imperva

SALES GUIDE

Imperva Data Security

Trusted by thousands of enterprises around the world, Imperva Data Security reduces data breach risk and compliance risk.

Elevator pitch

Data breaches are no longer a matter of if, but when. CISO's are worried about breaches going undetected. They don't know what's going on with their data – who's accessing it and how it is being used. Moreover, security teams struggle to keep up with the volume of security alerts and lack of skilled staff.

Imperva Data Security gives security teams visibility into who is accessing their sensitive enterprise data. We monitor and audit all access, including privileged users, to file servers and databases in real-time.

We use analytics to determine good data access from bad data access. By applying machine learning and user behavior analytics, we help security teams cut through the alert noise and pinpoint dangerous data activity.

Once suspicious data activity has been identified, we help remediate incidents with actionable insights, alerts and blocking. We help reduce the sensitive data landscape by masking non-production data.

Imperva Data Security also provides detailed reporting and helps you comply with various regulations, such as GDPR, PCI DSS and HIPAA.

Imperva Data Security reduces the risk of a data breach.

- Monitors who's accessing what data, when they accessed it, and what they did with the data
- Detects suspicious data access incidents and provides actionable insights
- Alerts or blocks unauthorized data activity
- Masks sensitive data to reduce the potential attack surface
- Addresses compliance requirements for PCI DSS, HIPAA, GDPR, and other industry regulations

Why Imperva Data Security Wins

- Pre-built machine learning analytics
- Actionable insights to streamline incident investigation
- Unified security and audit policy across different database platforms deployed on-premises or in the cloud
- Enterprise scalability with lower total cost of ownership

What is Imperva Data Security?

Imperva Data Security protects critical data no matter where it resides – in the cloud, on-premises and hybrid environments. It uncovers where sensitive data lives, monitors any data activity happening in databases and file servers, and detects suspicious data access while providing actionable insights.

It answers critical questions, such as: who is accessing what data, and when; how is the data being used. Pre-built behavior analytics and machine learning help detect and prioritize the high risk data access incidents, allowing security professionals to get ahead of potential data breaches. Once inappropriate data access is detected, customers can remediate incidents via alerting, blocking, or quarantining risky users. It also reduces the sensitive data landscape with data masking.

Imperva Data Security reduces data breach risk by continuously monitoring data activity and pinpointing risky data activity.

Data discovery and classification

You can't protect what you don't know about. Imperva Data Security uncovers forgotten or rogue databases, classifies sensitive data, and detects database vulnerabilities. It automates database discovery and provides visibility into unknown databases, identifying systems in scope for audits. Imperva also identifies security gaps, and automates your database security assessment process to detect vulnerabilities and misconfigurations.

Data activity monitoring

Imperva monitors database activity, detects and stops unauthorized data access, and simplifies compliance with data privacy and protection regulations. It enforces uniform security and compliance policy for data across on-premises and cloud environments, like Amazon Web Services (AWS) and Microsoft Azure. It also provides a single pane of glass monitoring across all types of data stores, including traditional RDBMS, big data and mainframes.

Data risk analytics

Imperva utilizes machine learning and behavior analytics to detect risky data access behaviors and unusual data activity, shortening the time to respond to a potential data breach. It prioritizes critical incidents and provides actionable insights while reducing the amount of alerts sent to the SIEM. Imperva Data Security tells you good users from bad users and detects insider threats, such as malicious, careless, and compromised users.

Data masking

Companies often make database copies to support different business initiatives, such as app development and testing QA. Imperva Data Security reduces the attack surface and sensitive data landscape via data masking. It de-identifies or pseudonomizes critical information with fictional but realistic values that maintains statistical and operational accuracy, enabling data utility without exposing sensitive data.

Identifying prospects

DATA BREACH RISK REDUCTION	**Is your customer concerned about undetected data breaches or insider threats?**	One of the biggest challenges that security professionals are facing today is that it can take months or even years to detect a breach. It's difficult to tell good users from bad users who could be malicious, careless, or compromised.
CLOUD MIGRATION	**Is your customer moving databases to the cloud?**	We're seeing more customers moving their databases to the cloud. However, they need to same visibility and security for data living in cloud databases that they have with their on premises environment.
COMPLIANCE NEEDS	**Does your customer need to comply with data protection and privacy regulations?**	Customers often need to comply with various data protection and privacy regulations such as GDPR, PCI DSS, HIPAA and more. When regulators show up, customers need to provide detailed reports to demonstrate compliance.

Who to engage

Imperva Data Security is typically owned by the security team. Because cyber security has become a board level concern, CISOs, Directors of Security and Risk Officers are a key sources of influence. Other key stakeholders that will play a role in the buying process include security operations, database operations and governance/risk/compliance teams.

Imperva data security is best suited for organizations who have large volumes of sensitive data, such as personally identifiable information or PII, that need to be protected. Customers typically initiate a project when their organization has experienced a data breach or a high-profile breach in their industry has occurred. Highly regulated and security conscious industries such as financial services or healthcare are also generally good targets.

Most security teams are overwhelmed with the number of security alerts.

FACT[1]

- Over 5200 breaches exposed over 7 billion records in 2017
- 78% of CISOs are concerned that breaches go undetected
- 54% of organizations ignore security alerts that should be further investigated
- $3.62 million is the average total cost of data breach
- CISOs #1 concern in 2018 is lack of competent in-house staff

- Pursure Initial Discovery with the CISO, Security Team or Risk Officer
- Use Discovery Questions to Identify Security Concerns
- Identify the Key Members of the Security Team
- Bring Potential Security Gaps to Light
- Bring Teams Together to Evaluate the Imperva Data Security Solution

[1] RiskBased Security-Data Breach QuickView Report, 2018, The Global CISO Study, ServiceNow, July 2017, Security Operations Challenges, Priorities, and Strategies, ESG, 2017, Ponemon- 2017 Cost of Data Breach Study, What CiSOs Worry About in 2018, Ponemon Institute, January 2018

Discovery questions

How confident are you that you know all the places sensitive data is stored? Listen for:

- Lack of visibility into where sensitive data is located
- Data spread across geographies and/or business units
- Sensitive data copied to non-production environments (e.g. Test and Dev or Data Analysts)
- Adoption of cloud infrastructure (e.g. Amazon Web Services/Azure)

How do you protect sensitive data like customer or employee personally identifiable information (PII)? Listen for:

- No or poor controls in place
- Concerns related to privileged users
- Lack of visibility into who accesses sensitive data

How does your security team know what is good vs. bad data access? Listen for:

- Challenges identifying risky data access
- Challenges keeping up with volume of alerts, false-positives and lack of actionable information
- Concerns that they are missing “real” incidents

What data protection or privacy laws does your organization need to comply with? How are you meeting those requirements today? Listen for:

- Multiple industry or government regulations like GDPR, PCI-DSS, SOX, etc.
- Failing past audits or need to address previous audit findings
- Challenges demonstrating they know where data is and who accesses what data

What would happen to you if your organization suffered a data breach? Listen for:

- Previous data breach at organization
- Company/board initiative to reduce breach risk
- Challenges related to detecting data breaches/reducing breach risk
- Challenges getting information to understand impact of breach (e.g. what and how many records were taken/altered)

Competitive landscape

Competitive solutions fall into roll your own or homegrown solutions, such as native audit logs dumped into a SIEM, or an enterprise data security solution like IBM Guardium.

IBM Guardium

Imperva beats IBM Guardium on analytics, effectiveness and total cost of ownership. Guardium is expensive to maintain and more cumbersome to deploy. A former Guardium customer was able to secure twice as many databases with Imperva data security with half the infrastructure required, decreasing deployment time and maintenance labor required. This led to lower total cost of ownership.

Native Audit + SIEM

Imperva beats the native audit plus SIEM approach on simplicity, effectiveness, and total cost of ownership. These homegrown solutions don't standardize log data across different database platforms, don't provide the database expertise and intelligence to identify meaningful incidents and often cost more when you factor in the people costs to build and maintain it.

What's in it for me?

Retire Quota Faster

Imperva Data Security deals can help you retire quota faster because they tend to be larger deals in the hundreds of thousands and even millions.

Growth Opportunity

In today's data driven world, customer's data environments continue to change and grow. As their environment grows, so does the opportunity to add Imperva Data Security to those new databases and platforms.

Simple, Easy-to-Understand Pricing

Imperva Data Security provides easy-to-understand pricing that is based on the number of databases that the customers want to protect. Our FlexProtect for Databases licensing program eliminates the need for complicated sizing exercises that can slow or stall a deal.

Sell with Confidence

Imperva Data Security is a proven data security product that delivers compelling value and differentiated capabilities.

Protect the pulse of your business.

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

+1 (866) 926-4678
imperva.com

imperva