Cyral

Understanding and Navigating the Data Security Landscape

In today's data-driven world, robust data security is a paramount concern for enterprises due to the prevalence of cloud computing, volume of data, services and identities and the escalating sophistication of cyber threats.

Organizations must safeguard their sensitive information from unauthorized access, breaches, and data loss in this challenging environment of rapidly proliferating data.

Many enterprises are overwhelmed with complexity when establishing effective security programs and selecting appropriate tools for data security. This whitepaper aims to cut through this confusion by providing a concise and strategic overview of the data security landscape. We present a framework that enables organizations to establish data security programs across their diverse services and infrastructure. Instead of prescribing specific step-by-step actions, the whitepaper emphasizes a strategic approach and highlights various tools and technologies for specific situations.

This whitepaper builds on top of a typical data security maturity model framework (like the one here: **https://docs.datasecurity.org/**). DSMM frameworks talk about technology, people, and processes, whereas this document aims to outline which tool to use in which situation.

Table of Contents

Outline for this framework

Cyral

1. Outline a set of controls that should be implemented as part of any data security program.

2. Provide a strategy for bucketing the various structured and unstructured datasets that your organization has to determine where these controls should be applied.

3. List out a recommendation of various types of products that are appropriate for each combination of control and the dataset type.

Data security controls

Cyral

The initial and essential step in any security program is to establish a set of controls that are suitable for the organization. For a data security program, your organization should consider the following controls:

- **Monitoring:** real-time monitoring of who accessed what data
- **Reporting:** tracking any changes in configuration and entitlements
- **Discovery:** data scanning, classification, and cataloging
- **Access Management:** federated authentication and authorization
- **Protection:** ensure data integrity and prevent tampering and corruption
- **Confidentiality:** secure data using masking, tokenization, etc.

These controls must be applied equally to privileged users, application users and any services.

Data governance programs often include two additional controls:

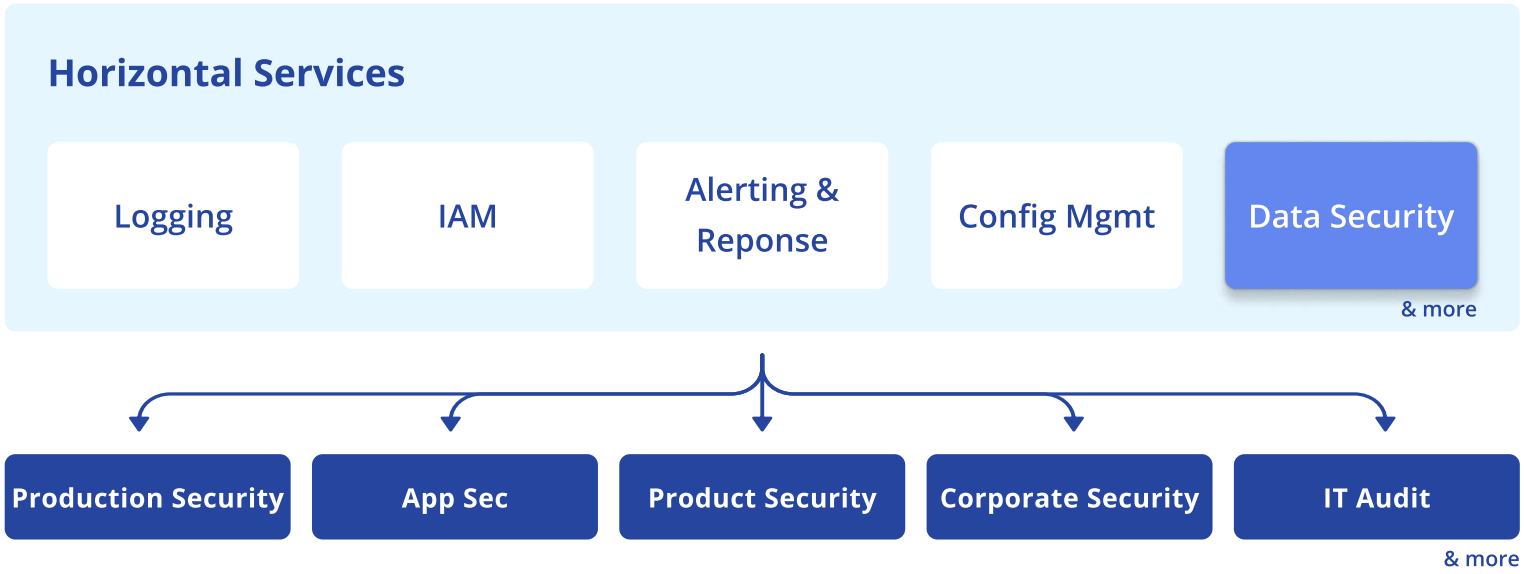
- **Data retention:** enforcing how long data is retained for and when/how it's deleted
- **Data ownership:** tracking who the custodian of specific datasets is

Because these controls pertain to data governance rather than data security, we do not explicitly include them in this framework.

It is essential to address encryption in a whitepaper on data security as it constitutes a fundamental component of any security program. It is a very strong and important control that should be regarded as an industry best practice. Our approach complements various encryption strategies employed for data at rest, in transit, and in use.

Ownership of these controls

All security controls are generally implemented as either a set of horizontal services shared across various security programs, or vertical services focused on specific programs like product security. Data Security spans a number of different IT and production environments, and cuts across applications, systems, services and infrastructure, and as such is best thought of as a horizontal service.



Strategy for implementing these controls

Cyral

Data security controls must be customized and prioritized according to the unique needs of any organization. This would depend on several factors including their business model, type of data they have, where they are in their security journey, and so on. Doing so maximizes security while optimizing resource allocation and operational efficiency.

However, in practice organizations often find that defining the location and risk of their datasets and implementing security controls on them is anything but straightforward. This complexity is often due to two reasons:

1. **Data proliferation**

   As organizations become data driven, they have more and more sensitive data which is seemingly everywhere.

2. **Heterogenous datasets**

   The implementation of specific controls for datasets is influenced by the type of asset where the data resides, necessitating thoughtful consideration of whether and how a particular control can be effectively deployed.

In practice, that becomes a hard problem so we have devised the following strategy for solving it:

We recommend bucketing your datasets into one or more “asset types”. Each asset type essentially represents a class of datasets that are roughly equivalent in risk and value to a given organization, and could be secured using a homogenous set of tools.

Based on a survey of nearly a 100 security leaders across a cross section of industry, we believe that the following list of asset types, while not exhaustive for every organization, is a good starting point and should be valuable for most scenarios.

Asset Types

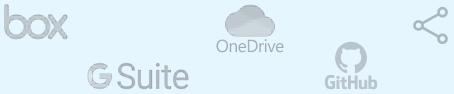
User Devices

Data types: Downloaded files

Databases

Data types: Source/production records, analytics data

Filestores



Data types: Shared documents, source files

SaaS apps

Data types: ERP, CRM, communications data

Production Servers

Data types: Temporary files

Enterprise systems datastores

Data types: Compressed/raw unstructured data

When getting feedback from security leaders, most outliers could be accommodated into the above. We list out a few examples that came out of our conversations:

- **Removable storage:** *user devices* or *production servers*
- **ETL pipelines:** *SaaS apps* or *Databases*
- **Network shares:** *Filestores*
- **Slack:** *SaaS apps*

If you have specific questions about your own dataset, please feel free to drop us a line at **datasecurity@cyral.com**

Which tool to use when?

In the table below, we outline product categories that can be used to provide specific data security controls for these given asset types. To make it more concrete, we also include up to two vendors that are perceived leaders in these categories.

Reference Table for Data Security Tool Selection

Asset Types

Controls	User Devices	Databases	Filestores	SaaS apps	Production servers	Enterprise systems datastores
Monitoring	EDR, DLP Crowdstrike, Netskope	DSG, DAM **Cyral**, Imperva	DLP, CASB Netskope, JupiterOne	DLP, CASB JupiterOne, Netskope	CSPM Wiz, Orca	File & System logs
Reporting	EDR, DLP Crowdstrike, Netskope	DSG, PAM, DSPM **Cyral**, CyberArk	DLP, CASB Netskope, JupiterOne	DLP JupiterOne	CSPM, PAM CyberArk, Wiz	SEIM Splunk, Datadog
Discovery	EDR, DLP Crowdstrike, Netskope	DSG, DSPM **Cyral**, BigID	DLP, CASB Netskope, JupiterOne	DLP, CASB JupiterOne, Netskope	CSPM Wiz, Orca	DLP Netskope, Crowstrike
Access Management	IAM BeyondTrust, AD	DSG, PAM **Cyral**, CyberArk	SASE, CASB Zscaler, Netskope	SASE, CASB Zscaler, Netskope	PAM CyberArk, Teleport	IAM AD
Protection	EDR, DLP Crowdstrike, Netskope	DSG **Cyral**	Native controls	Native controls	Network controls	Backup & Recovery Rubrik, Cohesity
Confidentiality	EDR Crowdstrike	DSG, Privacy Proxy **Cyral**, Immuta	Native controls	Enterprise Browser Island, Menlo Security	EDR Crowdstrike	ACLs & manual policies

Conclusion

How to use this framework

We encourage security leaders to prioritize their datasets by risk using the bucketing strategy based on asset type. They should then list out the specific tools and products that are being used to implement the desired controls for each asset type. It is also important to not implement these controls in a vacuum and connect them to other horizontal tools, such as for logging, IAM, alerting, etc.

This document aims to equip readers with the necessary knowledge to make informed decisions while navigating the complex landscape of data security with greater confidence. Organizations can implement an effective and efficient data security program by carefully tailoring controls to where their data lives. Security teams can leverage the above framework to choose different types of products for making sure they are prioritizing their investments based on overall risk and getting the most value by selecting the right type of products.

It is imperative for organizations to carefully assess their unique requirements while considering the examples and recommendations presented, and choose the solutions that best align with their data security goals and vendor evaluation processes. By doing so, organizations can enhance their security posture and mitigate risks effectively in today's ever-evolving threat landscape.

Acknowledgements

We'd like to express our sincere gratitude to the esteemed security leaders whose expertise and insight helped shape this white paper. We appreciate their invaluable support in advancing data security. Special thanks to:

- **Ahmed Pasha** — Global Head of Threat Management, Nomura Securities
- **Awwab Arif** — CISO, Bank of Hope
- **Arkadiy Goykhberg** — CISO, Branch Insurance
- **Gerhard Eschelbeck** — CISO, Kodiak Robotics
- **Karthik Rangarajan** — Platform and Product Security, OpenAI
- **Kevin Paige** — Former CISO, Flexport
- **Larry Viviano** — Director of InfoSec, IntelyCare
- **Martin Cholluj** — VP Security, Clickhouse
- **Michael Barrett** — Former CISO, PayPal
- **Nick McKenzie** — CISO, Bugcrowd
- **Nishant Bhajaria** — Data Governance Executive and Author
- **Ody Oupesou** — CISO, Ethos Life
- **Pathik Patel** — Head of Cloud Security, Informatica
- **Pete DeGroot** — CISO, Postmedia
- **Ralph Pyne** — CISO, Apollo
- **Solomon** — Former CISO, Wealthfront
- **Venkat Gopalan** — CDIO, Belcorp

About

Cyral provides controls for compliance, privacy, governance and protection for structured data, reducing risk, complexity, and cost. The Cyral Platform discovers data, unifies access controls for users and applications, and enables fine-grained authorization policies as code, which enables risk-based governance and limits the blast radius of data breaches.

For more information, visit **www.cyral.com** or follow **@CyralInc** on Twitter.