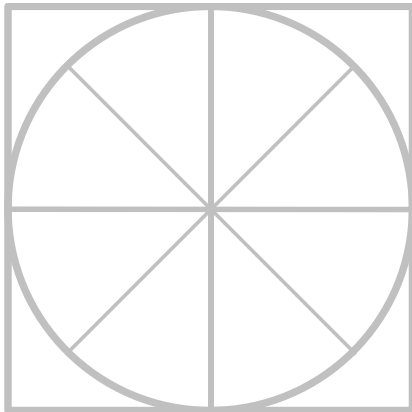


# THE RADICATI GROUP, INC.

## Data Loss Prevention – Market Quadrant 2018

• • • • • • • •



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

**October 2018**

---

\* Radicati Market Quadrant<sup>SM</sup> is copyrighted October 2018 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<sup>SM</sup> 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<sup>SM</sup> 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.....	3
MARKET SEGMENTATION – DATA LOSS PREVENTION .....	5
EVALUATION CRITERIA.....	7
MARKET QUADRANT – DATA LOSS PREVENTION .....	10
<i>KEY MARKET QUADRANT TRENDS</i> .....	11
DATA LOSS PREVENTION - VENDOR ANALYSIS .....	11
<i>TOP PLAYERS</i> .....	11
<i>TRAIL BLAZERS</i> .....	26
<i>SPECIALISTS</i> .....	29

---

Please note that this report comes with a 1-5 user license. If you wish to distribute the report to more than 5 individuals, you will need to purchase an internal site license for an additional fee. Please contact us at [admin@radicati.com](mailto:admin@radicati.com) if you wish to purchase a site license.

Companies are never permitted to post reports on their external web sites or distribute by other means outside of their organization without explicit written prior consent from The Radicati Group, Inc. If you post this report on your external website or release it to anyone outside of your company without permission, you and your company will be liable for damages. Please contact us with any questions about our policies.

---

## RADICATI MARKET QUADRANTS EXPLAINED

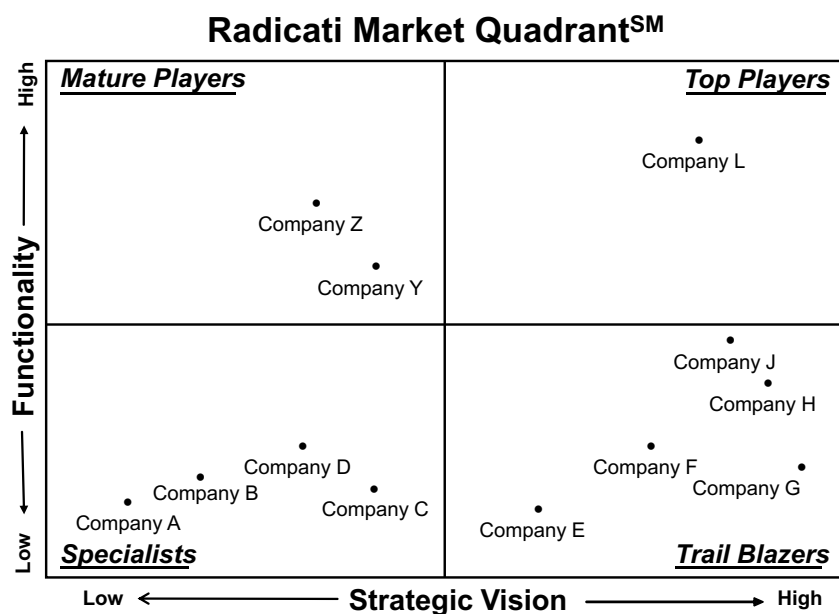
Radicati Market Quadrants are designed to illustrate how individual vendors fit within specific technology markets at any given point in time. All Radicati Market Quadrants are composed of four sections, as shown in the example quadrant (Figure 1).

- **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**

## 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.

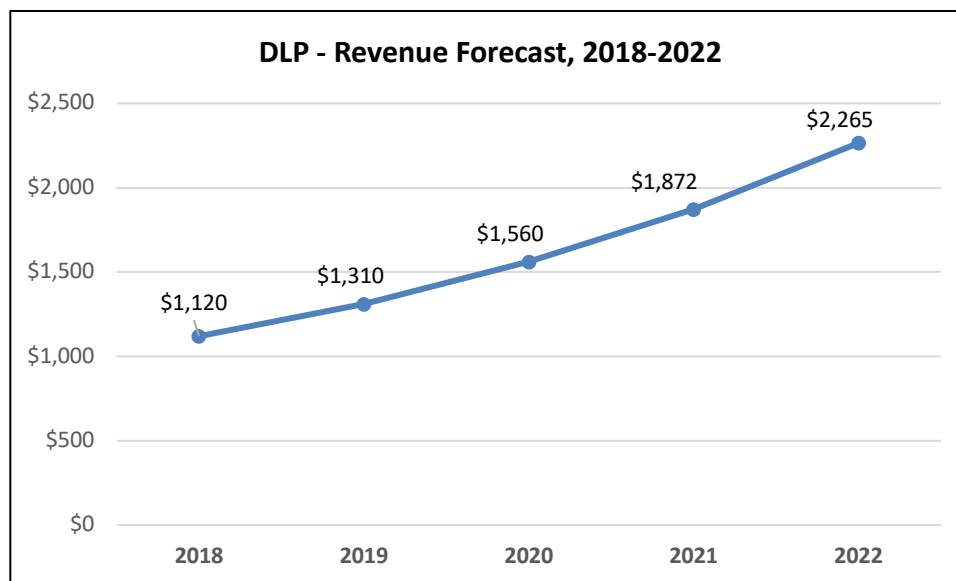
## MARKET SEGMENTATION – DATA LOSS PREVENTION

This edition of Radicati Market Quadrants<sup>SM</sup> 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, GTB Technologies, Matrix42, 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. 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.
- Amid increased risk concerns and a growing set of regulations, 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 \$1.1 billion in 2018, to over \$2.2 billion by 2022.



**Figure 2: DLP Revenue Forecast, 2018 – 2022**

## 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

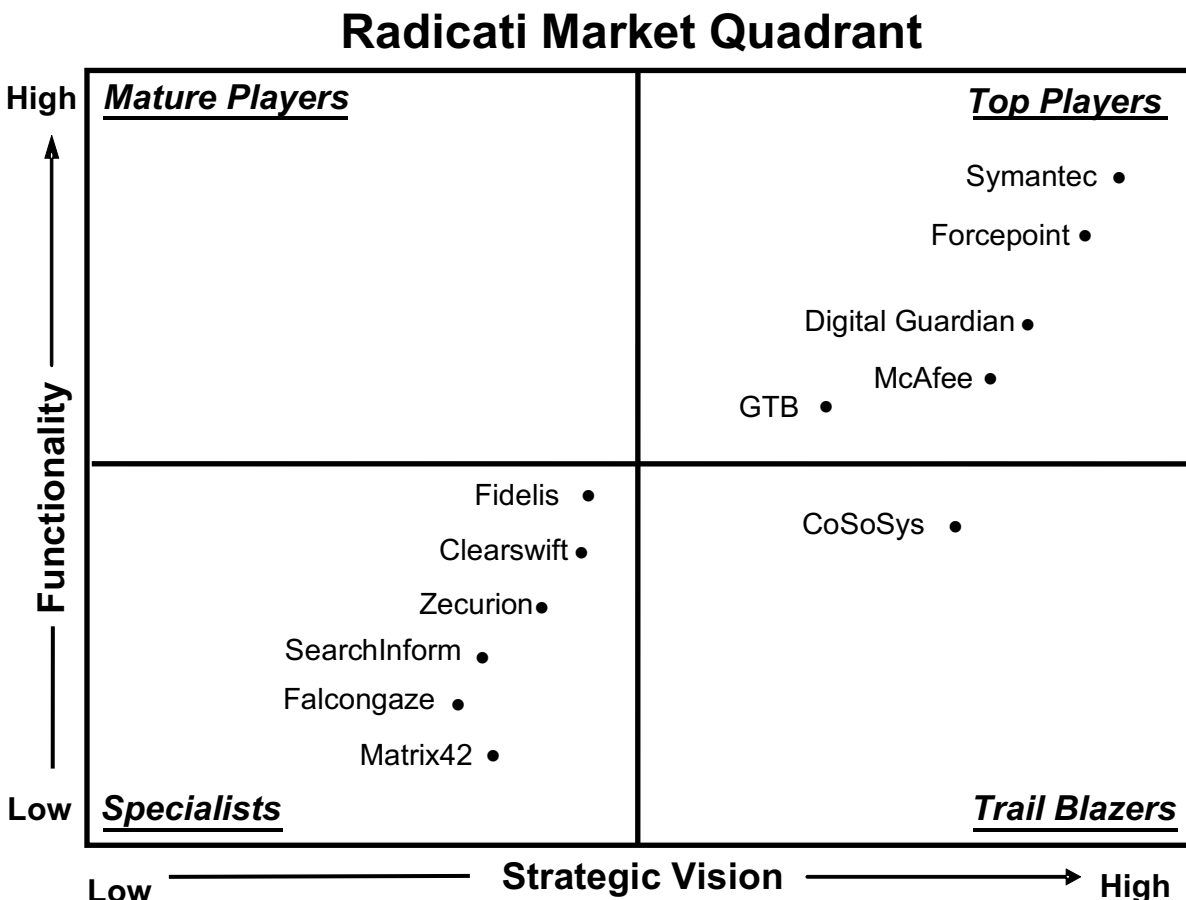


Figure 3: Data Loss Prevention Market Quadrant, 2018\*

\* Radicati Market Quadrant is copyrighted October 2018 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*, *Digital Guardian*, *McAfee*, and *GTB Technologies*.
- The **Trail Blazers** quadrant includes *CoSoSys*.
- The **Specialists** quadrant includes *Fidelis Cybersecurity*, *Clearswift*, *Zecurion*, *SearchInform*, *Falcongaze*, and *Matrix42*.
- 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](http://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 15.1** suite comprises the following product modules:

- **Symantec DLP Enforce Console** – provides central management of suite components, allowing security teams to set policies and workflows, review and remediate incidents, and perform system administration across all channels, on premises and cloud, from a single pane of glass.
- **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 Suite. It is a cloud-based detection service that integrates with Symantec CloudSOC CASB and Symantec Web Security Service to extend consistent DLP policies to the cloud. If sensitive data needs to be shared with third parties, it can be automatically protected via Symantec Information Centric Encryption (ICE).
  - *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 as a standalone solution, or bundled with Symantec Email Security.cloud. Sensitive emails can be automatically protected and tracked via Symantec ICE, to ensure that only authorized recipients can open them.
- **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 & Web* – monitors corporate email and web traffic; blocks sensitive emails or redirects them to an encryption gateway for secure delivery; blocks and removes sensitive content from posts; and alerts users to policy violations. It is available as software, or as an 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.
- **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 Information Centric Tagging** – provides the ability to manually apply data classification tags and watermarks to sensitive documents and emails. The tags can be applied by the user at creation of the file or when sending email. Tags are used to enable consistent policy enforcement and tiered policies based on sensitivity level. Tags can also be applied automatically, based on DLP policy. Administrators can view and manage policies for employee-identified sensitive data on the Symantec DLP Enforce console.
- **Symantec Information Centric Encryption** – provides the ability to apply identity verification and digital rights to a document as a response of a DLP policy. The document encryption follows the document across its lifecycle. The administrator can track data access and revoke documents remotely. The documents remain protected when moved to the public cloud, unmanaged mobile devices, or personal laptops.

- **Symantec Information Centric Analytics** – extends Symantec DLP with behavioral analysis capabilities. It helps simplify DLP incident triage and can pinpoint high risk and malicious users based on their behavior with sensitive information.
- **Veritas Data Insight & Data Insight Self-Service Portal** – collects file usage and access permission transaction data on NAS filers, Windows servers, and SharePoint libraries. It integrates with Symantec DLP to identify owners of sensitive files and risk hotspots on shares, find anomalous access patterns and outlier users, and lets security teams delegate incident remediation to end-users (e.g. data owners or custodians).

## STRENGTHS

- Symantec offers a sophisticated and comprehensive DLP solution which can help meet the complex needs of enterprises across all key data repositories and communication channels.
- Symantec has highly comprehensive data detection technologies available with advanced features such as machine learning, fingerprinting, image and form recognition, and data classification that cover a wide range of compliance and intellectual property protection use cases.
- Symantec's DLP solution includes a number of key capabilities, such as data classification, encryption and digital rights management, and user entity behavior analytics (UEBA).
- Symantec DLP solutions integrate fully throughout the entire Symantec product portfolio (e.g. with Symantec web security, email security, CASB, and others), delivering data protection through a consistent set of policies.
- Symantec DLP solutions are available in all form factors including cloud services, software, and virtual and hardware appliances. This is important for customers who may not be able to move to cloud due to regulatory requirements, and prefer on-premises solutions, or hybrid solutions.

## WEAKNESSES

- Symantec is somewhat more expensive than other DLP solutions on the market. However, it offers a rich feature set and when fully integrated with other Symantec security solutions delivers significant ROI in terms of detection accuracy, fine policy tuning, and data leak protection across all channels.
- While Symantec offers a rich portfolio of DLP solutions and components, it can be somewhat complex to manage for organizations with fewer resources. Smaller organizations can rely on managed services offered through Symantec partners.
- Symantec can improve the integration of its DLP capabilities with Symantec Endpoint Protection (SEP) solutions. The vendor has this on its roadmap.

## FORCEPOINT

10900 Stonelake Blvd  
3rd Floor  
Austin, TX 78759  
[www.forcepoint.com](http://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 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, insider threat detection, and threat protection solutions to organizations of all sizes.

## SOLUTIONS

Forcepoint offers three types of DLP solutions: **DLP for Compliance**, **DLP for IP Protection**, and **Dynamic Data Protection**. The IP Protection package includes the Compliance feature set,

plus structured and unstructured data fingerprinting, machine learning classifiers, and a DLP Analytics virtual appliance. Forcepoint Dynamic Data Protection bundles DLP Endpoint with a behavioral analytics module, to dynamically apply monitoring and enforcement controls to protect data based on calculated behavioral risk level of users and the value of data being accessed. This helps reduce the amount of alerts requiring investigation, and implements risk-based active data protection controls.

Forcepoint DLP is available in the following components, as well as a combined Forcepoint DLP Suite consisting of the Endpoint, Network and Discover elements:

- **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, ServiceNow, and Salesforce. The solution addresses data in motion, data in use, and data at rest use cases.
- **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.

## STRENGTHS

- Forcepoint supports deployment of DLP management and data classification components on-premises and in public clouds (i.e. 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**

- Forcepoint OCR is currently limited to network discovery and data in motion (i.e. web, email and ICAP). Forcepoint is planning to extend OCR support to additional DLP components as part of their roadmap.
- 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 only provides data in motion integrated encryption capabilities for removable media. It also supports email encryption when combined with Forcepoint Email Security.

## **DIGITAL GUARDIAN**

275 Wyman Street, Suite 250

Waltham, MA 02451

[www.digitalguardian.com](http://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 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.

Digital Guardian also supports User & Entity Behavior Analytics (UEBA) functionality to provide visibility into all user, computer, printer and file events to determine risky or anomalous behavior. The UEBA functionality integrates with advanced analytics in Digital Guardian Cloud to enable faster, more accurate identification of insider threats and help reduce incident response times. This capability is available to all subscribers of Digital Guardian Cloud, and does not require integration with third party components.

## STRENGTHS

- Digital Guardian offers flexible deployment models including on-premises, SaaS, or through its Managed Security Program (MSP).
- 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's kernel level endpoint agent is available for 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, rather than requiring defined policies which may be more difficult to construct.
- Digital Guardian supports 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.
- Digital Guardian's UEBA capabilities further enhance its ability to detect risky or suspicious user behavior.

## **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. The vendor has this on its near term roadmap.
- Digital Guardian's network DLP appliance (from the Code Green Networks acquisition) does not yet fully integrate with its endpoint DLP solution, requiring customers of endpoint and network DLP to write separate policies. The vendor is working to address this.

## **MCAFEE**

2821 Mission College Blvd.

Santa Clara, CA 95054

[www.mcafee.com](http://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 offers Exact Data Matching for structured data, such as sensitive data stored in an excel sheet in the database.
- **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. The Capture technology is also available, and can act as a digital recorder to replay DLP incidents after the fact for more thorough investigation.

- **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. It also integrates with McAfee Behavioral Analytics to track user activity.

**McAfee ePO (ePolicy Orchestrator)** 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.
- McAfee DLP is integrated with McAfee MVISION Cloud (formerly Skyhigh Security Cloud), which helps organizations to easily extend DLP policies into the cloud. Common data protection policies can be created across multiple environments, with the same data classification tags shared to ensure consistent data loss detection from device to cloud.
- McAfee ePolicy Orchestrator provides 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. 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 DLP does not currently provide agent support for Linux.
- 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.

## **GTB TECHNOLOGIES**

5000 Birch Street, Suite 3000  
Newport Beach, CA 92660  
[www.gttb.com](http://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 by inspecting and 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 (i.e. DLP as a Service, Discovery as a Service, and others). Managed services include fully managed services, as well as hybrid management. GTB solutions cover Windows, macOS, Linux and mobile operating systems. The platform provides the following functionality:

- *Data in use* – the GTB Endpoint Protector Agent is a multi-functional system that supports full TCP Scanning on all ports and protocols, Enterprise Data Detection, USB and Device Controls (including Printer DLP), application control with support for both white and blacklisting, as well as Data Discovery with Content Aware Data-Classification for both files and emails. The GTB Endpoint Protector integrates with the GTB IRM (Information Rights Management)/ DRM (Digital Rights Management) system and can protect and encrypt files based on content and context. Policies may be created based on protocols, sources, destinations, data, file types and more. Enforcement actions include: quarantine, block, log and alert, user remediation, user justification and more.
- *Data in motion* – provides inbound and outbound protection for both text and binary data (e.g. files and data streams, structured, semi-structured and unstructured data). GTB Cloud Data Protect, is a new solution which protects against the exfiltration of sensitive data from the cloud. The GTB Inspector supports multiple span ports, with separate support for webmail on HTTP/HTTPS and user warning when sending data over non-secured channels. Automatic routing of emails is provided to email encryption gateways, as well as support for ICAP and Secure ICAP for integration with proxy servers. All channels on all ports are supported including social media and blogs. Endpoint TCP for Data in motion is also available via the GTB Endpoint Protector.
- *Data at rest* – the GTB Endpoint Protector agent performs local scans on PCs, macOS 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. It also supports discovery of images using OCR, even if images are embedded inside files. Remediation actions include Copy, Move, Delete, Classify, Redact (images) and automatically, by policy apply IRM / DRM. The Discovery System is integrated with Microsoft AIP, as well as Symantec Vault.
- *GTB User behavior analytics* – provide analysis of items including number of files/emails sent or saved, size of the files sent or saved. Support allows further user entity behavior



(UEBA) analytics processing by SIEM providers.

- *GTB Drip DLP* – is supported and may be set based on source IP range, groups and for specific policies having a certain severity level and within a pre-defined time period.
- *GTB 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, as well as review and remediate incidents automatically to all system components including agents, discovery servers and inspectors. GTB provides hundreds of out-of-the-box 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. Through the Cloud Data Protect solution it can accurately block cloud data exfiltration.
- GTB's offers highly advanced detection techniques which include its own patented fingerprinting engine (AccuMatch) for partial data match and derivative work protection, OCR 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 Cloud Data Protect offers data protection against the exfiltration of data from the cloud.
- 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. The vendor has this on their roadmap.
- The GTB platform could provide more advanced off-network mobile data protection controls. The vendor has this on their roadmap for future release.
- Though market visibility is improving, GTB could still expand its market visibility. The vendor is working to address this.

## TRAIL BLAZERS

### CoSoSys

Str. Somesului 14, Ground Floor  
400145 Cluj-Napoca  
Romania

CoSoSys offers solutions for Data Loss Prevention (DLP), Device Control, eDiscovery and Mobile Device Management (MDM). The company is privately held.

## SOLUTIONS

CoSoSys **Endpoint Protector** is an all-in-one Data Loss Prevention (DLP) solution for Windows, macOS, Linux, as well as Mobile Device Management for iOS and Android. 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, HIPAA, NIST, and others. Administrators can define detection patterns based on proximity, dictionaries, regular expressions, and more. The movement of valuable data to unauthorized external individuals is monitored 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** – on premise DLP, available as hardware or virtual appliance, available 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 solution.
- **My Endpoint Protector** – is a cloud based DLP solution.
- **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 network or 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 sensitive data leaving their computers. Through close content inspection, transfers of important company documents are 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.
- *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.
- *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-approved 256bit AES CBC-mode encryption.

- *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, 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.
- *Mobile Device Management* – provides control over the use of Android and iOS mobile device fleets and macOS computers. It enables organizations to set security policies and access detailed tracking and asset management of all smartphones or tablets. It can also be used to push and monitor applications, network settings, and more.

Endpoint Protector enables a seamless management of all organization endpoints, regardless of operating system, from a single dashboard.

## **STRENGTHS**

- CoSoSys Endpoint Protector offers strong coverage for Windows, macOS and Linux, which 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 form factors formats, including hardware appliance, or virtual appliance, which meets 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.
- 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, but they only cover a limited number of languages.
- 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.

## **SPECIALISTS**

### **FIDELIS CYBERSECURITY**

4500 East West Highway, Suite 400  
Bethesda, MD 20814

Fidelis is a cybersecurity technology company that offers automated threat hunting, data protection and managed services. The company was originally known for its network DLP solutions, however, it acquired endpoint detection and response (EDR) vendor Resolution1 (2015) and deception vendor TopSpin (2017), and has since broadened its portfolio to the Automated Threat Hunting and 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 a feature of **Elevate**, its broader automated threat hunting platform. Elevate comprises network, endpoint and deception 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, 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 Office365, Cisco (i.e. IronPort), Proofpoint, SendMail and Postfix.
- *Fidelis Network Web* – integrates with standards-based Web Proxy and CASB solutions through an ICAP interface to add a DLP capability for proxy solutions like Symantec (i.e. Blue Coat), Forcepoint, McAfee, NetSkope, 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* – 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 (up to 360 days). The Collector allows the user 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. Microsoft recently added a VTAP (virtual network TAP) to Azure, which enables Fidelis to monitor cloud network traffic natively between virtual machines without an agent.

In addition, 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 K2, 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.
- 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 EMM/UEM mobile security solutions, and does not offer endpoint DLP.
- Fidelis is working to build awareness for its solution in the market for Automated Threat Hunting 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](http://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. In 2017, Clearswift was acquired by Swiss defense company, RUAG and forms the product group for their Cyber Security Business Unit.

## **SOLUTIONS**

Clearswift offers a portfolio of solutions which can be peered together allowing customers to extend their hygiene solutions to provide advanced DLP features across their environment in a cost-effective manner. Clearswift products are available on hardware or as 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 (SEG)** – provides Adaptive 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). Optical Character Recognition (OCR) support is provided as an option. 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 options (hosted or on-premise). The SEG supports AD 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.

- **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. Clearswift can also scan internal email in Office 365, providing extensive DLP functionality.
- **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 Adaptive DLP specific policies for customers that have existing web proxy solutions, such as Symantec (Bluecoat), F5, Cisco, IBM or similar other ICAP-based solution. This variant can be used in both forward and reverse proxy modes.
- **Clearswift Endpoint DLP (CED)** (formerly 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, 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 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, tracking granular information as well as whole files.

## **STRENGTHS**

- Clearswift has strong content DLP capabilities and offers "adaptive redaction" 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.
- 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.
- 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. These are scheduled for 2019.
- Clearswift does not currently provide support for Instant Messaging networks (e.g. Teams/Skype for Business.). Social Network support is provided by a partnership with SecureMySocial.
- Clearswift currently provides mobile DLP support for iOS and Android only through a partnership with AirWatch.

## **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, Mac, 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 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.
- **Traffic Control (Windows, Linux, Mac) (endpoint 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 Storage Security** (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.
- **Zecurion 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.
- **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** – 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 Avira Antivirus** – Zecurion, jointly with Avira, offers a comprehensive endpoint security solution integrated with its DLP platform for enterprises. The solution scans network traffic on all ports on endpoints. It secures files, running processes, and system memory on PCs and servers against advanced persistent threats, spyware, and other types of malware. Additionally, it helps blocks web attacks, defending against phishing attacks, infected websites, fake shopping carts, and drive-by downloads.

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 Mac, Linux 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 Traffic Control controls over 250 different social media services, including LinkedIn, 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 currently offers weak intrusion prevention/intrusion detection (IPS/IDS) system capabilities.
- Zecurion currently offers weak integration with SIEM systems.
- Zecurion offers only basic enforcement visibility through email alerts.
- Zecurion Mobile DLP is currently only available for Android devices.
- Zecurion does not currently offer or integrate with CASB capabilities. However, the vendor is working to develop some CASB capabilities of its own.

## 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, Jabber, MSN, Telegram, Whatsapp, Viber 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.

- *Cloud Data* – 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 over 300 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.
- *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’s management solution is available in all form factors, on-premises, cloud or hybrid.
- In addition to DLP, SearchInform offers a strong set of forensic technologies which assist in reconstructing user activity and violations activity.
- 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.

## **FALCONGAZE**

Building 9, 35 Nizhnyaya Krasnoselskaya st., office 302  
Moscow, 105066  
Russia  
[www.falcongaze.com](http://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 Russia, with a strong presence in Eastern European countries. The company is privately held.



## SOLUTIONS

Falcongaze's flagship DLP solution is **SecureTower**, an enterprise solution which provides functionality for user monitoring and analysis. SecureTower can intercept a vast range of corporate communication and data transfer channels, as well as detect sensitive content using various content-aware detection techniques. Linguistic analysis tools include 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 both Windows and Linux, whereas endpoint agents are only available for Windows OS.

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 over the following data channels:

- *Email messages* – sent via POP3, SMTP, IMAP and MAPI protocols, MS Exchange Server, IBM Lotus Notes/Domino, Kerio Connect, Sendmail and other mail servers, as well as Microsoft Office 365.
- *Web-traffic* – including email messages of webmail clients, chats, forums, and social networks.
- *Instant Messaging* – including OSCAR, XMPP (Jabber), YIM, SIP, Skype text/voice messages and files, Viber, Telegram, MS Lync, WhatsApp, Google Hangouts, and more.
- *Files and documents* – transferred via FTP, FTPS, HTTP and HTTPS protocols, as well as email attachments.
- *SSL traffic* – transmitted over encrypted protocols (e.g. HTTPS, FTPS, SSL for POP3, SMTP, etc.), as well as HTTP and HTTPS traffic sent via the ICAP protocol to corporate

proxy servers.

- *Cloud storage and Databases* – including MS SQL Server, Oracle, PostgreSQL, SQLite, MySQL contents, 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.

SecureTower also provides the ability to detect Drip DLP through the use of statistical safety rules (for adjustable time periods) that detect the slow leaking of information by monitoring sensitive data over multiple transfer instances.

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**

- The SecureTower solution can be deployed on-premises, in the cloud, or as a hybrid solution.
- SecureTower provides an extensive set of tools for personnel and business process analysis, as well as tools for investigating security incidents.
- SecureTower provides extensive capabilities for monitoring user activity and social interactions.
- SecureTower is simple to deploy and maintain, with many customer use cases covered out-of-the-box.
- SecureTower is a modular solution which allows customers to deploy only the components that best meet their needs.
- SecureTower provides support for detecting Drip DLP.

## WEAKNESSES

- SecureTower's endpoint agent is currently only available for Windows. Agents for macOS, Linux, and mobile platforms (i.e. iOS and Android) are on the vendor's roadmap.
- Integration with third-party SIEM and UEBA solutions is not available. However, the vendor is working to develop its own UEBA capabilities.
- While SecureTower provides some basic (i.e. access/read-only/block) controls on cloud storage, but it does not currently provide context-aware monitoring of users activity while accessing cloud storage.
- SecureTower lacks market visibility particularly outside of Russia and Central Europe. The vendor is working to address that.

## MATRIX42

Elbinger Strasse 7  
60487 Frankfurt am Main  
Germany  
[www.matrix42.com](http://www.matrix42.com)  
[www.egosecure.com](http://www.egosecure.com)

EgoSecure, founded in 2007, is a German-based data security company with a broad range of data security products aimed at businesses and consumers. In 2018, EgoSecure was acquired by Matrix42, a provider of workspace integration across physical, virtual, mobile and cloud-based environments. Matrix42 is a privately held company.

## SOLUTIONS

**EgoSecure Corporate Data Protection** is a modular solution with 20 different data security components available through mix-and-match options. This allows customers to choose only the components they need. Alongside DLP, EgoSecure also offers a rich set of encryption technologies which include full disk encryption, removable device encryption, network share

encryption, cloud storage encryption, mobile encryption, device control, and more. All EgoSecure functionality including Device Control, on-the-fly Encryption, DLP Data-In-Use control, and Data-At-Rest data discovery is delivered through a single agent and managed through a single management console. EgoSecure management servers can reside on the corporate network, in the cloud, or as hybrid solutions. However, EgoSecure currently does not offer its own (i.e. multi-tenant) cloud management services. EgoSecure is available on a Windows platform for both servers and workstations. In addition, VDI and terminal services environments (e.g. Citrix) are also supported. Mobile Encryption is available for iOS and Android, however, DLP control is not currently available on the mobile device side. Mac OS support is currently limited to device Control and Encryption. A Linux agent is under development. EgoSecure has a strategic partnership with Clearswift and is using its data classification engine.

EgoSecure DLP supports the following functionality:

*Data in use* – EgoSecure controls destinations and data paths, such as removable Media, cloud storage and networks shares. Control and audit is performed by the agent which resides on each controlled endpoint and is centrally managed through administrator configured policies.

*Data in motion* – EgoSecure controls user operations on the endpoint side. EgoSecure has full potential to extend this to email and web gateways through a partnership with Clearswift.

*Data at rest* – It is possible to create scheduled scans to check data stored on endpoints for specific content.

*Policy templates* – Pre-defined templates are provided for PCI, PII, SEC, SOX, HIPAA templates, pre-defined expression for passports, social security, driving licenses, IPv4 and IPv6 addresses, and more.

*Directory integration* – EgoSecure integrates with Active Directory, as well as Novell eDirectory and LDAP servers. Multi-tenant configurations with role-based management are supported for MSPs.

*Encryption* – EgoSecure is offers a full range of encryption technologies, including: Full Disk Encryption and Removable Device Encryption, to safeguard data against physical device loss,

theft or unauthorized access; Cloud Storage Encryption to protect data by applying on-the-fly encryption of data to DropBox, OneDrive, Google drive, Box, and OwnCloud/NextCloud; Local folder and Network Share encryption, as additional layer of data protection from unauthorized access.

*Administration* – EgoSecure provides an all-in-one management console for deployment, policy-based configuration, monitoring and reporting.

## **STRENGTHS**

- EgoSecure management server can be installed on-premises or in the cloud, hybrid options are also available.
- EgoSecure supports one agent and one console for all components.
- EgoSecure delivers a rich set of encryption technologies for different business scenarios, including easy-to-use, transparent file-level encryption and 2-factor authentication.
- EgoSecure delivers strong device control capabilities.
- EgoSecure components are available a modular solutions, with mix-and-match options where customers can choose only the required components.

## **WEAKNESSES**

- EgoSecure macOS client support is currently limited to device control and encryption, and lacks DLP functionality. A Linux agent is not currently available, but is under development.
- Basic MDM capabilities are available for iOS and Android, in future this will be enhanced by the SilverBack EMM product from Matrix42.
- EgoSecure offers MDM and mobile encryption capabilities for iOS and Android, however it does not currently provide any DLP controls on the mobile device side.
- EgoSecure currently lacks capabilities to detect Drip DLP, however, this is on the roadmap for future releases.

- While EgoSecure licenses the Clearswift DLP engine, it does not currently take advantage of the adaptive redaction capabilities which are a key differentiator of the Clearswift technology. EgoSecure, however, has this on their roadmap for future releases.
- EgoSecure lacks market visibility, particularly in North America. The vendor is working to address this.

**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](http://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, 2018-2022	Jun. 2018	\$3,000.00
Corporate Web Security Market, 2018-2022	Jun. 2018	\$3,000.00
Email Market, 2018-2022	Jun. 2018	\$3,000.00
Office 365, Exchange Server and Outlook Market Analysis, 2018-2022	Jun. 2018	\$3,000.00
Cloud Business Email Market, 2018-2022	Jun. 2018	\$3,000.00
Information Archiving Market, 2018-2022	Mar. 2018	\$3,000.00
Unified Endpoint Management Market, 2018-2022	Mar. 2018	\$3,000.00
Advanced Threat Protection Market, 2018-2022	Mar. 2018	\$3,000.00
Email Statistics Report, 2018-2022	Mar. 2018	\$3,000.00
Social Networking Statistics Report, 2018-2022	Feb. 2018	\$3,000.00
Instant Messaging Statistics Report, 2018-2022	Feb. 2018	\$3,000.00
Mobile Statistics Report, 2018-2022	Jan. 2018	\$3,000.00

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

### Upcoming Publications:

Title	To Be Released	Price*
Endpoint Security Market, 2018-2022	Nov. 2018	\$3,000.00
Secure Email Gateway Market, 2018-2022	Nov. 2018	\$3,000.00
Enterprise Data Loss Prevention Market, 2018-2022	Nov. 2018	\$3,000.00
Cloud Access Security Broker Market, 2018-2022	Nov. 2018	\$3,000.00

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

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