Forrester Opportunity Snapshot: A Custom Study Commissioned By Imperva | January 2018

Modern Database Architectures Demand Modern Data Security Measures

GET STARTED ▶

Modern Database Architectures Demand Modern Data Security Measures

Introduction

The fast-paced, ever-changing nature of today's world requires businesses to be more innovative and flexible than ever before to keep up with the market. As part of this, enterprises are evolving their database ecosystems through cloud and big data initiatives to enable greater agility and scalability. However, in order to maximize these benefits while minimizing risk, companies must evolve their data security practices in parallel through modern tools, such as database activity monitoring (DAM), to align with new imperatives for cloud computing.

In November 2017, Imperva commissioned Forrester Consulting to conduct a study of IT professionals to explore current security and compliance challenges faced by companies who are evolving their database ecosystems through cloud and big data initiatives. The objective was to understand how companies are approaching these challenges and understand what steps they are taking to ensure greater security and compliance with their databases.

DEMOGRAPHICS

Region

150 respondents from US-based companies

Company size (employees)

› **39% -** 1,000 to 4,999
› **28% -** 5,000 to 19,999
› **33% -** 20,000 or more

IT roles

› **28% -** Operations
› **28%** - Security and risk
› **25%** - Enterprise architecture
› **19% -** App dev

100% of companies surveyed are currently using big data or cloud-based database architectures.

Modern Database Architectures Demand Modern Data Security Measures

OVERVIEW   **SITUATION**   **APPROACH**   **OPPORTUNITY**   **CONCLUSIONS**

1 2 3

Security And Compliance Are Increasingly Important As Database Architectures Evolve

More and more companies today are adopting, or looking to adopt, big data and cloud-based architectures to meet growing business demands. As part of this trend, companies are also aware that security and compliance initiatives must adapt to keep pace with the nature of these new tools. In fact, over 50% of companies consider security and compliance to be significantly more important than before as they implement these new architectures.

How do security and compliance needs shift, as database architectures consolidate data onto big data platforms and/or migrate to the cloud?

- Somewhat more important
- Significantly more important

Security (data protection, identity and access management, incident response, etc.)   36%   57%

Compliance (HIPAA, GLBA, GDPR, FERC/NERC, SOX, etc.)   36%   51%

Base: 150 enterprise data security decision makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Imperva, November 2017

Modern Database Architectures Demand Modern Data Security Measures
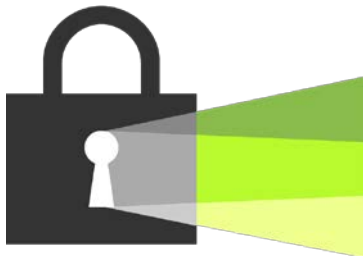
OVERVIEW   **SITUATION**   **APPROACH**   **OPPORTUNITY**   **CONCLUSIONS**

1 **2** **3**

Yet Companies Feel Underprepared To Deliver On Key Security Capabilities

When asked how important specific security capabilities were for securing new database environments, respondents placed high importance on capabilities such as sensitive data discovery or classification, vulnerability scanning and management, and automated analytics to detect breaches. However, when asked how prepared their organization was to deliver on those capabilities, the level of preparedness was very low. This highlights a major challenge as companies know what needs to be done to enable better security, but they lack the capabilities to do so.

How important are the following security capabilities and how prepared is your company to deliver on them?

■ Very important   ■ Very prepared

Capability	Very important	Very prepared
Sensitive data discovery or classification	41%	23%
Vulnerability scanning and management	38%	23%
Automated analytics to detect compliance violations or security breaches	33%	17%
Privileged user monitoring	26%	17%

Base: 150 enterprise data security decision makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Imperva, November 2017

Modern Database Architectures Demand Modern Data Security Measures

OVERVIEW   **SITUATION**   **APPROACH**   **OPPORTUNITY**   **CONCLUSIONS**

1 2 3

And Companies Face Similar Execution Challenges With Compliance

The story is the same with compliance. Companies place high importance on compliance capabilities such as proof of compliance, report automation, and privileged user audit. However, most companies are not well prepared to deliver on those capabilities. Overall, roughly three out of four companies do not feel very well prepared to delivery on any of their most important compliance capabilities. Compliance often goes hand in hand with security, and these challenges can be very damaging if not corrected.

How important are the following compliance capabilities and how prepared is your company to deliver on them?

■ Very important   ■ Very prepared

	Very important	Very prepared
Proof of compliance	46%	25%
Compliance report automation	32%	34%
Privileged user audit	27%	26%
Change reconciliation control	25%	20%

Base: 150 enterprise data security decision makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Imperva, November 2017

1

Security And Compliance Preparedness Is Impeded By Various Challenges

Maintaining a secure grip on big data and cloud-based databases is a difficult thing to accomplish. These new architectures introduce challenges around data protection, governance, scale, and system compatibility. Due to loss of direct physical control over the infrastructure, where data is housed as companies move their data to the cloud, concerns are high regarding the authorization of third-party control/access and monitoring of company data. Visibility and ownership of large data sets are reasons for concern as well.

System compatibility can also be hard for companies that are used to doing things the same way for so long. Legacy security measures may no longer be sufficient to cover new infrastructures; this forces companies to revise their approach. The lack of compatibility can lead to governance and visibility concerns, as companies struggle to ensure all systems are compatible and all data is properly protected.

What are the primary challenges your company faces with being better prepared to manage security and compliance?

Challenges with compatibility with other systems	46%
Internal data governance concerns	37%
Concern over third-party administrator access to my database	35%
Lack of visibility into database operational activity	33%
Not having direct ownership of architectures	31%

Base: 150 enterprise data security decision makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Imperva, November 2017

1 2

New Architecture Decisions Must Be Driven By Security, Agility, and Scalability

Even though many companies feel ill-prepared to deliver on new security and compliance capabilities with big data and cloud-based database architectures, most recognize that in the long run that these new architectures will enable them to be more secure and agile as a business. To achieve the benefits they want from their new architectures, companies identified their top five security and compliance capabilities which focus first on added security, but also include capabilities that enable companies to be more agile, such as automated analytics and consistent policies across databases, data lakes, etc.

Top 5 most important data security and compliance capabilities

Capability	
Vulnerability scanning and management	60%
Automated analytics for security/compliance	53%
Sensitive data discovery or classification	48%
Proof of compliance	45%
Consistent policies across data in RDMS, data lakes or cloud	43%

Base: 150 enterprise data security decision makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Imperva, November 2017

1 2

Database Activity Monitoring Tools Outperform Expectations For Security And Compliance Capabilities

To compensate for their preparedness gap with security and compliance capabilities, many companies are leveraging DAM tools to bring much needed visibility and control to their processes. DAM tools offer 1) monitoring of database activity to prevent internal and external fraud, 2) integration with identity directories and access management systems, 3) user activity analysis and threat detection, 4) data classification and discovery, and 5) governance to bridge monitoring and access control gaps between on-premises and cloud-based data assets.

Companies' initial expectation of DAM tools focuses on reducing security incidents and improving compliance, coupled with the hope of reducing time spent on security. Companies with DAM tools already in place reported these outcomes as realized; most notably with compliance and number of security incidents. The one instance where the realized benefit didn't surpass the expected benefit was with time spend on security. However, the reality is that tools such as DAM can offer greater security confidence and capabilities, but cannot be seen as a replacement for dedicated security and compliance efforts from IT teams.

Expected versus realized benefits of DAM solutions

■ Expected   ■ Realized

Benefit	Expected	Realized
Improved data compliance	40%	61%
Reduced number of security incidents	44%	49%
Better ability to create business intelligence based on data movement and transactions	31%	44%
Greater security confidence	31%	43%
Lower cost of investigation	39%	40%
Less time spend on security from IT teams	42%	30%

Base: 150 enterprise data security decision makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Imperva, November 2017

Modern Database Architectures Demand Modern Data Security Measures

Conclusion

New big data and cloud-based database architectures are being adopted in greater number due to the businesses advantages they provide, particularly in regard to added business agility and scalability. However, those benefits will be quickly eclipsed by security and privacy concerns if companies are unable to properly govern, discover, monitor, and secure those databases and ensure regulatory compliance, i.e., PCI, SOX, HIPAA, GDPR, etc.

Establishing a zero trust framework within the firm's data assets is impossible without controlling data, injecting identity into data assets (ownership, authorizations for the use of data, etc.), and controlling data paths on the network.

To achieve the above, firms need the automation, governance frameworks, proper tools, and capabilities to help them secure their data adequately and cost-effectively in hybrid cloud and on-premises environments. Database activity monitoring (DAM) solutions play a great role in providing companies with the right visibility, control, and automation to give them the confidence they need to know their data is secure and that they meet data protection and privacy compliance regulations.

METHODOLOGY

- This Technology Adoption Profile was commissioned by Imperva.

- The custom survey questions were fielded to 150 data security decision-makers at US enterprises with 1000+ employees managers.

- The customer survey was completed in November 2017.

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

Project Director

Chris Taylor
Sr. Market Impact Consultant