The Radicati Group, Inc.
www.radicati.com

THE RADICATI GROUP, INC.

Data Loss Prevention – Market Quadrant 2024 *

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

March 2024

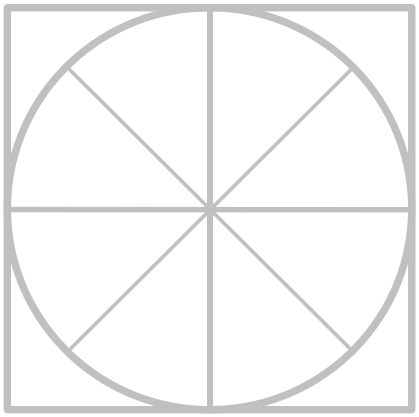

TABLE OF CONTENTS

==========

==========

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.

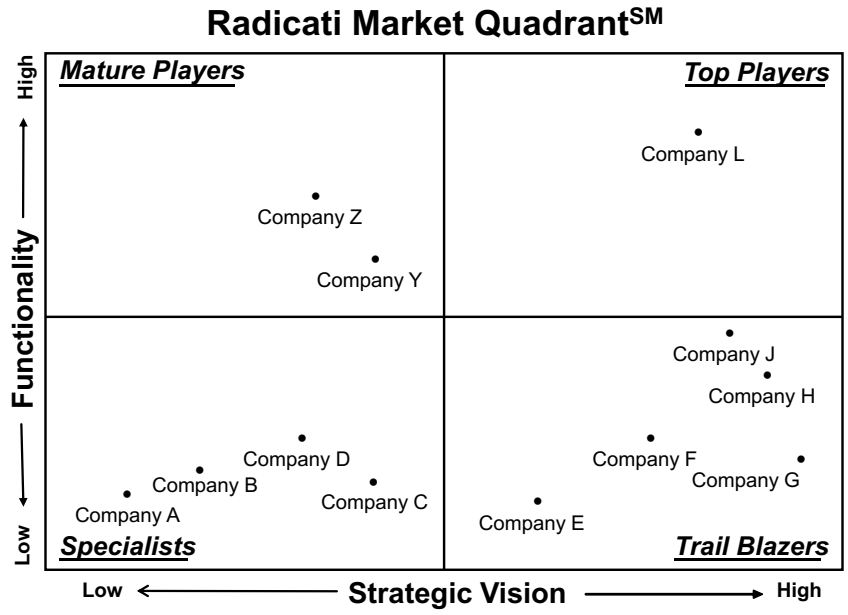

Figure 1: Sample Radicati Market Quadrant

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: *Forcepoint, Fortra, Microsoft, Netwrix, Next DLP, Proofpoint, Safetica, Symantec,* 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 $2.8 billion in 2024, to over $7.0 billion by 2028.

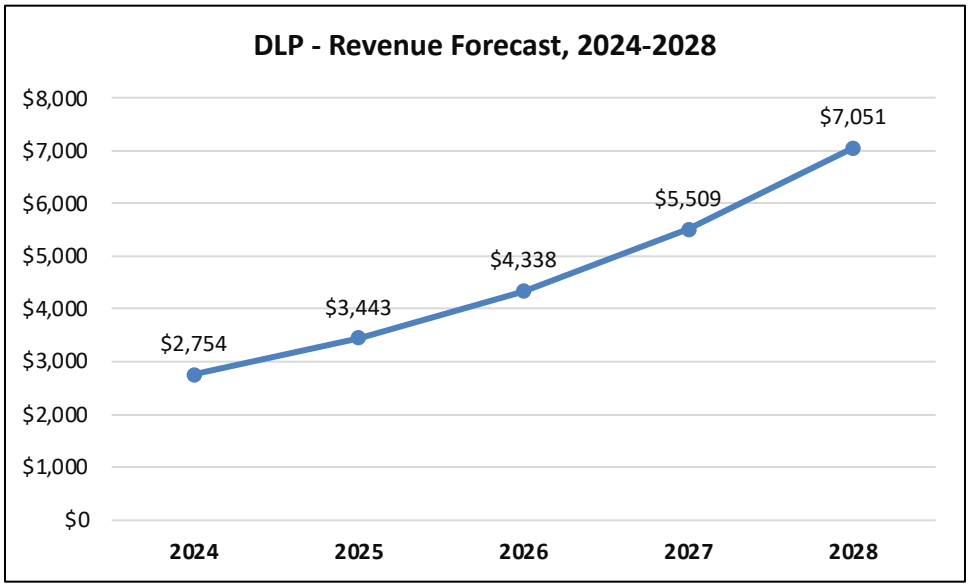

Figure 2: DLP Revenue Forecast, 2024 – 2028

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

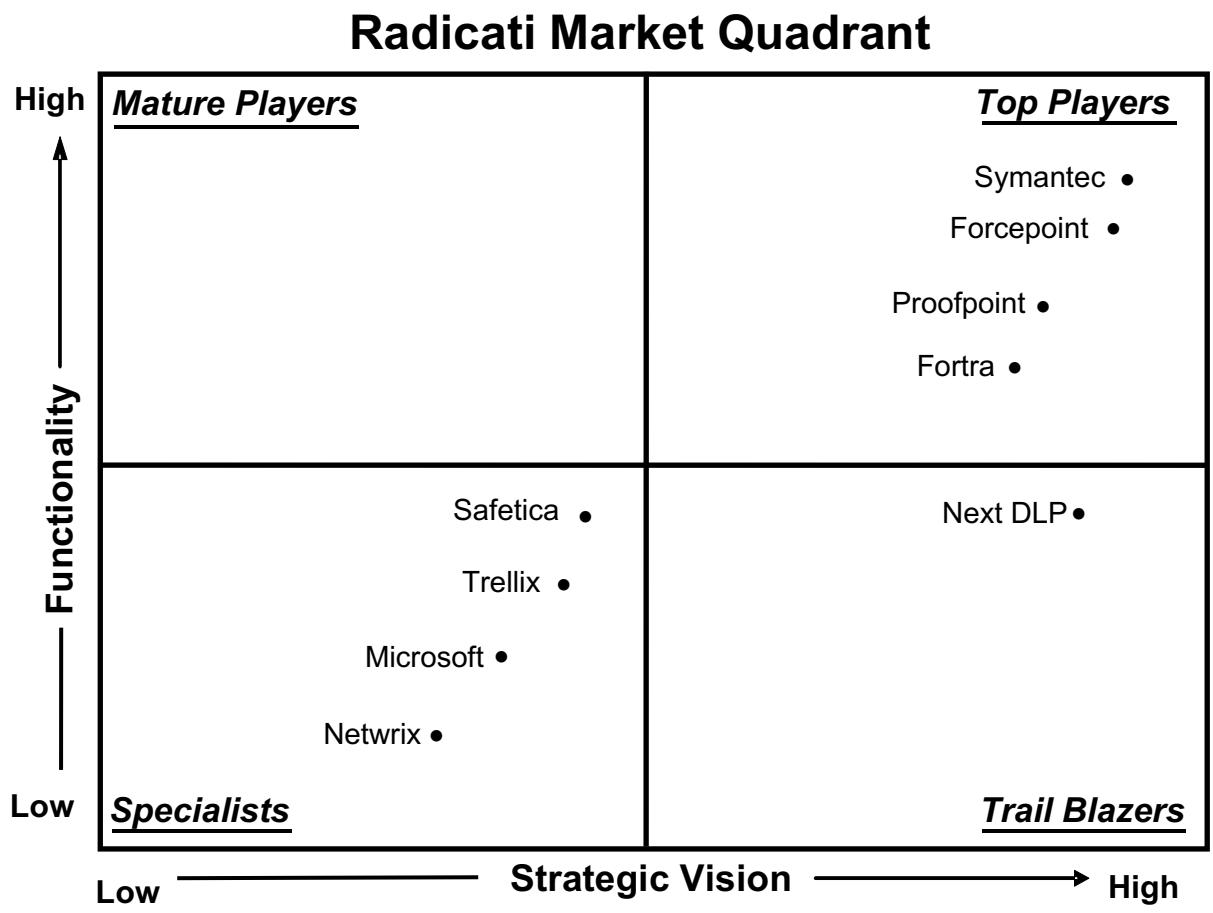

Figure 3: Data Loss Prevention Market Quadrant, 2024*

* Radicati Market Quadrant is copyrighted March 2024 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 *Symantec, Forcepoint, Proofpoint* and *Fortra*.
- The **Trail Blazers** quadrant includes *Next DLP.*
- The **Specialists** quadrant includes *Safetica, Trellix, 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

Symantec offers a wide range of security solutions (network, endpoint, information, email, and identity) for the enterprise market. Symantec operates one of the largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. Symantec is an operating division of Broadcom. Broadcom is publicly traded.

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 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, AIX, and Solaris servers; HCL Notes and SQL databases; Microsoft Exchange and SharePoint servers. 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 services that monitor and protect 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.

- **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. The SDI method provides a fast, simple way for organizations to protect a range of PII, healthcare and financial data types in tabular format.

- Symantec's DLP solution includes CloudSOC (CASB) support for data classification, integration with encryption (i.e. Seclore), labeling (i.e. Titus, Boldon James) 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 Mirror Gateway (agentless CASB support for unmanaged devices), 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.

WEAKNESSES

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

- Symantec would benefit from developing a unified single Symantec Enterprise Agent management solution with a single agent for DLP, SEP and Web Proxy (both cloud and on-premises managed). The vendor has this on its roadmap.

- While Symantec offers a broad portfolio of data security solutions, it can be somewhat complex to manage for organizations with fewer resources.

- 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.

FORCEPOINT

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

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

SOLUTIONS

Forcepoint offers behavior-informed solutions for DLP across all key channels and potential locations for unwanted data exposure and exfiltration. Forcepoint integrates context into all policies through rich data identification (regex, classification, machine learning, natural language

scripts, and large-scale fingerprinting) and continuous monitoring of risky behavior. This context streamlines policy creation, and incident management to reduce false positives and false negatives.

Forcepoint provides three types of DLP solutions:

- **Forcepoint ONE Data Security** – is cloud-native DLP SaaS solution on the endpoint, delivering data protection across email, web, print, USB, file shares and cloud applications. 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 and data classifier updates.

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

  - *Large Data Identification Library* – includes a library of over 1700 pre-defined classifiers and policy templates, covering 150 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.

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

- *Large Data Identification Library* – includes a library of over 1700 pre-defined classifiers and policy templates, covering 150 regions globally that simplify and accelerate DLP deployment and ongoing management.

- *Unified policy enforcement* – through Data Security Everywhere, organizations can 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 and prioritize 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.

- **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 managements.

Forcepoint DLP technology integrates with **Forcepoint Data Classification** and **Forcepoint Data Visibility**, providing optimized data discovery and classification for data-in-use and data-at-rest leveraging both predictive and generative AI as well as ML. It utilizes an AI model that is trained by hundreds of millions of files across all key industries. Models are also continually learning and can be trained to provide high classification accuracy. Forcepoint Data Visibility helps strengthen DLP efficacy through advanced Data Access Governance and other data security-focused data governance use cases (e.g., ROT data, dark data management, permissions management). Additional technologies available for Forcepoint DLP are RBI (remote browser isolation), and ZT CDR (Zero trust content disarm and reconstruct for steganography use cases).

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.

- Integration with Forcepoint CASB enables DLP policies to be extended to enterprise cloud applications via a cloud hosted service. This is a hybrid approach which enables incident and forensic data to be secured in a private data center, while policy enforcement can be done in the cloud.

- Forcepoint provides detection of Drip DLP across endpoint, cloud, email and network DLP components.

- Forcepoint provides an integrated security analytics solution which is used to identify high risk interactions with sensitive data and present a prioritized view of DLP cases with risk scores to help guide security operations teams.

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.

- Deployment of Forcepoint in multi-tenant environments could be improved through enhanced administrative controls.

- Forcepoint solutions are best suited for organizations with high end 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. Proofpoint is owned by investment firm Thoma Bravo and in 2023 acquired Tessian, an AI-based email security company.

SOLUTIONS

Proofpoint **Information Protection** protects organizations from data loss that originates from user accidental or intentional 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 people-centric data loss scenarios. It is a SaaS service available in as a modular platform. It provides support for Windows and MacOS endpoints. The solution comprises the following components:

- **Adaptive Email DLP** – uses historical email behavior, to flag incorrect email recipients and adapts as relationships change. A pop-up alert notifies users about potential mistakes before

an email is sent.

- **Email DLP and Encryption** – helps automate compliance by identifying sensitive or regulated data in emails to prevent loss. It comes with pre-built data identifiers and dictionaries. Organizations can create or upload custom dictionaries and identifiers that match their unique data needs, fine tune the matching strength of dictionary terms, and allow exceptions. Detection accuracy is enhanced through proximity and correlation analysis. Advanced methods are available for content-matching and text extraction from images, including index document matching, exact data matching and optical character recognition. Emails can be sent back to the sender for self-remediation of outbound policy violations, or routed elsewhere, such as to HR, IT, or others. Email Encryption helps secures external or internal-to-internal communication with controls and no-touch key management. A policy based DLP engine, allows to dynamically apply policies at the global, group and user levels through integration into LDAP or AD. 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.

- **DLP Transform** – enables a human-centric approach to data loss across cloud and endpoint. 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, it protects data using advanced methods for content-matching and text extraction. A unified administration and response console helps accelerate incident resolution.

- **Insider Threat Management** – allows monitoring of user data interaction and gaining insights into risky behavior. By understanding user behavior before, during and after an incident, organizations can uncover motivations and intentions 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 people-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, unified alert manager and threat hunting capabilities, classification, reporting, and dashboards that allow administrators to accurately determine DLP violations and insider threats.

- Proofpoint's 2022 acquisition of Dathena strengthened its Information Protection solution with intelligent classification. The platform relies on an AI model to sample and classify unstructured data in cloud and on-premises repositories.

- 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 is working 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, EU, Japan, and Australia. Proofpoint plans to add more data centers in other geographies.

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, in order 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.

- Fortra currently offers out-of-the-box ICAP integration with third-party CASB solutions, and is working to offer CASB, SASE, SSE, and SWG integration through a partnership with Lookout, a cloud security company.

- 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.

TRAIL BLAZERS

NEXT DLP

Huckletree West, Mediaworks,
191 Wood Lane,
London W12 7FP
United Kingdom
www.nextdlp.com

Next DLP provides data protection solutions, aimed at safeguarding sensitive data and Intellectual Property, detect and respond to insider threats, and meet security, compliance, and regulatory demands. The company is privately held.

SOLUTIONS

Next DLP's **Reveal**, is a cloud-native data protection platform that provides content and context-aware data loss prevention, insider risk management, behavioral analytics, SaaS application risk assessment and device control. A single-core license provides access to all the features the Reveal Platform delivers. Reveal uses a low-profile cross-platform endpoint agent and enterprise cloud connectors to provide visibility, detection and response controls across managed devices (Windows, macOS, Linux), unmanaged devices (mobile), and SaaS applications.

Reveal offers the following key features and capabilities:

- *Flexible SaaS and Hybrid Deployment Model* - the Reveal 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* – Reveal 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 analysts with a rich 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. Through Data lineage tracking and visualization analysts reviewing exfiltration incidents can see exactly where data originated and the journey it took across a managed endpoint, including file manipulation and transformation. The Reveal 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.

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

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

- *Reveal Activity Timeline* - the Activity Feed provides a powerful timeline UX where an analyst 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 Reveal.

- *XTND AI Powered Sequence Detection and Activity Reporting* – Reveal 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 Reveal agent includes a patent-pending, endpoint native Machine Learning system to 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* – Reveal is an open, 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

- Next DLP 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.

- Reveal provides visibility into endpoint activities without the need for policies. Once deployed, Reveal 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.

- Next DLP supports all leading platforms, Microsoft Windows, macOS, and Linux endpoints and servers.

- Reveal 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.

- Next DLP 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.

- Next DLP's solution 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

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

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

- Customers indicated that reporting and forensic capabilities could be improved.

- Customers also reported the need for improved policy customization.

- Next DLP is a relatively new entrant in the DLP market and still needs to raise its visibility. The vendor is working to address this.

SPECIALISTS

SAFETICA

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

Safetica offers data loss prevention and insider risk management solutions available on-premises and in the cloud, aimed at helping organizations secure internal data, guide employees on data protection, and stay compliant with regulations. Safetica is a global software company with a customer base covering over 120 countries. The company is privately held.

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. It provides features such as discovery for data audit, content and context-aware data classification and workspace analysis, insider risk detection and management, 3rd party integrations, workflow control, and AD support for multi-domain environments. It can be deployed in the cloud or on-premises. Safetica offers a web console with centralized policy handling, for easy log readiness and overall management.

Endpoint protection can be deployed either manually, or automatically via standard remote management tools such as standard MDM tools, Intune, GPO policy, LanDesk, or other specialized tools. While Safetica is distributed as a single package, each part of the system can be configured individually.

The Safetica product portfolio covers following data security scenarios:

- *Data flow discovery and risk detection* – Safetica audits and records any attempt to intentionally, or unintentionally leak data. Safetica risk analysis helps administrators detect and investigate possible data leaks.
- *Data classification* - Safetica classifies valuable data using its Safetica Unified Classification, which combines analysis of file content, file origin and file properties.
- *Data protection* – Safetica can analyze insider risks, detect threats, and help to mitigate threats swiftly, through instant notifications and policy enforcement.
- *Employee guidance* – Notifications in Safetica about how to treat sensitive data help raise data security awareness and educate employees.
- *Regulatory compliance* – Safetica helps organizations detect violations and comply with key regulations and data protection standards including GDPR, HIPAA, SOX, PCI-DSS, GLBA, ISO/IEC 27001, SOC2 or CCPA.
- *Workspace & behavior analysis* – Workspace and behavior analysis provides an extra level of detail to detect internal risks. It also helps understand how employees work,

print, and use hardware and software assets, thus enabling organizations to optimize costs and increase operational efficiency.

The Safetica product portfolio covers following key features and capabilities:

- *Data in use* – Data in use protection with flexible levels of granularity, applicable to files, applications, devices, cloud services, network storage and all common ports and protocols.

- *Data in motion* – data in motion auditing and protection cross-channel capabilities available for both encrypted and unencrypted communication. Integration is also available with third-party gateways such as FortiGate, FortiMail, and others. Centralized file download for forensic purposes is also available.

- *Data at rest* – Context-based scanning for all file types, content-based scanning including OCR for broad set of formats. Third-party data classification integration. All data manipulation can be logged.

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

- *Mobile DLP* – Safetica does not offer dedicated Mobile DLP, however, some data loss prevention scenarios can be addressed by Microsoft 365 integration (e.g., to cover email use on mobile phones).

- *Encryption* – Safetica offers centralized full disk encryption management for BitLocker along with portable device data encryption management to prevent BYOD risks. Safetica also detects other encryption solutions.

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

STRENGTHS

- Safetica is easy to deploy and maintain and has low hardware requirements for both endpoints and servers.

- Safetica is designed to address a broad set of use cases, including intellectual property protection, regulatory compliance, advanced user behavior, workspace analysis, and security audits with data flow discovery and risk detection.

- Safetica offers high visibility into the data flow and any related security risks, with advanced capabilities, such as hidden mode, protection against agent manipulation, administrative audit logs, and more.

- Safetica enables seamless integrations with IT security stack. It also provides reporting API for integration with analytic services like Power BI or Tableau.

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

- Safetica is attractively priced for mid-size and SMB environments.

WEAKNESSES

- Safetica lacks Drip DLP detection, however it does provide alerts for cumulative DLP violations. Enhanced Drip DLP functionality is on the vendor's roadmap.

- Safetica does not offer dedicated Mobile DLP, however, it allows for some data loss prevention scenarios to be addressed through Microsoft 365 integration.

- Safetica currently lacks support for Linux endpoints.

- Safetica currently supports only basic CASB integration, through Microsoft 365 and integration with Azure Information Protection classification. More advanced integration with CASB solutions is on the vendor's roadmap.

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 suite of DLP components to discover, monitor and prevent data loss on endpoints, network, and cloud to create a comprehensive DLP solution to help organizations apply consistent data security policies across their entire environment. Trellix DLP includes the following components:

- **Trellix DLP Endpoint** – controls data transfers that happen on endpoints via applications, removable storage devices, web, email, clipboard, screen capture, network sharing, as well as cloud. It can block, alert, notify, encrypt, quarantine, and perform other actions on sensitive data on an endpoint. DLP Endpoint provides Web Post support for Google Chrome browser. It is available for both macOS and Windows.

- **Trellix Device Control** – manages and controls the copying of data to removable media and storage devices, such as USB drives, CDs, DVDs, Bluetooth, imaging equipment, and more. Transfers can be blocked based on content, context, or device type. It is available for both Macs and PCs.

- **Trellix DLP Discover** – identifies and protects data at rest for both network storage and endpoint storage. The solution indexes content at rest within the network, including CIFS/NFS shares, databases, Microsoft SharePoint, Box, and endpoints. Discover allows administrators to see how the data is used, who owns it, where it is stored, and more. Trellix DLP Discover also offers fingerprint-based detection for unstructured data and Exact Data Matching for structured data, such as sensitive data stored in an excel sheet in the database.

Optical Character Recognition (OCR) functionality is included to recognize and protect text in scanned images and forms. Trellix DLP Discover can classify/declassify, fingerprint unstructured documents, move, and apply Microsoft Information Protection Label for Rights management.

- **Trellix DLP Prevent** – encrypts, redirects, quarantines, or blocks sensitive data being transferred via email, IM (instant messaging), HTTP/HTTPS, FTP transfers, and other methods. DLP Prevent scans inbound and outbound network traffic across all ports, multiple protocols, and various content types. Emails sent from mobile devices are automatically inspected for sensitive content when integrated with the mail gateway and for web content inspection. Mobile devices need to be configured to route their traffic via a web proxy integrated with Network DLP Prevent. DLP Prevent also offers fingerprint-based detection for unstructured data and Exact Data Matching for structured data, such as sensitive data stored in an excel sheet in the database. Optical Character Recognition (OCR) functionality is included.

- **Trellix DLP Monitor** – identifies, tracks, and reports data-in-motion in an organization. The solution monitors all outbound network data by integrating with egress devices over SPAN/TAP. DLP monitor is available as a physical or a virtual appliance, that can detect and manage over 300 content types. DLP Monitor offers fingerprint-based detection for unstructured data and Exact Data Matching for structured data, such as sensitive data stored in an excel sheet in the database. Optical Character Recognition (OCR) functionality is included.

- **Trellix DLP Capture** – acts as a digital recorder of all enterprise traffic through their edge devices irrespective of DLP rules. This aids in forensic investigations where incidents were not triggered due to lack of rules. The information stored in the Capture database gives administrators insight into a company's historical data to help set accurate DLP policies and reduce false positives.

Trellix ePO (ePolicy Orchestrator) is Trellix's administrative console which can be used to deploy, upgrade, uninstall products, set policies, manage incidents and workflows, develop compliance dashboard and reporting for all network and endpoint DLP components. It also includes out-of-box regulatory and compliance policies such as GDPR, PCI, HIPAA, and others.

Trellix also offers a cloud-native version of the ePO platform which can serve as a centralized administrative console. Customers can choose between on-premises, or SaaS based ePO.

STRENGTHS

- Trellix DLP is integrated with Skyhigh Security's Cloud DLP which helps organizations easily extend DLP policies into the cloud.

- Trellix ePO and Skyhigh integration provide single pane of glass incident workflow management, as well as allows for common policy management across endpoint, network, and cloud DLP.

- The Capture database included in the Trellix DLP solution logs all data in motion and delivers valuable analytics to administrators about how data is being used and sent, which makes it also useful for forensic 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 alleviate administrative burden.

WEAKNESSES

- Trellix DLP does not provide agent support for Linux.

- 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 does not provide OCR functionality on the endpoint.

- Trellix does not provide support for Microsoft Teams.

- 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.

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 Teams, SharePoint, OneDrive, Exchange, and others. Purview combines the former Azure Purview and Microsoft 365 compliance solutions and services into a single brand.

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.
- Power BI.

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.

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
- PowerBI sites

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 priority in recent years and is diligently introducing a rich set of features and functionality across its entire Microsoft 365 product offering.

- DLP comes mostly native, free of charge with many Microsoft 365 plans (in particular enterprise plans such as E3 and E5), 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'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 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 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 that involves additional solutions from other vendors.

NETWRIX

213 Fayetteville Street, 1st Floor
Raleigh, North Carolina
27601, 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, Azure and Google Cloud. The virtual appliance supports all popular hypervisors, e.g. VMware, HyperV, Citrix XenServer, and others. Endpoint Protector is also available as a CoSoSys 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 offers OCR image analysis capabilities, but they only cover a limited number of languages.

- Netwrix does not currently offer support for mobile DLP, or integrations with leading EMM or MDM solutions.

- Netwrix does not currently offer capabilities for detecting Drip-DLP.

- Netwrix does not currently 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

