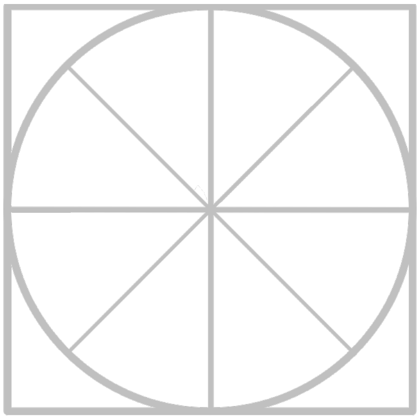
The Radicati Group, Inc.
www.radicati.com

THE RADICATI GROUP, INC.

Data Loss Prevention – Market Quadrant 2017



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

October 2017

[*] Radicati Market Quadrant^{SM} is copyrighted October 2017 by The Radicati Group, Inc. Reproduction in whole or in part is prohibited without expressed written permission of the Radicati Group. Vendors and products depicted in Radicati Market Quadrants^{SM} 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^{SM} 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.

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:

    - 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.

    - 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.

- 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.

- In other cases, a vendor may simply have become complacent and be out-developed by hungrier, more innovative Trail Blazers or Top Players.

- 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.

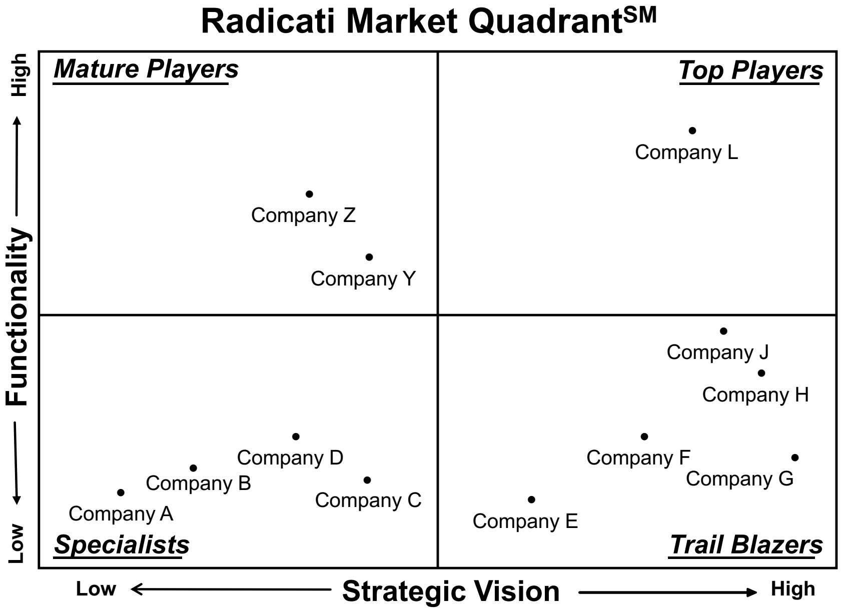


Figure 1: Sample Radicati Market Quadrant

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, Fidelis Cybersecurity, Forcepoint, GTB Technologies, McAfee, 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. Information Archiving).

- 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, the threat of data loss from internal threats is also significant due to insiders' easy access to data. 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 regulations worldwide also support increased 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 are increasingly affecting organizations of all sizes across all verticals.

- Against this backdrop of increased risk and growing regulations, organizations of all sizes are investing heavily in DLP solutions to protect data and ensure compliance. The worldwide revenue for DLP solutions is expected to grow from $970 million in 2017, to nearly $1.5 billion by 2021.

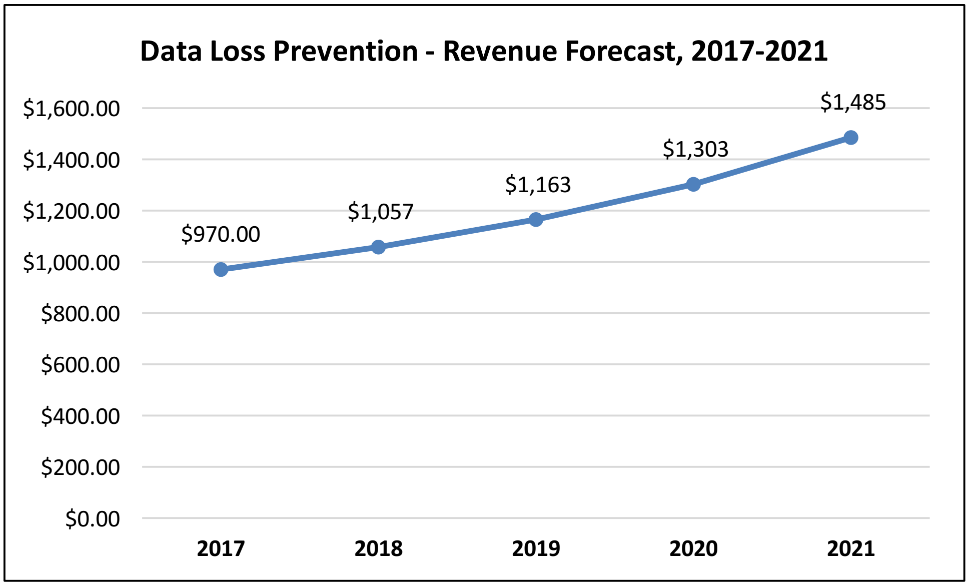


Figure 2: DLP Revenue Forecast, 2017 – 2021

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 datastore 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.

- **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

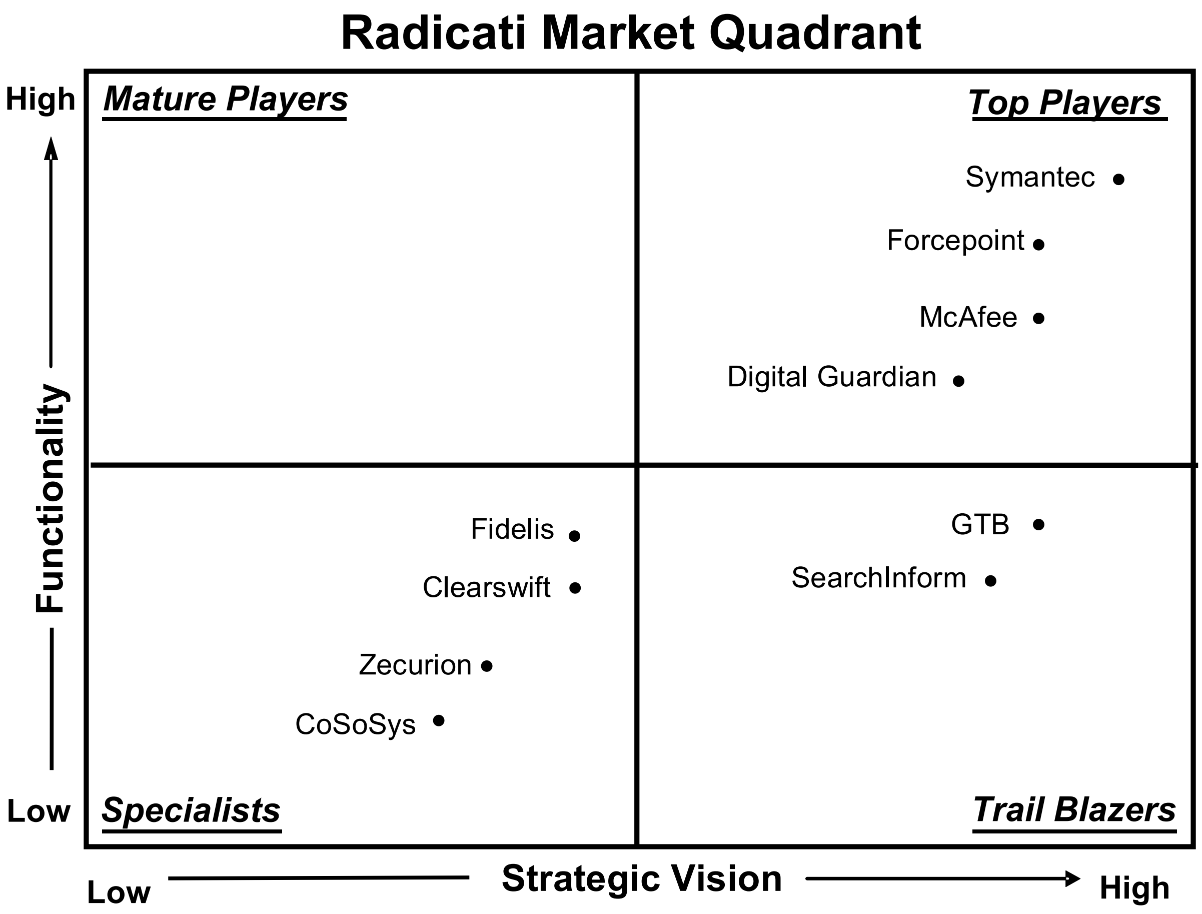


Figure 3: Data Loss Prevention Market Quadrant, 2017

[*] Radicati Market Quadrant is copyrighted October 2017 by The Radicati Group, Inc. Reproduction in whole or in part is prohibited without expressed written permission of the Radicati Group. 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*, *McAfee*, and *Digital Guardian*.
- The **Trail Blazers** quadrant includes *GTB Technologies*, and *SearchInform*.
- The **Specialists** quadrant includes *Fidelis Cybersecurity, Clearswift, Zecurion* and *CoSoSys*.
- There are no **Mature Players** in this market at this time.

DATA LOSS PREVENTION - VENDOR ANALYSIS

TOP PLAYERS

SYMANTEC

350 Ellis Street
Mountain View, CA 94043
www.symantec.com

Symantec offers a wide range of security solutions for enterprises and consumers. Symantec operates one of the largest civilian cyber intelligence networks in the world, allowing it to see and protect against the most advanced threats.

SOLUTIONS

Symantec's Data Loss Prevention solutions are available as cloud services, software, and virtual and hardware appliances. The **Symantec Data Loss Prevention 15.0** suite comprises the following product modules:

- **Symantec DLP Sensitive Image Recognition** – detects sensitive images and text embedded in images, such as scanned documents, screenshots, pictures and PDFs by leveraging a proprietary Form Recognition Technology and a built-in Optical Character Recognition (OCR) engine.

- **Symantec DLP Cloud Services** – are a set of cloud offerings which comprise:

    - *DLP Cloud Detection Service* - protects data in sanctioned and unsanctioned cloud apps such as Box, Dropbox, Office 365, Salesforce, and Google Apps. It is a cloud-based detection service that integrates with Symantec CloudSOC CASB and Symantec Web Security Service.

    - *DLP Cloud Service for Email* **-** protects corporate emails sent from Microsoft Exchange Server, Microsoft Office 365 Exchange Online, and Google G Suite. It is available standalone or bundled with Symantec Email Security.cloud to protect data and threats.

    - *DLP Cloud Service for Email with Cloud Console* - protects corporate emails sent from Microsoft Office 365 Exchange Online and Google G Suite. It is a SaaS solution with a cloud-based content detection service and cloud-based management console, the DLP Cloud Console. It is available standalone, or bundled with Symantec Email Security.cloud.

- **Symantec DLP for Network** – can be deployed on-premises or in a hybrid cloud environment, and comprises:

    - *DLP Network Monitor* - inspects and analyzes data over a wide range of network protocols: SMTP, HTTP, FTP, IM, NNTP, custom port-specific protocols, IPv6.

    - *DLP Network Prevent for Email* - monitors corporate email; blocks sensitive emails or redirects them to an encryption gateway for secure delivery; and alerts users to policy violations. It is available as software or virtual appliance.

    - *DLP Network Prevent for Web* - inspects and analyzes corporate web traffic (HTTP and HTTPS), removes sensitive content from posts or blocks posts altogether, and alerts users to policy violations. It is available as software, hardware appliance, or virtual appliance.

- **Symantec DLP for Endpoint** – offers coverage for endpoint data loss channels, including email, cloud applications, network protocols, removable storage, and virtual desktops. It comprises:

    - *DLP Endpoint Discover* - scans and inventories data stored on desktops and laptops. It can tag, delete or quarantine sensitive files on laptops and desktops.

    - *DLP Endpoint Prevent* - performs local scanning, detection, and real-time monitoring for a wide range of events on physical endpoints (e.g. Windows, macOS) as well as virtual endpoints and servers (e.g. Citrix, Microsoft Hyper-V, VMware).

- **Symantec DLP for Storage** – offers data scanning capabilities across a wide range of corporate repositories and endpoints. It includes:

    - *DLP Network Discover* - locates sensitive data at rest by scanning data repositories, including: local file systems on Windows, Linux, AIX, and Solaris servers; NAS filers; Microsoft Exchange and SharePoint servers; IBM Lotus Notes servers; and SQL databases.

    - *DLP Network Protect* - secures exposed files detected by Network Discover.

    - *Veritas Data Insight* - collects file usage and access permission transaction data on NAS filers, Windows servers, and SharePoint libraries. It integrates with DLP to identify owners of sensitive files and risk hotspots on shares, find anomalous access patterns and outlier users, and identify shares with wide accessibility.

    - *Veritas Data Insight Self-Service Portal* - integrates with DLP and enables security teams to delegate remediation of incidents discovered during scans to end-users (e.g. data owners or custodians).

- **Symantec DLP for Cloud** – comprises cloud email monitoring and cloud data discovery software, including:

  - *DLP Cloud Prevent for Microsoft Office 365 Exchange* - inspects all email in Exchange Online.

  - *DLP Cloud Storage for Box* - finds sensitive data at rest on Box Enterprise accounts and alerts users to policy violations through visual file tagging.

- **Symantec Information Centric Tagging** – provides the ability to apply tags and watermarks to classify sensitive documents. The tags can be applied by the user at creation of the file or when sending email. Tags can also be applied automatically based on DLP policy.

- **Symantec Information Centric Encryption** – provides the ability to apply digital rights to a document as a response of a DLP policy. The document encryption follows the document across its lifecycle. the administrator can delete documents remotely. the documents stay protected even when moved to the public cloud, unmanaged mobile devices or personal laptops.

- **Symantec Information Centric Analytics** – extends Symantec DLP with behavioral analysis capabilities. It can identify users with high risk base on their behavior with sensitive information.

- **Symantec DLP Enforce Console** – provides central management of suite components, where security teams can set policies, review and remediate incidents, and perform system administration across all channels from a single pane of glass.

Symantec DLP solutions also comprise a set of APIs for integration with third-party products and cloud applications, such as the DLP FlexResponse API, and DLP Detection REST API.

STRENGTHS

- Symantec offers a highly comprehensive DLP solution set to meet the complex needs of enterprises across all key data repositories, and communication channels. Symantec DLP solutions also integrate fully throughout the entire Symantec product portfolio.

- Symantec DLP solutions are available in all form factors including cloud services, software, and virtual and hardware appliances. This is important not just for customers who want cloud-based solutions, but also for customers who are not ready to move to cloud and prefer on-premises solutions, or combined hybrid solutions.

- Symantec's recent DLP 15.0 release offers further integration with its cloud encryption service, Information Centric Encryption, and its classification product, Information Centric Tagging.

- Symantec has highly comprehensive data detection technologies available with advanced features such as machine learning, image and form recognition, and data classification that cover a wide range of compliance and intellectual property protection use cases.

- Symantec provides strong support for Drip DLP detection.

WEAKNESSES

- Symantec is perceived as one of the more expensive DLP solutions available on the market, today. However, the addition of cloud-based DLP services and DLP appliances to its portfolio, allows Symantec to offer cost-effective options to customers of all sizes.

- While Symantec offers a rich and complete portfolio of DLP solutions and components, the correct integration of all capabilities can still be a challenge for customers.

- Customers we spoke with indicated that policy rules creation can be challenging and agent updates, when they occur, require manual intervention, which takes time and effort.

- Some Symantec's solutions for storage DLP (e.g. Veritas Data Insight*)* still rely on technology that was spun off to Veritas Technologies, as part of Symantec split into two companies of 2016. While the two companies maintain a strong working relationship, we believe that Symantec will in time bring this technology in-house.

FORCEPOINT

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

Forcepoint is a joint venture of Raytheon Company and Vista Equity Partners that was formed in 2015 out of a combination of Websense, Raytheon Cyber Products, and the Stonesoft and Sidewinder firewall assets it acquired from Intel Security in early 2016. In 2017, Forcepoint acquired the Skyfence CASB business from Imperva, as well as acquired RedOwl, a vendor of user behavior and security analytics. Forcepoint offers DLP, web, data, and email content security, cloud access security, next generation firewall, user behavior analysis, and threat protection solutions to organizations of all sizes.

SOLUTIONS

Forcepoint offers four separate DLP solutions, collectively known as the **Forcepoint DLP** when deployed together. The solutions comprise the following components:

- **Forcepoint DLP Endpoint** - protects data on endpoints in the enterprise covering Windows, macOS and Linux operating systems. The solution addresses data in motion, data in use, and data at rest use cases.

- **Forcepoint DLP Cloud Applications** - extends DLP policies into cloud applications, including Microsoft Office 365, Google G Suite, Box, DropBox and Salesforce. The solution addresses data in motion, data in use and data at rest use cases. It is provided via integration with Forcepoint CASB.

- **Forcepoint DLP Network** - monitors data that is being sent outside of an organization's network and applies the appropriate policies. It can alert, block, notify, audit, and quarantine data in web, email, FTP, IM, and other channels. It provides integrated OCR for a wide range of languages.

- **Forcepoint DLP Discover** - scans for confidential data within an organization via agent-based and agent-less methods. Data is scanned on file servers, databases, collaboration platforms (e.g., SharePoint), and email servers both on-premises or in the cloud. Content can be encrypted, removed, quarantined, audited, or have other actions take place. It provides integrated OCR for a wide range of languages.

Forcepoint DLP will also be part of the vendor's Human Point System, a unified platform for Forcepoint UEBA (User and Entity Behavior Analytics), Forcepoint DLP, and Forcepoint Insider Threat and Forcepoint CASB, which is due to launch in 2018.

STRENGTHS

- Forcepoint supports deployment of DLP management and data classification components on-premises and in public cloud (Microsoft Azure and Amazon AWS).

- In addition to Microsoft Windows, Forcepoint also offers support for Apple macOS and Linux systems, including detection of fingerprinted structured and unstructured data.

- Integration with Forcepoint CASB enables DLP policies to be extended to enterprise cloud applications via a cloud hosted service. This hybrid approach 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 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 security operations teams.

WEAKNESSES

- While Forcepoint currently offers powerful Endpoint, Network and Discover DLP components, at present these must be purchased separately. The vendor is planning to release a bundled option in the near term.

- The Forcepoint DLP Endpoint capabilities for Linux are currently not as developed as other operating systems. The vendor plans to address this in future releases.

- Forcepoint currently extends DLP policies to mobile devices through a partnership with AirWatch. Additional mobile controls are planned for early 2018.

MCAFEE

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

McAfee delivers security solutions and services for business organizations and consumers. The company provides security solutions, threat intelligence and services that protect endpoints, networks, servers, cloud and more.

SOLUTIONS

McAfee Data Loss Prevention offers a number of DLP components that can be mixed and matched to create a complete DLP solution. It provides the following:

- **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.

- **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 can scan and remediate data stored in Box.

- **McAfee DLP Monitor** – identifies, tracks, and reports on data in motion in an organization. The solution monitors all data in motion via its capture database that gives administrators insight into how best to set DLP policies. The appliance can detect and manage over 300 content types.

- **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.

- **McAfee DLP Endpoint** – controls data transfers that happen on endpoints via the network, applications, removable storage devices, and more. The solution can block, alert, notify, encrypt, quarantine, and perform other actions on sensitive data on an endpoint.

McAfee ePO (ePolicy Orchestreator) is McAfee's administrative console for all its solutions. It be used to can centrally set policies, manage incidents and workflows for all network and endpoint DLP components.

STRENGTHS

- McAfee DLP offers a combination of deployment options, including software agent, hardware appliance and virtual appliance.

- The fully unified McAfee Data Loss Prevention solution can be centrally managed via the McAfee ePolicy Orchestrator that also provides central management for all other McAfee solutions in an organization.

- In addition, McAfee ePolicy Orchestrator allows for common policy management across network and endpoint DLP via a common classification engine, dictionaries, regex engine and syntax. The use of a common text extraction engine across network and endpoint DLP ensures consistency of analysis of policies against files, as well as helps unify incident and case management.

- 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. It is 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.

- McAfee's bundled DLP suite, McAfee Total Protection for DLP, includes all DLP components at a discount. Also, features, such as Manual Classification, and DLP Prevent for mobile email have been added the existing licensing for free. McAfee Device Control is also included in McAfee DLP Endpoint license.

WEAKNESSES

- For McAfee Network DLP, virtualized environments currently support only VMware technology.

- McAfee recently added DLP agent support for macOS, however it still lacks feature parity with its Windows agent. DLP agent support for Linux is not available.

- McAfee currently lacks APIs for CASB integration with third party solutions.

- McAfee DLP does not currently 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.

DIGITAL GUARDIAN

860 Winter Street, Suite 3
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. The company is privately held and headquartered in Waltham, Massachusetts with offices worldwide.

SOLUTIONS

Digital Guardian provides a threat-aware data protection platform purpose built to stop 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, 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** – is designed to discover and protect sensitive data throughout the data lifecycle and across the enterprise. It helps protect sensitive data on the network layer, at the endpoint layer, in the cloud and on mobile devices through automated context-based and content/fingerprint-based classification, plus user-based data classification. The platform is available through flexible deployment options which include on-premises, SaaS, or as a managed security service backed by an analyst team with threat detection expertise.

- **Digital Guardian for Endpoint Data Loss Prevention** – stops sensitive data from getting out of an organization. It provides automated as well as user-based classification of sensitive data on endpoints, inspects and controls all content with context-aware DLP, and enforces DLP policies across all egress channels. It is available for Windows, Linux and macOS workstations.

- **Digital Guardian for Network Data Loss Prevention** – is a virtual or physical appliance that discovers and classifies sensitive and regulated data, prevents sensitive data from leaving via the network, monitors and controls all communications channels including email (SMTP), Web (HTTP/HTTPS), FTP and SSL.

- **Digital Guardian for Cloud Data Loss Prevention** – integrates with leading cloud storage and collaboration providers such as Box, Citrix and Microsoft. It discovers sensitive data in cloud storage, continuously audits files that have been uploaded, automatically remediates according to enterprise policies, and instantly alerts administrators and/or data owners when protected data has been identified.

- **Digital Guardian Analytics & Reporting Cloud (ARC)** – is an advanced analytics and reporting solution that delivers threat-aware data protection as a cloud-based, subscription service. It leverages streaming data from Digital Guardian endpoint agents and network appliances, to provide the deep visibility into system, data and user events. This visibility powers security analyst-approved dashboards to enable data loss prevention and endpoint detection and response through the same console. This is a key feature as it prevents data exfiltration from both internal and external attackers.

STRENGTHS

- Digital Guardian offers flexible deployment models including on-premises, SaaS, or through its Managed Security Program (MSP).

- Digital Guardian's data protection platform is designed to protect data against both internal and external threats using the same agent, network appliance and management console.

- Digital Guardian's kernel level endpoint agent enables deep data visibility and flexible controls with near feature parity across Windows, macOS, and Linux.

- Digital Guardian offers a mobile app for a secure document viewing, through the iTunes store, which allows users to view encrypted MS Office, Apple iWork, text or PDF docs on iOS devices.

- Digital Guardian Endpoint DLP is event-driven, where agents begin collecting information about data movement upon deployment vs. requiring defined policies that may be more difficult to construct.

- Digital Guardian works well with a broad range of integrations, such as SIEM, CASB, encryption, threat intelligence feeds, network sandboxes, and as well as connecting with web and email security gateways via ICAP.

WEAKNESSES

- Digital Guardian has limited mobile DLP capabilities, so customers would need to rely on existing mobile device management (MDM) or mobile application management (MAM) solutions.

- Digital Guardian can support cloud file storage and collaboration but only for supported vendors such as Box, Accellion, Citrix Share File, Office 365, One Drive, and others. Support for cloud applications like Salesforce.com, is currently available only through a CASB provider.

- While Digital Guardian integrates with Microsoft Office 365 to deliver Microsoft's Azure Information Protection digital rights management capability, they do not offer native DRM.

- Digital Guardian acquired their network DLP appliance (formerly Code Green Networks) in November 2015 and plans to complete the full integration of its capabilities with its endpoint DLP solution in the Q1 2018 timeframe. Until that integration is complete, customers of both endpoint and network DLP must write separate policies.

TRAIL BLAZERS

GTB TECHNOLOGIES

5000 Birch Street, Suite 3000
Newport Beach, CA 92660
www.gttb.com

GTB Technologies, founded in 2004, is a cybersecurity company that focuses on enterprise data protection and data loss prevention. The company is privately held.

SOLUTIONS

GTB's **DLP That Works** platform is designed to prevent the loss of data from malware, and trusted insiders by blocking sensitive data (structured, semi-structured or unstructured) regardless of file type, port or channel, in real-time. GTB solutions are available on-premises, cloud, or hybrid including SaaS options (DLP as a Service, Discovery as a Service, and others). Managed services include fully managed, as well as hybrid management. GTB solutions cover Windows, macOS, and Linux operating systems. The platform provides the following functionality:

- *Data in use* – the GTB Endpoint Agent is a multi-functional system that supports full TCP Scanning on all ports and protocols, full USB and Device Controls, full Applications Control with support for both white and black list plus full Data Discovery with Content Aware Classification for both files and emails. The GTB Endpoint agent also integrates with GTB IRM (Information Rights Management) system and can protect files based on content. Policies may be created based on protocols, sources, destinations, data, file types and more. Enforcement actions include: block, log and alert, user remediation and more.

- *Data in motion* – provides protection for both text and binary data (e.g. files and data streams, structured, semi-structured and unstructured data). It supports multiple span ports, with separate support for both webmail on HTTP and on HTTPS and user warning sending data over non-secured channels. Automatic routing of emails is provided to encryption gateways, as well as support for ICAP to receive handoffs from proxy servers. Supported channels include social media and blogs.

- *Data at rest* – the GTB Endpoint Agent performs local scans on PCs, Mac and Linux platforms. The GTB Discovery server performs over the network scans for: file-shares, Microsoft Exchange, Microsoft SharePoint, PST/OST files, databases and a broad range of cloud storage solutions, including Office 365, Box, Dropbox, AWS, Azure, Citrix ShareFile and 75 other cloud storage accounts. Scanning is accomplished without requiring the installation of any component on the target scan. Scanning supports both fingerprinting and pattern detection with the ability to auto-classify files based on such policies.

- *User behavior analytics* – provide analysis of items including Number of files sent or saved, size of the files sent or saved.

- *Drip DLP* – is supported and may be set based on IP range, groups and for specific policies having a certain severity level and within a pre-defined time period.

- *Mobile DLP* – The GTB Inspector is connected to a Mirror Port or a SPAN port and can view all mobile device data, as well as take enforcement actions if necessary.

Administration is available through the **GTB Central Console** which can deploy policies automatically to all components of the system including agents, discovery servers and inspectors. GTB provides hundreds of policy templates sorted by country for regulatory compliance and unstructured data protection. The solution supports both Multi-Domain and Multi-forest environments.

STRENGTHS

- The GTB DLP that Works platform is available in a variety of form factors that include on-premises, cloud, or hybrid.

- The GTB platform comprises a broad set of integrated DLP facets and solutions which cover a broad range of outbound or inbound channels and protocols.

- GTB's offers highly advanced detection techniques which include its own patented fingerprinting engine (AccuMatch), OCR (Optical Character Recognition) for image scanning, and support for Drip DLP.

- GTB's CASB solution offers visibility and control of data within cloud applications including Microsoft Azure, Office 365, Google G Suite, Box, Dropbox, Salesforce and 75 other cloud storage accounts.

- GTB DLP that Works platform provides an integrated DRM/IRM system which is content aware and can protect files based on DLP policies.

WEAKNESSES

- The GTB platform currently lacks antivirus and anti-malware support in the Endpoint Agent. GTB has this on its roadmap for Q1 2018.

- Increased bandwidth support (i.e. 100bmps) for the GTB Inspector, is on the vendor's roadmap with a Q2 2018 release.

- GTB could improve its market visibility. The vendor is working to address that.

SEARCHINFORM

8/1 Skatertnyi pereulok, building 1, offices 1-12
Moscow, Russian Federation

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 in the UK, Benelux and Latin America.

SOLUTIONS

SearchInform DLP offers information security across a wide range of communication channels, which includes privileged user management, work efficiency control, user behavior monitoring and more. It provides real time analysis of virtually all information flows to prevent data theft or leakage. It also helps to prevent harmful activities by the 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- 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. control of 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), and Instant Messaging (e.g. Skype, ICQ, MMP, XMPP/Jabber, MSN, Telegram, and more) and social networks (i.e. Facebook, LinkedIn, and others).

  - *Data at rest* – the ability to monitor and analyze over 100 types of files on PCs, network storage, NAS, databases, Microsoft SharePoint, and more.

  - *Policy controls* – the solution comes with over 250 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 additional policies that meet specific needs.

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

STRENGTHS

- SearchInform's management solution is available in all form factors, on-premises, cloud or hybrid.

- SearchInform offers a highly scalable solution which can scale to tens of thousands of endpoints under control.

- SearchInform offers strong image analysis capabilities through OCR and its own image analysis technology.

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

- SearchInform is quick to innovate and is continuously updating its solution to monitor and analyze data from an ever increasing number of data sources.

WEAKNESSES

- SearchInform currently lacks support for macOS devices.
- SearchInform does not provide CASB integration capabilities.
- SearchInform does not provide mobile DLP capabilities either on its own or through integration with MDM or EMM vendors.
- SearchInform lacks market visibility particularly outside of Russia and Central Europe. The vendor is working to address that.

SPECIALISTS

FIDELIS CYBERSECURITY

4500 East West Highway, Suite 400
Bethesda, MD 20814

Fidelis is a cybersecurity technology company that offers automated threat detection and response platform and services. The company was originally known for its DLP solutions, but acquired endpoint security vendor Resolution1 in 2015, and has since pivoted to the Automated Detection and Response market. The company is privately held through an investment from Marlin Equity Partners.

SOLUTIONS

Fidelis offers DLP as a feature of **Elevate**, its broader automated threat detection and response platform. Elevate comprises network and endpoint modules which can be deployed in various form factors including on-premises, cloud, and hybrid models. Fidelis Elevate offers only DLP in motion though the monitoring of application content in sessions. The solution is largely OS agnostic.

Fidelis provides network DLP analysis through two network layer sensors designed to integrate with 3rd-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 Cisco (i.e. IronPort), Proofpoint, SendMail and Postfix.

- *Fidelis Network Web* – integrates with standards-based Web Proxy solutions through an ICAP interface to add a DLP capability for proxy solutions like Symantec (i.e. Blue Coat), Forcepoint and others. The Fidelis Network sensor also allows monitoring of social networks, such as Twitter and Facebook through its session inspection technology.

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

In addition, the Fidelis Cybersecurity Threat Research Team (TRT) regularly makes streaming policy updates available to customers on the basis of ongoing research. These policy updates are delivered to the customer automatically via the Fidelis Insight Cloud service.

The Fidelis Elevate network sensors are configurable from a single management UI, called K2 that can be deployed on premises or in the cloud.

STRENGTHS

- Fidelis solutions can be deployed in various form factors including on-premises, cloud, and hybrid models.

- Fidelis offers a good set of out-of-the-box policies and rules for securing sensitive information.

- Fidelis offers DLP as part of a broader solution for network and endpoint 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 currently offer a common user interface for configuration of its network and endpoint solutions. This is on the vendor's future roadmap.

- Fidelis does not integrate with EMM and does not offer endpoint DLP.

- Fidelis is working to build awareness for its solution in the market for Automated Detection and Response which tends to de-emphasize its visibility in the DLP market.

CLEARSWIFT

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

Clearswift is an information security company with offices in the USA, UK, Australia, Germany and Japan with over 20 years of secure content, email and web security expertise. Clearswift was acquired in January 2017 by Swiss defense company, RUAG.

SOLUTIONS

Clearswift offers a portfolio of solutions which can be peered together allowing customers to extend their hygiene solutions to provide DLP features across their environment in a cost effective manner. Clearswift products are available on bare metal, vSphere, Hyper-V, AWS and Azure. Clearswift also sells its solutions in a hosted option. The Clearswift portfolio includes:

- **SECURE Email Gateway (SEG)** – provides DLP features (and strong hygiene features) that permit SMTP email to be scanned leaving and entering the company. Policy rules can be set to be granular to identify email from individuals, departments, or whole domains as required. DLP features include keyword search across headers, subject, body and attachments (which also includes document properties), file type matching including customer defined type files (including byte patterns, not just extensions). When used with the Information Governance Server (IGS) it also provides document/partial document matching. The SEG 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). Sensitive content that requires secure delivery can use the built-in TLS options as well as message based encryption methods such as S/MIME, PGP or password, as well as a portal based encryption option. The SEG supports AD integration and can provide rules that require end users to copy outbound emails to their managers or other compliance mailboxes.

- **SECURE Exchange Gateway (SXG)** – permits scanning of internal mail in a Microsoft Exchange environment using all of the same DLP features as the SEG. The SXG system allows large organization to compartmentalize content into their own business unit or region depending on their Microsoft Exchange topology. SEG and SXG, being both email based are also able to share message areas (i.e. quarantine stores), message tracking, as well as reporting for a richer administrative experience.

- **SECURE Web Gateway (SWG)** – features a HTTP proxy and content filtering engine that performs hygiene features and URL classification. Time based controls and quota-based control access to permit sites restrict the risks of Shadow IT and unauthorized data sharing. The SWG also supports HTTP/S interception so as to be able to inspect content using all of the available methods (as in SEG) to secure web sites from upload and download of sensitive data.

- **SECURE ICAP Gateway (SIG)** – can augment existing web filtering investments with DLP specific policies for customers that have existing web proxy solutions, such as Bluecoat, F5, Cisco, or similar other ICAP-based solution. This variant can be used in both forward and reverse proxy modes.

- **Critical Information Protection (CIP)** – 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 or network shared drives (i.e. data at rest).

- **Information Governance Server (IGS)** – acts as a central store where end users can register sensitive information, and permits 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.

STRENGTHS

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

- Clearswift's DLP policy rules are built with 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 has a built-in data classification system that is highly tunable, and which also allows flexible "confidence" levels of classification to be configured. Third-party data classification from Titus and Boldon James are also supported.

- Clearswift's data and document sanitization features can remove content in file metadata, such as document properties and revision history, as well as remove active content, such as macros and embedded executables.

- 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 support needs macOS and Linux. Both are scheduled for 2018.

- Clearswift does not currently provide support for Instant Messaging networks (e.g. Teams/Skype for Business) or Social Networks.

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

- Clearswift still needs to deliver OCR capabilities. These are on the vendor’s roadmap for early 2018.

ZECURION

14 Penn Plaza, 9th floor
New York, NY 10122

Zecurion, founded in 2001, develops security solutions that protect against information loss. The company is privately held, with headquarters in Moscow and New York and offices in Europe.

SOLUTIONS

The Zecurion DLP solution monitors all local and network data leakage channels, intercepts all traffic leaving the corporate network, detects sensitive information being transmitted, and based on established security policies allows or restricts the transmission of data. All intercepted traffic is archived and further investigated for analysis of any data loss incidents. It supports analysis of more than 500 file types and has the capability to block leakage in real time. The solution enables organizations to create flexible policies for different types of USB devices, different groups and individual users. Zecurion is currently available for Windows and Mac devices. The vendor also offers Mobile DLP for iOS and Android devices. The solution is available in different form factors including on-premises, cloud and hybrid.

Zecurion DLP is available through the following product components:

- **Zecurion Zgate** (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.

- **Zecurion Zlock (Windows)** (endpoint DLP) – allows 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.

- **Zecurion Zlock for Mac** (endpoint DLP) – similarly to the Windows version, allows security officers to create policies for different types of USB devices, different groups and individual users.

- **Zecurion Zserver** (data at rest DLP) – serves to securely protect data stored on servers and on backup media. The system encrypts the information contained on hard drives, disk arrays and SAN storage using a proprietary encryption method.

- **Zdiscovery** (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.

- **Zecurion Mobile DLP** – offers content analysis for Android devices. It provides complete monitoring of corporate information on employees' mobile devices, preventing data leaks at various stages of information processing, storage, and transfer. In the event of theft or loss, the device can be blocked by a security officer. The solution also stores shadow copies of SMS and MMS, as well as monitors the running of applications using black- and whitelists.

- **Zecurion DLP Cloud** – is a combined Zserver/Zgate offering that deploys DLP as a service with additional protection on the public cloud, where administrators can centrally manage keys and policies. It also helps sustain compliance as a centralized key management platform to demonstrate compliance with data security policies and compliance mandates, such as PCI-DSS and HIPAA.

Zecurion DLP uses a single web console to define and enforce policies across all endpoints, cloud solutions and mobile devices. 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 both the Mac and Windows-based platforms is handled through the single management console.

STRENGTHS

- Zecurion DLP is available in different form factors including on-premises, cloud and hybrid.
- Zecurion Zgate 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 Skype (i.e. Teams).
- Zecurion provides full archiving of all data seen by endpoint agents, and can also capture screen shots and other end-user screen activities.

WEAKNESSES

- Zecurion does not currently provide support for Linux devices. The vendor has this on its roadmap.
- Zecurion does not currently offer capabilities for detecting Drip-DLP. The vendor has this on its future roadmap.
- Zecurion does not currently offer or integrate with CASB capabilities. The vendor has this on its future roadmap.
- Zecurion has low market visibility in North America. The vendor is working to address that.

COSOSYS

Str. Croitorilor 12-14, 2nd Floor
400162 Cluj-Napoca
Romania

CoSoSys offers solutions for Data Loss Prevention (DLP), eDiscovery, Device Control and Mobile Device Management (MDM). The company is privately held, with headquarters in Romania and offices in Germany, USA, South Korea and the United Arab Emirates.

SOLUTIONS

CoSoSys **Endpoint Protector** is an all-in-one Data Loss Prevention (DLP) solution for Windows, macOS, Linux, as well as Thin Clients (i.e. Android, iOS). 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 filtering capabilities which range from file type and predefined content to custom content filters based on dictionaries and regular expressions. The movement of valuable data to unauthorized external individuals is monitored through the exit points and administrators are alerted in the case of a policy violation. All reports can be viewed in a centralized management console. The solution is offered in various form factors as follows:

- **Endpoint Protector** – offers on premise DLP, which is available as hardware or as a virtual appliance. It can also be delivered through services like AWS.

- **My Endpoint Protector** – is a cloud based DLP solution. For large deployments or OEM deals, the servers can be hosted/managed on a SaaS basis.

- **Endpoint Protector Basic** – is a standalone Device Control solution, aimed at the needs of small businesses or isolated endpoints (e.g. a production line, with no Internet connection).

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 any sensitive data leaving their computers. Through close content inspection, transfers of important company documents can be logged and reported. File transfers are allowed or blocked based on predefined company policies.

- *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 such as HIPAA, GDPR, and more. Based on scan results, remediation actions can be taken such as encrypting or deleting files for data breach protection.

- *Device Control* – gives organizations 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 in order to protect sensitive data from data theft.

- *Enforced Encryption* – makes sure all confidential data transferred to USB storage devices is automatically encrypted. Via a secured password, users can safely transfer confidential data and access it on any computer or only on company computers. IT Administrators can remotely reset encryption passwords for users that have forgotten their passwords. They can also send messages to users, request a password change or wipe confidential data in case a device is lost or stolen.

- *Mobile Device Management* – provides enhanced control over the use of Android and iOS mobile device fleets and macOS computers. It enables companies to set strong security policies and access detailed tracking and asset management of all smartphones or tablets. It can also increase productivity by pushing and monitoring applications, network settings and more.

Endpoint Protector enables a seamless management of all a company's endpoints regardless of their operation system, all from a single dashboard.

STRENGTHS

- CoSoSys Endpoint Protector offers strong coverage of all platforms including Windows, macOS and Linux (several Linux distributions: Ubuntu, openSUSE, RedHat and more), which makes it a good choice for organizations running mixed OS environments.
- Endpoint Protector also enables a seamless management of all a company's endpoints regardless of their operating system, all from a single dashboard.
- CoSoSys offers diverse form factors formats, including hardware appliance, virtual appliance, or on AWS, which meets the needs of customers with a wide range of infrastructures.
- CoSoSys Endpoint Protector is easy and fast to install and deploy through flexible policy management and an intuitive user interface.
- The CoSoSys Endpoint Protector solution is designed to also be easily managed by non-specialized technical personnel.

WEAKNESSES

- While CoSoSys offers its own solutions for mobility management (MDM and MAM), it does not currently offer a DLP component for these solutions. It does however, offer an SDK solution that can be used to extend DLP capabilities to mobile apps.
- CoSoSys currently offers OCR image analysis capabilities only to a limited number of countries.
- 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 lacks market visibility outside of Europe and Asia. The vendor is working to address that.

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, 2017-2021	Jun. 2017	$3,000.00
Corporate Web Security Market, 2017-2021	Jun. 2017	$3,000.00
Email Market, 2017-2021	Jun. 2017	$3,000.00
Office 365, Exchange Server and Outlook Market Analysis, 2017-2021	Jun. 2017	$3,000.00
Cloud Business Email Market, 2017-2021	Jun. 2017	$3,000.00
Information Archiving Market, 2017-2021	May 2017	$3,000.00
Enterprise Mobility Management Market, 2017-2021	Apr. 2017	$3,000.00
Advanced Threat Protection Market, 2017-2021	Apr. 2017	$3,000.00
Mobile Statistics Report, 2017-2021	Apr. 2017	$3,000.00
Social Networking Statistics Report, 2017-2021	Feb. 2017	$3,000.00
Instant Messaging Market, 2017-2021	Feb. 2017	$3,000.00
Email Statistics Report, 2017-2021	Feb. 2017	$3,000.00

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

Upcoming Publications:

Title	To Be Released	Price*
Endpoint Security Market, 2017-2021	Nov. 2017	$3,000.00
Secure Email Gateway Market, 2017-2021	Nov. 2017	$3,000.00
Enterprise Data Loss Prevention Market, 2017-2021	Nov. 2017	$3,000.00

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

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