Informatica

White Paper

Data-Centric Security for a Hybrid World

GDPR compliance in cloud and on-premises environments

About Informatica

Digital transformation changes expectations: better service, faster delivery, with less cost. Businesses must transform to stay relevant and data holds the answers.

As the world's leader in Enterprise Cloud Data Management, we're prepared to help you intelligently lead—in any sector, category or niche. Informatica provides you with the foresight to become more agile, realize new growth opportunities or create new inventions. With 100% focus on everything data, we offer the versatility needed to succeed.

We invite you to explore all that Informatica has to offer—and unleash the power of data to drive your next intelligent disruption.

Table of Contents

Executive Summary

Most organizations today store sensitive customer, product, and other essential data in an increasing number and variety of platforms and physical locations across the globe. This business-critical data is often located in public cloud, on-premises, and Software as a Service (SaaS) applications. With Informatica Intelligent Cloud Services™, for example, Informatica provides infrastructure security in the form of failover data centers, user authentication and access control, network security protocols, encryption, and security layers at the operating system, database, and application levels.[1]

Hybrid environments provide new challenges for data compliance and security teams. The dynamic nature of data, users, and applications requires additional measures to ensure that the organization's critical data is tracked, understood, and protected always. The risks are not hypothetical, as demonstrated in high-profile cloud and on-premises breaches and by the fines from new regulations such as the General Data Protection Regulation (GDPR).

In these dynamic hybrid environments, you need the intelligence and automation to ensure sustained data protection and compliance, with the ability to answer questions such as the following:

- Where is all the data that needs to be protected?
- Who is accessing data with what applications?
- Does current access and use adhere to regulations and data-use policies?
- Are data protections appropriate, and is data risk remaining at acceptable levels, or are there conditions creating more risk that we should remediate?

The results of the discovery and classification of sensitive data become the foundation for decision support regarding data risk, security, and compliance in a hybrid data ecosystem. This paper provides a framework of security considerations and strategies in hybrid environments with a data-centric approach that can:

- Apply analytics, automation, and artificial intelligence (AI) to identify and protect sensitive data from all sources in a hybrid environment, using a single interface for dashboards and reporting.
- Comply with evolving data governance and security regulations.
- Provide audit readiness.
- Alert key stakeholders when anomalous user behavior occurs.

Informatica Data Masking and Informatica Secure@Source® provide exceptional capabilities to perform these functions, adding an integrated, data-centric layer of security for all sensitive data sources in a hybrid ecosystem.

[1] Monahan, David, "Informatica Cloud Security Architecture Overview," Enterprise Management Associates (EMA), March 2016.

Data Security for Your Hybrid Reality

According to research firm IDC, the world is predicted to create 180 zettabytes of data in 2025, up from less than 10 zettabytes in 2015.[2] Organizations across all industries rely on the accuracy, availability, and security of their data to generate revenue, serve customers, increase productivity, and support other mission-critical business processes.

The continued exponential growth in data volume and usage also includes sensitive data across multiple silos, both on-premises and in the cloud, and in a variety of data formats. These conditions have rendered traditional data security methods obsolete, requiring a new approach to data security across an organization.[3]

There is also a strong trend where a large percentage of the data an organization uses is coming from external sources. It is critical to understand the sensitivity of this data at the time it is onboarded into the organization and before it is proliferated to multiple systems and analytics uses. However, most companies cannot accurately identify where all their sensitive data is located, especially if it is in unstructured formats or across various on-premises and cloud applications, relational databases, data warehouse appliances, and big data sources. This lack of knowledge increases an organization's risk, and for these reasons, data breaches are currently the top IT security risk.[4]

With data breaches on the rise, in tandem with the proliferation of sensitive data, organizations must develop a risk mitigation strategy that includes a data-centric security product with these key features:

- Visibility into all data sources to locate and classify sensitive data from across the organization.
- Ability to implement protection mechanisms for sensitive data to mitigate breaches.
- Compliance with current data security and privacy regulations, including the use of automation and AI to monitor user behavior and report anomalies in near real time.
- Rich analytic visualization tools for sensitive data management.
- Transparent and robust reporting capabilities for audit readiness.

Gartner predicts that by 2020, data-centric audit and protection products will replace disparate siloed data security tools in 40% of large enterprises, up from less than 5% today.[5] These data-centric protection solutions, including Informatica Data Masking and Informatica Secure@Source, provide a centralized view of at-risk data so that all key stakeholders across an organization can track sensitive data movement and apply protection mechanisms as required by governance policies and regulations.

[2] "2016 IoT Midyear Review – The Report Card for Everyone," IDC, August 4, 2016.
[3] "Market Guide for Data-Centric Audit and Protection," Gartner, March 21, 2017.
[4] "Data Breaches and Sensitive Data Risk," Ponemon Institute, February 2016.
[5] "Market Guide for Data-Centric Audit and Protection," Gartner, March 21, 2017.

Four-Point Strategy for Protecting Sensitive Data

"Sensitive data risk" is the impact of losing sensitive data, and the leading cause of this loss is a data breach. A common misperception is that simply locating sensitive data is enough to remediate risk. However, locating and classifying this data is only the first step in a comprehensive risk remediation strategy.

The next steps involve assessing your organization's risk based on the results of the location and classification analysis and determining a strategy for reducing the risk that involves all key stakeholders—not just the IT organization—with automated controls that enforce data governance policies. Your strategy should also include procuring and implementing a robust, data-centric security product that provides capabilities for regulatory compliance, rich analytic visualizations of sensitive data for dashboards and audit reporting, and protection for all sensitive data types across the organization. The chosen data-centric security product must also protect sensitive data from all sources in your hybrid environment: public cloud, SaaS applications, on-premises applications and databases, unstructured data, and data warehouse appliances.

1. Discovery and Classification

A common approach to discovery is to review existing sources and send questionnaires. However, this highly manual approach is inadequate because it consumes valuable time and resources and it is often inaccurate and out-of-date, with reliance on self-reporting rather than actual monitoring of user behavior.

Organizations need to ask themselves:

- What data do we store, who has access to it, and for what purposes?
- How do we manage user privileges and data rights?
- How will we protect sensitive data and ensure that the appropriate controls are in place?

Other considerations for discovery and classification compliance include:

- Defining and understanding your data landscape (including on-premises and cloud databases, applications, and unstructured data).
- Building a plan to manage externally sourced data.
- Mapping which systems contain sensitive data.
- Procuring a solution that can map the movement of the data across your ecosystem, while maintaining a near-real-time view with analytics and reporting tools.

2. Compliance

Organizations struggle to identify, monitor, and remediate data risks to comply with data privacy and security regulations. Further, they must monitor, analyze, and alert on data access or movement that could jeopardize compliance.

The GDPR, enforceable from May 25, 2018, was adopted with the intent to strengthen and unify data protection for all individuals within the European Union, thereby simplifying the regulatory environment for international business. Many businesses have not yet prepared for this regulation and will not be sufficiently compliant; but noncompliance could result in significant fines and reputational damage. On the other hand, compliance can provide the opportunity for competitive advantage as a sensitive data privacy and security differentiator, while also driving data-driven digital transformation outcomes.

Organizations need to develop intelligent policies that identify data stores that contain GDPR-relevant "data domains." These policies are multifactor, with logic that determines which combinations pose a privacy threat.

3. Protection

In 2017, there were 1,120 data breaches with a total of nearly 171 million records exposed.[6] Clearly, despite large investments in infrastructure-level security, critical data remains vulnerable. Organizations need to continuously secure high-risk data, identify suspicious behavior and unauthorized use or movement of critical data assets, and automate and orchestrate remediation.

Organizations should identify critical data risks and remediate them with data-centric controls (rather than classic cybersecurity tools). For example, these controls include data masking and encryption solutions. In addition, organizations should monitor user access and behavior. Excessive data access or unusual behavior can indicate that users are not adhering to privacy policies or that their credentials have been stolen.

4. Audit Readiness and Response

Companies undergo more audits and assessments of sensitive data than ever before. They struggle to provide proof to auditors that they have visibility and protection of critical data.

Organizations should be able to immediately respond to auditors and provide evidence that they know where data exists, what the data's risks are, how the data is protected, and how the data is being used. They should consider that auditors will want reports and visualizations that are abstracted for departments or locations and that provide the ability to drill-down on specific data domains.

[6] "2016 Data Breach Category Summary," Identity Theft Resource Center, December 31, 2016.

Conclusion

Top-tier infrastructure security protocols are necessary to protect any hybrid environment that transmits confidential data to users, data center servers across the globe, and throughout cloud applications. The continued onslaught of data breaches and growing compliance requirements indicates that organizations must implement adequate processes and tools for identifying, analyzing, and protecting sensitive data.

In the current climate of heightened security risk and regular data breaches, companies must develop a robust digital security strategy to continuously monitor, analyze, and remediate risks to their sensitive data. They need to monitor data in near real time for signals of misuse or breach, excessive access, unusual behavior, or cross-border transfers. With data-centric security solutions such as Informatica Data Masking and Informatica Secure@Source, organizations can improve their data risk posture to help mitigate the impact of data breaches or internal misuse and meet the stringent requirements of regional and industry regulations.

Recommendations

1. Perform a risk assessment to gain a clear understanding of where your sensitive data is located, how far it propagates through your data ecosystem, and which sets of sensitive data are most vulnerable.
2. Based on your assessment results, prioritize your organization's top ten sources of the most sensitive data; determine a strategy and product for protecting it; and implement the strategy for data security.
3. Define, document, and distribute your organization's compliance policies and the key stakeholders that are accountable for GDPR compliance. Build a strategic plan for May 2018 and beyond.

More Information

For more information about sensitive-data security risks and protection considerations, refer to the following publications:

- "Detect and Protect: A Data-Centric Approach to Security," Informatica, April 2017.
- "Data Breaches and Sensitive Data Risk," Ponemon Institute, February 2016.

Informatica

Worldwide Headquarters 2100 Seaport Blvd., Redwood City, CA 94063, USA Phone: 650.385.5000, Toll-free in the US: 1.800.653.3871

IN09_0418_03429