imperva

DATASHEET

Imperva Database Security

Simplify data compliance and stop breaches

Today's digital and knowledge economy is fueling exponential data growth by using more data to drive value for the business. To protect your data, and your business, you need compliance and security solutions that take a data-centric approach. Imperva Database Security helps organizations unleash the power of their data by reducing the risk of non-compliance or a security breach incident.

A better way to manage data risk

The complexity of achieving compliant and secure data is daunting to a large enterprise organization. Rapid platform change and scarce security resources make it almost impossible to keep up with on your own. Security staff is often overwhelmed by a deluge of alerts coming from multiple security tools.

Imperva provides an automated solution to streamline compliance processes and help security staff pinpoint data risk before it becomes a serious event. With Imperva Database Security you can quickly cover your most critical assets, for fast time to value, and then gradually widen the net.

Imperva standardizes audit and security controls across large and complex enterprise database environments, mitigating risks to sensitive data on-premises, in the cloud, and across multiple clouds.

Imperva risk-based analytics help limited security staff be more effective at detecting risky or suspicious behavior by eliminating false positives, and clearly prioritizing the issues that are most important.

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

Gain visibility and fix vulnerabilities

Many organizations don’t actually know where all of their sensitive data is and whether it’s exposed. Such blind spots create security risks that lead to careless mistakes, or create opportunities that attackers can exploit, often through hidden vulnerabilities or misconfigured databases. Imperva Database Security helps organizations reduce non-compliance and breach risk by locating sensitive data and identifying the vulnerabilities that could lead to data compromise.

Imperva Database Security automatically discovers databases on the network and in the cloud. In the process, it can automatically identify and classify sensitive data, using a number of techniques including dictionary and pattern-matching methods.

Imperva vulnerability assessments capabilities scan your databases with over 1,500 pre-defined vulnerability tests, based on CIS and DISA STIG benchmarks to help you keep your databases covered for the latest threats.

Make staff more effective with actionable insights

Imperva Database Security incorporates advanced Data Risk Analytics that correlate user data access activity over time across all database servers.

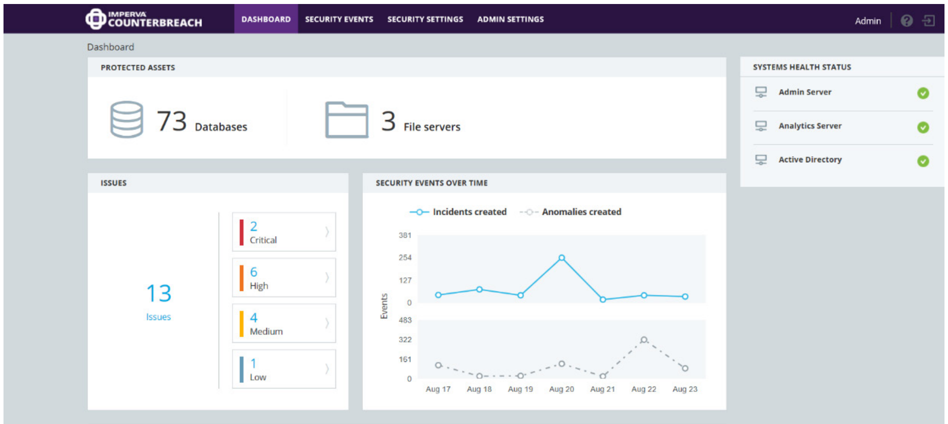
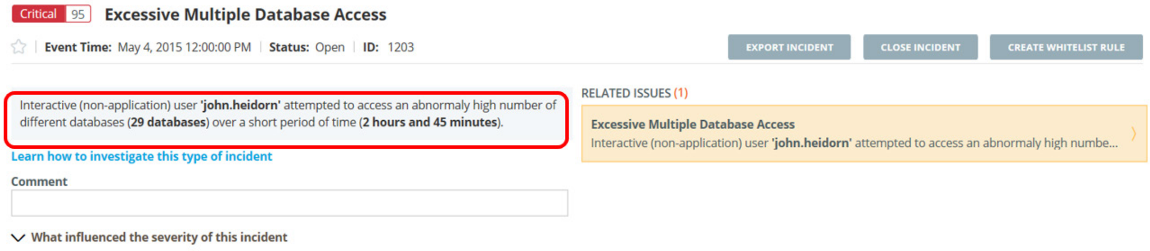


Figure 2: The dashboard is easy to read and allows security professionals to focus on few high-risk incidents.

This helps identify risky or potentially malicious data access behavior even if the behavior attempts to be evasive. Any incident that is flagged is labeled by category, scored by a set of risk metrics, and prioritized. Incidents are explained in plain language, making it easy for security teams to respond (see Figure 3).



Excessive Multiple Database Access

Event Time: May 4, 2015 12:00:00 PM | **Status:** Open | **ID:** 1203

Interactive (non-application) user **'john.heidorn'** attempted to access an abnormaly high number of different databases (**29 databases**) over a short period of time (**2 hours and 45 minutes**).

Learn how to investigate this type of incident

Comment

What influenced the severity of this incident

RELATED ISSUES (1)

Excessive Multiple Database Access
Interactive (non-application) user **'john.heidorn'** attempted to access an abnormaly high numbe...

Figure 3: Incidents are assigned a risk score and grouped with related incidents giving security professionals actionable insights to quickly respond.

Protect in real-time

Imperva Database Security enforces compliance and security policy across heterogeneous data environments. Out-of-box and/or templatized security policies for broad regulations such as PCI, GDPR and CCPA keep sensitive data such as PII under limited access control or confined within borders. Customized policies can be created for specialized requirements. As a data-centric solution, Imperva Database Security creates a security barrier for the database itself, looking for threats and attacks in SQL instructions. If a threat is detected, it flags it, creates an alert, and if appropriate, blocks (terminates) the offending data access attempt.

Continuously monitor

An organization shouldn't rely exclusively on encryption and role based access controls to protect their data. To mitigate the risk of a data breach, organizations need continuous visibility into who's accessing what data and whether that data access activity is good or bad.

Imperva Database Security provides continuous monitoring to capture and analyze 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.

It unifies auditing across diverse on-premises platforms, providing oversight for relational databases, NoSQL databases, mainframes, big data platforms, and data warehouses. It also supports databases hosted 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 easier to fulfill audit requests.

Remove risk in development and test

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 spread of sensitive data in non-production environments significantly increases the data breach and compliance risk.

Imperva Database Security Masking capabilities provide a proactive control that protects sensitive data from unnecessary exposure without slowing development processes. 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, enabling development simulation and test but removing the risk.

Flexible licensing and deployment

Imperva FlexProtect is a flexible licensing option for securing data enterprise-wide. A single license offers you the ability to deploy Imperva Database 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

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

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