IDC MarketScape

IDC MarketScape: Worldwide DLP 2025 Vendor Assessment

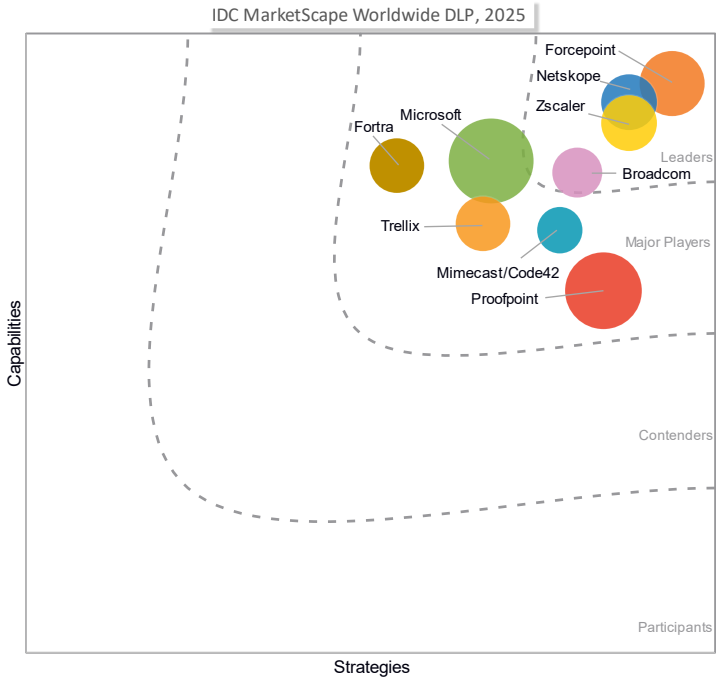
Jennifer Glenn

THIS EXCERPT FEATURES NETSKOPE AS A LEADER

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide DLP Vendor Assessment



Source: IDC, 2025

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

March 2025, IDC #US53234325e

ABOUT THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide DLP 2025 Vendor Assessment (Doc # US53234325).

IDC OPINION

This study evaluates the data loss prevention (DLP) solutions from nine global vendors. This study assesses the capabilities delivered with the DLP solution, as well as the strategic vision for the product.

DLP covers multiple channels in the enterprise, including web browsers, email, networks, endpoints, and cloud applications. While the channels vary, by and large, the principles of preventing data loss are the same. Data identified by an organization as sensitive or confidential is monitored for its movement. The movement is logged, and action is taken. Sometimes the action is to block the data from moving. Other times action is allowed, but evidence is collected and used for policy adjustment, as well as user education or reprimand.

The Evolution of DLP

A 2021 IDC Market Share on data loss technologies (a more inclusive approach to data loss tools) declared, "DLP is dead; long live the DLP." An apt vision for the dynamics that have shaped this market in the years since.

Digital transformation moved enterprise data out of on-premises silos, freeing it up to be shared more easily between applications and users. Advanced privacy and compliance regulations aimed to put more control around the use of sensitive and confidential information — requiring organizations to understand and appropriately classify enterprise data in order to adhere to these requirements. Then in 2023, GenAI ramped up significantly — and exposed the vulnerability and gaps in our data security and privacy practices.

DLP has been a cornerstone technology for large, global organizations. Its evolution has been bumpy but resilient and dynamic. It evolved to meet the sharing requirements of digital transformation. During this time, DLP was vilified for putting roadblocks to business operations. When privacy and compliance regulations took center stage following several high-profile data breaches, DLP vendors adjusted their logging and reporting to demonstrate adherence to these requirements — and it became a necessary technology. Even as the technology provided vital information for audits, the additional policies and management became onerous because data security teams were still being vilified for slowing business growth but still didn't want to miss

anything. The result was what we saw in 2021; DLP technology wasn't making anyone happy, even as it continued to do the job for which it was intended.

From this historical perspective, it's interesting to see how changes in the enterprise environment have impacted attitudes toward DLP technology.

First, corporate culture has evolved. Most enterprises don't want to stop their employees from getting work done. They want to demonstrate a culture of collaboration and information sharing. This is how the world works now. And the security team doesn't want to be known as the department of "no." They do not wish to show any whiff of impeding business or ruining this culture. However, their jobs and reputation are on the line, so they need to make sure everything is documented.

This is not to say that detecting and blocking confidential data is no longer important — it most definitely is, particularly for highly regulated industries. For many organizations, blocking data from leaving seems to take a back seat to collecting detailed evidence of violations and using that data to re-educate or reprimand employees.

Second, the skills shortage in technology has been discussed ad nauseum. However, it's more than just a skills issue. Security teams are shrinking. This means fewer staff to create and manage complex DLP policies. Organizations are looking for simplicity in installation and management, as well as detailed but nontechnical reporting that can easily be sent to non-security teams, like HR or legal.

Third, consolidation of security tools is a reality. For many years, we heard the siren of consolidation. Too many tools. Too many licenses. Too many integrations to keep up with. Still, consolidation didn't really manifest right away. Organizations still wanted best-for-them technologies across multiple channels. However, as DLP solutions have matured and reached some level of parity (though not exact) in functions; consolidation is not only easier but makes the most sense for the teams and the business.

Finally, another big change is that DLP is no longer just for large organizations. Compliance requirements and granular policy management meant DLP was traditionally reserved for very large organizations that had the staff and financial resources to handle it. In 2025, midmarket and small enterprises have to adhere to privacy and compliance rules as well. These organizations are looking for DLP solutions that can assist in protecting and controlling sensitive data. This means DLP vendors need to have flexible deployment and licensing options.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

The process for this IDC MarketScape on DLP began in July 2024. IDC sent prequalification surveys to vendors that offered any form of data loss technologies. The

list was quite substantial, and it became clear that specific conditions were required to make adequate comparisons between solutions.

There are a number of very capable DLP solutions available from organizations that are not included in this evaluation, including several DLP vendors that serve specific geographies, some of the newer solutions with limited revenue and time on the market, and many of the secure access service edge (SASE) vendors. There are two of the SASE vendors included here, but they had met the requirements as laid out.

The following conditions need to be met for inclusion in this evaluation:

- The offering should be commercially available for use as a DLP that is managed by the customer.
- The product must be available as an individual product (e.g., has its own SKU).
- The DLP product must be offered and available on a worldwide basis with sales in a minimum of two global regions.
- The product must have at least $15 million in revenue in calendar year 2023.
- The product capabilities supported, at a minimum, include data discovery and classification, prebuilt policy templates and support/wizards for custom policy templates, data activity insights, and cross-platform compatibility.

ADVICE FOR TECHNOLOGY BUYERS

The interesting thing about DLP in 2025 is that there is a DLP solution for just about every organization and use case. Each vendor in this evaluation has strengths or weaknesses that are likely to be important to each buyer's need. We spoke with a number of customers for this evaluation. Conversations with these users identified a number of factors that buyers should consider when looking at a DLP.

Some things to consider:

- **Use cases:** Knowing how the DLP will be used and what use cases it's intended for will provide a clearer direction on the type of solutions to fit that need. Managing internal risks requires a different set of functionality and metrics than preventing exfiltration of data from attackers. While most DLP is used for adhering to privacy and compliance requirements, if that is the sole purpose, these needs require a different set of features than monitoring for intellectual property theft.
- **Staff resources:** Buyers should consider how much staff they can dedicate to implementing and managing the DLP. For this evaluation, many of the users we spoke with had very small teams dedicated to data security — and in some cases, there isn't a single dedicated person. For these organizations, it was

important to have a solution that was easy to manage and didn't require a lot of time to tune or adjust policies. For the very large organizations, or those that dealt with highly regulated data such as health information, most had a sizable staff dedicated to data security, making granular management of policies less onerous.

- **Reporting:** One of the DLP capabilities that came through loud and clear on this assessment was the value of reporting. When considering a DLP vendor, it's important to know how your success will be measured — and who will be evaluating that measurement. Each vendor has its own style of reporting risks not only to the data security analyst but also to teams outside of the security department. Incident investigations or data/privacy violations mean something different to the C-suite, compliance auditors, HR, and legal. The ability to customize reports is important.
- **Integration and consolidation:** Cost will always factor into DLP purchase decisions. But cost is more than just the price tag on the initial purchase. As discussed previously, resources needed to operate the DLP play a major factor in "total cost" as do integrations with other tools. For midmarket and smaller enterprises, consolidation of DLP tools with other security solutions is almost necessary because of the way these teams are built.

Other things users considered important are less tangible than those listed previously. Many of the customers we spoke to wanted to feel included in the process of improving the product. Data security needs can be fluid with adjustments to regulations, new application integrations, and just general market changes. It's important to find a DLP vendor that demonstrates a willingness to — at a minimum — listen to suggested changes or feedback.

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

Netskope

Netskope is positioned in the Leaders category of the 2025 IDC MarketScape for worldwide DLP.

Netskope is a cybersecurity vendor based in Santa Clara, California. Its products and solutions are designed for protecting people, devices, and data across wherever they are. IDC evaluated Netskope's Cloud DLP solution, which includes DLP capabilities for

the network, applications, endpoint, and email. The Netskope Cloud DLP can be deployed as on-premises software, SaaS, or hybrid.

Netskope offers the full scope of capabilities in its DLP offering. It can be used for both structured and unstructured data and offers an option for images. The solution can be used for data at rest, data in use, and data in motion. Furthermore:

- **Discovery and classification:** Netskope offers a broad spectrum of features in its discovery and classification capability. This includes the ability to identify sensitive data by asset type, file origin, keywords, user behavior, and user device posture. Advanced behavior detection is offered as an add-on. The solution's discovery features are available for differential or metadata scans of an organization's environment. The company also has patented technology that is intended to help customers create classifiers based on their own data.
- **DSPM/mapping:** Netskope offers a broad spectrum of features for its DSPM and mapping capability. These include the ability to track field data from structured data stores and also to match traffic based on conditions. Netskope acquired Dasera in October 2024, adding DSPM capabilities to the Netskope One platform. The Netskope DSPM scans the organization's data landscape, cataloging the location, access privileges, and risky use of sensitive data for exfiltration or privacy violations. The data is continuously monitored for access, use, and movement violations.
- **Insider risk:** Netskope offers a broad range of features in its insider risk capabilities, including the ability to identify user behavior and data source. Data flow analysis and vulnerability identification are also available with the core offering.
- **Enforcement:** Netskope offers the full range of enforcement features in its core offering. These include blocking, deletion, and entity obfuscation when storing incident information.
- **Reporting:** Netskope includes a broad range of reporting features with its DLP core offering. Its TrueInstance detection feature gathers transactional information from SaaS applications and then uses synthetic API calls to determine if an incident occurs in a personal or corporate instance of that application. Netskope reporting is centralized across its product lines.

In early 2024, Netskope released a Digital Rights Management solution that is designed to offer customers seamless integration with any classification vendor. In July 2024, Netskope announced API-based controls for the OpenAI ChatGPT Enterprise product. Information intended for use in ChatGPT Enterprise is scanned for confidential data that would violate compliance or privacy regulations. Based on customer policy, that data would be prevented from being used within the ChatGPT tool.

Note: Netskope operates primarily as a SASE vendor. Revenue for this DLP product is currently reflected in the network security functional market shares and forecasts.

Strengths

- The Netskope DLP offers the ability to work with any classification vendor, as well as the ability to use that classification for policies that can be managed and applied across its entire product line.
- Netskope customers called out the company specifically for its great customer service and the ability to influence feature development.

Challenges

- While Netskope offers a very wide range of DLP capabilities and features, in its core solution, the endpoint DLP requires a separate license. For customers, this can add unexpected costs.
- Security teams are actively looking to consolidate data security functions to as few vendors as possible. Potential customers using other similar solutions are likely to consolidate using the solutions already installed.

Consider Netskope When

Netskope has a broad range of deployment and licensing options, making it suitable for organizations of any size. Netskope has a sizeable customer base for its Security Service Edge platform. Customers using this platform will likely see benefits of adding the DLP function to this offering.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here, and now. Under this category, IDC analysts will look at how well a vendor is building and delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings,

customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

IDC defines data loss prevention (DLP) as software that discovers, categorizes, monitors, and protects data according to organizational policies, wherever it is stored or used. DLP solutions are intended to help enterprises secure personal, confidential, or sensitive data, as well as to demonstrate compliance with privacy and/or industry regulations. This means that specified data is not accessed, used improperly, or removed without authorization whether that data is at rest, in motion, or in use. This also includes critical capabilities for ensuring confident enforcement decisions, such as discovery and classification functions that provide context around the sensitivity of the data being monitored and controlled with DLP technologies.

DLP solutions are categorized within the information protection submarket within the information and data security functional market. Information protection includes technologies that protect the confidentiality, integrity, and availability of data that is valuable to the business. Within this market, there are four technology detail segments: messaging security, data loss technologies, data access governance, and data privacy compliance. For more information, see *IDC's Worldwide Security Products Taxonomy, 2025* (IDC #US53164625, February 2025).

LEARN MORE

Related Research

- *Market Analysis Perspective: Worldwide Information and Data Security, 2024* (IDC #US52564124, September 2024)
- *IDC's Data Privacy Survey: The Unification of Privacy and Security* (IDC #US52357524, June 2024)
- *North American Security Tools and Vendors Consolidation Study: Insights on Product Consolidation Plans* (IDC #US52023024, April 2024)
- *Worldwide Trusted Access and Network Security Market Shares, 2022: Security as a Service Outpaces Expectations* (IDC #US51153419, August 2023)
- *IDC MarketScape: Worldwide Network Edge Security as a Service 2023 Vendor Assessment* (IDC #US50723823, June 2023)

Synopsis

The IDC study evaluates the data loss prevention (DLP) solutions from nine global vendors, focusing on their capabilities and strategic vision. DLP solutions monitor and protect sensitive data across various channels, including web browsers, email, networks, endpoints, and cloud applications. This assessment is based on a comprehensive framework that looks at how each vendor is meeting the current requirements for DLP buyers as well as the strategic vision for addressing future risks.

"Data loss prevention solutions have been in the market for well over a decade. Digital transformation, privacy and compliance requirements, and the rapid adoption of AI technologies have demonstrated the value and vulnerability of enterprise data. In turn, buyers are demanding more from their data loss solutions to assist them in addressing both current and future risks." — Jennifer Glenn, research director, Information and Data Security, IDC

ABOUT IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com