imperva

DATASHEET

Imperva Data Security

Reduce the risk of a data breach while enabling digital transformation

The data security landscape is rapidly changing, and today's digital and knowledge economy is fueling exponential data growth with unprecedented user access. With more legitimate users accessing more data to drive value for the business, your security strategy should take a data-centric approach. This enables total access to data rather than locking down and limiting access by default. Imperva Data Security helps organizations unleash the power of their data while reducing the risk of a data breach.

Uncover hidden risks with discovery and assessment

An essential step in protecting data is uncovering blind spots such as rogue or vulnerable databases. These blind spots create security risks as attackers can exploit hidden or misconfigured databases that contain sensitive data. Imperva Data Security helps organizations reduce the risk of a data breach by locating sensitive data and identifying database vulnerabilities.

Imperva Data Security discovers databases on the network, classifies sensitive data and detects database vulnerabilities. Discover databases by scanning specific network segments on-demand or at scheduled intervals. Once databases are discovered, Imperva Data Security classifies the data stored in the database using dictionary and pattern-matching classification methods. Conduct vulnerability assessments with over 1,500 pre-defined vulnerability tests, based on CIS and DISA STIG benchmarks.

Detect and contain data breaches with continuous data monitoring and analytics

To mitigate the risk of a data breach, organizations need visibility into who's accessing what data and whether that data access activity is good or bad. But today's escalating threat landscape, exponential data growth, and increasing number of users with legitimate data access makes it impossible to determine whether a data access event is appropriate by simply relying on role-based access controls.

KEY FEATURES AND BENEFITS

- Detect and prioritize data threats using data science, machine learning and behavior analytics
- Pinpoint risky data access activity – for all users including privileged users
- Gain visibility by monitoring and auditing all database activity
- Protect data with real-time alerting or user access blocking of policy violations
- Uncover hidden risks with data discovery, classification and vulnerability assessments
- Reduce the attack surface with static data masking

Imperva Data Security provides continuous monitoring with separation of duties. It captures and analyzes all database activity from both application and privileged user accounts, providing detailed audit trails that show who accesses what data, when, and what was done to the data. Our robust security rules engine enables organizations to customize security policies, and provides real-time alerts or blocking for policy violations.

Imperva Data Security enforces a unified security and compliance policy across heterogeneous data environments. It standardizes log events across various platforms, providing a consistent view over relational databases, mainframes, big data platforms, and data warehouses. It also supports databases in Microsoft Azure and Amazon Web Services (AWS) — including PaaS offerings such as Azure SQL and Amazon Relational Database Services (RDS). Detailed data activity is captured automatically, making it so much easier to fulfill audit requests.

To uncover dangerous data access activity that exposes the organization to a higher risk of a data breach, Imperva Data Security utilizes data science, machine learning, and behavior analytics. The data risk analytics capabilities create a contextual behavior baseline by analyzing user behavior and database activity information to help discern behavior that's normal from "normal but not right." It distills millions of data access events and pinpoints high-risk incidents, reducing the number of alerts to a handful of manageable narratives (see Figure 1). It then prioritizes these critical incidents by applying grouping and scoring capabilities. Incidents are explained in plain language, making it easier for security teams to respond (see Figure 2). As a result, only a few high-risk incidents surface and far fewer incidents get sent to a SIEM.

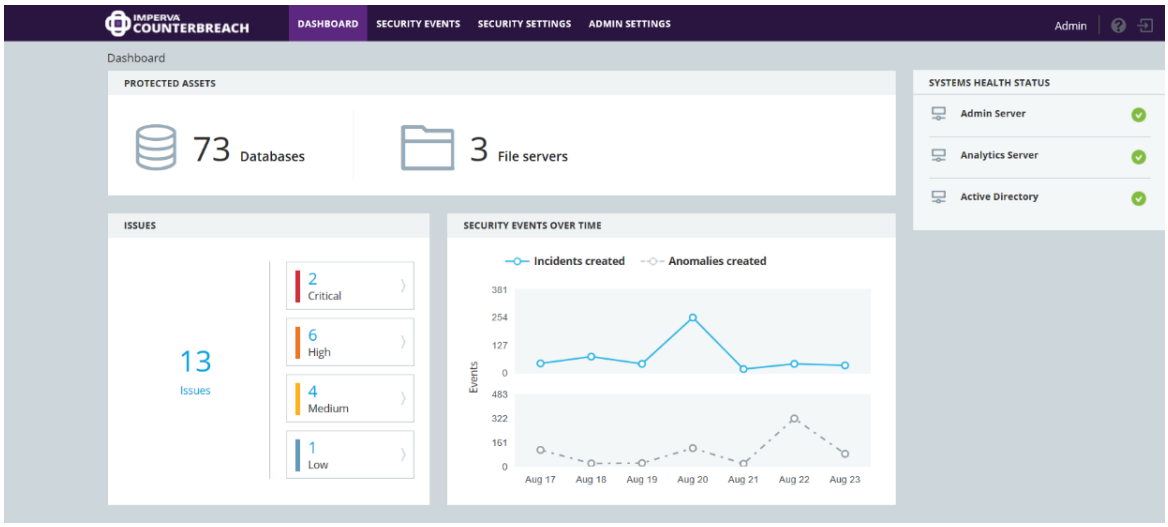

Figure 1: The dashboard is easy to read and allows security professionals to focus on few high-risk incidents.

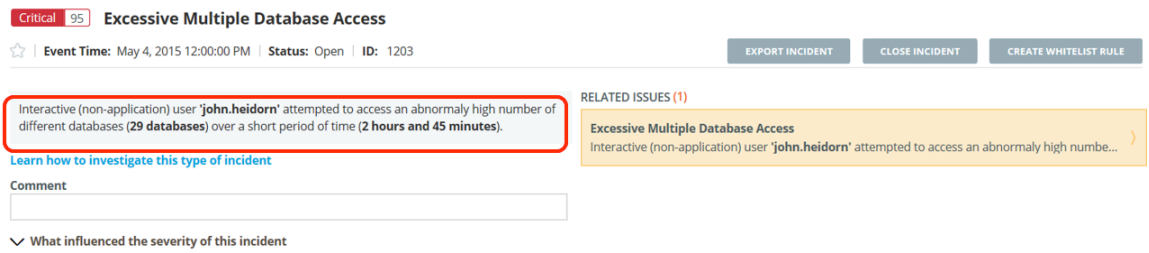

Figure 2: Incidents are assigned a risk score and grouped with related incidents giving security professionals actionable insights to quickly respond.

Reduce the attack surface with static data masking

As organizations look to leverage the value of the data they hold, copies of production data are made for non-production environments such as development, test, research and analytics, and outsourcing. Industry analysts estimate that 82% of organizations have more than 10 copies of each production database.[1] The exponential spread of sensitive production data throughout an organization increases the data breach and compliance risk. To mitigate data breach and non-compliance risks, organizations can reduce the attack surface by narrowing down the sensitive data landscape.

The Imperva Data Security static data masking capabilities provide a proactive control that protects sensitive data from unnecessary exposure while enabling data-driven business processes. It de-identifies data such that the data can no longer directly identify the subject. Using a variety of transformation techniques, 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 Adam Smith who is 60 years old, and his SSN is 123-44-5555. After the data is masked, it might become Tom White, 56 years old, with an SSN of 747-88-9999.

ORIGINAL DATA

NAME	SSN	AGE	GENDER
Adam Smith	123-44-5555	60	Male
Jenny Park	987-65-4321	28	Female

MASKED DATA

NAME	SSN	AGE	GENDER
Tom White	747-88-9999	56	Male
Amy Kim	747-88-9998	24	Female

Figure 3: Data masking example.

Flexible licensing

FlexProtect is a flexible approach to securing data. A single license offers you the ability to deploy Imperva Data Security how and when you need it. You're protected regardless of the number, location or type of devices or services used. FlexProtect helps you protect your data wherever it lives — in the cloud, on-premises or in a hybrid configuration.

FLEXPROTECT BENEFITS

- Reduce the cost of uncertainty when moving to the cloud
- Predict costs even as your in-the-cloud and on-premises infrastructure changes over time
- Flexibility to scale as your business scales

[1]Copy Data Management report, IDC, April 2016

Imperva is an analyst-recognized, cybersecurity leader championing the fight to secure data and applications wherever they reside.

+1 (866) 926-4678
imperva.com