happiest minds
The Mindful IT Company
Born Digital . Born Agile

Data Centric Security Infrastructure

Yasar Shaikh

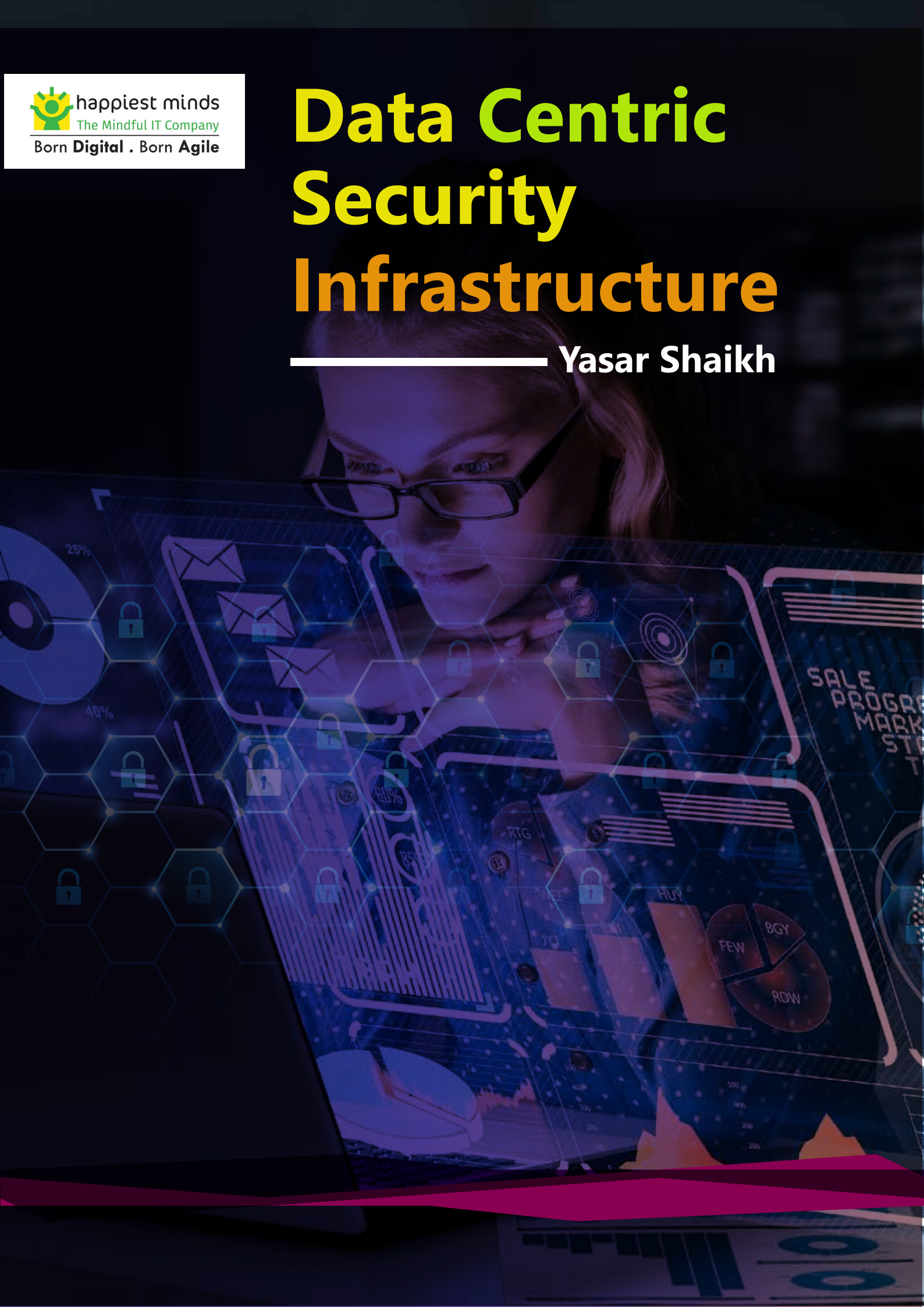

Table of Contents

Executive Summary

Many organizations today gather and store sensitive product, customer, and other vital data in various platforms and physical locations throughout the globe. This sensitive and business-critical data is often stored in a public cloud, on-premises, and Software as a Service (SaaS) applications.

Hybrid environments give new challenges to information compliance and security groups. The dynamic nature of knowledge, users, and applications need extra measures to confirm that the organization's critical information is tracked, understood, and guarded continually. The risks aren't theoretic, as incontestable in a high-profile cloud and on-premises breaches and by the fines from new rules like the General Data Protection Regulation (GDPR).

In these dynamic environments, you require the insight and robotization to guarantee supported information security and compliance, with the capacity to address the following:

- Where is all the information that needs to be secured?
- Who has access to the Data and with what Applications?
- Do current access permissions and use the meet to regulations and data-use policies?
- Are Information Security Controls appropriate, and is data risk constant at acceptable levels, or are there conditions that require immediate remediation and warrant more risk?

Discovery and Classification results of the confidential data become the pillars for decision support about data security, Risk & Compliance in a data ecosystem. The information below in the article provides the basics of security considerations in a typical environment with an approach focused on data centricity that can:

- Application of analytics, artificial intelligence, and automation to discover and protect the confidential information through all risk vectors in an environment, using a single application/interface for on-demand/BAU Dashboards and audit reporting.
- Compliance with changing data governance and other security regulations.
- The approach should provide Audit Readiness.
- Notify key stakeholders when suspicious user behavior occurs.

Data Centric Security For Your Organization

As per research firm IDC, it is predicted that the world will create about 180 Zettabytes of data by the end of 2025. The number had gone up from 10 Zettabytes in 2015. Every Organization across any industry rely upon their data to be accurate, available and secure so that it can generate business, service customers, raise productivity and support other critical business processes.
The constant rising growth in data volumes and usage also covers confidential data across different silos (on-prem & cloud) in various data formats. Due to these conditions, traditional data security methods have become obsolete thus demanding a new approach for data security in an organization.

A strong trend also reflects that a significant chunk of data which an organization uses comes from external sources. It is essential to understand the confidentiality of this data when it enters the organization before it is reflected across multiple systems. However, most companies fail to identify the location of their sensitive data more often if the data comprises of unstructured formats across applications (on-prem & cloud), significant data sources, relational databases, and data warehouse appliances. Due to the Organizations risk being increased due to this lack of knowledge, Data Breaches have currently become a top IT security risk.

With data breaches increasing rapidly, in conjunction with the increase of sensitive data, organizations must design a risk mitigation strategy that includes a data-centric security solution having the following features:

- Ability to scan, discover and classify sensitive and confidential data across the entire organization.
- Ability to implement protective responses to mitigate breach at times painful data loss.
- Should be compliant with all data security and privacy regulations includ ing regulation and laws that talk about the use of AI and Automation to monitor user behavior and report incidents in real time.
- Should support and provide excellent visual analytic for sensitive data management.
- Should ensure Audit readiness by providing Transparent and robust reporting capabilities.

It is predicted by Gartner that by 2020 data-centric audit and protection product will replace disparately placed data security tools in almost 40% of large organizations, up from 5% today. These data-centric solutions provide a comprehensive view of Data at risk which helps all key business resources across an organization can monitor the movement of sensitive data and apply responses as dictated by government policies and regulations.

Four Fold Approach for Sensitive Data Protection

"Sensitive data risk" is the term used to describe the loss of sensitive data and the leading cause of this loss is a data breach. A widespread misconception though is that risk remediation can be achieved only by simply location sensitive data. However, discovery and classification are the first steps in a comprehensive risk remediation strategy.

The next moves involve evaluating the organizations' risk on the basis of location and classification analysis and formulating a strategy to reduce the risk that involves major key business owners and not just the IT organization with defined controls that publish data governance policies. The strategy should also include a plan to procure and implement a robust data-centric security solution that provides functions for regulato-ry compliance, analytic visualizations of sensitive data for dashboards and reporting and protection of complete sensitive data across the organization.

Discovery and Classification

A common practice for discovery is to examine the existing data sources and send questionnaires. However, this approach is highly inadequate as it is very time consuming and utilizes a high resource. It also makes it highly inaccurate and out of date with more reliance on self-reporting rather than monitoring user behavior.

Organizations need to assess:

- What data is stored and who has access to it and for what purpose?
- How are user privilege and data rights managed?
- How will sensitive data be protected and what are the appropriate controls are in place?
- Other considerations for discovery and classification compliance include:
- Scape and understanding your data landscape (including on-premises and cloud databases, applications, and unstructured data).
- Design a plan to manage externally sourced data.
- Mapping which systems contain sensitive data.
- Implementing a solution that can track the movement of the data across your ecosystem, while maintaining a near-real-time view with analytics and reporting tools.

Compliance

Organizations find it difficult to identify, monitor, and remediate data risks to meet with data privacy and security regulations. Additionally, they must also monitor, analyze, and alert on data access or movement that could risk compliance.

The GDPR Regulation which came into existence from May 25, 2018, was implemented with the purpose to strengthen and unify data protection across the European Union, thus simplifying the regulatory landscape for international business. Many businesses have not organized themselves for this regulation and will not be necessarily compliant, and non-compliance can lead to major fines and damage in reputation. Secondly, compliance with regulations can provide the organization with a competitive advantage as a data privacy and security differentiator, while also driving the outcomes for a data-driven digital transformation.

Organizations need to design effective policies that discover data stored that save GDPR-relevant "data domains." These are most multifactor policies with rules that regulate which combinations possess a privacy threat.

Protection

There were 1,120 data breaches and a total of about 171 million records exposed in the year 2017. Despite considerable investments in the Infrastructure level security, sensitive data remains at risk. Organizations need to work on securing the high-risk data constantly, suspicious discovery behavior, respond to unauthorized use or movement of sensitive data assets and automate remediation.

The organization should be able to discover confidential and sensitive data risks and remediate them with controls that a data-centric rather than traditional cyber security tools. For instance, these controls cover data masking and encryption solutions. Additionally, organizations should also monitor user behavior and access controls. Excessive Data Access or unusual behavior can point to the fact that users are not following privacy policies or their credentials have been compromised.

Audit Readiness & Response

Companies are constantly going through the audit scrutiny and assessments of sensitive data, and most times they struggle to provide auditors that they are in control and have complete visibility of their confidential data. Organizations should be equipped to respond to auditors and prove that they have visibility about the data location, risks and how it is protected & used. They should account for the fact that the auditors would request reports and visual summary based on departments or locations that can further help to monitor specific data domains.

Conclusion & Recommendations

Conclusion

Top of the line Infrastructure security protocols is needed to safeguard any environment that sends confidential data users, servers across the globe, cloud application, etc. The increasing data breaches and growing requirement to meet compliance regulations indicate that an organization must implement the right processes and solutions for discovering, analyzing, and protecting sensitive data.

In the present scenario where security risk is heightened, and data breaches have become common, the company must resort to a digitally robust security strategy to constantly monitor, assess and respond to threats to their confidential information. Organizations need real-time monitoring of data misuse, behavior anomalies, correct access controls. With data-centric security solutions available to address this pressing need, organizations can improve their security landscape and avoid the impact of data breaches and help them meet the strict regional and industrial 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.

About Author

Yasar Shaikh represents the Data Security Practice at Happiest Minds. He is a Computer Science Graduate with an MBA degree in Information Systems. Having worked on multiple security solutions, Yasar has a strong understanding of the Data Security Lifecycle and Landscape and can assess, manage and deploy most of the solutions that fall under the Data Security umbrella. In Addition to Data Security, Yasar also has good experience and knowledge in Data Center Management for Large Organizations.

About Happiest Minds Technologies

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, AI & Cognitive Computing, Internet of Things, Cloud, Security, SDN-NFV, RPA, Blockchain, etc. Positioned as "Born Digital . Born Agile", our capabilities spans across product engineering, digital business solutions, infrastructure management and security services. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality.

Headquartered in Bangalore, India Happiest Minds has operations in USA, UK, The Netherlands, Australia and Middle East.

To know more about our offerings. Please write to us at **business@happiestminds.com**