva data security utilizes modern technologies such as machine learning and behavior analytics combined with our domain expertise to help you detect and contain data breaches, accelerate incident response, reduce the sensitive data landscape, and automate audit and compliance reporting, without raising labor costs. The solution offers numerous capabilities and customer proven results to support your overall data security needs.