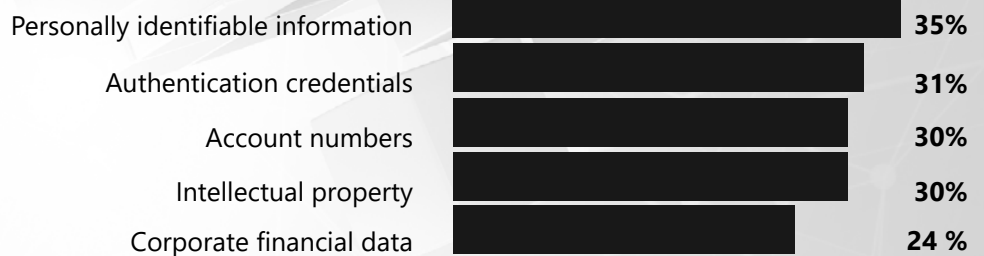# Data Security Services

By 2020, Data-Centric audit and protection products will replace disparate, isolated Data Security tools in **40%** of large enterprises, up from less than **5%** today say Gartner, a leading research and advisory company.

Data Security Governance and the Orchestration of the policies across disparate data silos and platforms will be critical challenges for organizations over the next decade.

" **What types of data were potentially compromised or breached in the past 12 months?** "

(Multiple responses accepted)

Personally identifiable information	35%
Authentication credentials	31%
Account numbers	30%
Intellectual property	30%
Corporate financial data	24 %

Base: 371 North American and European network security decision makers whose firms have had a security breach in the past 12 months
Source: Forrester Data Global Business Technographics* Security Survey, 2017

18% reported payment/ credit card data as potentially compromised

Key Business Drivers for Data-Centric Security

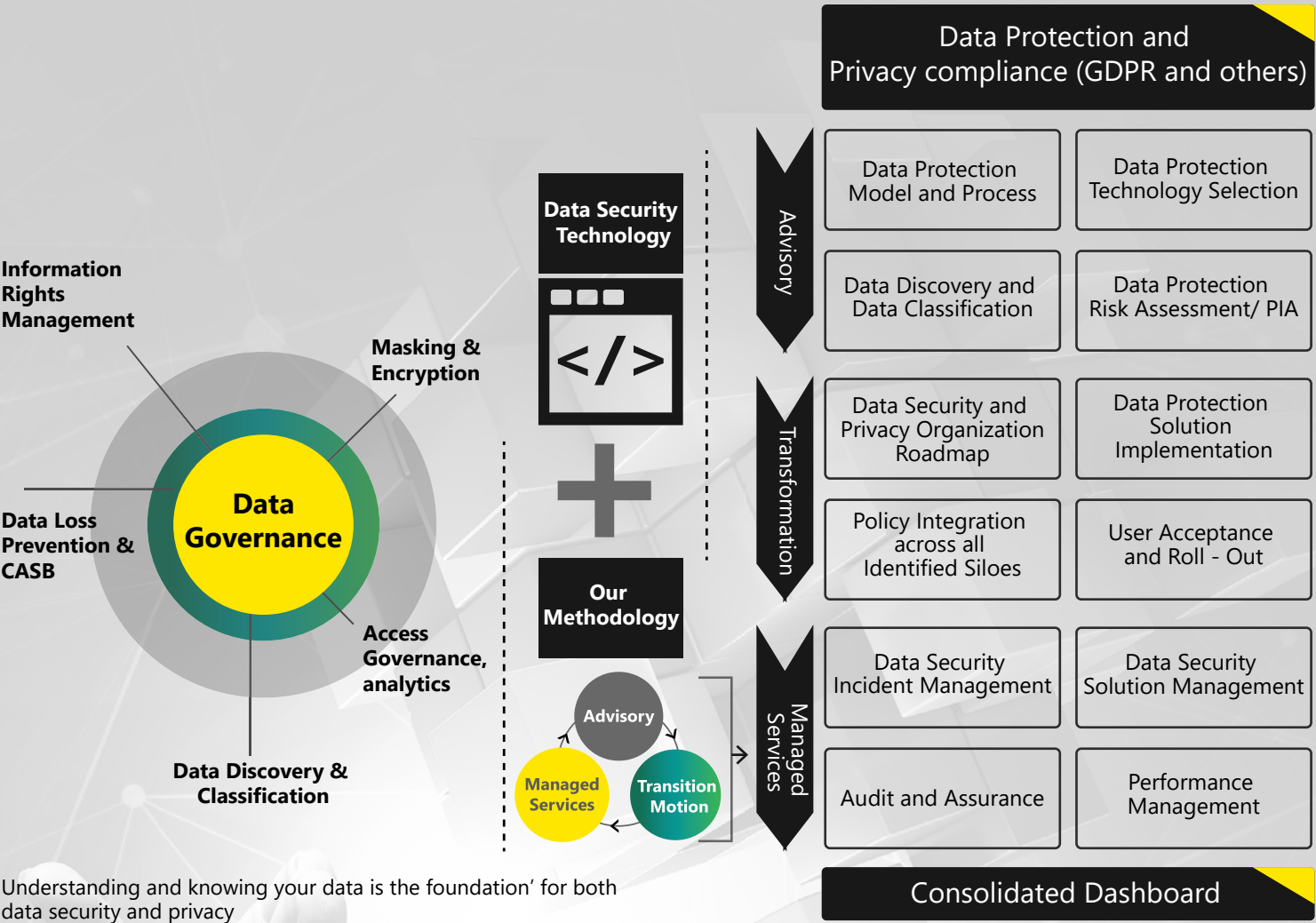|	
The Velocity of Sensitive Data:	The exponential growth of personal and sensitive data processing in segregated environments is challenging for the current data security methods, skill-sets, and technology.
Regulatory Landscape:	Rapidly evolving Data Privacy and Security Regulatory landscape globally. For example, EU GDPR introduces stringent data security and privacy requirements.
Variety of Sensitive Data:	Sensitive Data is not constrained to any storage silos but is rapidly proliferated by digital business processes and applications in structured and unstructured on premise silos, and in public clouds.
The Volume of Third Parties:	With Augmented data flow across global partner network and lack of holistic Data Governance, third party Data Security risk continues to rise.
Siloed Approach:	Disconnected team and non-coordinated approach to discover, manage, protect and monitor the sensitive and confidential data.
Data Breaches:	Organizations are facing an increasing wave of publicized data breaches resulting in significant financial liabilities, brand damage and loss of customers.

Happiest Minds Data Security Solution Offerings

Data Protection and Privacy compliance (GDPR and others)

Information Rights Management

Masking & Encryption

Data Governance

Data Loss Prevention & CASB

Access Governance, analytics

Data Discovery & Classification

Data Security Technology

`</ >`

+

Our Methodology

Advisory

Managed Services

Transition Motion

Advisory	
Data Protection Model and Process	Data Protection Technology Selection
Data Discovery and Data Classification	Data Protection Risk Assessment/ PIA

Transformation	
Data Security and Privacy Organization Roadmap	Data Protection Solution Implementation
Policy Integration across all Identified Siloes	User Acceptance and Roll - Out

Managed Services	
Data Security Incident Management	Data Security Solution Management
Audit and Assurance	Performance Management

Consolidated Dashboard

Understanding and knowing your data is the foundation' for both data security and privacy

---

Happiest Minds Data-Centric Solution Key Use Cases

Problem: Understanding the why, what, how and who of PII your organization process and get processed
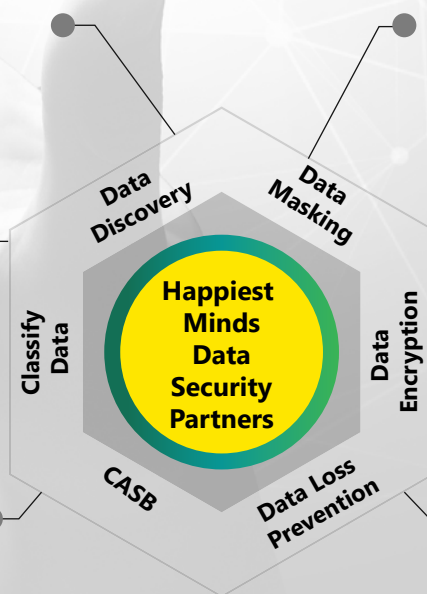**Solution:** ePII discovery and mapping with drill down and filtering mechanism
USP: This is the foundational requirement for SARs

Problem: PII needs to be protected and simultaneously usable during various stages of business process
Solution: De-identify the specific data set dynamically without need of a separate key management process

Problem: Basis for deploying required data security controls is missing or not effective. Lack of user awareness on data sensitivity
Solution: Architect classification schema and classify all existing and new data/metadata

Problem: Hacker and insider threats pose increasing risk to sensitive data in storage mediums and during transit
Solution: Encrypt data and decrypt during its use with secure keys

Problem: Lack of doud user access and device governance (including shadow IT)
Solution: Visibility into cloud application usage, Securing cloud services by detecting anomalous activity and setting homogenous security policies and controls

Problem: Prevent leakage and unauthorized access to sensitive information in motion or at rest
Solution: Ensures critical data is only leaves the network when approriate. Analyze, track and report data usage pattern

Happiest Minds Data Security Partners

- Data Discovery
- Data Masking
- Classify Data
- Data Encryption
- CASB
- Data Loss Prevention

For a Global Professional Services Firm

About Customer

Customer is a professional service accounting, tax, HR and payroll service firm, operating on an international scale. With a network of offices across over 80 countries, they have the in-country expertise and knowledge to help businesses expand and operate both within and beyond their home markets.

Strategy and Objectives

- Value from investment into security programs to protect the customer's data and comply with local offices regulatory requirements on data security
- Implementing an enterprise wide data security encryption solution to protect critical data from possible misuse and compromise
- Secure cloud environment and provide real time data protection

Service Offered

- Protect Data at Rest and when services are online
- Protect Database at Rest and when online
- Protect Office 365 Messaging platform. SharePoint online, One Drive
- Protect VM's in phase 1 for 14 sites – 120 servers
- Controlled secure keys by their respective location administrators
- Auditing and SIEM integration

Value Delivered

Encrypting critical and sensitive data across 1200+ server hosted across the globe and in cloud environment

Improved Risk and Compliance posture with automated breach reporting.

Centralized management of keys to assure control of data across every physical and virtual server

Efficient management of data-at-rest security across the enterprise

Protect Data at Rest
critical and sensitive data
Efficient management
automated breach reporting
Auditing and SIEM

Design and Implementation of Data Governance solution

German investment bank and financial services firm

About Customer

German investment bank and financial services company headquartered in Frankfurt, Hesse, Germany. The company is a universal bank resting on three pillars – the Private & Commercial Bank, the Corporate & Investment Bank (CIB) and Asset Management (DWS)

Strategy and Objectives

- Addressing the regulatory and compliance concerns related to data access governance
- Reduce / Eliminate the overhead in Manual access management
- To save time, resources, compliance costs, and complication

Service Offered

- Assessment of current data architecture
- Toll set-up documentation
- Roll out of data access governance platform
- User acceptance functional and operational tests
- User training
- Ongoing support and management

Value Delivered

🕐	**Reduce the time it takes to identify a data breach, from months to minutes**
◎	**Pinpoint the exact location of sensitive data across the enterprise and in the cloud.**
◉	**Understand what sensitive data is connected to and mingling with, and who is accessing it**
🛡	**Protect sensitive data at the element level with masking and encryption strategies**

Our partners

Microsoft | trust hub | TITUS | EXONAR | FORCEPOINT | McAfee | CYBERARK

skyhigh | DATAGUISE | THALES | SECLORE | VARONIS | boldonjames

happiest minds
The Mindful IT Company
Born Digital . Born Agile

Business Contact
business@happiestminds.com

Media Contact
media@happiestminds.com