EXECUTIVE SUMMARY

The Eight Most Common

Data Security Challenges that DSPM Solves

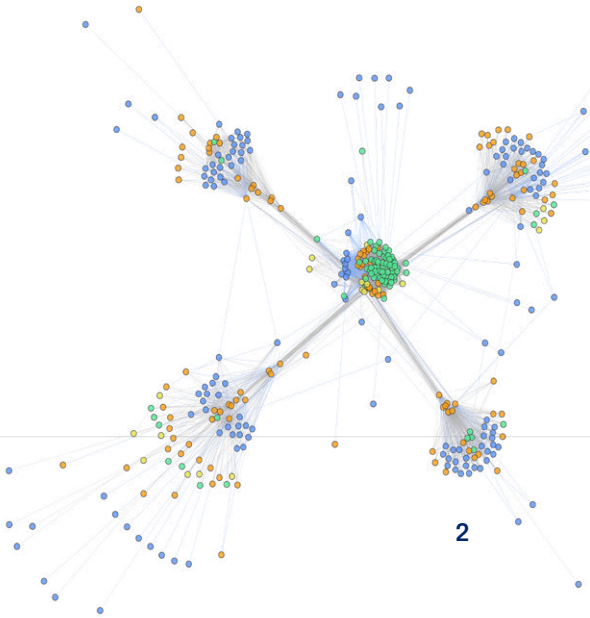
SYMMETRY SYSTEMS

Highlights from The Eight Most Common Data Security Challenges that DSPM Solves

To put it simply, organizations depend on data to operate. From day-to-day operations to strategic decisions, data keeps an organization ticking. The volume of data is immense, and data growth is explosive. And with all that scale and growth comes data security challenges. As the pioneer behind Data Security Posture Management (DSPM), Symmetry System's DataGuard is redefining what a data-centric approach to cybersecurity looks like–security from the data out, not the perimeter in–using a deployment approach that can examine data in different environments: the cloud, on-prem, or both.

Using information gleaned from millions of customer data points, this document presents the eight most common data security challenges that Symmetry regularly sees. We discuss how these issues happen, the risks associated with them, and the remediations and best practices to improve overall data security.

Download E-Book Here



Report Highlights

Data Security Posture Management

DSPM directly addresses the issues security, data, and IT teams have related to understanding the details associated with sensitive data–who has access, how it is being used, where it's located, and how safe it is. DSPM is about data visibility–first, by identifying data at the data object level and mapping which identities that have access to what data, and then exploring how the data flows across the environments.

The Zero Trust Component

Comprehensive DSPM solutions like DataGuard accelerate **Zero Trust** adoption. By providing SecOps, InfoSec, IT, and data teams accurate insight into who has access to data and from where, organizations can identify data security risks, as well as actionable recommendations on how to reduce that risk.

In This Case, Eight Is Not That Great

Let's discuss these eight challenges of data security:

1 Lack of Data Inventory

Organizations simply don't know what data they have, where it is, or why it is important.

2 Dormant Data Stores

They're old, unused, and potentially ripe for an attack because no one's paying attention.

3 Over-Privileged Data Stores

Just like over-privileged identities, an over-privileged data store has widespread access enabled, inviting trouble.

4 Dormant Identities

The single most common data security issue and one of the overlooked paths to breaches and attacks.

5 Over-Privileged Identities

It's common for organizations to overestimate the level of access and privilege an identity needs.

6 Delayed or Incomplete Employee and Vendor Offboarding

Symmetry's engineers have discovered instances where departed vendors or employees still retain admin-level access to sensitive systems and data.

7 Inadequate Segregation of Duties between Development, Test, and Production Environments

Companies often fail to enforce segregation of duties between development, test, and production environments.

8 Application and Backup Misconfiguration

There are a lot of ways applications, systems, or backups can be misconfigured. Symmetry often sees things like inadequate access controls, unprotected files and directories, and access to unnecessary or unused features.

Find out the implications of these eight data security challenges and what you can do to resolve them in the full e-book.

Download E-Book Here

How DSPM and DataGuard Work

Understand how DSPM works and how it can offer full visibility into data stores, including the location of sensitive data, who has access to it, and what operations have been performed against it. Read about the data collection, analysis, and reporting steps in the full e-book. You can download it here.

SYMMETRY SYSTEMS

symmetry-systems.com