The Radicati Group, Inc.
www.radicati.com

THE RADICATI GROUP, INC.

Data Loss Prevention – Market Quadrant 2021 *

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

November 2021

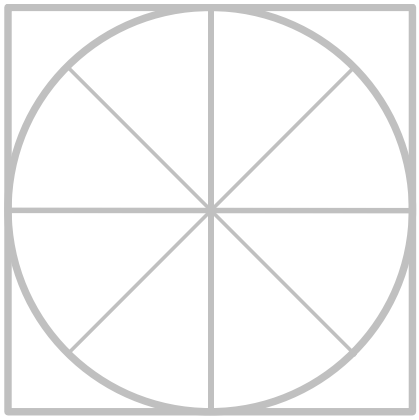

TABLE OF CONTENTS

==========

==========

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.

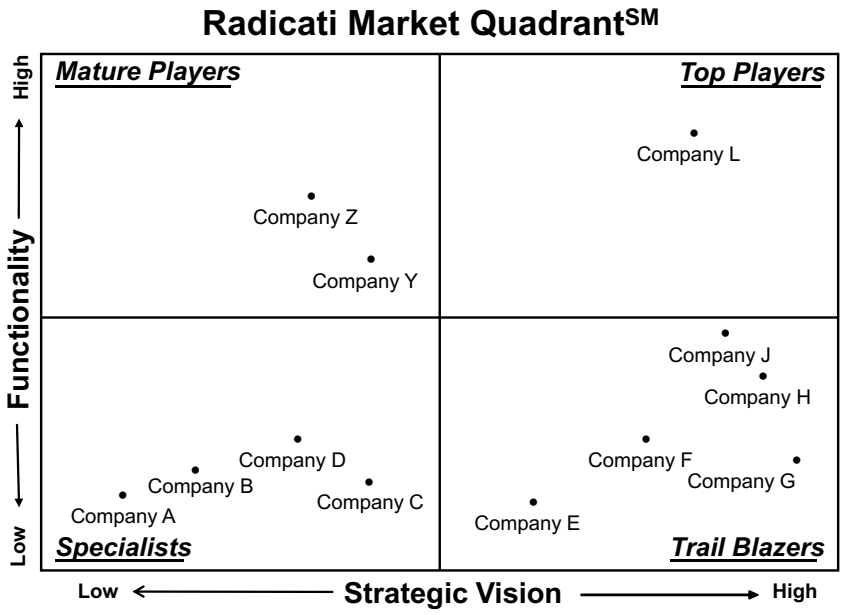

Figure 1: Sample Radicati Market Quadrant

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: *Clearswift, CoSoSys, Digital Guardian, Falcongaze, Fidelis Cybersecurity, Forcepoint, McAfee, Safetica, SearchInform, Symantec,* and *Zecurion*.

- 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 are not 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 exists 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 also support 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 $1.5 billion in 2021, to nearly $3.5 billion by 2025.

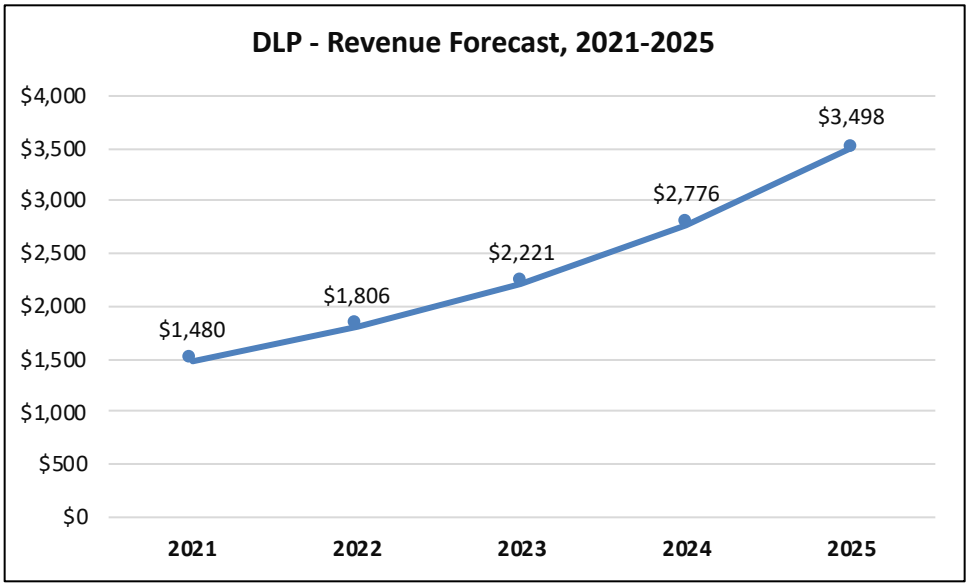

Figure 2: DLP Revenue Forecast, 2021 – 2025

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

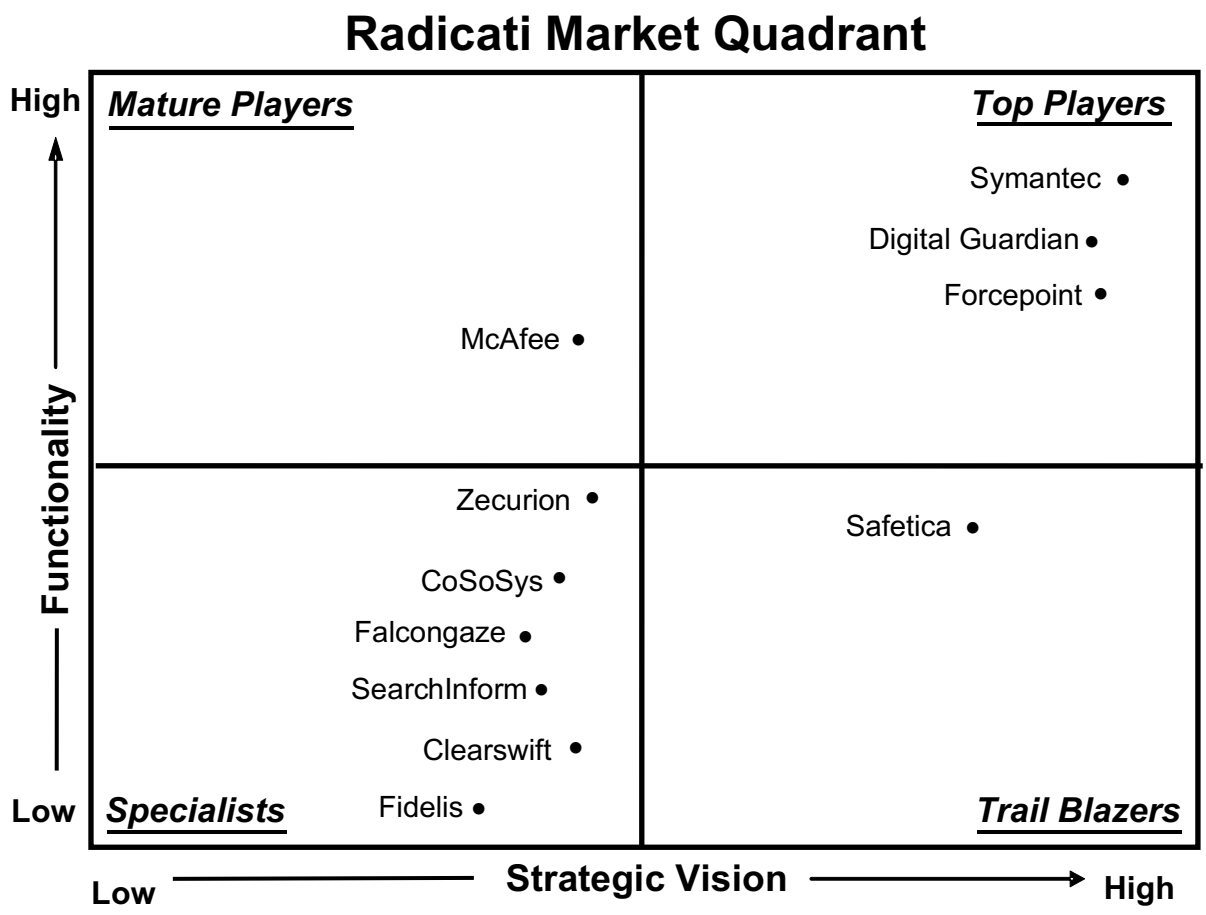

Figure 3: Data Loss Prevention Market Quadrant, 2021*

* Radicati Market Quadrant is copyrighted November 2021 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, Digital Guardian,* and *Forcepoint*.

- The **Trail Blazers** quadrant includes *Safetica*

- The **Specialists** quadrant includes *Zecurion*, *CoSoSys*, *Falcongaze, SearchInform*, *Clearswift* and *Fidelis Cybersecurity.*

- The **Mature Players** quadrant includes *McAfee*.

DATA LOSS PREVENTION - VENDOR ANALYSIS

TOP PLAYERS

SYMANTEC

1320 Ridder Park Drive
San Jose, California 95131
United States
www.broadcom.com

Symantec offers a wide range of security solutions (network, endpoint, information 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. The solution comprises a number of 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 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 robust file protection capabilities on top of Network Discover. It automatically cleans up and secures all of 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. It also educates business users about policy violations.

  - **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. Networks Prevento for Web 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.

- **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** – Symantec CloudSOC 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 and IaaS** – CloudSOC CASB for SaaS and CloudSOC CASB for IaaS are cloud based services that monitor and protect stored, transferred, and shared data. Supported cloud applications include Microsoft Office365, Google Workspace (G Suite), Box, Salesforce, ServiceNow, and others.

  - **CASB Gateway** – Symantec CloudSOC 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** – Symantec DLP Cloud Detection Service inspects content extracted from cloud app and web traffic and automatically enforces

sensitive data policies. Cloud to cloud integration with Symantec CloudSOC protects data in motion and at rest across more than 100 unsanctioned and sanctioned cloud apps, including Office 365, Google Workspace (G Suite), Box, Dropbox, and Salesforce.

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

- **DLP for Email (with Office365 and Gmail)** – Symantec DLP Cloud Service for Email continuously monitors corporate email traffic, using built in intelligence and advanced detection to minimize false positives. It protects against data leaks in real time with automated message modification or blocking to enforce downstream encryption or quarantine. For data shared with third parties, it can automatically enable identity based encryption and digital rights for email bodies and attachments.

STRENGTHS

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

- Symantec offers a sophisticated and comprehensive DLP solution which can help meet the complex needs of enterprises of all sizes.

- Symantec DLP offers a strong set of content detection technologies through advanced capabilities such as machine learning, fingerprinting, image recognition, and tagging.

- Symantec's DLP solution includes a number of key capabilities, such as CloudSOC (CASB) support for data classification, encryption and digital rights management, and user entity behavior analytics (UEBA).

- Symantec DLP is fully integrated with key components of Symantec's product portfolio, in particular CloudSOC Mirror Gateway (agentless CASB support for unmanaged devices), Email Security, Endpoint Security, and Web Security. This delivers a consistent policy architecture and enforcement across multiple channels of potential data loss.

WEAKNESSES

- Symantec solutions can be somewhat more expensive than other DLP solutions on the market. However, the new packages deliver rich feature sets which when fully integrated with other Symantec security solutions provide significant protection benefits and operational cost efficiencies.

- While Symantec offers a broad portfolio of data security solutions, it can be somewhat complex to manage for organizations with fewer resources. Smaller companies, however, can rely on managed services offered through Symantec partners.

- 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.

- Symantec lost some mindshare following the Broadcom acquisition. The vendor has implemented a number of changes to address this.

DIGITAL GUARDIAN

275 Wyman Street, Suite 250
Waltham, MA 02451
www.digitalguardian.com

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 late 2021, Digital Guardian was purchased by HelpSystems, which also owns Clearswift (covered separately in this report).

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 that is 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 provide organizations with the information needed to 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 for organizations that wish to keep their entire data protection program within their control.

- 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 a single agent for both DLP and managed detection and response (MDR), which makes it an attractive choice for organizations with limited IT resources.

- Digital Guardian offers easy integration with Microsoft Information Protection (MIP), 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 its own CASB solution. However, it provides out-of-the-box ICAP integration with third party CASB solutions, and has developed a tight integration with the Censornet Platform.

- Digital Guardian was recently acquired by HelpSystems. At the time of this writing, it is too early to know what impact this may have on company direction.

FORCEPOINT

10900 Stonelake Blvd
3rd Floor
Austin, TX 78759
www.forcepoint.com

Forcepoint offers behavior-based solutions for DLP, web, data, and email content security, cloud access security, next generation firewall, user behavior analysis, insider threat detection, and threat protection solutions to organizations of all sizes on a worldwide basis. In early 2021, Forcepoint was acquired from Raytheon by Francisco Partners.

SOLUTIONS

Forcepoint Data Security Suite, brings together all critical capabilities for DLP into three separate editions, as follows:

- **Forcepoint Data Security Suite – Workforce Edition** – offers the basic capabilities for a DLP deployment and includes DLP Endpoint, DLP Discover, and DLP for Network.

- **Data Security Suite – Cloud Edition** – adds capabilities for visibility and control in the cloud. It includes the elements of the Workforce Edition but also includes DLP for Cloud Apps via API, and DLP for Cloud Email.

- **Data Security Suite Enterprise Edition** – adds additional cloud capabilities, Cloud Web and CASB inline DLP inspection with application control, as well as Risk-adaptive DLP with behavior analytics. This combines contextual user risk analysis and global policies to help reduce false positives.

Forcepoint DLP technology includes a library of over 1500 pre-defined templates and classifiers with the objective of simplifying and accelerating deployment of DLP, limiting the need for creating individual classifiers. Forcepoint's data identification technology also includes structured and unstructured data fingerprinting, machine learning classifiers, and natural language scripts. Forcepoint Risk Adaptive Protection dynamically applies monitoring and enforcement controls to protect data based on calculated behavioral risk level of users and the value of data being accessed. This contextual risk analysis helps reduce the amount of alerts requiring investigation, and implements data protection controls based on the contextual risk of individual users. Forcepoint DLP solutions are available for Microsoft Windows (Windows 7, 8, 10 and 11), and Apple macOS (BigSur, Monterrey, and previous versions).

STRENGTHS

- Forcepoint supports deployment of DLP management and data classification components across a comprehensive set of channels including endpoint, web, network, email and cloud including public cloud (i.e. Microsoft Azure, and Amazon AWS). This allows for a unified policy strategy with centralized management, that can be deployed across all channels.

- 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 OCR is currently limited to network discovery and data in motion (i.e. web, email and ICAP). The vendor is planning to extend OCR support to additional DLP components as part of its roadmap.

- The Forcepoint DLP Endpoint capabilities for Linux are not currently as developed as those for Windows and macOS.

- Forcepoint currently only provides data in motion integrated encryption capabilities for removable media. It can also support email encryption when combined with Forcepoint DLP for Cloud Email, or third party encryption solutions.

- Forcepoint does not yet have a DLP SaaS offering. However, this is on the vendor's roadmap.

TRAIL BLAZERS

SAFETICA

Laubova 1729/8, 130 00 Prague 3
Prague, Czech Republic
www.safetica.com

Safetica offers data loss prevention and insider threat protection solutions, both on-premise and cloud-based, aimed at helping organizations secure internal data, guide employees on data

protection, and stay compliant with regulations. Safetica is a Czech company with worldwide distribution and a global customer base. The company is privately held.

SOLUTIONS

Safetica ONE is an “all-in-one" data loss prevention and insider threat protection solution that helps to prevent human mistakes and malicious acts to secure sensitive data while maintaining efficient business operations. It is available in three tiers: Safetica ONE Discovery for data audit, classification and workspace analysis; Safetica ONE Protection with DLP & insider threat protection features; and Safetica ONE Enterprise with 3rd party integrations, workflow control, and AD support for multi-domain environments. It can be deployed on-premises, or on public or private cloud servers.

Safetica NXT is a cloud-native SaaS insider threat prevention solution that helps companies detect data security risks and investigate incidents from day one. The backend infrastructure runs in Microsoft Azure cloud, while data security is executed by clients on endpoints. It is based on a multi-tenant architecture which is suitable for both self-managed and MSP service offerings.

Safetica ONE and NXT, are both available for Windows and macOS platforms and integrate with Microsoft 365.

Safetica also offers the two following optional add-on modules:

- **Safetica UEBA** – offers deeper insights in user activities, helps uncover behavior anomalies and offers detailed resource usage information.

- **Safetica Mobile** – is an MDM solution which helps secure and manage mobile devices remotely, as well as audit incoming files on Android.

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

The **Safetica Management Console** offers centralized policy handling, and is used to maintain Safetica ONE installations, set security policies, manage deployed endpoints or display monitored data to administrators.

The Safetica solution supports the following capabilities:

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

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

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

- *Policy controls* – the solution comes with one-click templates for chosen regions and/or regulations.

- *Mobile DLP* – Safetica Mobile offers auditing and basic security tools on mobile devices. The solution is fully integrated with the Safetica ONE infrastructure, but enforcement of DLP policies on mobile devices is still on the roadmap.

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

- *Drip-DLP* – Safetica ONE 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.

The **Safetica Management Console** offers centralized policy handling, and is used to maintain Safetica installations, set security policies, manage deployed endpoints or display monitored data to administrators.

STRENGTHS

- Safetica ONE and Safetica NXT are easy to deploy and maintain. Both solutions have low hardware requirements for endpoints and servers.

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

- Safetica ONE and Safetica NXT offer 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 ONE 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 focuses on the SMB market, and has limited support for very large enterprise deployments (i.e. >10,000 seats).

- Safetica ONE and Safetica NXT currently lack support for Linux endpoints.

- Safetica ONE currently supports only basic CASB integration, with regards to data security in Microsoft 365 and integration with Azure Information Protection classification. More advanced integration with CASB solutions would be beneficial.

SPECIALISTS

ZECURION

14 Penn Plaza, 9th floor
New York, NY 10122
www.zecurion.com

Zecurion, founded in 2001, is vendor of IT security solutions aimed at helping companies protect against insider threats. The company is privately held, with headquarters in Moscow and New York.

SOLUTIONS

The **Zecurion DLP** solution delivers capabilities to control data leak channels, monitor employee handling of data, and prevent data breaches. Zecurion DLP 11 is currently available for Windows, and Linux devices. The solution is available in different form factors including on-premises, cloud and hybrid.

Zecurion DLP is available through the following product components:

- **Traffic Control** (network DLP) – uses hybrid content analysis, combining digital fingerprints, Bayesian methods, and heuristic detection to filter outbound traffic and detect confidential data. It works over email, webmail, social networking, instant messaging, and other online channels to block the loss of sensitive information.

- **Device Control (Windows, Linux, Mac)** (endpoint DLP) – allows flexible control over the use of devices connected to ports (e.g. USB, LPT, COM, IrDA, IEEE 1394, PCMCIA, and internal devices), as well as built-in network cards, modems, Bluetooth, Wi-Fi, CD / DVD-drives, and local or network printers. It offers fine-grained controls beyond basic "allow/block" policies, through sophisticated policies combined with content analysis and encryption.

- **Traffic Control (Windows, Linux, Mac)** (endpoint DLP) - uses hybrid content analysis, combining digital fingerprints, Bayesian methods, linguistic analysis, regular expressions,

data templates, heuristic detection, etc. to filter outbound traffic and detect confidential data. It works over email, webmail, social networking, instant messaging, and other online channels to block the loss of sensitive information.

- **Discovery** (data at rest DLP) – serves to detect sensitive, inappropriately stored information in file servers (shared folders), Microsoft SharePoint and Exchange servers, databases and document management systems (e.g. Oracle Database, Microsoft SQL Server, and IBM DB2), as well as workstations and laptop computers. It uses hybrid analysis to accurately determine the category of information and decide if it is stored in the proper place, based on corporate policy and on industry standards.

- **Staff Control** – keeps track of employee working hours, logs employees' actions at workplaces, and evaluates efficiency. The module checks the activities of personnel for compliance with corporate standards and safety policies. Zecurion Staff Control compares activity profiles of chosen users. The analysis includes: activity for the selected period (productive time, inappropriate use of PC, not defined, inactivity, away from the PC); main indicators (productivity, away from the PC, remote work, productive time, etc.); applications and categories, websites and more.

- **User Behavior Analytics module** – aims to gain an understanding of the context of user action and their intent. The solution ensures a comprehensive view of risks with parameters such as: emotions, behavior profile and analysis, working hours, connection map, and more. Zecurion DLP provides a risk score and change dynamics to assess employees. Security Officers may place greater supervision on high-risk employees, while allowing lower-risk employees to operate with less limitations.

- **Investigation Module (IRP)** – simplifies investigations and shortens the incident response cycle. It offers cybersecurity teams a 360° view of actual tasks with all the statuses, data on the investigation stage, executants, and deadlines. During the investigation, cybersecurity team members can leave comments on the task and discuss progress with other participants (from CISO to analyst), attach documents and incidents as proof.

Zecurion DLP uses a single web console to define and enforce policies across all endpoints and cloud solutions. The console offers pre-built policy templates, workflows, graphical reporting features and remediation capabilities to minimize the threat of data loss caused by internal

threats. Policy management for Mac, Linux and Windows-based platforms is handled through the single management console.

STRENGTHS

- Zecurion Traffic Control controls over 250 different social media services, including Linkedln, Facebook, Google+ and Yahoo, as well as IM, web mail and file hosting. It also supports voice interception and file transfer capture over WhatsApp, Skype, MS Teams and Telegram.

- Zecurion provides full archiving of all data seen by endpoint agents, and can also capture screen shots and other end-user screen activities.

- Zecurion DLP includes a User Behavior Analytics (UBA) module, which includes self-learning analytics and policy violation predictions.

- Zecurion provides risk-based employee assessments, which can display a risk score and behavior dynamics for each employee.

- Zecurion offers features such as Screen Photo Protection, and Screen Watermarks, for enhanced protection against photo capture of screen information.

- Zecurion ensures simplicity of investigations and shortens the incident response cycle with its proprietary Investigation Module.

WEAKNESSES

- The latest version of Zecurion DLP offers only limited support for macOS, and no support for Android or iOS.

- Zecurion DLP does not currently offer CASB functionality. However, the vendor has this on its roadmap.

- Zecurion offers only basic enforcement visibility through email alerts.

- Zecurion needs to invest to raise its market visibility, particularly in North America.

CoSoSys

1 Glenwood Avenue, 5th Floor
Raleigh, North Carolina
27603, United States
www.endpointprotector.com

CoSoSys offers solutions for Data Loss Prevention (DLP), including Device Control, eDiscovery, Content Aware Protection, and Enforced Encryption. The company is privately held.

Solutions

CoSoSys' **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. It covers all major exit points such as email, cloud file sharing applications, 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, 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 five 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 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, cloud applications, 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 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 a smartphone 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 256bit 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.

CoSoSys 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

- CoSoSys' Endpoint Protector offers strong coverage for Windows, macOS and Linux, with feature parity across platforms 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.

- CoSoSys offers diverse deployment options, including virtual appliances, thus meeting the needs of customers with a wide range of infrastructures.

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

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

WEAKNESSES

- CoSoSys offers OCR image analysis capabilities, but they only cover a limited number of languages.

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

- CoSoSys does not currently offer capabilities for detecting Drip-DLP. The vendor has this on its future roadmap.

- CoSoSys does not currently offer or integrate with CASB capabilities. The vendor has this on its future roadmap.

- CoSoSys has low market visibility outside of Europe, and some regions in Asia.

FALCONGAZE

117a Nezavisimosti ave., 10th floor, office 2
Minsk, 220114
Belarus
www.falcongaze.com

Falcongaze, founded in 2007, offers information security solutions for Data Loss Prevention, as well as monitoring of personnel activities and archiving of business communications. The company is based in Belarus, with a strong presence in Eastern European countries. The company is privately held.

SOLUTIONS

Falcongaze's DLP solution, **SecureTower**, is an enterprise solution which can intercept a vast range of corporate communication and data transfer channels, as well as detect sensitive content using various content-aware detection techniques. It brings together DLP, staff efficiency and loyalty monitoring, and identification of potentially risky employee behavior. Linguistic analysis tools leverage contextual analysis based on dictionaries and morphological analysis. SecureTower can be deployed on-premises, cloud, or as a hybrid solution. Server components can be deployed on Windows OS, whereas endpoint agents are only available for Windows and Linux.

SecureTower can provide statistical analysis, based on customized rules, on the number of messages, emails and files sent, web activity, computer and application activity. Extended regular expressions provide efficient search of data, such as: addresses, phone numbers, SSN, ID, bank account numbers, and more. Hash computation is used to detect the presence of protected files on users' computers, and digital fingerprinting of sensitive content allows detection of transfer of whole files, or parts of its contents.

SecureTower provides control for the following data channels:

- *Email messages* – transferred by POP3, SMTP, IMAP and MAPI protocols, Microsoft Exchange Server, HCL Notes/Domino, Postfix, Sendmail and other email systems, as well as consumer mail services, such as Gmail, Hotmail, Yahoo, Yandex.Mail, Mail.ru, Rambler, and others.

- *Web-activities* – provides information about websites visited by employees, time spent and messages sent in relation to website activity.

- *Instant Messaging* – including Skype, Lync, Microsoft Teams, Telegram, WhatsApp, Google Hangouts, Viber, Discord, Zoom, Slack, Rocket.Chat, Cisco Jabber, MRA, YAHOO, XMPP, SIP, and more.

- *Social Media* – control of online chats, blogs, forums and social networks including Facebook, Twitter, LinkedIn, Instagram, Bitrix24, vk.com, ok.ru as well as other social networks used for business communication.

- *Files and documents* – transferred via FTP, FTPS, HTTP and HTTPS protocols (including email attachments), files transferred to network shares, USB storage devices, cloud storage, and printed files.

- *Databases* – including MS SQL Server, Oracle, PostgreSQL, MySQL, SQLite, and others.

- *External devices* – data transferred to external devices, such as USB storage devices, external HDDs, and others. Including computer and terminal server network resources, printed documents and images, speech recognition engines, OCR engines, IP telephony (i.e. voice and text via the SIP protocol), and more.

- *Clipboard* – covers text, images, files transferred through copy/paste operations.

SecureTower also provides the ability to detect anomalies in employee behavior through UEBA algorithms, it maintains an archive of all interactions for a designated time period and security policies can be applied in retrospective.

Management is provided through two consoles: an administrator console, for IT personnel that serves to configure the server components; and a client console, that allows security officers to set up rules, view reports, investigate incidents, and more.

STRENGTHS

- SecureTower provides an extensive set of tools for the protection of sensitive data, business process analysis, as well as the investigation of security incidents.

- SecureTower provides extensive capabilities for monitoring user activity and social interactions.

- SecureTower is simple to deploy and simple to maintain. It offers numerous out-of-the-box reports and security rules.

- SecureTower is a modular solution, which allows customers to buy and use only the components that best meet their needs.

- SecureTower provides support for detecting Drip DLP.

- SecureTower can be integrated with third party SIEM solutions.

WEAKNESSES

- SecureTower's endpoint agents are currently only available for Windows and Linux operating systems. Agents for macOS and mobile platforms (i.e. iOS and Android) are on the vendor's roadmap.

- Secure Tower offers only limited analysis capabilities for data at rest.

- SecureTower does not currently offer its own CASB capabilities, or partner with third party CASB providers.

- SecureTower lacks market visibility outside Eastern Europe and Asia.

SEARCHINFORM

8/1 Skatertnyi pereulok, building 1, offices 1-12
Moscow, Russian Federation
www.searchinform.com

SearchInform is an information security company focusing on cybersecurity threats, protecting business and government institutions against data theft and harmful human behavior. The company is headquartered in Moscow, with offices worldwide.

SOLUTIONS

SearchInform RM (risk monitor) Platform is a comprehensive solution that includes DLP (data loss prevention), DCAP (data centric audit and protection), DBM (database protection), employee productivity analytics and digital forensic suite. Searchinform offers information security across a wide range of communication channels, and provides privileged user management, work efficiency controls, user behavior monitoring and more. The solution provides real time analysis of virtually all information flows to prevent data theft or leakage. It also helps to prevent harmful activities by insiders, such as fraud, corruption, espionage, sabotage, changes in/abuse of access rights, and more. SearchInform DLP offers a client-server architecture, where client applications are deployed on monitored devices (e.g. desktops, servers, network switches and other equipment) while the server part can be deployed on-premises, in the cloud, or hybrid. Platforms supported include Windows and Linux. The platform offers the following capabilities:

- *Data in Use* – file control (i.e. opening, creating, changing, deleting, etc.), program control (i.e. tracking time spent in application and on web sites), print controller for local or network printing, device controller, data encryption, monitor control for screen control, web camera controls, microphone controls, and key logger controls.

- *Data in Motion* – includes cloud storage (e.g. Amazon S3, Evernote, Dropbox, Microsoft Office 365, Microsoft OneDrive, Google Docs, and more). It also provides control for FTP, HTTPs, email solutions (i.e. IMAP, MAPI, POP3, SMTP, NNTP, WebMail), Instant Messaging (e.g. Skype, ICQ, MMP, Jabber, MSN, Telegram, WhatsApp, Viber and others), and social networks (i.e. Facebook, LinkedIn, and others).

- *DCAP* – Finds files in a document flow that contain critical information, and assigns certain TAG type to each file: personal data, trade secret, credit card numbers, etc. Audits user file system operations. Specialists responsible for risk mitigation have access to information about changes made to those files (creating, editing, moving, deleting, etc.). Facilitates confidential information access control – automatically monitors open resources, files available to a specific user or group, privileged accounts. Allows to differentiate access to files based on their content.

- *DBM (data base monitoring)* – Monitors user DB queries, prevents data breaches and audits database activity, controls privileged user access rights.

- *Cloud Security*– System compatibility with cloud services (e.g. azure SQL, Azure AD, Azure Exchange, and other public and private clouds). Also, the ability to check cloud storage information for compliance with security policies and monitor communication in the corporate infrastructure. Three technologies are currently available: control of data transfer between cloud services and corporate PCs; control of data exchange within the corporate network (from any connected device); and control at the cloud service level.

- *Policy controls* – the solution comes with out-of-the-box security policies for a wide range of use cases and targeted at the needs of specific vertical industries. Additionally, SearchInform specialists will work with customers to create custom policies that meet specific needs.

- *Drip-DLP* – SearchInform offers proprietary technology for content analysis and is able to single out data leakage incidents in streams of data of any size.

- *Forensic suite* – is a set of technologies that provide for detailed reconstruction of violations for official investigations. Violations of security policies can be supported through a video recording of user actions, audio recording of sound activity at the PC, file system activity, data audit on active processes or web browser tabs, as well as data from a webcam for biometric identification of the violator. In addition, visualization tools are included to help visualize violations on a user relationship chart, or reconstruct the route of data flow through network channels from the time the data was created until when it left the corporate environment.

STRENGTHS

- Searchinform combines a wide range of functions in a single platform giving an integrated single-pane of glass view of an organization's security posture (i.e. integrating DLP, DCAP, DBM and more)

- In addition to DLP, SearchInform offers a strong set of forensic technologies which assist in the investigation process.

- SearchInform has built-in role-based differentiation of access rights to confidential files.

- SearchInform offers strong integration with cloud services (e.g. azure SQL, Azure AD, Azure Exchange, and other public and private clouds)

- SearchInform monitoring covers a wide range of communication channels that include all traditional channels, as well as complex emerging new channels such as end-to-end Instant Messaging and social media.

WEAKNESSES

- SearchInform currently lacks support for macOS devices.

- SearchInform does not provide CASB integration capabilities, which may disappoint customers wanting to bring together DLP and CASB policy management.

- SearchInform can require significant amount of storage space (for instance, the "raw data saving option" can generate huge amounts of data). The vendor recommends deploying adequate amounts of storage resources.

- The SearchInform server cannot be installed on open source OS and DBMS.

- SearchInform does not provide mobile DLP capabilities, either on its own or through integration with MDM or EMM vendors.

- SearchInform lacks market visibility outside of Russia and Central Europe. The vendor is working to address that.

CLEARSWIFT

1310 Waterside
Arlington Business Park
Theale, Reading RG7 4SA
United Kingdom
www.clearswift.com

Clearswift (a HelpSystems company) is a cybersecurity software company which offers solutions for detecting, inspecting, and securing critical data over email, web, and the cloud. In 2019, Clearswift was acquired by HelpSystems, and its solutions are now part of the HelpSystems Data Security Suite. In late 2021, HelpSystems also acquired Digital Guardian (covered separately in this report).

SOLUTIONS

Clearswift offers a portfolio of solutions that can be peered together allowing customers to extend their hygiene solutions to provide adaptive Data Loss Prevention (DLP) features across their environment in a cost-effective manner. Clearswift products are available on hardware and software, including vSphere and Hyper-V support. Clearswift also sells its solutions in the cloud with AWS and Azure support, as a hosted or a managed service. The Clearswift portfolio includes:

- **Secure Email Gateway** – provides Adaptive DLP features (and strong hygiene features) that permit SMTP emails to be scanned before leaving and entering the company. Granular policy rules can be set to identify emails from individuals, departments, or whole domains as required. DLP features include keyword search across headers, subject, body, and attachments (which also includes document properties) and file type matching including customer-defined type files (which also includes byte patterns, not just extensions). Optical Character Recognition (OCR) support is provided as an option. When used with the Information Governance Server (IGS), OCR also provides document/partial document matching. The Secure Email Gateway also supports the Adaptive Redaction features that can

be used to reduce the overhead of minor violations by either redacting content such as keywords in a document, or sanitizing documents (e.g. clearing document properties or change tracking in documents that could hold sensitive information). Image threat mitigation includes bi-directional anti-steganography and image text redaction. Sensitive content that requires secure delivery can use built-in TLS options, as well as message-based encryption methods such as S/MIME, PGP or password, and portal-based encryption options (hosted or on-premise). The Secure Email Gateway supports Active Directory integration and can provide rules that require end users to copy outbound emails to their managers or other compliance mailboxes. It can be deployed to augment Office 365 security. Through partnerships, Clearswift can deliver a broader integrated solution portfolio, which includes browser isolation, data classification, digital rights management and protection against phishing and business email compromise.

- **Secure Exchange Gateway** – permits scanning of internal mail in a Microsoft Exchange environment using all of the same DLP features as the Email Gateway. The Exchange Gateway allows large organizations to compartmentalize content into their own business unit or region depending on their Microsoft Exchange topology. The Secure Email and Exchange Gateways can share message areas (i.e. quarantine stores), message tracking, as well as reporting for a richer administrative experience. Clearswift can also scan internal email in Office 365, providing extensive DLP functionality.

- **Secure Web Gateway** – features an HTTP proxy and content filtering engine that performs hygiene features, DLP, and URL classification. The Secure Web Gateway supports HTTP/S interception to enable it to inspect content either being downloaded or uploaded.

- **Secure ICAP Gateway** – can augment existing web filtering investments with Adaptive DLP-specific policies for customers that have existing web proxy solutions, such as Broadcom (Symantec), F5, Zscaler or similar other ICAP-based solution. It can also be integrated with manage file transfer software to provide enhanced security and DLP for file transfers. This variant can be used in both forward and reverse proxy modes.

- **Clearswift Endpoint DLP** – extends DLP to endpoints, by permitting what data can be written to external devices (i.e. data in use), as well as to perform scheduled scans of local, network shared or cloud drives (i.e. data at rest). It also provides granular device control and

removable media encryption functionality.

- **Information Governance Server (IGS)** – acts as a central repository where end users can register sensitive information and permit any of the Gateways to query the central store to check for and act upon potential data-in-motion breaches. IGS also provides information provenance reporting for compliance purposes, tracking granular information as well as whole files.

STRENGTHS

- Clearswift has strong content DLP capabilities and offers adaptive remediation options that can automatically remove inbound and outbound sensitive data and threats, while leaving the remainder of the content intact to avoid impacting business productivity.

- Clearswift's DLP policy rules have an intuitive flow that is easy to use and provides additional drill-down options when necessary. The policies are shared across all communication channels to ensure consistent discovery of information.

- Clearswift offers Optical Character Recognition (OCR) support as part of its DLP functionality. This offers comprehensive support for image formats, including PDF scanned documents, and works with all major languages, including Japanese. Image text redaction is also available.

- Clearswift's Adaptive Redaction features remove content which breaks policy rules, including file metadata, revision history and active content, including macros and embedded executables. This mitigates data loss, unwanted data acquisition and risk from weaponized documents. Anti-steganography functionality also mitigates the image-based threats of outbound exfiltration, as well as inbound malware payload delivery.

- Clearswift has an Information Governance solution which is fully integrated into their DLP solution, which enables tracking and policy management at an information level (rather than file level) across multiple communication channels.

WEAKNESSES

- Clearswift's endpoint platform still needs to add endpoint DLP support for macOS and Linux.

- Clearswift does not currently provide support for Instant Messaging networks (e.g. Microsoft Teams). Social Network support is provided through a partnership with SecureMySocial.

- Clearswift currently provides mobile DLP support for iOS and Android only through a partnership with AirWatch.

- Clearswift does not provide support for drip DLP.

- While Clearswift offers an ICAP Gateway for integration with third party CASB solutions, this does not satisfy customers looking for a solution that will allow them to easily drive common policies across both CASB and DLP.

- Although Clearswift offers a strong solution, and the acquisition by HelpSystems has extended exposure to HelpSystems' customers in North America, the vendor is still less visible than other competing vendors in the DLP market.

FIDELIS CYBERSECURITY

4500 East West Highway, Suite 400
Bethesda, MD 20814
www.fidelissecurity.com

Fidelis Cybersecurity offers automated threat detection, hunting and response solutions. The company was originally known for its network DLP solutions, however, it has broadened its portfolio to the Automated Threat Detection and Response market for network, endpoint and cloud. The company is privately held through an investment from Marlin Equity Partners.

SOLUTIONS

Fidelis offers network DLP as part of its **Elevate** platform, which captures rich metadata from the threat landscape and combines that content to enable real-time and retrospective analysis. Elevate comprises network, endpoint, deception, extended detection and response (XDR), cloud access security broker (CASB) modules which can be deployed in various form factors including on-premises, cloud, and hybrid models. Fidelis Elevate offers only DLP in motion through monitoring of application, protocol and content data in sessions. The solution is largely OS agnostic.

Fidelis provides network DLP analysis through five network layer sensor locations (direct, internal, cloud, email and web) with the last two designed to integrate with third party email appliances and web proxy solutions as follows:

- *Fidelis Network Mail* – integrates in the SMTP conversation by providing full SMTP support through Fidelis' embedded MTA, as well as a Milter interface as an additional integration method for email hygiene solutions like Microsoft 365, Cisco, Proofpoint, SendMail and Postfix. It can be deployed in the Microsoft 365 cloud to provide DLP for mail, as well as email threat prevention and detection.

- *Fidelis Network Web* – integrates with third party Web Proxy and CASB solutions through an ICAP interface to add a DLP capability for proxy solutions like Broadcom, McAfee, Netskope, and others. The Fidelis Network sensor also allows monitoring of social networks for DLP, such as Twitter and Facebook, through its session inspection technology.

- *Fidelis Network Collector* – is an add-on component that stores network and content metadata for over 300 attributes plus custom tags from the sensors providing visibility into data leaks that occurred in the past. The Collector allows users to search, pivot and hunt on content and context for leakages on-demand or create scheduled automations. It also integrates with IP-to-ID solutions allowing for user attribution.

- *Fidelis Network Sensors* – include direct sensors at gateways for ingress and egress monitoring, indirect sensors for data center and internal monitoring, plus cloud sensors for virtual machine monitoring. Fidelis leverages Microsoft’s VTAP (virtual network TAP) to Azure to monitor cloud network traffic natively between virtual machines without an agent.

Fidelis also supports Amazon's VPC Traffic mirror for cloud apps natively without an agent.

The Fidelis Cybersecurity Threat Research Team (TRT) regularly makes streaming policy updates available to customers based on ongoing research and machine learning. The policy updates are delivered to customers automatically via the Fidelis Insight Cloud service.

The Fidelis Elevate network sensors are configurable from a single management UI, called Command Post, that can be deployed on premises, in the cloud, or provided by Fidelis as a managed cloud service.

STRENGTHS

- Fidelis solutions can be deployed in various form factors including on-premises, cloud, and hybrid models, or as a managed detection and response (MDR) service.

- Fidelis offers a good set of out-of-the-box policies and rules for securing sensitive information. It has added OCR support to its email DLP capabilities.

- Fidelis offers DLP as part of a broader solution for network, endpoint, and deception post breach threat detection and response, which will appeal to organizations that want to deploy an integrated solution for compromise intelligence, detection and response automation.

WEAKNESSES

- Fidelis does not offer DLP for data-at-rest, or data-in-use, focusing instead on DLP for data in motion, and bringing that together with its broader threat automation detection and response capabilities.

- Fidelis does not integrate with mobile security solutions and does not offer endpoint DLP.

- Fidelis does not offer visibility into encrypted traffic.

- Fidelis has lost visibility in the DLP space, choosing instead to focus on automated threat detection and response.

MATURE PLAYERS

MCAFEE

2821 Mission College Blvd.
Santa Clara, CA 95054
www.mcafee.com

McAfee Enterprise offers security solutions, threat intelligence and services that protect business endpoints, networks, servers, the Cloud and more. In July 2021, McAfee Enterprise was acquired by a consortium led by Symphony Technology Group (STG). In September 2021, STG also announced the acquisition of FireEye products and its intent to combine McAfee Enterprise and FireEye products into a new pure play cybersecurity company.

SOLUTIONS

McAfee Total Protection for Data Loss Prevention (DLP) offers a number of DLP components for endpoint, network, and cloud that can be mixed and matched to create a complete DLP solution. It is a key component in McAfee's MVISION Unified Cloud Edge (UCE) vision, a device to cloud strategy that converges CASB, DLP and Web technologies to help organizations apply consistent data security and threat protection policies across their entire environment. McAfee Total Protection for Data Loss Prevention includes the following components:

- **McAfee 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 databases, Microsoft SharePoint and endpoints and allows administrators to see how this data is used, who owns it, where it is stored, and other details. McAfee DLP Discover also offers 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.

- **McAfee 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. McAfee DLP Prevent for Mobile Email provides content-aware protection to mobile email by intercepting emails downloaded to the mobile device, via ActiveSync proxy with DLP capability, requiring no agent to be installed. The Capture technology is also available, and can act as a digital recorder to replay DLP incidents after the fact for more thorough investigation. DLP Prevent also offers Exact Data Matching for structured data, such as sensitive data stored in an excel sheet in the database. It includes Optical Character Recognition (OCR).

- **McAfee DLP Monitor** – identifies, tracks, and reports on data-in-motion in an organization. The solution monitors all outbound network data. 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. DLP monitor is available as a physical or a virtual appliance, that can detect and manage over 300 content types. It includes Optical Character Recognition (OCR) functionality.

- **McAfee DLP Endpoint** – controls data transfers that happen on endpoints via applications, removable storage devices, the cloud and more. 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 also includes out-of-box GDPR policies.

- **McAfee 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.

- **MVISION Cloud Integration** – extends DLP policies to the cloud. On-premises DLP content rules and policies can be synced with MVISION Cloud as well as applied to cloud services.

McAfee ePO (ePolicy Orchestrator) is McAfee's administrative console which can be used to set policies, manage incidents and workflows for all network and endpoint DLP components. McAfee also offers **MVISION ePO**, a cloud-native platform which can serve as a centralized administrative console. McAfee is migrating customers to the cloud-based platform.

STRENGTHS

- McAfee DLP is integrated with McAfee MVISION Cloud (its CASB offering), which helps organizations easily extend DLP policies into the cloud.

- McAfee ePO and MVISION ePO, 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 McAfee 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 McAfee 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

- McAfee DLP does not provide agent support for Linux.

- McAfee DLP does not offer specific features for Drip DLP detection. While such detection can be set up through rules, customers we spoke with indicated that it is somewhat cumbersome.

- While offering a rich set of features, McAfee DLP requires an experienced IT team to properly install and maintain the solution in a way that fully leverages its capabilities.

- While highly capable, a fully featured deployment of McAfee DLP tends to be somewhat more expensive than competing solutions.

- McAfee is undergoing a number of ownership transitions and management changes, first being spun off from McAfee as McAfee Enterprise, and more recently being united with FireEye Products into a combined company. At the time of this writing, it is too early to know what effect this will have on the company's future direction.

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**
- **Compliance**
- **Instant Messaging**
- **Unified Communications**
- **Mobility**
- **Web Technologies**

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:

- Management Consulting
- Whitepapers
- Strategic Business Planning
- Product Selection Advice
- TCO/ROI Analysis
- Multi-Client Studies

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

MARKET RESEARCH PUBLICATIONS

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

Currently Released:

Title	Released	Price*
Microsoft SharePoint Market Analysis, 2021-2025	May 2021	$3,000.00
Email Market, 2021-2025	Apr. 2021	$3,000.00
Microsoft Office 365, Exchange and Outlook Market Analysis, 2021-2025	Apr. 2021	$3,000.00
Cloud Business Email Market, 2021-2025	Apr. 2021	$3,000.00
Corporate Web Security Market, 2021-2025	Apr. 2021	$3,000.00
APT Protection Market, 2021-2025	Apr. 2021	$3,000.00
Information Archiving Market, 2021-2025	Mar. 2021	$3,000.00
Email Statistics Report, 2021-2025	Feb. 2021	$3,000.00
Instant Messaging Statistics Report, 2021-2025	Feb. 2021	$3,000.00
Social Networking Statistics Report, 2021-2025	Jan. 2021	$3,000.00
Mobile Statistics Report, 2021-2025	Jan. 2021	$3,000.00
Endpoint Security Market, 2020-2024	Nov. 2020	$3,000.00
Secure Email Gateway Market, 2020-2024	Nov. 2020	$3,000.00

*** Discounted by $500 if purchased by credit card.**

Upcoming Publications:

Title	To Be Released	Price*
Secure Email Gateways Market, 2021-2025	Dec. 2021	$3,000.00
Endpoint Security Market, 2021-2025	Dec. 2021	$3,000.00
Enterprise DLP Market, 2021-2025	Dec. 2021	$3,000.00

*** Discounted by $500 if purchased by credit card.**

All Radicati Group reports are available online at http://www.radicati.com**.**

