The Radicati Group, Inc.
www.radicati.com

THE RADICATI GROUP, INC.

Data Loss Prevention – Market Quadrant 2025 *

An Analysis of the Market for Data Loss Prevention Revealing Top Players, Trail Blazers, Specialists and Mature Players.

March 2025

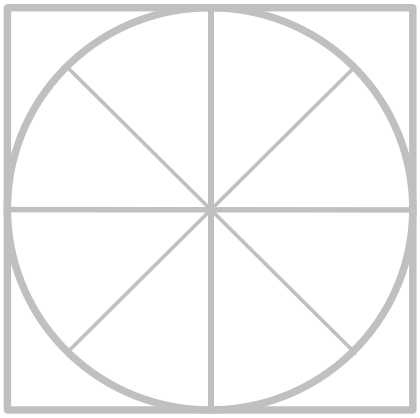

TABLE OF CONTENTS

==========

==========

RADICATI MARKET QUADRANTS EXPLAINED

Radicati Market Quadrants are designed to illustrate how individual vendors fit within specific technology markets at any given point in time. All Radicati Market Quadrants are composed of four sections, as shown in the example quadrant (Figure 1).

- ***Top Players*** – These are the current market leaders with products that offer, both breadth and depth of functionality, as well as possess a solid vision for the future. Top Players shape the market with their technology and strategic vision. Vendors don't become Top Players overnight. Most of the companies in this quadrant were first Specialists or Trail Blazers (some were both). As companies reach this stage, they must fight complacency and continue to innovate.

- ***Trail Blazers*** – These vendors offer advanced, best of breed technology, in some areas of their solutions, but don't necessarily have all the features and functionality that would position them as Top Players. Trail Blazers, however, have the potential for "disrupting" the market with new technology or new delivery models. In time, these vendors are most likely to grow into Top Players.

- ***Specialists*** – This group is made up of two types of companies:

    a. Emerging players that are new to the industry and still have to develop some aspects of their solutions. These companies are still developing their strategy and technology.
    b. Established vendors that offer very good solutions for their customer base, and have a loyal customer base that is totally satisfied with the functionality they are deploying.

- ***Mature Players*** – These vendors are large, established vendors that may offer strong features and functionality, but have slowed down innovation and are no longer considered "movers and shakers" in this market as they once were.

    a. In some cases, this is by design. If a vendor has made a strategic decision to move in a new direction, they may choose to slow development on existing products.

b. In other cases, a vendor may simply have become complacent and be out-developed by hungrier, more innovative Trail Blazers or Top Players.
c. Companies in this stage will either find new life, reviving their R&D efforts and move back into the Top Players segment, or else they slowly fade away as legacy technology.

Figure 1, below, shows a sample Radicati Market Quadrant. As a vendor continues to develop its product solutions adding features and functionality, it will move vertically along the "y" functionality axis.

The horizontal "x" strategic vision axis reflects a vendor's understanding of the market and their strategic direction plans. It is common for vendors to move in the quadrant, as their products evolve and market needs change.

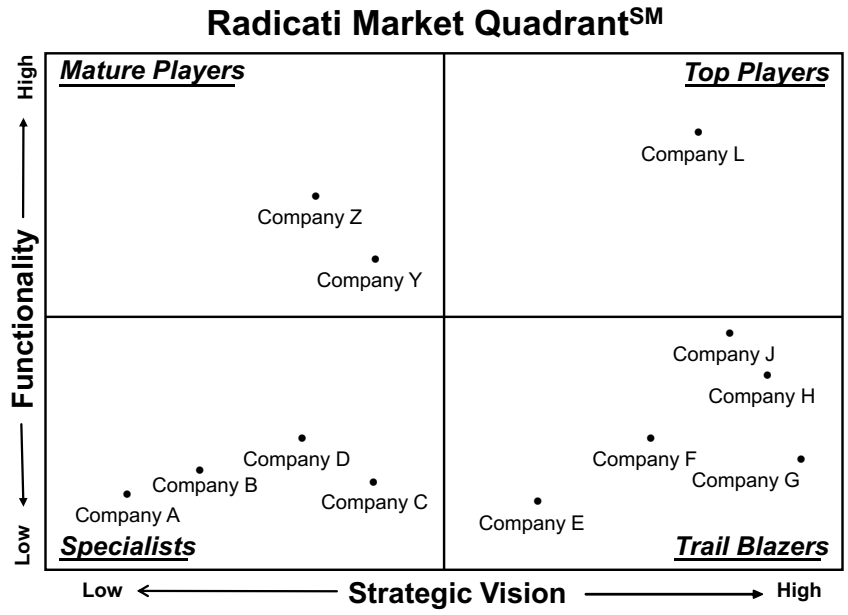

Figure 1: Sample Radicati Market Quadrant

INCLUSION CRITERIA

We include vendors based on the number of customer inquiries we receive throughout the year. We normally try to cap the number of vendors we include to about 10-12 vendors. Sometimes, however, in highly crowded markets we need to include a larger number of vendors.

MARKET SEGMENTATION – DATA LOSS PREVENTION

This edition of Radicati Market Quadrants[SM] covers the "**Data Loss Prevention**" (DLP) market, which is defined as follows:

- **Data Loss Prevention** solutions – are appliances, software, cloud services, and hybrid solutions that provide electronic data supervision and management to help organizations prevent non-compliant information sharing. These solutions serve to protect data at rest, data in use, and data in motion. Furthermore, these solutions are "content-aware" which means they can understand the content that is being protected to a much higher degree than simple keywords. Leading vendors in this segment include: *Broadcom, Forcepoint, Fortinet, Fortra, Microsoft, Mimecast, Netwrix, Proofpoint, Safetica,* and *Trellix*.

- We distinguish between three types of DLP solutions:

  - *Full DLP solutions* – protect data in use, data at rest, and data in motion and are "aware" of content that is being protected. A full-featured content-aware DLP solution looks beyond keyword matching and incorporates metadata, role of the employee in the organization, ownership of the data, and other information to determine the sensitivity of the content. Organizations can define policies to block, quarantine, warn, encrypt, and perform other actions that maintain the integrity and security of data.

  - *Channel DLP solutions* – typically enforce policies on one specific type of data, usually data in motion, over a particular channel (e.g. email). Some Channel DLP solutions are content-aware, but most typically rely only on keyword blocking.

  - *DLP-Lite solutions* – are add-ons to other enterprise solutions (e.g. information archiving) and may or may not be content-aware. DLP-Lite solutions will typically only monitor data at rest, or data in use.

- This Market Quadrant deals only with Full DLP solutions, as defined above. Channel DLP and DLP-Lite solutions <u>are not</u> included in this report as they are usually purchased as a component of a broader security or data retention solution (e.g. Compliance and Data

Governance).

- External threats to data exist in a myriad of forms through advanced persistent threats (APT), espionage, and other attempts to gain unauthorized access to data. While external threats are a problem, data loss from internal threats is also a significant concern. Internal data loss can be malicious, such as a disgruntled worker copying sensitive data to a flash drive, or it can be the result of negligence due to an honest mistake, such as an employee sending a customer list to a business partner that shouldn't have access to it.

- Increased worldwide regulations have fostered growing adoption of DLP solutions. Laws that mandate the disclosure of data breaches of customer data, compliance with government and industry regulations, as well as recent regulations such as the European General Data Protection Regulation (GDPR) and the EU-US Privacy Shield affect organizations of all sizes, across all verticals.

- Organizations of all sizes continue to invest heavily in DLP solutions to protect data and ensure compliance. The worldwide revenue for DLP solutions is expected to grow from nearly $3.4 billion in 2025, to over $9.0 billion by 2029.

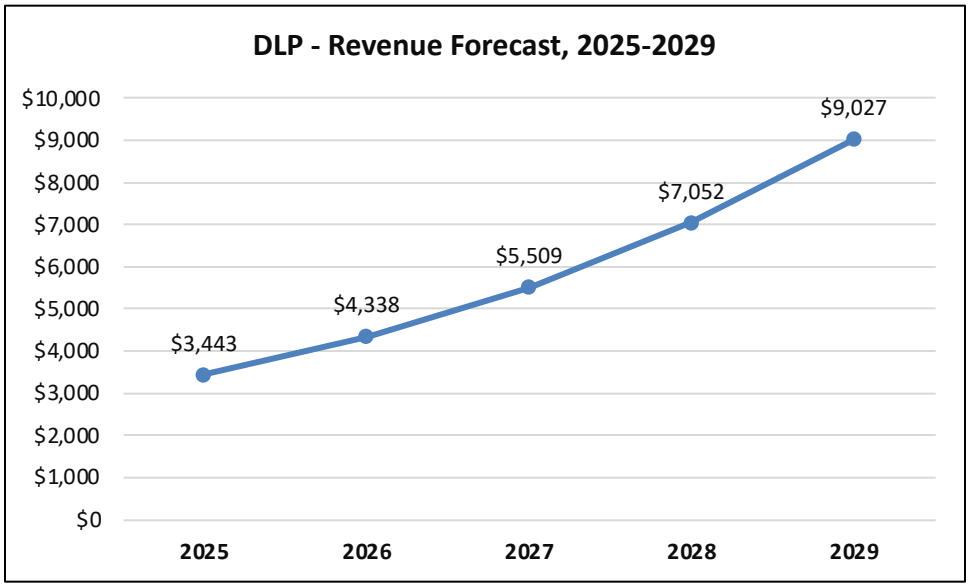

Figure 2: DLP Revenue Forecast, 2025 – 2029

EVALUATION CRITERIA

Vendors are positioned in the quadrant according to two criteria: *Functionality* and *Strategic Vision*.

Functionality is assessed based on the breadth and depth of features of each vendor's solution. All features and functionality do not necessarily have to be the vendor's own original technology, but they should be integrated and available for deployment when the solution is purchased.

Strategic Vision refers to the vendor's strategic direction, which comprises a thorough understanding of customer needs, ability to deliver through attractive pricing and channel models, solid customer support, and strong on-going innovation.

Vendors in the *Data Loss Prevention* space are evaluated according to the following key features and capabilities:

- ***Deployment Options*** – availability of the solution in different form factors, such as on-premises, appliance and/or virtual appliance, cloud-based services, or hybrid.

- ***Platform Support*** – the range of computing platforms supported, e.g., Windows, macOS, Linux, iOS, Android, and others.

- ***Data in use*** – the ability to assign management rights (manually or automatically) to files and data that specify what can and cannot be done with them (e.g., read-only, print controls, copy/paste controls, etc.). In addition, the ability to specify which devices and protocols (e.g., Bluetooth) can be used when accessing sensitive data. For devices, DLP solutions should be able to specify the type and brand of authorized devices that can interact with sensitive data.

- ***Data in motion*** – web controls and content inspection that prevent the sending of sensitive data through the web, email, social networks, blogs, and other communication channels. Integration with secure web gateways and email gateways is an important aspect of this function.

- ***Data at rest*** – refers to data store scanning, fingerprint scanning and the ability to monitor all stored data at regular intervals in accordance with established corporate data policies.

- ***Policy templates*** – built-in and easily customizable policy templates to help adhere to industry regulations (e.g., HIPAA, PCI, and others) and best practices.

- ***Directory Integration*** – integration with Active Directory, LDAP, etc. to help manage and enforce user policies.

- ***Enforcement visibility*** – employee alerts and self-remediation capabilities, such as confirmations and justifications of data policy breaches.

- ***Mobile DLP*** – monitoring of data on mobile devices fully integrated with organization-wide DLP controls. Integration with Mobile Device Management (MDM) / Enterprise Mobility Management (EMM) capabilities, or partnerships with leading MDM/EMM vendors.

- ***Centralized Management*** – easy, single pane of glass management across all deployment form factors, i.e., cloud, on-premises, hybrid, etc.

- ***Encryption*** – vendor-provided embedded encryption capabilities or through add-ons.

- ***Drip DLP*** – features to control the slow leaking of information by monitoring multiple transfer instances of sensitive data.

- ***Cloud Access Security Broker (CASB) integration*** – either through the vendor's own CASB capabilities or through partners.

In addition, for all vendors we consider the following aspects:

- *Pricing* – what is the pricing model for their solution, is it easy to understand and allows customers to budget properly for the solution, as well as is it in line with the level of functionality being offered, and does it represent a "good value".

- *Customer Support* – is customer support adequate and in line with customer needs and response requirements.

- *Professional Services* – does the vendor provide the right level of professional services for planning, design and deployment, either through their own internal teams, or through partners.

***Note**: On occasion, we may place a vendor in the Top Player or Trail Blazer category even if they are missing one or more features listed above, if we feel that some other aspect(s) of their solution is particularly unique and innovative.*

MARKET QUADRANT – DATA LOSS PREVENTION

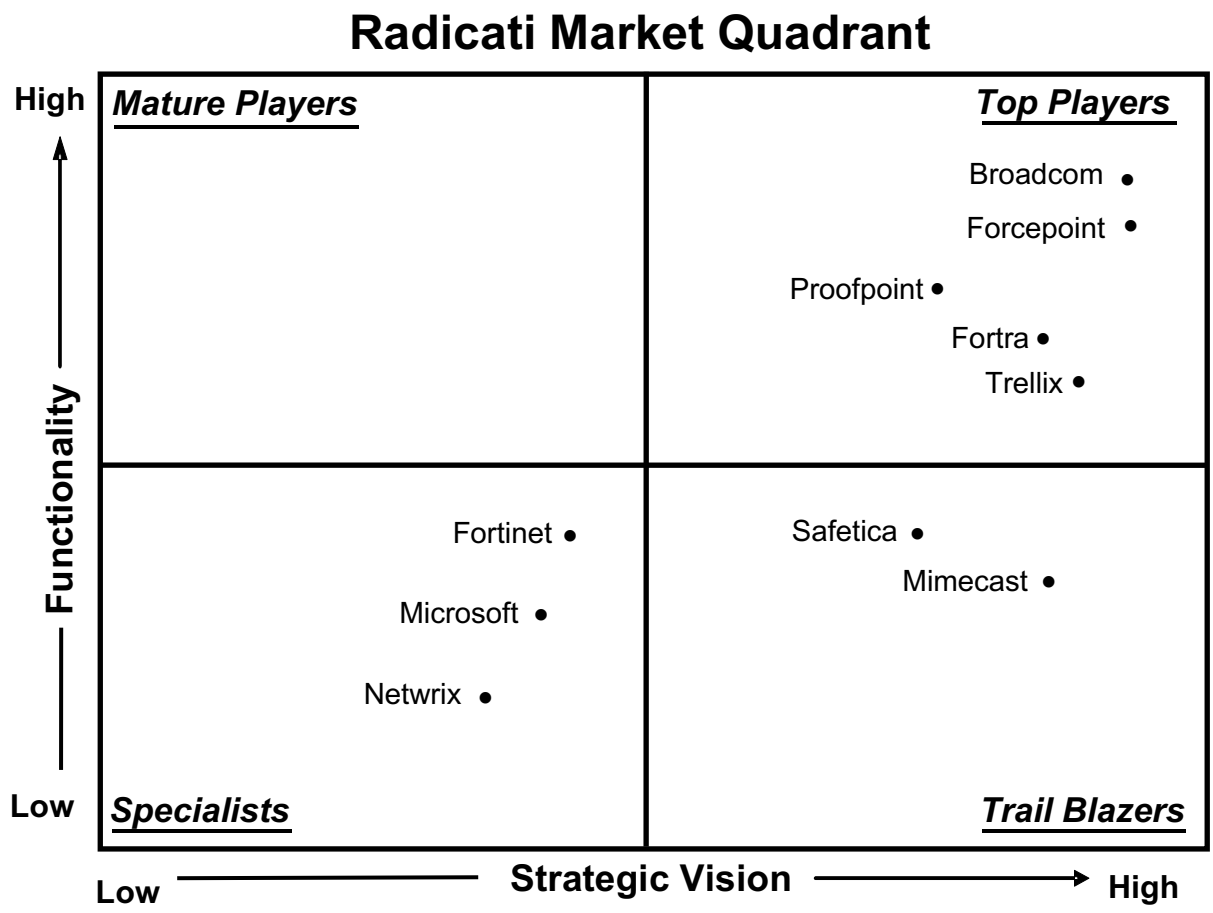

Figure 3: Data Loss Prevention Market Quadrant, 2025*

* Radicati Market Quadrant is copyrighted March 2025 by The Radicati Group, Inc. This report has been licensed for distribution. Only licensee may post/distribute. Vendors and products depicted in Radicati Market Quadrants should not be considered an endorsement, but rather a measure of The Radicati Group's opinion, based on product reviews, primary research studies, vendor interviews, historical data, and other metrics. The Radicati Group intends its Market Quadrants to be one of many information sources that readers use to form opinions and make decisions. Radicati Market Quadrants are time sensitive, designed to depict the landscape of a particular market at a given point in time. The Radicati Group disclaims all warranties as to the accuracy or completeness of such information. The Radicati Group shall have no liability for errors, omissions, or inadequacies in the information contained herein or for interpretations thereof.

KEY MARKET QUADRANT TRENDS

- The **Top Players** in the Data Loss Prevention market today are *Boradcom, Forcepoint, Proofpoint, Fortra* and *Trellix*.
- The **Trail Blazers** quadrant includes *Safetica* and *Mimecast.*
- The **Specialists** quadrant includes *Fortinet, Microsoft* and *Netwrix.*
- There are no **Mature Players** in this market at this time.

DATA LOSS PREVENTION - VENDOR ANALYSIS

TOP PLAYERS

SYMANTEC BY BROADCOM

3421 Hillview Ave
Palo Alto, California, 94304
United States
www.broadcom.com

Broadcom, a publicly traded organization, offers a wide range of cybersecurity solutions under the Symantec and Carbon Black brands. The security solutions include information protection, endpoint, network, email and identity aimed at organizations of all sizes. Symantec and Carbon Black operate one of the largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats.

SOLUTIONS

Symantec DLP covers cloud, endpoint, network, and storage with on-premises and cloud hosted management options. The solution comprises several components which are available through a DLP Core and DLP Cloud solution.

- **DLP CORE** extends data loss prevention across the enterprise, detects insider risks, and protects critical information from exfiltration. It consists of:

  - **DLP for Endpoints** – DLP Endpoint Discover scans local hard drives and gives visibility into any sensitive data stored by users on laptops and desktops (Windows, Mac, and Linux) to establish a baseline inventory. It provides a number of responses including quarantining files, flagging files for Symantec Endpoint Protection, as well as custom response actions such as encryption, DRM, or redacting confidential information enabled by the Endpoint FlexResponse API. DLP Endpoint Prevent monitors users' activities and enables fine-grained control over a wide range of applications, devices, and platforms. It leverages vendor supplied native APIs to ensure comprehensive monitoring capabilities for common applications like the Browser (e.g. Chrome), Microsoft Office Suite applications, and more. It also provides a wide range of responses including identity-based encryption and DRM for files transferred to USB. Endpoint Prevent also alerts users to incidents using on-screen pop-ups or email notifications. Users can override policies by providing a business justification or canceling the action (in the case of a false positive).

  - **DLP for Storage** – DLP Network Discover finds confidential data by scanning network file shares, databases, and other enterprise data repositories. This includes local file systems on Windows, Linux servers; HCL Notes and SQL databases; Microsoft Exchange and SharePoint servers. Symantec DLP supports the ability to scale and achieve high scan throughput of up to 1 TB/hour (not limited to) while scanning file shares. DLP Network Protect adds file protection capabilities on top of Network Discover. It automatically cleans up all the exposed files it detects, and offers a broad range of remediation options, including quarantining or moving files, copying files to a quarantine area, or applying policy identity-based encryption and DRM to specific files.

  - **DLP for Network** – DLP Network Monitor, captures and analyzes outbound traffic on the corporate network, and detects sensitive content and metadata over standard, non-standard and proprietary protocols. It is deployed at network egress points and integrates with network tap or Switched Port Analyzer (SPAN). DLP Network Prevent for Email protects sensitive messages from being leaked or stolen by employees, contractors, and partners. It monitors and analyzes all corporate email traffic, and optionally modifies, redirects, or blocks messages based on sensitive content or other message attributes. DLP

Network Prevent for Web protects sensitive data from being leaked to the Web. It monitors and analyzes all corporate web traffic and optionally removes sensitive HTML content or blocks requests. It is deployed at network egress points and integrates with HTTP, HTTPS or FTP proxy server using ICAP.

- **User and Entity Behavior Analytics** – Information Centric Analytics is a user and entity behavior analytics (UEBA) platform that provides an integrated, contextually enriched view of cyber risks in the enterprise. It collects, correlates, and analyzes large amounts of security event data from across diverse sources, including all data exfiltration channels (data telemetry), user access (identity telemetry), corporate asset data, and alerts from other security systems (threat telemetry). Backed by patented machine learning, ICA delivers rapid identification and prioritization of user and entity-based risks. Symantec DLP allows adaptive policies to be created based on user risk.

- **Sensitive Image Recognition** – Optical Character Recognition provides the capability to extract text from images, scanned documents, screen shots, pictures and more. Form Recognition detects form images that contain sensitive data in a wide variety of image formats including Microsoft Office documents, PDF and JPEG.

- **DLP CLOUD** safeguards data across cloud apps, email, and the web. It comprises:

  - **CASB Audit** – discovers and monitors every cloud app used across the organization, identifies their users and highlights any risks and compliance issues they may pose. It provides visibility into Shadow IT, and blocks access to unapproved cloud services.

  - **CASB for SaaS** – is a cloud-based service that monitors and protects stored, transferred, and shared data. Supported cloud applications include Microsoft Office365, Google Workspace, Box, Salesforce, ServiceNow, and others.

  - **CASB for IaaS** – is a cloud-based service that monitors and protects stored, transferred, and shared data. Supported cloud applications include Microsoft Azure, Amazon Web Services and Google Cloud. Additionally, it provides integrated cloud security posture management to identify misconfiguration based on standards such as CIS Benchmarks, or PCI.

- **CASB Gateway** – continuously monitors and controls the use of cloud apps to enforce policies. It offers deep visibility into user activity across thousands of cloud apps and services, and both tracks and governs activity of sanctioned and unsanctioned cloud apps (i.e. with adaptive access options based on user risk).

- **DLP Cloud Detection Service for CASB** – inspects content extracted from cloud app and web traffic and automatically enforces sensitive data policies. Cloud to cloud integration with Symantec CASB protects data in motion and at rest across more than 100 unsanctioned and sanctioned cloud apps, including Microsoft 365, Google Workspace, Box, Dropbox, and Salesforce.

- **DLP Cloud Detection Service for Cloud SWG** – integrates with Symantec Cloud Secure Web Gateway to monitor even encrypted web traffic for protection of roaming and mobile users.

- **DLP for Email (with Microsoft365 and Gmail)** – continuously monitors corporate email traffic and protects against data leaks in real time with automated message modification or blocking to enforce downstream encryption or quarantine.

STRENGTHS

- Symantec DLP solutions are tightly integrated and available in two simple packages that cover on-premises (DLP Core) and cloud-managed (DLP Cloud) form factors.

- Symantec DLP solutions can manage and enforce a single policy across all DLP channels (cloud, endpoint, and on-premises) through a single pane of glass.

- Symantec DLP offers a strong set of content detection technologies through advanced capabilities such as machine learning, exact data matching, fingerprinting, image recognition, structured data identifiers (SDI) and tagging.

- Symantec's DLP solution includes CloudSOC (CASB) support for data classification, integration with encryption (i.e. Seclore), labeling (Microsoft Purview Information Protection) and digital rights management (i.e. Microsoft), and user entity behavior analytics (UEBA).

- Symantec DLP is fully integrated with key components of Symantec's product portfolio, in particular Email Security, Endpoint Security, and Network Security (i.e. ZTNA and Web Isolation). This delivers a consistent policy architecture and enforcement across multiple channels of potential data loss. Symantec DLP includes a rich collection of REST APIs allowing customers to build Symantec DLP into their wider cybersecurity infrastructure.

WEAKNESSES

- Symantec solutions are best suited for organizations with high end data security requirements.

- While Symantec offers a broad portfolio of data security solutions, it can be somewhat complex to manage for organizations with fewer resources. However, organizations can work with regional delivery partners (i.e. Catalyst partner network) to access DLP expertise.

- While Symantec continues to innovate in this space and has strong brand recognition, it is perceived to be more focused on the needs of enterprise customers than those of small to mid-market customers. The vendor is addressing this through its Catalyst partner network.

FORCEPOINT

10900-A Stonelake Blvd
Quarry Oaks 1, Suite 350
Austin, TX 78759
www.forcepoint.com

Forcepoint offers security solutions focused on minimizing the risk of data breaches and non-compliance through AI-powered data discovery, classification, remediation, and protection with continuous monitoring. Forcepoint is owned by private equity firm Francisco Partners.

SOLUTIONS

Forcepoint offers risk-centric solutions for DSPM, DDR, and DLP across all key channels and potential locations (including GenAI systems) to stop unwanted data exposure and exfiltration.

Forcepoint integrates context into all policies through rich data identification (powered by its AI Mesh which combines regex, classification, machine learning, natural language scripts, and large-scale fingerprinting) and continuous monitoring of data movement and risky behavior. This context streamlines policy creation, and incident management while reducing false positives and false negatives.

Forcepoint provides three ways of deploying its unified DLP solutions:

- **Forcepoint ONE Data Security** – is a cloud-native DLP SaaS solution that unifies data protection and management across endpoints, email, web, print, USB, file shares and cloud applications, enabling enforcement and administration from a centralized platform. Key DLP features include:

    - *Cloud Architecture* – auto-scaling architecture on AWS lets organizations scale to large numbers of endpoints and allows over-the-air updates for endpoint enhancements, data classifier updates, and high availability.

    - *Unified Policy Management* – allows data patterns to be defined once and applied from a single policy across key channels of potential data exfiltration.

    - *Large Data Identification Library* – includes over 1700 pre-defined classifiers and policy templates, covering 160 regions globally to simplify and accelerate DLP deployment and ongoing management.

    - *Risk-Adaptive Protection* – mitigates insider risks by analyzing user behavior and Forcepoint DLP incidents. It computes the user's risk using Forcepoint's Indicator of Behavior (IoB) analytic models. This risk score is actively communicated to DLP policies, enabling automated policy enforcement based on user risk levels across endpoints, cloud applications, web, and email. Additionally, Risk-Adaptive Protection assists in prioritizing workflow by highlighting critical alerts.

    - *Device Control* – enables visibility into data movement across removable storage devices. With granular access controls, administrators can manage the use of these devices connected to user endpoints.

- *Forensics* – delivers enhanced visibility into data movement enabling organizations to investigate security incidents to understand the cause of a data breach, enhance policy effectiveness, and streamline compliance. In legal situations, it provides evidence of data handling for litigation or regulatory scrutiny.

- **Forcepoint Data Security Suite –** is a comprehensive on-premises DLP solution covering endpoint, cloud applications, network, web, and email through a unified policy enforcement and management console. Key DLP features include:

  - *Large Data Identification Library* – includes a library of over 1700 pre-defined classifiers and policy templates, covering 160 regions globally that simplify and accelerate DLP deployment and ongoing management.

  - *Unified policy enforcement* – allows organizations to manage, define policies and manage incident alerts from a single interface without needing separate DLP instances across Endpoint, Email, CASB, and SWG.

  - *Protect intellectual property* – advanced DLP classifiers help analyze data unique to the organization and can be used to coach users to make good decisions about data handling or block unauthorized actions while prioritizing incidents by risk.

  - *Risk-Adaptive Protection* – mitigates insider risks by analyzing user behavior and Forcepoint DLP incidents. It computes the user's risk using Forcepoint's Indicator of Behavior (IoB) analytic models. This risk score is actively communicated to DLP policies, enabling automated policy enforcement based on user risk levels across endpoints, cloud applications, web, and email. Additionally, Risk-Adaptive Protection assists in prioritizing workflow by highlighting critical alerts.

  - *App Data Security API* – helps simplify custom application security, by utilizing a REST API, organizations can safeguard data within custom applications, even beyond traditional protocols like SMTP, HTTP, and FTP, allowing direct protection of sensitive information in custom applications without the need for an agent.

  - *GenAI Smart Search* – is a help tool integrated directly in the solution which allows users to ask questions using natural language directly within the management console. It

simplifies support by providing specific answers, eliminating the need to visit the support site, which makes information access faster and easier.

- **Hybrid DLP** – provides organizations with two options for deploying DLP in a cloud environment.

  - *Cloud hosted* – in conjunction with specific partners, on-premises DLP can be hosted in the cloud, removing the need for companies to manage the supporting hardware infrastructure.

  - *Partial and Fully managed* – also through partners, on-premises DLP is hosted in the cloud and can be partially or fully managed by the partner. This includes policy management and day-to-day incident management.

Forcepoint DLP technology integrates with **Forcepoint DSPM (Data Security Posture Management)** and **Forcepoint DDR (Data Detection & Response)**, providing optimized data discovery, classification, prioritization, and remediation for data-in-motion, data-in-use, and data-at-rest leveraging both predictive and generative AI. It uses AI Mesh technology based on a networked AI architecture, which utilizes a GenAI Small Language Model (SLM) and advanced data and AI components, to efficiently capture context from unstructured text. It is customizable and offers rapid, accurate classification without the need for extensive ongoing training. Forcepoint DSPM and DDR help strengthen DLP efficacy by ensuring organizations dramatically reduce their overall data risk (e.g., ROT data, dark data management, permissions management, duplicates, misplaced data/data sovereignty issues). Forcepoint DSPM and DDR integrate with Forcepoint DLP, providing accurate classification that strengthens data identification and enables Forcepoint DLP to provide policy enforcement. Forcepoint DLP policies are enforced on the web and in SaaS apps via Forcepoint Web Security and Forcepoint CASB, respectively.

STRENGTHS

- Forcepoint offers a variety of flexible cloud and on-premises deployment models.

- Forcepoint's Unified policy enforcement allows organizations to manage, define policies and manage incident alerts from a single interface without needing separate DLP instances across

Endpoint, Email, CASB, and SWG.

- Forcepoint's AI-Mesh technology leverages a generative AI based Small Language Model (SLM) and other techniques, delivering fast, accurate data classification without the need to be trained on millions of files.

- Forcepoint integrates with OpenAI's APIs for ChatGPT Enterprise and Microsoft's APIs for Copilot, providing visibility and control over sensitive data that is used with GenAI.

- Forcepoint Drip DLP allows for data leakage detection in partial files – across channels like endpoint, cloud, email and network.

- Forcepoint provides forensics capabilities which deliver visibility into how data is being used, enabling customers to better investigate incidents, identify causes of breaches, and enhance data security policies.

WEAKNESSES

- Forcepoint DLP does not offer a Linux agent, although it can cover Linux use cases via network/agentless DLP, (web, email, CASB controls with GPO locking down of channels such as print and USB).

- Mobile DLP support is based on cloud reverse proxy which some organizations may find cumbersome.

- Forcepoint solutions are highly sophisticated and best suited for organizations with complex data security requirements.

PROOFPOINT

925 Maude Ave
Sunnyvale, CA 94085
www.proofpoint.com

Proofpoint delivers solutions for archive and compliance, email security, data loss prevention, identity threat defense, insider threat management and security awareness. The company also has a managed security services arm. In 2024, Proofpoint acquired Normalyze, a provider of Data Security Posture Management (DSPM) solutions. Proofpoint is owned by investment firm Thoma Bravo.

SOLUTIONS

Proofpoint **Data Security** protects organizations from data loss that originates from users' accidental or intentionally malicious behavior. It brings together solutions for email, cloud, and endpoint DLP. The product combines content, behavior, and threat telemetry across multiple channels to address the full spectrum of human-centric data loss scenarios. It is a SaaS service available as a modular platform. It provides support for Windows and MacOS endpoints. The solution comprises the following components:

- **Adaptive Email DLP** – Uses behavioral AI to learn about employees' normal email sending behaviors, their trusted relationships and how they communicate sensitive data. It then analyzes each email to detect anomalous behavior, notifying administrators of potential data loss incidents, such as mis-delivered emails, mis-attached files, and email sending to unauthorized accounts.

- **Data Security Posture Management (DSPM**) – Addresses possible blind spots in data environments, while prioritizing the reduction of human-centric risks. It relies on an AI-powered agentless scanner, which accurately identifies and classifies sensitive data at scale across diverse environments. It identifies where sensitive data resides and who has access to it, to help security teams close gaps and reduce the attack surface. The solution helps discover and classify data stores, prioritize critical information, identify risky and excessive access, detect and remediate exposure risks, and streamline compliance and auditing processes.

- **DLP Transform** – Enables a human-centric approach to data loss across endpoint, cloud, and email. It prevents data loss from managed and unmanaged devices. By combining rich context on content and user behavior, it provides visibility into data exfiltration by careless or malicious insiders. On the endpoint, it collects telemetry on data movement but also on user interactions with data such as renaming a file and changing its extension. This helps organizations understand the behavior of risky users. In the cloud channel, DLP Transform protects data using advanced methods for content-matching and text extraction. In the email channel, DLP Transform automates compliance by identifying sensitive or regulated data in emails to prevent loss. It comes with pre-built data identifiers and dictionaries. Organizations can also create or upload custom dictionaries and identifiers that match their unique data needs, fine tune the matching strength of dictionary terms, and allow exceptions. Email encryption also serves as a TLS fallback to ensure fail-safe encryption. Recipients have flexible options to access encrypted messages, including web portal, mobile, or Outlook client. A unified administration and response console helps accelerate incident resolution.

- **Insider Threat Management** – Monitors users' data interaction and provides insights into risky behavior. By understanding user behavior before, during and after an incident, organizations can uncover their motivation and intention to help determine the best response. In addition, it supports the capture of screenshots of risky user activity, helping provide irrefutable evidence and accelerate investigations.

STRENGTHS

- Proofpoint delivers a solid human-centric DLP solution which helps correlate email, cloud and other threat intelligence with behavioral insights and advanced data detection (including AI-powered classification, Exact Data Matching and others) to determine data loss potential and upstream risk.

- The solution is available as a flexible, scalable, cloud-native platform that includes workflows, a unified alert manager and threat hunting capabilities, classification, reporting, and dashboards that allow administrators to accurately determine DLP violations and insider threats.

- Proofpoint's acquisition of Normalyze strengthened its Data Security solution with AI-powered DSPM technology, allowing organizations to discover, classify and protect data at scale across SaaS, PaaS, public or multi-cloud, on-premises and hybrid environments.

- Proofpoint also provides organizations with skilled experts to co-manage their DLP program, this is a key advantage with organizations with limited IT teams.

WEAKNESSES

- Proofpoint pricing can be somewhat complex if SKUs for add-ons (such as OCR for image analysis, screen capture for insider threat, and others) are included. The vendor has worked to address this with new packages.

- Proofpoint's function and feature releases on MacOS lag somewhat behind those for Windows. Support for Linux is not available.

- Customers reported some complexity with agent installation and updates. The vendor is working to address this through simplified packaging.

- Data center presence is currently limited to US, Canada, EU, Japan, and Australia. Proofpoint plans to add more data centers in other geographies, including the Middle East.

FORTRA'S DIGITAL GUARDIAN

11095 Viking Drive, Suite 100
Eden Prairie, MN 55344
www.digitalguardian.com

Fortra's Digital Guardian provides data loss prevention software aimed at stopping internal and external threats across endpoint devices, corporate networks, servers, databases and cloud-based environments. In 2021, Digital Guardian was purchased by Fortra (previously HelpSystems). Digital Guardian Data Loss Prevention, Titus Data Classification, and Vera Digital Rights Management together make up the Fortra Data Protection solution, aimed at protecting sensitive

data. Fortra is owned by private equity firms TA Associates, Charlesbank, HGGC and Harvest Partners.

SOLUTIONS

Digital Guardian provides a data protection platform purpose-built to stop both malicious and unintentional data loss from insiders and malicious data theft from outside attacks. The platform performs across the corporate network, traditional endpoints, and cloud applications, leveraging a big data security analytics cloud service, powered by AWS, to enable it to see and block all threats to sensitive information. The Digital Guardian platform comprises the following components:

- **Digital Guardian Data Protection Platform** – the platform, powered by AWS, is designed to operate on traditional endpoints, across the corporate network, and cloud applications, to see and block threats to sensitive information. It is available either as SaaS solution, or as a managed service deployment.

- **Digital Guardian for Endpoint Data Loss Prevention** – captures and records events at the system, user, and data level, both when connected to the corporate network, or offline. Granular controls allow organizations to fine tune responses based on user, risk level, or other factors. It is available for Windows, macOS, and Linux endpoints.

- **Digital Guardian for Network Data Loss Prevention** – helps support compliance and reduce risks of data loss by monitoring and controlling the flow of sensitive data via the network, email or web. Digital Guardian DLP appliances inspect all network traffic and enforce policies to ensure protection. Policy actions include allow, prompt, block, encrypt, reroute, and quarantine.

- **Digital Guardian for Cloud Data Loss Prevention** – allows organizations to adopt cloud applications and storage while maintaining the visibility and control needed to support compliance. It integrates with leading cloud storage providers to scan repositories, enabling encryption, removal, or other automated remediation of sensitive data before the file is shared in the cloud. Data already stored in the cloud can also be scanned and audited at any time.

- **Digital Guardian Analytics & Reporting Cloud (ARC)** – is an advanced analytics, workflow and reporting cloud service that delivers no-compromise data protection. Leveraging streaming data from Digital Guardian endpoint agents and network sensors, ARC provides deep visibility into system, user and data events. This visibility powers security analyst-approved dashboards and workspaces to enable data loss prevention and endpoint detection and response through the same console.

- **Digital Guardian for Data Classification** – is designed to automatically locate and identify sensitive data then apply labels to classify and determine how the data is to be handled. A set of comprehensive data classification solutions, from automated content and context-based classification to manual user classification, are optimized for regulatory compliance, intellectual property protection, and mixed environments.

- **Digital Guardian for Data Discovery** – provides visibility and auditing of sensitive data at rest across the enterprise. Digital Guardian's data discovery appliances use automatic, configurable scanning of local and network shares using discovery specific inspection policies to find sensitive data wherever it is located. Detailed audit logging and reports help demonstrate compliance, protect confidential information and reduce data loss risk.

STRENGTHS

- Digital Guardian's data protection platform protects sensitive data against both internal and external threats using the same agent, network appliance and management console. It also allows enterprises to mark data as confidential based on the context in which it was created and then relies on this contextual information to 'follow' data so that appropriate controls can be applied to avoid the egress of sensitive information.

- Digital Guardian offers a range of deployment options, including a SaaS-based platform, powered by AWS, or delivered as a fully managed solution. An on-premises option is also available.

- Digital Guardian provides a rich set of policy templates (policies and rules with configurable parameters) for a wide range of use cases via the DG Content Server, a securely protected server in its MSP environment.

- Digital Guardian protects against Drip DLP, through the detection of slow leaks of small amounts of sensitive data across multiple instances of transfers across different protocols by leveraging stateful rules on the endpoint to monitor for suspicious activity over time, and reporting which summarizes trends of user activity over time.

- Digital Guardian offers easy integration with Microsoft Purview Information Protection (MPIP), as well as leading solutions for SIEM, SOAR, threat intelligence, and more.

WEAKNESSES

- Digital Guardian has limited mobile DLP capabilities, so customers would need to rely on third party MDM/EMM solutions.

- Digital Guardian does not offer native CASB, SASE, SSE, and SWG integration, however it offers this through a partnership with Lookout, a cloud security company.

- While reporting is centralized in the Analytics and Reporting Cloud (ARC) platform, currently network appliance (nDLP) and endpoint agent (eDLP) have separate policy managers.

- Fortra is working to deliver a unified platform that will support enhanced integration across its acquisitions of Digital Guardian, Fortra Data Classification Suite (formerly Titus) and Digital Guardian Secure Collaboration (formerly Vera). Customers should check carefully on the level of integration of features and functionality.

TRELLIX

6220 America Center Dr.
San Jose, CA 95002
https://www.trellix.com

Trellix is a cybersecurity company founded in 2022 when a consortium led by Symphony Technology Group (STG) acquired and merged McAfee Enterprise and FireEye. Trellix offers

security solutions, threat intelligence and services that protect business endpoints, networks, servers, and more. Trellix is privately held.

SOLUTIONS

Trellix Data Loss Prevention (DLP) is a comprehensive security solution that protects organizations against data loss across endpoints, networks, email, web, and cloud environments. The solution can be deployed as individual products or in the form of various product suites, offering flexibility in implementation while maintaining consistent data security policies across an organization's infrastructure. Trellix DLP comprises the following components:

- **Trellix DLP Endpoint Complete** – safeguards against unauthorized data transfers across multiple channels, including applications, storage devices, browsers, email, and cloud services. The solution includes built-in Device Control (also available separately) and offers various protective actions such as blocking, alerting, encrypting, and quarantining sensitive data. It provides web protection through API-based content inspection for Google Chrome Enterprise and extension-based inspection for other major browsers like Chrome, Edge, Firefox, and Safari. The solution supports macOS and Windows platforms.

- **Trellix Device Control** – is available as part of Trellix DLP Endpoint Complete, or as a standalone solution, it manages data transfers to various removable storage devices on the endpoint including USB drives, CDs, DVDs, Bluetooth, and imaging equipment. The solution can block transfers based on content, context, or device type, and is compatible with both macOS and Windows systems.

- **Trellix DLP Discover** – protects and manages data at rest across networks, web, and email environments. The solution scans and indexes content within network shares and databases, (including Microsoft SharePoint and Box), providing administrators visibility into data usage, ownership, and storage locations. It offers fingerprint-based detection for unstructured data and Exact Data Matching for structured data across 400+ content types. The solution can perform various actions including classification/declassification, document fingerprinting, content relocation, and application of Microsoft Information Protection Labels. OCR capabilities are available either as a Network-only add-on or through the OCR Suite included in the Data Security Suite package.

- **Trellix DLP Network Prevent** – monitors and controls sensitive data transfers across email, instant messaging, HTTP/HTTPS, and FTP protocols. The solution integrates with cloud email and web gateways through an Amazon Machine Image (AMI), or directly with Trellix Collaboration Security to protect data in cloud email and services (AWS, M365, Google Workspace, Slack), cloud storage (Dropbox, Box, OneDrive) and cloud applications (Salesforce, WebEx, Microsoft Teams, Slack). It scans both inbound and outbound traffic across all ports and 400+ content types, including mobile device communications when properly configured through a web proxy. The solution features fingerprint-based detection for unstructured data and Exact Data Matching for structured data. Based on detection, it can encrypt, redirect, quarantine, or block sensitive content. OCR capabilities are available either as a Network-only add-on or through the OCR Suite included in the Data Security Suite. The solution includes Capture capabilities that record network traffic for forensics, auditing, and rule optimization, even when DLP rules aren't triggered.

- **Trellix DLP Network Monitor** – identifies, tracks, and reports data-in-motion across an organization's network through SPAN/TAP integration with egress devices. It is available as a physical or virtual appliance and can detect and manage over 400 content types using fingerprint-based detection for unstructured data and Exact Data Matching for structured data. The solution includes Capture capabilities that record network traffic for forensics, auditing, and rule optimization, even when DLP rules aren't triggered. OCR functionality is available either as a Network-only add-on or through the OCR Suite included in the Data Security Suite.

Trellix ePolicy Orchestrator (ePO) is a centralized management platform available on-premises, or via SaaS, through hybrid and private cloud deployment. It provides comprehensive administration of all DLP products, enabling deployment, policy management, incident handling, and compliance reporting. The platform comes with pre-built regulatory compliance policies (GDPR, PCI, HIPAA, and others) and supports two-way integration with SIEM, SOAR, and incident management platforms, as well as Trellix encryption protection tools.

STRENGTHS

- Trellix DLP offers organizations flexible options for extending data loss prevention to cloud environments through DLP Network Prevent integrations or integration with Skyhigh

Security.

- Trellix ePO provides a single pane of glass to administer policy management across endpoint, network, and the cloud through built-in capabilities with Skyhigh Security and DLP Network Prevent.

- Capture capabilities included in Trellix DLP Network solutions log all data in motion and deliver valuable analytics to administrators about how data is being used and sent, which makes it also useful for investigation, and audit purposes.

- The Trellix DLP solution offers both automated and manual classification by end-users. The Manual Classification, which is included free in the DLP Endpoint license helps increase end-user data protection awareness and reduce administrative burden.

WEAKNESSES

- Trellix DLP does not provide agent support for Linux. The vendor has this on its roadmap.

- Trellix DLP does not offer specific features for Drip DLP detection. While such detection can be set up through rules, this can be somewhat cumbersome.

- Trellix supports data protection for Microsoft 365 applications, including Teams, only through an integration between DLP Network Prevent and Trellix Collaboration Security.

- While offering a rich set of features, Trellix DLP requires an experienced IT team to properly install and maintain the solution in a way that fully leverages its capabilities. Trellix is addressing this through its newly launched Thrive customer support program.

TRAIL BLAZERS

SAFETICA

99 S. Almaden Boulevard #600
San Jose, CA 95113
www.safetica.com

Safetica offers Data Loss Prevention (DLP) and Insider Risk Management (IRM) solutions designed to protect sensitive data, ensure compliance and mitigate potential risks from insider threats. Safetica is a privately held company, with a customer base in over 120 countries.

SOLUTIONS

Safetica offers an “all-in-one" data loss prevention and insider risk management solution that helps prevent user mistakes and malicious acts to secure sensitive data while maintaining efficient business operations. The solution utilizes AI to provide wide incident context and proactive protection. It offers features such as data flow inspection, anomaly detection, data discovery with all flavors of data classification like content and context-aware, workspace risk analysis, insider risk detection and management, and wide range of 3rd party integrations and compatibility to ensure detect and respond wokflows in organization’s security stack.

Safetica can be deployed in the cloud or on-premises and offers a web console with centralized policy handling for easy log consumption and security management. Safetica’s Windows and macOS endpoint agents can be deployed manually or automatically via standard remote management tools such as MDM tools, Intune, GPO policy, LanDesk, and others. While Safetica is distributed as a single package, each part of the system can be configured individually.

Cloud security features can be integrated with an organization's Microsoft 365 and Entra ID tenants to monitor and protect SharePoint Online data and Exchange Online email messages and their attachments. This can be combined with a Microsoft Outlook add-in to protect hybrid access even outside the company perimeter and BYOD devices.

The Safetica product portfolio covers the following data security scenarios:

- *Gain data visibility and discover sensitive data* – Safetica helps discover and classify valuable data using Safetica Unified Classification, which combines analysis of file content, file origin, and file properties.

- *Protect sensitive and business-critical data* – Safetica protects sensitive data, source code, or blueprints from accidental or intentional leakage.

- *Prevent insider risks and promote security awareness* – Safetica analyzes insider risks, detects threats, and mitigates risks. Notifications about how to treat sensitive data help raise awareness around data security and educate users.

- *Maintain data security for remote work* – Safetica provides full capabilities, including data protection, complete contextual visibility, and incident-driven training, regardless of location or network status.

- *Detect and mitigate regulatory compliance violations* – Safetica helps detect, prevent, and mitigate regulatory violations. Its audit capabilities support incident investigation to comply with leading regulations and data protection standards like GDPR, HIPAA, SOX, PCI-DSS, GLBA, ISO/IEC 27001, or CCPA.

The Safetica product portfolio covers the following key features and capabilities:

- *Contextual, AI-Controlled Defense* – Safetica's proprietary technology combines data classification, contextual risk analysis, and adaptive protection policies to detect anomalies and unusual user behavior as well as to autonomously respond with dynamically applied security measures tailored to each user's standard behavior.

- *Contextual risk analysis* – Safetica applies proprietary technology to evaluate the risk of data operations by analyzing the operation's context: detect data classification, assignment of data destination, user typical working hours, user insider risk level, and more.

- *Smart Insights* – Safetica consolidates key security events and findings and serves them as actionable tasks for administrators to review, investigate, and act upon.

- *Data in use* – Safetica provides data-in-use auditing and protection with flexible levels of granularity, covering files, applications, devices, cloud services, network storage, and all common ports and protocols.

- *Data in motion* – Safetica offers data-in-motion auditing and protection with cross-channel capabilities across common communication channels. It integrates with third-party solutions such as Microsoft 365 file storage (SharePoint Online, OneDrive for Business), Microsoft Exchange Online, and more.

- *Data at rest* – Data-at-rest discovery enables discovery of sensitive files on protected endpoint devices or network storages, defined via contextual- or content-based classification rules. Discovery supports a broad set of supported file types, including OCR capability to analyze text in image-based files. Supports recognition of third-party data classification labels (e.g. Microsoft Purview, Boldon James, etc.) and offers a range of pre-defined classification templates for various regions and security regulations.

- *Policy controls* – The solution comes with pre-defined policy templates for chosen regions and/or regulations.

- *Drip-DLP* – Safetica monitors slow- or cumulative-sensitive data leaks by evaluating all transferred data from individual sources or to each destination, with instant alerts to administrators.

STRENGTHS

- Safetica offers fast deployment, low-maintenance management, and minimal hardware requirements for both endpoints and servers.

- Safetica is designed to address a broad set of use cases, including intellectual property (IP) protection, regulatory compliance, advanced user behavior, workspace analysis and protection, and security audits.

- Safetica offers high visibility into the data flow, user behavior, and related security risks, with advanced capabilities, such as protection against agent manipulation, management

audit trail, and more.

- Safetica enables seamless integrations with the IT security stack. It also provides reporting API to integrate with analytic services like Power BI or Tableau. Safetica also supports forwarding detected security events to a third-party SIEM or ticketing solutions.

- Safetica benefits from a highly developed partner network to help integrate the solution fully with the customer environment.

- Safetica delivers affordable, scalable protection optimized for mid-market and SMB organizations.

WEAKNESSES

- Safetica does not provide full-blown Drip-DLP detection, however, it does generate administrator alerts (Insights) about continuous or cumulative data transfers and can apply automatic remediation when the amount is abnormal.

- Safetica does not offer dedicated Mobile DLP, however, it allows for some data loss prevention scenarios to be addressed through its integration with Microsoft365.

- Safetica currently lacks support for Linux endpoints.

- Safetica offers API-based integrations with Microsoft365, Entra ID, and Microsoft Purview Information Protection sensitivity labels, however, its integration data classification capabilities are not on the same level as the classification possibilities on endpoint devices, and it does not offer data-at-rest discovery for Microsoft365 cloud files. Improved data classification and cloud data-at-rest discovery are on the vendor's roadmap.

- Safetica lacks the machine learning capabilities to predict risks, that are becoming prevalent in competing solutions.

MIMECAST

1 Finsbury Avenue
London
EC2M 2PF
www.mimecast.com

Mimecast is a cybersecurity company that provides integrated solutions for email, messaging, and collaboration security, data protection, and threat intelligence. Founded in 2003, Mimecast specializes in protecting organizations from cyber threats, ensuring compliance, and managing risk across email, collaboration platforms, and cloud applications. The company is UK based, with North American headquarters in Lexington, MA and offices globally. Mimecast is privately held.

SOLUTION

Mimecast **Incydr** is a cloud-first, API-driven Data Loss Prevention (DLP) solution that provides visibility and control over data exfiltration across endpoints, cloud applications, email, and collaboration platforms. It is designed to detect and respond to risky file movements, insider threats, and unauthorized data sharing using policy-based enforcement, machine learning-driven anomaly detection, and integration with security orchestration platforms.

Mimecast Incydr key features and capabilities include:

- *Real-Time Data Movement Monitoring* – Tracks and analyzes file transfers across endpoints, cloud storage, web browsers, email, and messaging apps to detect unauthorized data sharing. It also identifies copy/paste actions, USB transfers, cloud uploads, and file-sharing activities that may indicate exfiltration attempts.
- *Cloud and Collaboration Security* – Integrates with Google Drive, OneDrive, Box, Salesforce, Microsoft 365, and Slack for DLP enforcement in cloud environments. It also supports API-based CASB/SASE integrations for cloud-to-cloud data movement detection.
- *Behavioral Analytics & Risk-Adaptive Policies* – Uses User and Entity Behavior Analytics (UEBA) to detect anomalous data movement based on historical behavior

patterns. Dynamically adjusts policy enforcement based on user risk scores and insider threat indicators.

- *Adaptive Enforcement & Response Controls* – Supports escalating policy actions for repeat violations, including automated alerts, micro-educational nudges, and manager approvals. Integrates with SIEM, SOAR, and ITSM solutions (Splunk, IBM QRadar, ServiceNow, Microsoft Sentinel) for incident response automation. Enables network isolation and containment actions via EDR and CASB platforms.

- *GenAI & Emerging Technology DLP Protections* – Monitors file uploads and copy-paste actions in unsanctioned AI tools such as ChatGPT, Google Gemini, Jasper, and Perplexity. Enforces data protection policies across AI-generated content workflows.

STRENGTHS

- Mimecast Incydr uses User and Entity Behavior Analytics (UEBA) to dynamically adjust DLP policies based on user behavior, anomaly detection, and contextual risk assessment. This provides proactive, adaptive enforcement rather than relying solely on static rules.

- Mimecast Incydr provides policy enforcement across email, endpoints, cloud storage, messaging, and web browsers, ensuring comprehensive data protection across communication channels.

- Incydr integrates with SIEM, SOAR, and ITSM platforms (Splunk, IBM QRadar, Microsoft Sentinel, ServiceNow, Jira) to enhance incident response and security automation.

- Mimecast offers native integrations with CASB and SASE providers, including Microsoft Defender for Cloud Apps (MCAS), Netskope, Zscaler, McAfee MVISION Cloud, and Cisco Umbrella, for cloud-to-cloud exfiltration monitoring.

WEAKNESSES

- Mimecast Incydr is only available as a cloud service. Customers interested in on-premises or hybrid deployments will need to consider alternative vendors.

- Mimecast Incydr is focused mainly on data-in-motion protection. Data-at-rest scanning, if desired, needs to be handled through third-party integrations.

- Mimecast Incydr does not offer native encryption capabilities. Encryption enforcement is handled via third-party integrations (e.g. Microsoft 365 Message Encryption, PGP, S/MIME).

- Mimecast Incydr enforces mobile DLP policies only through partner integrations with MDM/UEM vendors (i.e., Microsoft Intune, VMware Workspace ONE, MobileIron, Citrix Endpoint Management).

SPECIALISTS

FORTINET

909 Kifer Road
Sunnyvale, CA 94086
www.fortinet.com

Fortinet is a cybersecurity company which develops firewalls, endpoint security and intrusion detection systems. In 2024, Fortinet acquired Next DLP, a UK based developer of cloud based DLP solutions. Fortinet is a publicly traded.

SOLUTIONS

Fortinet's **FortiDLP**, is a cloud-native endpoint data protection solution that combines Data Loss Prevention, Insider Risk Management, SaaS Data Security, Behavioral Analytics, and Risk-Informed User Education. It integrates into Fortinet's broader **Security Fabric**, providing protection across managed devices (Windows, macOS, Linux), unmanaged devices (mobile), and SaaS applications.

FortiDLP is available in three versions:

- *Standard* – which focuses on DLP functionality through integrated device control, inline DLP for Web, Email, Cloud Drive and connected media, real-time data classification, secure

data flow, Microsoft MIP/AIP label support, file forensics, and more.

- *Enterprise* – which adds insider risk management and SaaS data security through connectors for Google Workspace, Microsoft Office 365, and File Sharing controls.

- *Managed Service* – which includes product deployment and provisioning, optimization of DLP rules, and on-going product maintenance and reporting.

It offers the following key features and capabilities:

- *Lightweight Cross-Platform Endpoint Agent* – The FortiDLP agent combines ML-powered behavioral analytics, activity monitoring, advanced content inspection, Secure Data Flow and automated DLP policy enforcement. FortiDLP supports Windows, macOS, and Linux with near complete feature parity. Native integration to Microsoft Information Protection (MIP) is also supported.

- *Flexible SaaS and Hybrid Deployment Model* - the FortiDLP management console is updated regularly with new features, policy templates and security analytics. Forensics, such as documents and media files, are automatically captured and stored within the customer's private cloud or on-premises data center.

- *Rich out-of-the-box data visibility, risk assessment, and policy creation* – FortiDLP agents and cloud connectors automatically collect, enrich, and index a broad range of activity event types (e.g. authentication, web, email, applications, USB, file creation, sharing and download activity). This data set is then used to highlight and report on data exposure risk, create data protection policies, and provide activity data set to support investigations.

- *Context and Content-Aware Data Protection Policies* – Secure Data Flow automatically identifies and tracks data based on its origin and DLP policies can be enforced based on where data originated. The tracking system also detects and records file manipulation. The FortiDLP agent autonomously evaluates content and classifies data at creation, usage and movement. The content inspection engine automatically identifies files containing PII, PHI, and PCI data. Endpoint file data does not need to be sent into the cloud for content inspection.

- *Cloud and Mobile Data Security* - FortiDLP cloud connectors for Microsoft 365 and Google Workspace extend data protection policies to unmanaged mobile devices.

- *Activity Timeline* - the Activity Feed provides a timeline UX where analysts can quickly see all DLP alerts, insider risk detections and user activity events across all devices and cloud drives associated with a user or endpoint under investigation.

- *Investigate Data Protection Search Engine* - enables analysts to carry out threat hunting queries across the rich alert, detection and event data set collected by FortiDLP.

- *XTND AI Powered Sequence Detection and Activity Reporting* – FortiDLP automatically identifies, sequences and risk scores high-risk activity chains. This capability enables analysts to prioritize their investigation time. Detections are also automatically mapped using MITRE's ATT&CK Insider Threat Knowledge TTPs.

- *Machine Learning (ML) and Behavioral Analytics* – the FortiDLP agent includes an endpoint native Machine Learning system which can detect unique and anomalous activity, such as the first time a file transfer application is executed or a sudden increase in files being copied into an unsanctioned cloud drive.

- *API-powered Integrations* – FortiDLP is an API-driven platform that provides easy integration with business applications, including HR-IS, SIEM, SOAR/HA, Service Desk, and more.

- *Integration to Entra ID (Azure AD), Google Directory, Active Directory and LDAP* – serves to synchronize users and entity attributes to provide useful context for investigations. This allows for policy assignment based on user attributes, i.e., user department, location, group membership, employee lifecycle changes, and more.

STRENGTHS

- FortiDLP offers a low-profile endpoint agent that delivers protection via personalized user behavior analytics and machine learning on the endpoint. The agent independently monitors its own health through self-auditing and automatic generation of performance reports for

inspection by system administrators.

- FortiDLP integrates with Fortinet Security Fabric which offers seamless integration with Fortinet's suite of products (e.g., FortiGate, FortiClient, FortiAnalyzer) and provides a unified security approach.

- FortiDLP provides visibility into endpoint activities, for all leading platforms, Microsoft Windows, macOS, and Linux endpoints and servers. Once deployed, it offers instant telemetry to inform policies which can be added at any time to define activities and data types that need more robust monitoring and controls.

- FortiDLP provides a single management console for all product capabilities including agent deployment, reporting, analysis, ongoing system administration, and more. For MSSP partners it also provides the ability to manage multiple customers/tenants using a common white labeled MSSP Console.

- Fortinet also offers Managed Services, through a team of experienced security analysts, that can act as an extension to the customer security team and manage their data protection needs on a day-to-day basis.

- FortiDLP is well aimed at the DLP needs of mid-market organizations which may not already have extensive DLP policies in place and can scale to large enterprises.

WEAKNESSES

- FortiDLP is a cloud-based service. While it offers the ability to host in customer private cloud environments, customers requiring purely on-premises deployments will need to look elsewhere.

- FortiDLP does not scan pre-existing data at rest. However, the Secure Data Flow feature identifies and annotates information on the origin of new files.

- FortiDLP lacks some of the more advanced features, like user behavior analytics (UBA) or deep content inspection for complex data types, that are typically available in more advanced

competing solutions. This may not make it suitable for organizations with highly complex DLP needs.

- Setting up and managing DLP policies in FortiDLP can be complex, especially for organizations without dedicated IT security teams.

- FortiDLP works best within the Fortinet ecosystem. Organizations not using Fortinet products may find it less appealing or more difficult to integrate.

MICROSOFT

1 Microsoft Way
Redmond, WA 98052
www.microsoft.com

Microsoft offers products and services for businesses and consumers, through a portfolio of solutions for office productivity, messaging, collaboration, and more.

SOLUTIONS

Microsoft offers DLP as part of its larger **Purview** suite of solutions which address risk and compliance for Microsoft 365 services, including Microsoft Teams, SharePoint Online, OneDrive for Business, Exchange Online, and others. Purview combines the former Azure Purview and Microsoft 365 compliance solutions and services into a single brand. Microsoft has also extended DLP protections to Microsoft 365 Copilot, through **Microsoft Purview DLP for Microsoft 365 Copilot. In addition, Microsoft offers Purview Data Loss Prevention for Fabric, which** allows organizations to apply Purview DLP policies to detect the upload of sensitive data (e.g. social security numbers) to a lakehouse in Fabric, Microsoft's data analytics platform.

Purview allows organizations to implement data loss prevention strategies by defining and applying DLP policies which can identify, monitor and protect sensitive items across:

- Microsoft 365 services such as Teams, Exchange, SharePoint, and OneDrive.

- Office applications such as Word, Excel, and PowerPoint.
- Windows 10, Windows 11 and macOS endpoints.
- Non-Microsoft cloud applications.
- On-premises file share and on-premises SharePoint.
- Fabric and Power BI workspaces.
- Microsoft 365 Copilot

DLP detects sensitive items through deep content analysis which includes primary data matches to keywords, evaluation of regular expressions, internal function validation, secondary data matches that are in proximity to the primary data match, machine learning algorithms, and other methods to detect content that matches existing DLP policies. DLP also uses machine learning algorithms and other methods to detect content that matches existing DLP policies.

The **Microsoft Purview Compliance Portal** provides a central policy management console that allows administrators to define and manage DLP policies across different services. DLP policies can be set up to monitor user actions on on sensitive items at rest, in transit, or in use and protective actions can be taken accordingly. All DLP monitored activities are recorded to the *Microsoft 365 Audit log*, which can be viewed and searched from the Microsoft Purview Compliance Portal, and are routed to *Activity explorer*, which provides a historical view of activities on labelled content. When a user performs an action that meets the criteria of a DLP policy, and alerts are configured, DLP provides alerts in the *DLP alert management dashboard*. A **DLP on-premises scanner** solution extends DLP protection to on-premises file shares and SharePoint document libraries.

DLP policies can be applied to data at rest, in use, or in motion in locations, such as:

- Exchange Online email
- SharePoint Online sites
- OneDrive accounts
- Teams chat and channel messages
- Microsoft Defender for Cloud Apps
- Windows 10, Windows 11, and macOS (three latest released versions) devices
- On-premises repositories
- Fabric and PowerBI sites
- Microsoft 365 Copilot

Microsoft Purview Double Key Encryption helps secure sensitive data that is subject to the strict protection requirements. The use of a *Microsoft Purview Customer Key* helps meet regulatory or compliance obligations for controlling root keys, and explicitly authorizes Microsoft 365 services to use the given encryption keys to provide value added cloud services, such as eDiscovery, anti-malware, anti-spam, search indexing, and others.

Microsoft 365 E3 and E5 licenses include DLP support for email and files. A Microsoft 365 E5 license is required for DLP for Teams Chat and Endpoint DLP.

STRENGTHS

- Microsoft has made compliance and data protection a high priority and is diligently introducing a features and functionality across its entire Microsoft 365 product offering. Microsoft Purview DLP is tightly integrated with Exchange Online, SharePoint, OneDrive, Teams, and Office apps, providing consistent protection across the entire Microsoft ecosystem and enabling a unified approach to data governance.

- Microsoft Purview DLP offers comprehensive coverage protecting data across email, files, Team chats, and endpoints. It also extends to third party cloud applications (e.g. Google Drive, Dropbox) and on-premises data repositories through Microsoft Defender for Cloud Apps.

- DLP comes mostly native, free of charge with many Microsoft Office 365 plans (in particular E3 and E5 enterprise plans), where an additional fee is required, it is usually very small.

- Microsoft solutions are well thought out to help organizations meet compliance requirements, as well as reduce the risk of data loss through exfiltration or malicious tampering.

WEAKNESSES

- Microsoft offers a rich ecosystem of compliance solutions, however, integrating all components correctly and maintaining them fully integrated throughout Microsoft's continuous upgrade cycle can be daunting for many organizations.

- Microsoft DLP solutions are primarily geared to an Microsoft ecosystem, integration with third party cloud apps and non-Windows devices is somewhat limited, leaving potential protection gaps.

- Microsoft's DLP solutions continue to evolve rapidly, which can make it difficult for customers to understand how the various features match up with their own compliance goals and how to plan for future growth.

- Microsoft offers DLP features with many different plans at different price points, but it is often difficult for customers to understand exactly what features they are getting with what plans.

- Microsoft customers we spoke to as part of this research, often indicated that they view Microsoft's DLP and compliance functionality as a steppingstone to a more complete compliance deployment through the deployment of additional solutions from other vendors.

NETWRIX

6160 Warren Pkwy Suite 100
Frisco, TX
75034, United States
www.endpointprotector.com

Netwrix a cybersecurity vendor which offers endpoint solutions, recently purchased CoSoSys a provider of solutions for Data Loss Prevention (DLP), including Device Control, eDiscovery, Content Aware Protection, and Enforced Encryption. Netwrix is privately held, and has offices in the United States, EMEA and Asia Pacific.

SOLUTIONS

Netwrix **Endpoint Protector** is a comprehensive and cross-platform Data Loss Prevention (DLP) solution for Windows, macOS and Linux. The solution focuses on avoiding unintentional data leaks, protects from malicious data theft and offers seamless control of portable storage devices, even when employee endpoints are offline. It covers all major exit points such as email,

cloud file uploads, messaging apps, printers, portable storage devices and more. It offers content monitoring and filtering capabilities, for both data at rest and in motion, ranging from file type to predefined content based on dictionaries, regular expressions and machine learning. It supports key data protection regulations such as GDPR, CCPA, HIPAA, PCI DSS, NIST and others. Administrators can define detection patterns based on proximity, dictionaries, regular expressions, and more. The movement of valuable data to unauthorized external individuals is monitored and controlled through the exit points and administrators are alerted in the case of a policy violation. Endpoint Protector enables seamless management of all organization endpoints, regardless of operating system, from a single dashboard.

Endpoint Protector is offered in various form factors, including as a virtual appliance, as well as an instance on AWS, Microsoft Azure and Google Cloud Platform (GCP). The virtual appliance supports all popular hypervisors, e.g. VMware, HyperV, Citrix XenServer, and others. Endpoint Protector is also available as a hosted SaaS solution.

Endpoint Protector features four specialized modules that can be mixed and matched based on client needs. The modules comprise:

- *Content Aware Protection* – gives organizations detailed control over sensitive data leaving their computers. Through close content inspection, transfers of PII, PHI, PCI, or important company documents are blocked, logged, and reported. File transfers can be allowed or blocked based on predefined company policies, and can be applied to web, mail, instant messaging apps, file shares, and more. Contextual Detection is also available which offers an advanced way of inspecting confidential data based on both content and context. The Deep Packet Inspection functionality currently available on Windows, macOS and Linux allows network traffic inspection at an endpoint level and offers a detailed content examination of file transfers. A User Remediation feature is also available.

- *Device Control* – gives organizations granular control over USB devices, Bluetooth and peripheral ports' activity on employees' computers through a simple web interface. Organizations can implement strong device use policies that will scan data transfers to portable storage devices, or block their usage (or certain features, e.g. allow charging of iPhones but not data transfer) in order to protect sensitive data.

- *Enforced Encryption* – can be automatically deployed or manually installed on USB devices in the root folder, after which any data copied onto the device will be automatically encrypted with government-grade 256 bit AES CBC-mode encryption. The encrypted data can be accessed both on Windows and macOS endpoints.

- *eDiscovery* – offers the possibility to scan sensitive data at rest, stored on employees' endpoints based on specific file types, predefined content, file name, regular expressions or compliance profiles for regulations such as HIPAA, GDPR, PCI DSS and others. Scans can also take into account the proximity to dictionary keywords or Regular Expressions, as well as various thresholds. Based on the scan results, remediation actions can be taken, such as encrypting or deleting files that violate policies for data breach protection.

Netwrix also offers *sensitivity.io*, a data loss prevention API for developers which allows them to discover and protect sensitive data, and easily design HIPAA, PCI and other compliance policies into their apps. It is available as distinct modules, with specific SDKs, for data loss prevention and data classification.

STRENGTHS

- Netwrix Endpoint Protector offers strong coverage for Windows, macOS and Linux, with feature parity across platforms, zero-day support and a lightweight agent. This makes it a good choice for organizations running mixed OS environments.

- Endpoint Protector enables seamless management of all company endpoints from a single dashboard.

- Netwrix Endpoint Protector is available in diverse deployment options, including virtual appliances, thus meeting the needs of customers with a wide range of infrastructures.

- Netwrix Endpoint Protector is easy to install and deploy through flexible policy management and an intuitive user interface.

- Netwrix Endpoint Protector solution is designed to also be easily managed by non-specialized technical personnel.

WEAKNESSES

- Netwrix lacks some of the advanced features, such as deep content inspection or advanced machine learning capabilities or user behavior analytics (UBA), which are typically found in competing DLP solutions,
- Netwrix offers OCR image analysis capabilities, but it only covers a limited number of languages.
- Netwrix does not offer support for mobile DLP, or integrations with leading EMM or MDM solutions.
- Netwrix does not offer capabilities for detecting Drip-DLP.
- Netwrix does not offer or integrate with CASB solutions.

THE RADICATI GROUP, INC.
http://www.radicati.com

The Radicati Group, Inc. is a leading Market Research Firm specializing in emerging IT technologies. The company provides detailed market size, installed base and forecast information on a worldwide basis, as well as detailed country breakouts, in all areas of:

- **Email**
- **Security**
- **Social Media**
- **Instant Messaging**
- **Archiving & Compliance**
- **Wireless & Mobile**

The company assists vendors to define their strategic product and business direction. It also assists corporate organizations in selecting the right products and technologies to support their business needs.

Our market research and industry analysis takes a global perspective, providing clients with valuable information necessary to compete on a global basis. We are an international firm with clients throughout the US, Europe and the Pacific Rim. The Radicati Group, Inc. was founded in 1993.

CONSULTING SERVICES

The Radicati Group, Inc. provides the following Consulting Services:

- Strategic Business Planning
- Management Advice
- Product Advice
- TCO/ROI Analysis
- Investment Advice
- Due Diligence

MARKET RESEARCH PUBLICATIONS

The Radicati Group, Inc. develops in-depth market analysis studies covering market size, installed base, industry trends and competition.

To learn more about our reports and services,
please visit our website at www.radicati.com

