# Innovation Insight for Data Security Platforms

Published 20 May 2022 - ID G00761943 - 14 min read

By Analyst(s): Joerg Fritsch

Initiatives: Security of Applications and Data

DSPs draw on diverse capabilities to protect structured or unstructured data. To help security and risk management leaders make the right decisions about these products, we identify two key types of DSP — broad-spectrum and specialized — and examine their benefits, uses and risks.

**Additional Perspectives**

- Summary Translation: Innovation Insight for Data Security Platforms (07 June 2022)

## Overview

### Key Findings

- As organizations move their data stores and analytics platforms to the cloud they require streamlined data security policies and access controls that are better integrated than the products they were using on-premises.
- Organizations will use data security platforms (DSPs) for new data-related projects in the cloud, while continuing to struggle with fragmented legacy data security software for their on-premises data stores. This is because they plan to move most of their data and applications to the cloud in the midterm.
- Some DSPs can be effective in both cloud and on-premises architectures.
- There is a growing ecosystem of DSP startups. They compete on the basis of their integration of multiple controls, the variety of data stores they support, the privacy filters they offer, and their support for data in artificial intelligence/machine learning (AI/ML) pipelines.

### Recommendations

To detect and respond to disruptions, security and risk management leaders responsible for the security of applications and data should:

- Assess DSPs for all new data security projects, such as the transition to data mesh architectures and cloud-based data lakes.
- Choose DSP products that provide well-integrated, broad-spectrum controls for data stewardship, policies and late-binding access. Popular late-binding access controls used by DSPs are cryptographic technologies such as tokenization and format-preserving encryption (FPE), dynamic data masking (DDM), and proprietary connectors and agents.
- Favor broad-spectrum DSPs that implement the data security controls required for compliance and risk mitigation in their IT environment — for example, DSPs that use tokenization as a standardized access control, as opposed to DSPs that use different access controls depending on the data store.
- Plan for coverage gaps or only partially resolved data security issues, as DSPs are still evolving.

## Strategic Planning Assumption

By 2027, at least 70% of data security platform (DSP) expenditure will go to vendors of DSPs with broad (not specialized) capabilities, up from approximately 10% in 2022.

## Introduction

DSPs provide consolidated security and protection capabilities for data. They aggregate formerly siloed capabilities under a common policy instrument, considerably streamlining data security. Broad-spectrum DSPs are key enablers of data security in, for example, data lakes and AI pipelines, where they accelerate digital business performance. For more information about the history and definition of DSPs, see 2022 Strategic Roadmap for Data Security Platform Convergence.

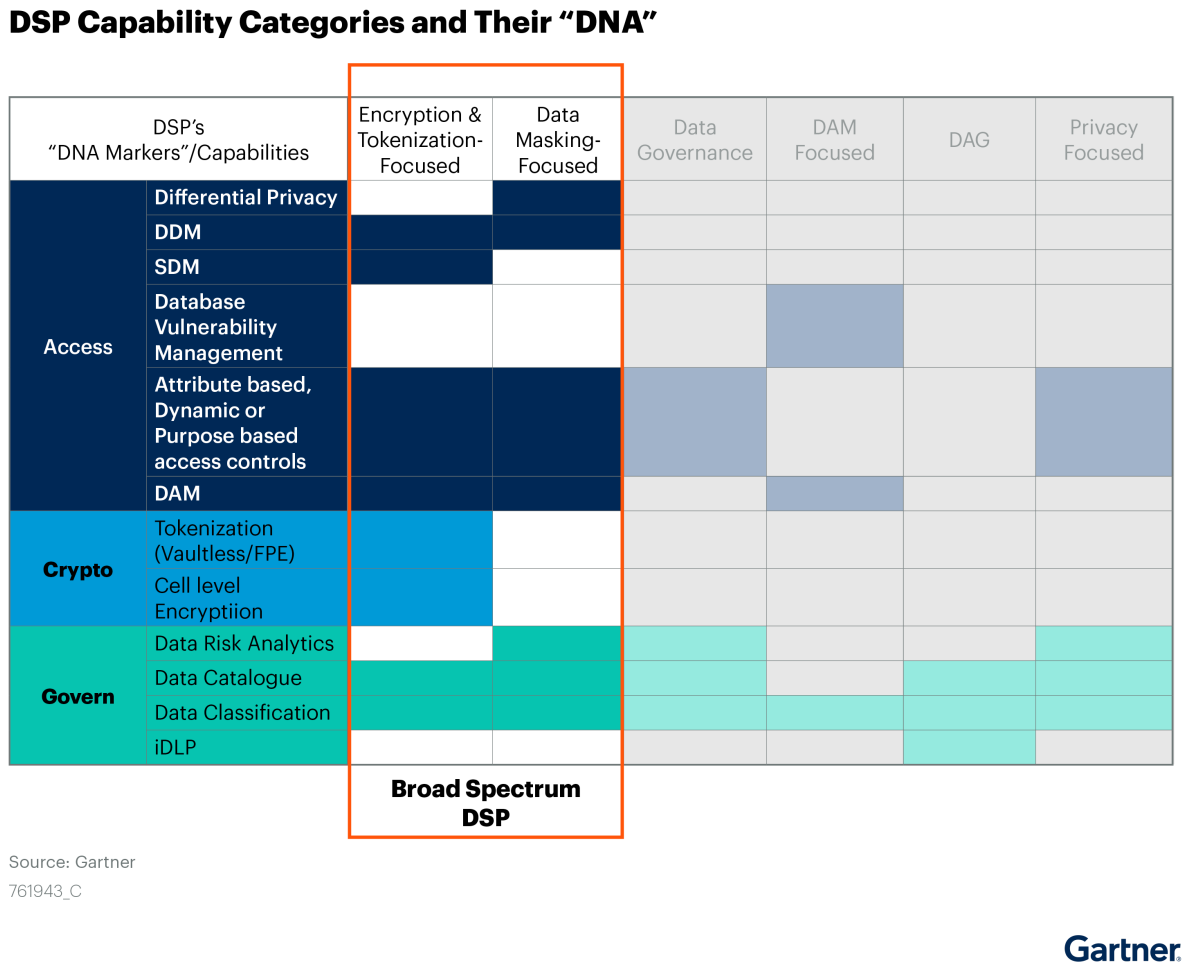
The data security sector is highly dynamic. It is evolving rapidly in response to the increased attention paid to personal data, the transition of data lakes and AI pipelines to the cloud, the desire to consolidate security architecture and tools, and geopolitical impacts on overall cybersecurity. In the 2022 Gartner CISO: Security Vendor Consolidation XDR and SASE Trends Survey, 75% of organizations responded that they are actively pursuing security vendor consolidation, compared with 29% in the 2020 Gartner Security and IAM Solution Adoption Trends Survey.

## Description

DSPs protect data against varied data threats and risks, such as data breaches and unintended disclosure, compliance risks and cyber risks. The best DSPs also secure data so that it can be shared internally and externally.

DSP vendors' capabilities often fall into six categories that differ in terms of pedigree and technical focus. Figure 1 illustrates these categories and the most common capabilities within them by analogy with a DNA marker chart.

### Figure 1: DSP Capability Categories and Their "DNA"




The DSP market includes a limited number of DSPs with a broad range of capabilities ("broad-spectrum DSPs"), and others that concentrate on one particular capability ("specialized DSPs"). As more enterprises adopt advanced analytics and cloud-based data lakes, they will prefer broad-spectrum DSPs.

*A broad-spectrum DSP generally combines data discovery and policy definition capabilities across silos with unified late-binding access controls exceeding the scope and granularity of those enforced by data stores. Popular late-binding access controls used by DSPs are cryptographic technologies such as tokenization and format-preserving encryption (FPE), dynamic data masking (DDM), and proprietary connectors and agents.*

DSP products are operated and managed either as on-premises software or, more often, as SaaS-based subscription offerings. Many vendors offer both options to meet enterprises' requirements for both a product and a service.

## Capabilities of Broad-Spectrum DSPs

DSPs that fall into the following categories generally have a broad range of capabilities:

- **Tokenization and encryption:** This is a generally broad set of capabilities that has evolved from the combination of traditional tokenization platforms with FPE technologies where data masking is frequently applied in a postprocessing step. In recent years, vendors have extended their platforms' capabilities to include data discovery, dynamic access controls and hardware security modules (HSMs). Although products in this category are centralized platforms with centralized policy configuration, they generally need to integrate with a third-party data catalog for data security governance.
  - Examples of vendors: Prime Factors, Protegrity and SecuPi.
- **Data masking and governance:** These capabilities enable a comprehensive data access and management platform for the automation of policy enforcement. Access controls are frequently enforced using DDM and dynamic access controls. This group generally includes fine-grained data governance and control capabilities. Common capabilities are DDM, dynamic access controls and data governance.
  - Examples of vendors: IBM, Immuta, Okera, Privacera and Privitar.

## Capabilities of Specialized DSPs

DSPs specializing in a primary capability are typically used to supplement the capabilities of broad-spectrum DSPs according to an organization's industry use cases and regulatory requirements. Capability categories include:

- **Data catalogs and governance:** This category focuses strongly on data cataloging and metadata management, in many cases combined with data discovery and dynamic access controls.
  - Examples of vendors: Alation and Collibra.
- **Database activity monitoring (DAM):** Products with DAM capabilities support many data stores, vendors, and multiple regulatory frameworks or business applications. They generate levels of data security visibility similar to, or exceeding, those of the previous categories, but do not protect data with masking, encryption or externalized access controls. They are limited to reporting and alerting, unless they are integrated with additional products.
  - Examples of vendors: Ankki, DBSEC, IBM and Imperva.
- **(Unstructured) data access governance:** Capabilities in this category are designed to inventory and visualize the effective levels of user access to files. There is a strong focus on data classification, file analysis and data loss prevention for unstructured data. Products in this category are extending beyond their traditional territory by adding, for example, access control capabilities and management capabilities for data subject rights requests.
  - Examples of vendors: Forcepoint, Netwrix, Proofpoint, Symmetry Systems and Varonis.
- **Privacy dashboards:** Products that fall into this category have extended privacy dashboards and management capabilities with dynamic access controls. Some vendors are looking to extend their platforms with, for example, DDM or tokenization capabilities, effectively taking a similar path to products in the data masking and governance category.
  - **Examples of vendors:** OneTrust and TrustArc.

---

*There is a clear distinction between DSPs that focus on structured data and DSPs that focus on unstructured data. Leading vendors on both sides are evaluating whether, and how, they can bridge the gap between the two types. However, buyers and use cases for the two types frequently differ, which makes it difficult to architect and sell DSP products that address both structured and unstructured data.*

---

## Benefits and Uses

There are tangible benefits to using a broad-spectrum DSP as a core component of data security architecture. Table 1 illustrates the applicability of this type of DSP across all industries (see Table 1).

### Table 1: Popular Use Cases for Broad-Spectrum DSPs

(Enlarged table in Appendix)

| *Use Case* | *Analysis and Benefits* |
|---|---|
| Cloud-based data lakes to support, for example, data and analytics | By switching to a broad-spectrum DSP, you can prevent direct user access to your data by, for example, requiring (data-store-agnostic) authorization or transformation of that data when it is accessed. Some DSPs implement scalable access policies, which dramatically reduces the number of access policies needed, as compared with, for example, traditional role-based policies. |
| Obfuscation and deidentification of personal data | A broad-spectrum DSP can obfuscate or deidentify data, while, If required, preserving its format and length. |
| Creation of data for development and testing | Sensitive data protected by a broad-spectrum DSP can be used directly for development and testing, so there is no need to create masked copies of data. Alternatively, smaller amounts of data can be prepared using DDM. |
| Monetization and other use of data by sharing subsets | Leading broad-spectrum DSPs provide end-to-end visibility into where data is used, and track authority and accountability. Some can watermark data before it is shared. |
| Defense against cybersecurity threats | Broad-spectrum DSPs discover, classify and control access to sensitive data. Some also use the security posture for the surrounding infrastructure, data stores and applications to determine risk levels and control requirements so as to enable what is known as data security posture management. In this way, DSPs can help mitigate cybersecurity threats. |
| Efficiency and consolidation | DSPs appeal to enterprises because of their ease of deployment, which reduces complexity and cost. In the 2022 Gartner CISO: Security Vendor Consolidation XDR and SASE Trends Survey, 55% of respondents said they were pursuing consolidation to increase efficacy and efficiency, whereas only 35% said they were doing so to save money. |

Source: Gartner (May 2022)

Specific uses of broad-spectrum DSPs in particular industries include:

- **Finance:** There is a large installed base of tokenization products in this industry, tokenization being a popular means of reducing the required extent of Payment Card Industry Data Security Standard (PCI DSS) compliance. As some tokenization platforms have grown into DSPs, Gartner has observed clients in this industry using DSPs as access controls and data-masking tools for personal data.
- **Retail:** DSPs are used to secure data stores — such as those storing customer profiles from loyalty programs — from exfiltration and to reduce cyberinsurance fees.
- **Internet of Things (IoT) predictive maintenance:** Manufacturers of IoT and medical devices are increasingly using cloud-based data lakes for the gathering of predictive maintenance data. The use of DSPs is generally considered a best practice for this purpose.

## Risks

Although DSPs can score quite highly for consolidation of data security products and controls, cost-effectiveness and privacy, they do have limitations and pose some risks, such as the following:

- Some capabilities of broad-spectrum DSPs can overlap with key capabilities of leading data integration and data virtualization platforms. For example, some DSPs proxy and expose universal secure data interfaces, similar to best-of-breed data integration tools.
- The quality of the data security provided by a DSP often depends on the maturity of data security governance and the policies, standards and guidelines derived from it. You can hardly protect your data if you have no mandate to do so or have no idea what the security requirements are.
- DSPs that use cryptographic technologies, such as tokenization and FPE, to protect data need significant planning and considerable implementation effort to integrate with all required business applications and use cases.
- Onboarding of data from a variety of sources may need an additional data catalog to curate the data. Many DSPs have limited data-cataloging functionality, which might not meet complex collaboration requirements.

- Even broad-spectrum DSPs sometimes have roots in particular data stores or platforms, such as Databricks or Apache Hadoop platforms. Although vendors almost always claim to support a wide range of data stores, implementation can be difficult and protracted when dealing with stores beyond vendors' original territory.
- Broad-spectrum DSP vendors may not focus enough on adding privacy-enhancing computation technologies, such as differential privacy and synthetic data technologies, to their platforms, whether organically or through acquisition. Venture capital firms might not provide the extra funds required to make necessary acquisitions.
- Use of DSPs currently means vendor lock-in. Switching between broad-spectrum DSPs is not practicable.
- DSPs have a bias toward structured data. Many businesses would like to protect structured and unstructured data equally, but find that leading DSP vendors are slow to provide better support for, among other things, data discovery and classification of unstructured data and file-level encryption.

## Adoption Rate

Broad-spectrum DSPs are emerging technology products with a low to medium degree of enterprise adoption. Their future looks promising, thanks to increased venture capital funding, the emergence of startups, and the substantial business benefits offered by their capabilities. Moreover, we expect some specialized DSPs will grow into broad-spectrum DSPs, or at least gain additional capabilities, via in-house development, that extend their reach.

DSP technology is still nascent, so most organizations become aware of it only when they move their data to the cloud and find that their traditional controls no longer suffice. This technology has tremendous potential to become a new de facto standard for the protection of data, but it is licensing models and pricing, rather than technology, that may eventually decide DSPs' fate.

## Alternatives

Fragmented data security controls are the obvious alternative to DSPs. There are use cases in which existing vendor relationships and an inability to prove the short-term benefits of a DSP may lead to continued use of fragmented, stand-alone data security products. Regulators and cyberinsurers are only just waking up to the risks of using outdated data security controls — or no data security controls — for production data. Therefore, at present, they may merely nudge organizations toward using DSPs for some scenarios, most likely those involving data stores that contain personally identifiable information.

## Recommendations

To detect and respond to disruptions, security and risk management leaders responsible for the security of applications and data should:

- Assess DSPs for all new data security projects, such as the transition to data mesh architectures and cloud-based data lakes.
- Choose DSP products that provide well-integrated, broad-spectrum controls for data stewardship, policies and late-binding access. Popular late-binding access controls used by DSPs are cryptographic technologies such as tokenization and FPE, DDM, and proprietary connectors and agents.
- Favor broad-spectrum DSPs that implement the data security controls required for compliance and risk mitigation in their IT environment — for example, DSPs that use tokenization as a standardized access control, as opposed to DSPs that use different access controls depending on the data store.
- Plan for coverage gaps or only partially resolved data security issues, as DSPs are still evolving.

## Representative Providers

Representative providers of broad-spectrum DSPs:

- **Cyral:** Data Security and Governance Platform
- **IBM**
- **Immuta:** Immuta

- **Okera:** Okera Platform
- **Prime Factors:** EncryptRIGHT
- **Privacera:** Privacera Platform
- **Privitar:** Privitar Modern Data Provisioning Platform
- **Protegrity:** Protegrity Data Protection Platform
- **Satori Cyber:** DataSecOps platform
- **SecuPi:** SecuPi Platform

## Evidence

Gartner conducted contextual research as part of its Discovery Project initiative. This involved interviewing clients pursuing cloud data and analytics migration initiatives to improve our understanding of best practices and challenges relating to strategy, adoption, skill sets and technical implementation. This document draws on that research's findings and its insights from users of broad-spectrum DSPs.

**The 2020 Gartner Security and IAM Solution Adoption Trends Survey:** This survey was conducted to learn what security solutions organizations were benefiting from and what factors affected their choice of, or preference for, such solutions. The research was conducted online during March and April 2020 among 405 respondents from North America, Western Europe and Asia/Pacific. Companies from different industries were screened to ensure they had annual revenue of less than $500 million. Respondents were required to be at managerial level or above (excluding C-suite level) and had to have primary involvement in, and responsibility for, risk management in their organization.

*Disclaimer: Results of this study do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.*

**The 2022 Gartner CISO: Security Vendor Consolidation XDR and SASE Trends Survey:** This survey was conducted to determine how many organizations are pursuing vendor consolidation efforts, the primary drivers for consolidation, the expected or realized benefits, and how consolidation efforts are being prioritized. A primary aim of the survey was to collect objective data on extended detection and response (XDR) and secure access service edge (SASE) for consolidation of our megatrend analysis. The survey was conducted online during March and April 2022 among 418 respondents from North America (the U.S. and Canada), Asia/Pacific (Australia and Singapore) and EMEA (France, Germany and the U.K.). Results were from respondents representing organizations with $50 million or more in 2021 annual revenue. Industries represented included manufacturing, communications and media, IT, government, education, retail, wholesale trade, banking and financial services, insurance, healthcare providers, services, transportation, utilities, natural resources, and pharmaceuticals, biotechnology and life sciences. Respondents were screened for job title, company size and job responsibilities — they had to be in information security/cybersecurity or IT roles, and have a primary involvement in information security.

*Disclaimer: Results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.*

Detailed briefings were conducted with several vendors named in this document.

[1] Okera uses a diverse set of approaches and connectors.

[2] Privacera enforces security policy using Apache Ranger. It focuses on the scope and integration possibilities of Apache Ranger.

## Recommended by the Author

Some documents may not be available as part of your current Gartner subscription.

2022 Strategic Roadmap for Data Security Platform Convergence

Predicts 2022: Consolidated Security Platforms Are the Future

Market Guide for Data Masking

Quick Answer: How Do Other Organizations Deploy Data and Analytics Security Governance in the Cloud?

## Table 1: Popular Use Cases for Broad-Spectrum DSPs

| *Use Case* | *Analysis and Benefits* |
|---|---|
| Cloud-based data lakes to support, for example, data and analytics | By switching to a broad-spectrum DSP, you can prevent direct user access to your data by, for example, requiring (data-store-agnostic) authorization or transformation of that data when it is accessed. Some DSPs implement scalable access policies, which dramatically reduces the number of access policies needed, as compared with, for example, traditional role-based policies. |
| Obfuscation and deidentification of personal data | A broad-spectrum DSP can obfuscate or deidentify data, while, If required, preserving its format and length. |
| Creation of data for development and testing | Sensitive data protected by a broad-spectrum DSP can be used directly for development and testing, so there is no need to create masked copies of data. Alternatively, smaller amounts of data can be prepared using DDM. |
| Monetization and other use of data by sharing subsets | Leading broad-spectrum DSPs provide end-to-end visibility into where data is used, and track authority and accountability. Some can watermark data before it is shared. |
| Defense against cybersecurity threats | Broad-spectrum DSPs discover, classify and control access to sensitive data. Some also use the security posture for the surrounding infrastructure, data stores and applications to determine risk levels and control requirements so as to enable what is known as data security posture management. In this way, DSPs can help mitigate cybersecurity threats. |

| *Use Case* | *Analysis and Benefits* |
| --- | --- |
| Efficiency and consolidation | DSPs appeal to enterprises because of their ease of deployment, which reduces complexity and cost. In the 2022 Gartner CISO: Security Vendor Consolidation XDR and SASE Trends Survey, 55% of respondents said they were pursuing consolidation to increase efficacy and efficiency, whereas only 35% said they were doing so to save money. |

Source: Gartner (May 2022)