Vendor Landscape: Data Loss Prevention Solutions

Key Vendors For Email, Endpoint, Network, Web, And Cloud DLP Capabilities

by Heidi Shey

August 4, 2016 | Updated: August 12, 2016

Why Read This Report

Policies to control data use and movement require enforcement mechanisms. Data loss prevention (DLP) capabilities give security and risk (S&R) professionals the means to enforce those policies and prevent sensitive data exposure. This report highlights the different channels of data loss and examines the varied landscape of vendors offering DLP capabilities today as a feature, standalone solution, or suite.

Key Takeaways

The DLP Landscape Expands Three Ways

As DLP suites evolve, DLP fast becomes a feature in other security technologies, and as DLP-as-a-managed-service grows, S&R pros have a variety of ways to acquire DLP capabilities.

Eight Core Capabilities To Consider For DLP

When selecting a tool for DLP, evaluate vendor capabilities for data discovery, data classification, contextual analysis, content analysis, inspection of encrypted data, policy creation, policy enforcement actions, and response and reporting.

Vendor Landscape: Data Loss Prevention Solutions

Key Vendors For Email, Endpoint, Network, Web, And Cloud DLP Capabilities

by Heidi Shey
with Stephanie Balaouras, John Kindervag, Alexander Spiliotes, and Peggy Dostie

August 4, 2016 | Updated: August 12, 2016

Table Of Contents

2 Today's DLP Landscape Expands Across Three Segments

3 A Capabilities Overview: What To Expect And Consider

5 DLP Vendor Landscape

Recommendations

20 Plan Your Strategy And Evaluate Options As DLP Becomes A Feature

22 Supplemental Material

Notes & Resources

Forrester interviewed 25 vendor companies: BAE Systems, Check Point, CipherCloud, CipherMail, Clearswift, CloudLock, CoSoSys, DeviceLock, Digital Guardian, Elastica, Fidelis Cybersecurity, Forcepoint (formerly Raytheon/Websense), Intel Security, Microsoft, Mimecast, Netskope, Proofpoint, Somansa, Spirion (formerly Identity Finder), Symantec, Trend Micro, Trustwave, Watchful Software, ZixCorp, and Zscaler.

Related Research Documents

Market Overview: Data Loss Prevention

Rethinking Data Loss Prevention With Forrester's DLP Maturity Grid

TechRadar™: Data Security, Q1 2016

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

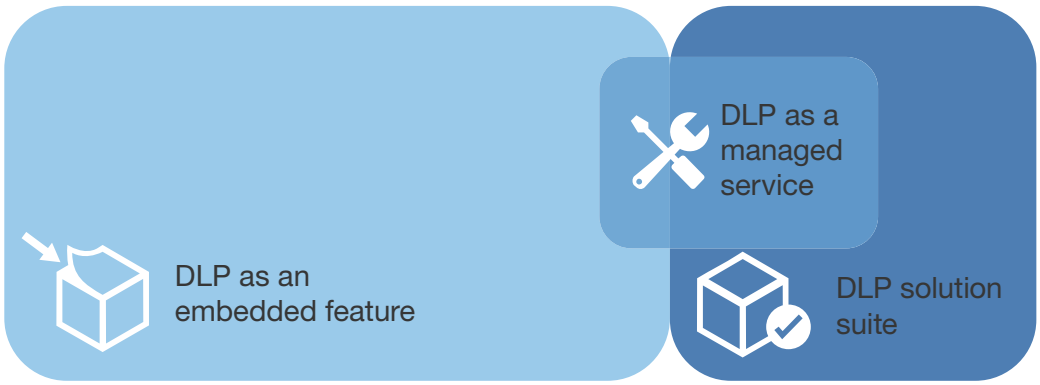
© 2016 Forrester Research, Inc. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. Unauthorized copying or distributing is a violation of copyright law. Citations@forrester.com or +1 866-367-7378

Today's DLP Landscape Expands Across Three Segments

In the past, DLP was a distinct market with a set of well-defined vendors offering DLP products, namely DLP suites. But as DLP evolves from a product to a feature, today's DLP landscape is diverse. There is a multitude of ways for security teams to acquire DLP capabilities; as the vendor landscape expands, one can find (see Figure 1):[1]

- **DLP as a feature of another security technology or solution.** This is sometimes referred to as DLP-lite; you can also think of it as a very targeted form of DLP to address a specific channel of data loss. In this context, DLP is a feature in a next-generation firewall, cloud security solution, endpoint security solution, email security gateway, web security gateway, or other security tool.
- **DLP as a solution suite.** If you want it all, and from one vendor, this is it. These are solutions that cover data at rest, in motion, and in use. These DLP solution suites address multiple channels of data loss (e.g., email, endpoint, web, and cloud) and help to make centralized management of DLP policies a possibility. These solutions are becoming more than just DLP and are evolving into integrated security solutions that address prevention, threat detection, and response.
- **DLP as a managed service.** Sitting somewhere between DLP as a feature and DLP as a solution suite, there's DLP as a managed service. Service providers can help to manage processes, policies, and infrastructure for a DLP implementation.[2] Provider offerings range from managing a full DLP-specific solution suite for you to including DLP capabilities as a part of an adjacent managed service (e.g., email security that includes email DLP). Example vendors include Digital Guardian, EY, InteliSecure, PwC, and Wipro.

FIGURE 1 A View Of Today's DLP Market



© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

A Capabilities Overview: What To Expect And Consider

As you evaluate the best approach to acquire DLP for your organization, there are core functions and capabilities that you can expect to see and consider. Think of the following as a starting point for assessing the key capabilities that matter most to your organization and for evaluating different solutions.

Data Discovery And Data Classification Are Basics That Form A Foundation For Security

You have to know what data you're trying to protect, where it's located, where it should be located, and how sensitive it is, in order to create the necessary data use and handling policies as well as DLP policies. Regardless of whether the DLP solution you're considering includes data discovery and data classification as features, both are foundational capabilities for your data security and protection program.[3] If the solution doesn't include these as native capabilities, it should integrate with tools to do this because:

- **Data discovery identifies the location of sensitive data.** Discovery is the ability to perform data discovery and identify where sensitive data is located at rest, such as data on endpoints, hosts, databases, storage networks, file shares, and cloud storage. It is typically found in solutions that cover endpoint or cloud DLP such as CloudLock (recently acquired by Cisco) and Spirion (formerly Identity Finder), or DLP suites like Intel Security (McAfee) and Symantec. This is a capability that you may already have within your organization through standalone data discovery or eDiscovery tools.[4]
- **Data classification tags sensitive data.** Classification allows for the labeling or tagging of data to identify its sensitivity. Typically, this is at a file level, but some DLP solutions can classify content itself within files, classify by context, or classify by user. The large majority of DLP solutions have a data classification capability. Classification can be user-driven (manual), automated, or both. Many DLP solutions also integrate with standalone data classification tools like those from Boldon James or Titus.

Scanning And Inspection Functions Influence Depth Of DLP Capabilities

To determine if data movement is in violation of policies, DLP solutions must have a means to scan and inspect data. Expect to see solutions use a combination of contextual analysis and content analysis techniques to detect policy violations and sensitive data loss. Inspection of encrypted data is where the landscape is the most diverse — and generates controversy and concern among S&R pros. Approaches to data inspection and analysis are key to identifying policy violations.

- **Contextual analysis fine-tunes DLP policies.** Solution providers use contextual information like identity, file ownership, communication channel, use of peripherals (like USB sticks and their serial numbers), platform in use (e.g., Google Drive, Office 365), IP address, time stamps, document properties, email headers, geolocation, encryption type, traffic direction, and more in their solutions to better fine-tune DLP policies. The type of contextual information will vary depending on the solution, but you can expect to see this in use.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

- **Content analysis helps the solution detect policy violation.** The use of regular expressions is standard when it comes to identifying credit card or account number data. Dictionaries and keyword matching are common. You'll also find data fingerprinting and use of hashes or checksums, particularly for exact or partial document matching. Some solution providers go a step further in ways to address intellectual property protection use cases. Forcepoint's OCR capabilities can detect text in screen shots and photos. Symantec's vector machine learning performs statistical analysis on unstructured data and checks it against similar content or documents.
- **Inspection of encrypted data provides visibility.** Encrypted data can be inspected by diverse means, depending on the vendor and the channels of data loss their DLP capabilities cover. Email DLP solutions like BAE Systems and ZixCorp deployed at the gateway inspect traffic before emails are encrypted. Trend Micro relies on browser APIs to inspect and scan data prior to encrypting. Some solutions will use proxies or essentially decrypt and re-encrypt data via authorized man-in-the-middle. Digital Guardian can function as an SSL proxy to detect and decrypt protocols running over SSL/TLS. Fidelis Cybersecurity has native built-in decoders to inspect SSL/TLS, analyzing the encrypted channel rather than decrypting traffic for inspection. Zscaler's cloud platform for DLP establishes an SSL tunnel between the destination server and the user's browser, allowing for decryption and inspection of HTTPS traffic between the user's browser and destination server. DLP suites often provide a variety of options to inspect encrypted data; for example, Forcepoint offers free-of-charge web-proxy licenses and embedded web proxies.

Policy Creation, Enforcement, And Response Actions Highlight Resource Requirements

Since DLP solutions and capabilities are policy enforcement engines, this comprises a category of functions that you must ensure map to your use cases for DLP. Identify the channels of data loss that you' re looking to protect, and take into consideration user experience and business impact for enforcement actions associated with policy violations. Assess your readiness and ability to respond to DLP violations and security incidents, effort needed to create your DLP rules to align with business requirements, and resources to manage these rules over time. As you evaluate solutions, compare:

- **Policy creation via wizards and manual actions to customize DLP policies.** Policy management is typically done through a web-based management console. Some solutions will include policy wizards to help streamline policy creation. Policy templates for specific compliance requirements (like HIPAA or PCI DSS), business group categories (e.g., finance, HR), or other topics (e.g., profanity) provide an easy and quick way to get started. Expect to have to create your own custom policies as your DLP program matures beyond compliance use cases and covers sensitive corporate data and intellectual property.
- **Policy enforcement actions to respond to policy violations.** These are the actions that can happen when the DLP engine detects a violation of data movement policy. Standard actions include allow, quarantine, force encrypt, block, send for review, or prompt for justification. Specific channels of data loss can have unique enforcement actions as well. Clearswift can strip

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

attachments from email as well as redact sensitive data while allowing the rest of the message to move. CloudLock can automatically revoke cloud app access. Fidelis Cybersecurity can flag the host (IP address of violator), add tags to metadata, send files to a malware detection stack for analysis, and whitelist. Intel Security (McAfee) can apply rights management.

› **Response and reporting to understand data movement and manage incidents.** You can count on DLP solutions to log policy violations and report them to an assigned admin and dashboard. Many will also feed this data into a SIM/SIEM tool like HP ArcSight, IBM QRadar, RSA, or Splunk. What happens next — more advanced response, reporting, and analysis capabilities — will vary a great deal. This variation and push to provide greater value is a major reason that many of the DLP solution suites are rapidly morphing into integrated security solutions to tackle prevention, threat detection, and response as a means to differentiate. It's also a differentiator for managed service providers; any provider can help you to monitor DLP, but the bigger value is in their capacity for escalating and responding to those alerts.

DLP Vendor Landscape

As DLP evolves from a product into a feature, we see a vast and varied lineup of vendors who offer DLP capabilities. Much like purchasing a car, it helps to at least narrow down the type of vehicle. After all, there's a huge difference in terms of capacity, performance, and cost between a minivan and sports car even though both will get you from point A to point B. For DLP, start by considering your channel of data loss of focus.

Email DLP Is The Most Mature DLP Channel

Email DLP is a common focus for many firms, particularly those in the healthcare industry and others where compliance mandates require encryption for email containing sensitive data. As a result, email DLP is the most mature of the DLP channels. DLP controls are built in to modern antimalware email gateways. Some providers of DLP suites like Clearswift and Forcepoint also offer email DLP as a standalone solution. Notable vendors (non-suites) include (see Figure 2):

› **BAE Systems.** BAE Systems' Insider Threat Prevention is a part of its Email Protection Services offering which provides email DLP capabilities. Highlights include DLP Policy Packs (vertical-specific policy compliance), policy workflow that allows admins to send mail to multiple quarantines for approval at varying levels, and APIs to facilitate identifying of document repositories and customer lists to exclude. Top industries served are financial services, transportation/logistics, and retail. Target customers are midsize companies to multinational enterprises.

› **CipherMail.** CipherMail's Email Encryption Gateway includes DLP capabilities. Outgoing email is encrypted if a DLP rule requires the email to be encrypted. Three versions of the solution are available: a free, open source community edition, a small and medium-size enterprise edition, and

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

an enterprise edition. Top industries served are healthcare and financial services. Customers range from small companies seeking basic capabilities available in the free open source community edition to multinationals in need of more advanced features.

- **Microsoft Office 365.** Data Loss Prevention in Office 365 is available for Exchange Online, Exchange Server 2016 SharePoint 2016, and OneDrive for Business. DLP capabilities are packaged into Microsoft's premium Enterprise E3 offering and above, which includes other security and compliance capabilities. Policy tips and email notifications serve to help with end user education and empowerment. It can be combined with Microsoft's Rights Management services (RMS). Top industries served are financial services, manufacturing, and public sector. Target customers are primarily enterprise organizations, although the solution is available for midsize companies too.
- **Mimecast.** Mimecast's Secure Email Gateway includes DLP capabilities. It's deployed as a cloud service and is a part of Mimecast's cloud security platform. The solution also integrates with Mimecast's Large File Send service to apply DLP rules to outbound large file shares. Top industries served are professional services, financial services, and healthcare. Target customers are organizations in regulated industries with a heavy reliance on email and large percentage of knowledge workers.
- **Proofpoint.** Proofpoint's Information Protection Suite includes DLP capabilities for email and data at rest including file servers, NAS devices, SANs, and SharePoint sites. The suite is a cloud-based offering that blends DLP with data access control governance. It provides insight into access control lists for visibility into where sensitive data exists and who has access to sensitive data. Top industries served are financial services, healthcare, and retail. Target customers are mainly enterprise companies.
- **ZixCorp.** ZixDLP is a SaaS solution that addresses data loss for outbound emails. Highlights include group management (admins can manage as well as delegate responsibilities to department leaders), comprehensive policy templates (built in part via ZixCorp's expertise from its email encryption business), and an intuitive management interface. Top industries served are financial services, healthcare, and IT services. Target customers are US-based companies of all sizes.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FIGURE 2 Email DLP Vendors

	Does the solution have the ability to perform data discovery?	Does the solution have the ability to perform data classification?
BAE Systems	Yes, in message headers, body content, and attachments	No
CipherMail	No	No
Mimecast	Yes, if using Mimecast for email archiving	Yes
Microsoft Office 365	Yes	Yes
Proofpoint	Yes	Yes
ZixCorp	No	Yes

	What contextual info is considered for DLP rules and policy violations?	How does the solution analyze content to find DLP policy violations?	Does the solution have the ability to inspect encrypted traffic?
BAE Systems	IP address, country/origin of sender	Proximity checking, fingerprinting	Yes, if deployed at the gateway to inspect before applying encryption
CipherMail	N/A	Regex	No
Mimecast	N/A	Regex, word library, weighted word dictionary, MD5 hash, exact and partial match	Yes
Microsoft Office 365	Email/site/documents, etc., by user/domain and applicable permissions	Regex, dictionary, proximity, checksum, corroboration detection, document fingerprinting (fuzzy hashing)	Yes, within Office 365
Proofpoint	AD group, file ownership, file permissions and attributes, location	Regex, exact data match, weighted keyword match	No
ZixCorp	N/A	Regex, dictionary, pattern masks	Yes, if deployed before email encryption appliance in the message flow

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FIGURE 2 Email DLP Vendors (Cont.)

	What types of default policy templates are available?	What are actions in response to policy violations?	How does the solution report, audit, document policy violations?
BAE Systems	Prebuilt policy packs (e.g., GLBA, HIPAA, PCI)	Allow, quarantine, encrypt, redact, block, log, archive, send for review, prompt for justification	Incident dashboard, workflow analysis, real-time message tracking
CipherMail	SSNs, credit cards, IBANs, email addresses	Alert, block, encrypt, manual inspection and release, quarantine	Alert sender and/or DLP manager(s). Log policy violations.
Mimecast	Variety of policy templates for major compliance requirements (e.g., PCI, HIPAA, SOX, etc.)	Block, quarantine, reject (IP-level SMTP rejection), reject and notify, smart tag, smart folder, reroute, change retention policy, encrypt, notify, monitor	Alert sender or recipient. Admin dashboard.
Microsoft Office 365	Variety of policy templates (e.g., country-specific, PCI, HIPAA, US state laws)	Notify, allow, encrypt, block, send for manager approval, quarantine, require approval, modify access rights	Built-in DLP reporting to Office 365 reporting, incident management, API to export to SIM
Proofpoint	Variety of policy templates across protected data types (e.g., PHI, PCI, PII, HIPAA)	Quarantine, stub (remove) attachment, encrypt, escalate	Admin dashboard
Zix	Policy filter templates (e.g., industry, profanity, SSNs, US state laws)	Alert, release after log, quarantine for review, encrypt. All messages have a configurable expiration date.	Admin dashboard

Endpoint DLP Is In Demand For Corporate-Managed Devices

Endpoint DLP is another popular starting point for DLP initiatives. It's typically a software agent that looks for out-of-policy data on desktops and laptops, providing device control capabilities (for example, controlling data leakage to USB drives). Some endpoint DLP agents, especially those from DLP suites, may also perform data discovery and classification, or include other functionality like application whitelisting.[5] Notable (non-suite) vendors include (see Figure 3):

› **CoSoSys.** Endpoint Protector from CoSoSys addresses the endpoint, cloud, email, printers, thin clients, network share, and portable storage devices. It's available as an on-premises solution with hardware appliance and virtual appliance as well as a cloud-based solution. The Endpoint Protector virtual appliance is also available as Amazon EC2 Instance. Highlights include ease of implementation, scalability, and DLP coverage for Mac OS X and Linux. Top industries served are financial services, automotive, healthcare, and media. Target customers are organizations of all sizes from SMBs to conglomerates.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

› **Spirion.** Spirion's Sensitive Data Manager covers both endpoint and cloud at rest. Highlights include Spirion's ability to locate sensitive data with near zero false positives, coverage for unstructured files, and portability of classification tags. Windows, OS X, and Linux agents can be installed on endpoints or used to search remote endpoints and data stores that don't have agents installed, including databases, SharePoint, Exchange/Office 365, Box, DropBox, and Microsoft OneDrive. Top industries served are healthcare, higher education, and financial services. Target customers are enterprise and mid-market companies, particularly those with difficult-to-locate data use cases (such as for protecting intellectual property).

FIGURE 3 Endpoint DLP Vendors

	Does the solution have the ability to perform data discovery?	Does the solution have the ability to perform data classification?
CoSoSys	Yes, for local data	No
Spirion	Yes, performs discovery locally, remote, or in the cloud	Yes

	What contextual info is considered for DLP rules and policy violations?	How does the solution analyze content to find DLP policy violations?	Does the solution have the ability to inspect encrypted traffic?
CoSoSys	User info and attempted actions (e.g., copy/paste), application info, type of connected device	Predefined content (e.g., PII, SSNs, etc.), custom content based on dictionaries, regex	Yes, through a driver at the local level
Spirion	Location, file ownership, attributes set by the user, classification type, surrounding attributes/data	Proprietary predicate logic formulas, Regex, exact data match, hashes, dictionaries, verification if/or logic	No

	What types of default policy templates are available?	What are actions in response to policy violations?	How does the solution report, audit, document policy violations?
CoSoSys	Policy templates for PCI, HIPAA	Block, encrypt, alert admin, send reports to the server, warn users	Real-time reporting dashboard. Option to forward logs to SIM.
Spirion	Policy templates for PCI, PII (including EU PII), PHI, and financial data	Quarantine, encrypt, destroy, redact, and alert	Central management console, endpoint alerts, email alerting & scheduled reports. Splunk integration

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

Network DLP Is Popular For Insider Threats And Advanced Attacks

Network DLP tools capture and analyze network traffic (not just HTTP and HTTPS protocols), providing real-time situational awareness about what's happening on your network. Typical use cases also include detecting insider threats and advanced persistent threats and supporting continuous monitoring mandates. Notable (non-suite) vendors include (see Figure 4):

- **Check Point.** Check Point has a DLP Software Blade offered as part of its integrated network security product suite, which includes access control and threat prevention security technologies. Customers can enable DLP on any existing Check Point security gateway. Top industries served are manufacturing, transportation, and financial services. Target customers are companies of all sizes, particularly companies with 1,000 to 5,000 employees.
- **Fidelis Cybersecurity.** Fidelis Network offers DLP functionality at the network level, across all ports and protocols (network and application). It provides full visibility over all network protocols, applications, and content. Fidelis Network Sensors reassemble, decode, and analyze traffic traversing the network in real time, shining a light on bidirectional traffic at ingress and egress points. Top industries served are financial services, retail, technology, healthcare, and government. Target customers are large Fortune 5000 organizations and government agencies.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FIGURE 4 Network DLP Vendors

	Does the solution have the ability to perform data discovery?	Does the solution have the ability to perform data classification?
Check Point	Yes	Yes
Fidelis Cybersecurity	No	Yes, for PII via Fidelis Identity Profile Analyzer

	What contextual info is considered for DLP rules and policy violations?	How does the solution analyze content to find DLP policy violations?	Does the solution have the ability to inspect encrypted traffic?
Check Point	User identity, traffic direction	Keywords, documents based on a corporate template, file attributes, regex, weighted keywords, fingerprinting, dictionary and custom CPcode matches	Yes
Fidelis Cybersecurity	User behavior, location (IP address, AD or LDAP user definition, email, country of origin, reputation feed entry, flagged host), session attributes	Regex, YARA rules, keywords, keywords in sequence, URL feed, smart identity profiling, file name, encrypted file, protocol signature, file signature	Yes. Native decoders don't decrypt, but provide context on encrypted channel analyzed. Option to inspect encrypted traffic with third-party SSL-visibility appliance

	What types of default policy templates are available?	What are actions in response to policy violations?	How does the solution report, audit, document policy violations?
Check Point	Policy templates in multiple categories (e.g., financial, best practice, compliance, HR, IP, PII)	Detect and log, inform user and allow, ask user for reason, block and notify	Log and make available to SIM
Fidelis Cybersecurity	Variety of policy templates (e.g., PII, finance/banking, HIPAA, PCI, source code, SCADA, DoD). Additional templates available from Fidelis Insight and Fidelis Download Center.	Alert, alert and block, flag host, add tag to metadata, throttle, quarantine, reroute email, remove attachment, send for malware analysis, whitelist	Fidelis CommandPost UI for dashboard, search, alerts, reports, audit log

Web DLP Is For Targeted Inspection Of Web Traffic

Web DLP looks for data leaks via web channels (HTTP and HTTPS protocols). Many of these tools have a foundation in web content filtering. They must inspect encrypted HTTPS traffic and be bidirectional — they must be able to inspect both outbound and inbound traffic. The ability to inspect

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

inbound traffic can protect users from web-based malware often hidden in an innocent-looking file that then infects their machines. Some providers of DLP suites like Forcepoint and McAfee also offer web DLP as a standalone solution. Notable (non-suite) vendors include (see Figure 5):

› **Blue Coat.** Blue Coat's Secure Web Gateway has DLP capabilities. It can track data with fingerprinting capabilities and monitor SSL traffic across the web gateway. Activating and installing DLP capabilities is quick, taking less than a day. Top industries served are telecommunications, financial services, education, and manufacturing. Target customers are midsize and enterprise companies.

› **Zscaler.** Zscaler DLP is offered as an add-on product to Zscaler's Internet Security Platform and deployed from the cloud. It inspects data in motion between all types of devices and the cloud. It automatically decrypts and inspects SSL-encrypted content inline in real time. An ICAP integration is available for on-premises DLP solutions, so DLP violations caught by Zscaler can be processed by the on-premises DLP workflow if desired. Top industries served are insurance, financial services, and manufacturing. Target customers are companies of all sizes.

FIGURE 5 Web DLP Vendors

	Does the solution have the ability to perform data discovery?	Does the solution have the ability to perform data classification?
Zscaler	No	No

	What contextual info is considered for DLP rules and policy violations?	How does the solution analyze content to find DLP policy violations?	Does the solution have the ability to inspect encrypted traffic?
Zscaler	Identity (user, group, dept.), location, time interval, URL category, cloud application, file type and size	Dictionaries for specialized numbers with checksums, document type, fuzzy and exact matching	Yes, bidirectional. Option to choose what traffic to inspect to meet privacy requirements. Option to trust Zscaler's Root CA or chain from customer PKI infrastructure.

	What types of default policy templates are available?	What are actions in response to policy violations?	How does the solution report, audit, document policy violations?
Zscaler	Dictionaries to address specific content types. One or more dictionaries can combine to create a policy.	Allow, block, alert	Admin console, email notifications. All incident metadata stored in cloud, can stream to a SIM in real time. Zscaler does not store content of policy violations.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

Cloud DLP Is The Most Sought-After DLP Capability Today

Cloud DLP helps to bring visibility and control for data going into specific cloud applications and platforms.This can include everything in the cloud from Office 365 and Google Drive to Dropbox, Salesforce to Slack, as well as Amazon Web Services. Notable standalone vendors include (see Figure 6):

- **CipherCloud.** CipherCloud provides Integrated DLP as part of its overall platform. It protects data in Box, OneDrive, Salesforce, ServiceNow, SharePoint, and other popular file storage services. APIs can meet use cases across multiple cloud categories including file sharing, CRM, ITSM, HR, and other apps. It integrates with on-premises DLP solutions via the ICAP protocol. Top industries served are financial services, healthcare, and telecom. Target customers are enterprises in regulated industries.
- **CloudLock.** CloudLock DLP is offered as part of the CloudLock Security Fabric, which addresses five core use cases: Cloud DLP, Threat Protection (User and Entity Behavior Analytics), Risk & Compliance Management, App Discovery & Control, and SecOps & Forensics. Highlights include involving end users in remediation through notifications and an API-centric approach where all components of CloudLock can integrate into third-party solutions as well as cloud apps. Top industries served are retail, manufacturing, and financial services. Target customers are in regulated industries and typically midsize or large enterprises.
- **Elastica.** Elastica's Protect application within its CloudSOC platform provides DLP functionality. The solution is offered as a cloud subscription service and covers all data uploaded, stored, shared, and downloaded from cloud applications and services. Highlights include Elastica's ContentIQ technology, which can dynamically classify documents based on their content. Top industries served are financial services, retail, and consulting services. Target customers are midsize to large enterprises with a high concentration of intellectual property.
- **Netskope.** Netskope Active Cloud DLP protects data in Box, Dropbox, Egnyte, Google Drive, Office 365, Salesforce, and any app being proxied via the Netskope Active Platform. It tracks cloud activities at the user, app, and activity level for sanctioned and unsanctioned cloud usage on any device, including both browserbased and native apps or sync clients and whether accessed onpremises, remotely, or through a mobile device. Highlights include a variety of prebuilt policy templates and DLP software building blocks for custom DLP profiles. It integrates with on-premises DLP solutions. Top industries served are healthcare, financial services, and retail. Target customers are midsize to large enterprises.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FIGURE 6 Cloud DLP Vendors

	Does the solution have the ability to perform data discovery?	Does the solution have the ability to perform data classification?
CloudLock	Yes	Yes
CipherCloud	Yes	Yes
Elastica	Yes	Yes
Netskope	Yes	No

	What contextual info is considered for DLP rules and policy violations?	How does the solution analyze content to find DLP policy violations?	Does the solution have the ability to inspect encrypted traffic?
CloudLock	Platform, object type/size, ownership, exposure type, violation thresholds	Regex, false positive heuristic suppression algorithms, clustering, machine learning	No, but can for at rest (via native Google, SFDC capabilities)
CipherCloud	Users, location, content, file types, cloud applications, folders, recipients	Regex, data match, keyword, phrases, dictionaries, Luhn checks, proximity	No
Elastica	Cloud service, user info and activity, file and device properties, location, exposure type, ThreatScore	Supervised and unsupervised machine learning algorithms, regex, keywords, phrases, dictionaries	Yes
Netskope	Identity, group, org unit, device type, classification, location, app, category, content type, activity like upload, download, or view	Proximity, volume thresholds, int'l. support incl. double-byte characters, fingerprinting, content exact match, and/or rules, validation mechanisms such as Luhn check	Yes

	What types of default policy templates are available?	What are actions in response to policy violations?	How does the solution report, audit, document policy violations?
CloudLock	Hundreds of default DLP policies across a multitude of dimensions (context only, sensitive data type, etc.)	Notify admin, notify user, revoke app, selective encrypt, quarantine, revoke sharing, transfer ownership, and more	Admin dashboard, audit log, CSV export. Integrates with SIM.
CipherCloud	Predefined policy templates (i.e., HIPAA, GLBA, credit cards)	Quarantine, delete, encrypt, user-remediate, restrict share, block, notify, tombstone file	Admin dashboard. Integrates with SIM.
Elastica	Variety of default policies (e.g., PCI, PII, PHI, GLBA, FERPA, virus, source code, country-specific)	Notify user/file owner, notify admin via email or text, block, encrypt, quarantine, delete, create ticket in ITSM system	Admin dashboard with alerts for review; permanent logs saved.
Netskope	Policies for PII, PCI, HIPAA, source code, profanity. Also a wizard to create custom policy and/or tune existing.	Alert, block, encrypt, legal hold, quarantine, tombstone file, coach user, require user justification	Logs, metadata. In-product incident mgmt. Integration with incident mgmt., ticketing systems.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

DLP Suites Cover All Channels Of Data Loss

DLP suites do it all and cover every channel of data loss. As a result, with the exception of a few, these are typically extensive deployments. Many companies also opt to deploy and use only one part or module of the suite (e.g., endpoint DLP only or web DLP only), leaving open the possibility of later deploying other components. Despite the price tag, many large enterprises opt for a DLP suite because of a suite's capabilities to address intellectual property data loss scenarios and provide benefits such as operational efficiencies and ease of policy management. Notable vendors include (see Figure 7):

- **Clearswift.** Clearswift's DLP solutions come as either a native DLP offering (ARgon & CIP) or integrated within their Email, Exchange, Web, and ICAP Gateways. Solutions can be deployed on-premises (physical appliance or virtual machine — vSphere) or in the cloud (e.g., with AWS or Azure). DLP-as-a-service is offered by managed service partners, using Clearswift's email or web (including ICAP) DLP technologies as the base DLP policy engine. A highlight is Clearswift's Adaptive Redaction (data redaction, document sanitization, structural sanitization) capability. Top industries served are financial services, government, and defense. Target customers are companies with 1,500 to 7,500 employees.
- **DeviceLock.** DeviceLock's DLP suite is comprised of five modules: DeviceLock (endpoint), NetworkLock (email, web, social networks, FTP, cloud services), ContentLock (emails, chats, blog posts), Discovery, and Search. It's deployed as an on-premises software product and uses Microsoft Active Directory as its native management platform. A highlight is its endpoint-resident 25+ language optical character recognition (OCR), which extracts and inspects pieces of text from images.[7] Top industries served are financial services, government, and healthcare. Target customers are midsize to enterprise companies; the solution is properly priced for SMBs as well.
- **Digital Guardian.** Digital Guardian (DG) for DLP is offered as a module of the Digital Guardian Data Protection Platform. It's available on-premises, as a managed service, or as a hybrid of both where the hardware resides at the customer site and is managed remotely. A highlight is DG's kernel-level endpoint agent, which provides deep visibility and contextual information that can be used for DLP as well as endpoint detection and response capabilities. Top industries served are manufacturing, healthcare, and financial services. Target customers are global enterprises (10,000+ employees) and government agencies for on-premises and companies of all sizes for DG's managed services program.
- **Forcepoint.** Forcepoint's Triton AP-Data can be deployed as software, hardware, or a virtual appliance, and at the endpoint. It consists of the following core offerings for DLP: Gateway (email, FTP, third-party integrations), Discover (DLP for local network and cloud services), and Endpoint (Windows, OS X, Linux). DLP capabilities are also available in the Triton AP-Web and AP-Email on-premises and hybrid gateways and SaaS services. A highlight is Forcepoint's modular, flexible deployment and threat detection capabilities. Top industries served are financial services, manufacturing, and healthcare. Target customers are regulated industries and companies with significant investments in intellectual property.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

- **Intel Security (McAfee).** McAfee offers DLP capabilities in its suites and standalone solutions. McAfee Complete Data Protection — Advanced suite includes DLP and encryption capabilities for endpoints. McAfee Total Protection for DLP suite protects data on-premises, in the cloud, and on endpoints and can be delivered via a software agent or through physical or virtual appliances. Additional DLP products include Device Control, DLP Discover, DLP Endpoint, DLP Monitor, and DLP Prevent. A highlight is location and application tagging to retain security settings and simplify policy creation. Top industries served are healthcare, financial services, high-tech, and retail. Target customers are companies of all sizes, with a majority as large enterprises in regulated industries.
- **Somansa.** Somansa DLP consists of DLP+ Center (centralized management console), Mail-i (network, covering outbound traffic for email, IM, FTP, web), Privacy-i (endpoint), Storage (file servers and databases), Cloud (cloud email and storage), and Mobile. Privacy-i is also available as a SaaS solution. Somansa's Halconeye (DLP and database audit and protection) is a customized appliance designed for SMBs. Top industries served are financial services, healthcare, and manufacturing. Target customers are companies of all sizes.
- **Symantec.** Symantec DLP consists of the following server and client components and cloud services: Enforce Management Platform (reporting, analytics), Cloud Service (for Office 365, Gmail, Exchange Server) Cloud Storage (for Box), Cloud Prevent (for Office 365), Endpoint, Mobile, Network (email, web), Storage (file servers, shares, database, NAS, SharePoint), and APIs for reporting and response. Different components are available as hardware, software, or virtual appliance, hybrid and hosted SaaS. A highlight is breadth and depth of capabilities. Top industries served are financial services, healthcare, and manufacturing. Target customers are enterprises with 1,000 to 5,000 employees and Global 2000 companies.
- **Trend Micro.** Trend Micro offers a different approach to DLP, in which DLP is a feature integrated into Trend Micro products. Customers can activate DLP functionality right away for use. Its integrated DLP module is a part of the following solutions: Cloud App Security, Endpoint Security, Mail Server Security, Security for Microsoft SharePoint, IM Security, Gateway Messaging Security, and Web Gateway Security. A highlight is central management via Trend Micro Control Manager for all the DLP integrated products and technologies. Top industries served are financial services and healthcare. Target customers are companies of all sizes.
- **Trustwave.** Trustwave's enterprise DLP solution consists of DLP Monitor (all web-based channels), Protect Web (ICAP with a web proxy), and Protect Email; these are provided as software, virtual appliance, and appliance. DLP capabilities are also included in its Secure Web Gateway, Secure Email Gateway, and Endpoint Protection Suite; these are delivered from the cloud, as software, virtual appliance, and appliance. A highlight is the support of Trustwave's SpiderLabs team for authoring and refinement of risk categories and policies across DLP solutions. Top industries served are financial services, hospitality, and telecommunications. Target customers are companies of all sizes.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

› **Watchful Software.** Watchful Software's RightsWatch provides an approach to DLP that can be used either in conjunction with an established DLP solution or as a simpler, cost-effective alternative. RightsWatch combines data classification, information rights management, and DLP to protect data and enforce handling policies regardless of whether it's at rest, in motion, or in use. Top industries served are financial services, energy, and healthcare. Target customers are companies with 1,000 or more employees.

FIGURE 7 DLP Suite Vendors

	Does the solution have the ability to perform data discovery?	Does the solution have the ability to perform data classification?
Clearswift	Yes	Yes, via Information Governance Server
DeviceLock	Yes	No
Digital Guardian	Yes	Yes
Forcepoint	Yes	Yes
Intel Security	Yes	Yes
Somansa	Yes	Yes
Symantec	Yes	No
Trend Micro	Yes	Yes
Trustwave	Yes	No
Watchful Software	Yes	Yes

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FIGURE 7 DLP Suite Vendors (Cont.)

	What contextual info is considered for DLP rules and policy violations?	How does the solution analyze content to find DLP policy violations?	Does the solution have the ability to inspect encrypted traffic?
Clearswift	Identity, file attributes, document properties, flow direction, comms channel. On endpoint, includes peripheral details (e.g., serial #).	Regex, file matching, custom exp, exact tokens with checksum, binary pattern, image checksum, structured data query validation	Yes
DeviceLock	User/group, flow direction, time, encrypted/not, email domains, file type, app control, granular access permissions (port/device/IP protocol)	Keywords, regex, dictionaries, 10-language morphological keyword analysis, OCR. Verified file types/properties, Boolean operators, hit threshold, IRM tag.	Yes
Digital Guardian	Source/destination file and hardware details, current/parent processes, user info, network transfer details, and more	Regex, keyword, dictionaries, entities (e.g., last name), Bayesian analysis. Support 90+ languages and extraction of 300+ file types.	Yes
Forcepoint	Location, user behavior, website reputation, app type, LDAP, endpoint details, website reputation, and more. Drip DLP rules to identify "low and slow" data theft over time.	Regex, weighted dictionaries, proximity analysis, validation scripts and file type ID, Boolean log operands, OCR, 13 language name detection/recognition, machine learning, fingerprinting	Yes
Intel Security	File attributes, prebuilt or web and customer app definitions, identity, source/destination details	Regex, dictionary, fingerprinting, proximity, partial word match, location- or app-based tag, etc.	Yes
Somansa	Provides reinforced rules if it determines conditions aren't safe based on contextual info (e.g, user location, PC security status)	Keyword, regex, object tagging, exact document matching, structured data fingerprinting, lexicon and conceptual analysis	Yes
Symantec	User attributes, user behavior, data owner, user risk summary, device ID, destination, protocol, app name/signature, historical incident trends	Fingerprinting, vector machine learning, form recognition, file type, keywords, regex, binary signature matching, and more	Yes
Trend Micro	Email clients, FTP, webmail, peer-to-peer applications, printers, cloud service, and more	Based on data identifier types: keywords, regex, file attributes	Yes
Trustwave	Dependent on product/solution and its specific type(s) of data sources (e.g., IP addresses, port numbers, file paths, etc.)	Data matching, regex, contextual linguistics/concept models	Yes
Watchful Software	User identity, drive, file details, apps in use	Regex, exact data matching, keywords, text strings	No

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FIGURE 7 DLP Suite Vendors (Cont.)

	What types of default policy templates are available?	What are actions in response to policy violations?	How does the solution report, audit, document policy violations?
Clearswift	Default policies remove active content, document properties, redact credit card #s. Variety of templates (e.g., PCI, HIPAA, etc.).	Alert, block, quarantine, strip attachment, delay message, redact (1-3 types of adaptive redaction techniques) encrypt, manager release	Native reporting and notification. SIM integration.
DeviceLock	Prebuilt policy templates for supported regulations (e.g., industry, country, social, and more)	Block/allow, block encrypted/ allow encrypted, detect, log event, log data/shadow, alert, pop-up message, delete, set permissions, audit, delete container, and more	Admin dashboard, event export, SIM integration, email alert, and more. DeviceLock Search Server (full-text search in central database, shadow log repository).
Digital Guardian	Variety of policy templates (e.g., USB/storage, PII, PCI, ITAR/EAR, etc.) from DG Content Server.	Alert, user and decision prompts, warn, justify, block, encrypt, quarantine endpoint	Continuous forensic log of all user, app, data, network, system-level activity. Replay in DG Management Console. Admin dashboard, email alerts. Multiple format report export. SIM integration.
Forcepoint	Variety of policy templates for global regulations, IP protection. Advanced policies for malicious insider data theft detection.	Audit, block, quarantine, self remediate (confirm), encrypt, classify, apply EDRM, ransom note, tombstone (remove file, leave marker file stub)	Centralized audit and reporting, role-based admin. Incident case management. By default a copy of incident forensic data stored in encrypted forensic store.
Intel Security	Variety of policy templates (e.g., PII, SOX, source code, ITAR, HIPAA, EAR, FISMA, FERPA, etc.) and how-to guides	Alert, block, encrypt, notify, quarantine, redact, request justification, apply rights management, monitor, remove, bounce and redirect email	McAfee ePolicy Orchestrator console: reporting, incidents, case management, auto notifications to various business stakeholders.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FIGURE 7 DLP Suite Vendors (Cont.)

	What types of default policy templates are available?	What are actions in response to policy violations?	How does the solution report, audit, document policy violations?
Somansa	Policy templates for compliance (e.g., PCI, GLBA, HIPAA, country PII, etc.)	Alert, block, quarantine, encrypt, permanent wipe, etc.	Web-based central management console
Symantec	Variety of templates, vertical-specific solution packs. Policy resources via Symantec DLP Exchange.	Block, remove sensitive data, notify, quarantine, apply visual tag, apply encryption or DRM, API to call third-party app to execute remediation actions	Centralized, web-based interface for reporting, incident management. Symantec DLP IT Analytics (create cubes, reports, dashboards, track metrics).
Trend Micro	200+ predefined templates across 62 countries. Also includes PCI, HIPAA, GLBA, SOX, Japan My Number	Log, block, pass, client-side alert, forensic data capture, user justification, pass but encrypt, and more channel-specific actions	Everything is recorded in the DLP logs, including who touches the file, file types, exact matched content, time, action, channel, templates that trigger rules, and more.
Trustwave	70+ policies provided for common DLP areas such as compliance, intellectual property protection and acceptable use	Copy, move, delete, quarantine, block, encrypt	SIM integration. Console for overall administration, analysis and reporting. Risk Dashboard with drill down, advanced search, case/ investigation management
Watchful Software	Predefined custom templates available	Block, encrypt, warn, classify	Logs server events and user side events. SIM integration. Reports to help understand *who* has done *what*, *when*, and *how* with classified data.

Recommendations

Plan Your Strategy And Evaluate Options As DLP Becomes A Feature

It used to be that if you were looking for a DLP solution, a DLP suite was the natural choice. In a world where DLP is fast becoming a feature and there are different ways to acquire DLP capabilities, a DLP suite may still be the best option; however, depending on your requirements, DLP as a feature may be a better fit your needs. Assess the following to help better define your DLP approach and strategy:

› **Identify and prioritize channels of data loss focus.** Where are you most at risk for data loss: email, endpoint, cloud, other? Understand how employees work and how data must flow for your business. In many cases, you will find overlaps as vendors and solutions straddle and cover one or more channels of data loss. Prioritizing your focus will help to narrow down the types of solutions and vendors to consider for DLP capabilities.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

- **Evaluate where you may already have DLP as a feature.** Are you making the most of what you already have? In some security solutions and appliances (e.g., NGFW, email gateway, web gateway, endpoint security solutions), DLP is an added module or license. If it's there, take it for a test drive. It may be sufficient for your needs, or you may find reasons to cross this option off your list in favor of another alternative. For example, an organization with a compliance-driven DLP deployment may find that DLP as a feature meets requirements, whereas an organization looking to focus more on protecting intellectual property may prefer the additional data fingerprinting or OCR capabilities more commonly found within a DLP suite.
- **Assess available resources of deploying and managing DLP capabilities.** There are tradeoffs, of course. DLP as a feature or as an integrated capability will typically require fewer resources to deploy, yet the DLP engine and solution capabilities for reporting and remediation may not be as robust as a suite, and the ongoing management and updating of policies across multiple tools over time may prove less operationally efficient for some. A DLP suite will give you all the bells and whistles and more, but in some instances can require more FTEs to deploy and fine-tune before you can scale back resources to manage policies and escalation on an ongoing basis.
- **Focus on DLP processes and plan your road map for DLP maturity.** Implementing DLP isn't as simple as selecting a few policy templates. The technology isn't the challenge. You must focus on processes for DLP maturity and success — discovering where your data is located and how it needs to flow, classifying what data is considered sensitive to understand what to protect and how, consolidating data into fewer locations for manageability, creating DLP policies with business data owners, and then enforcing the policies and periodically reviewing results to ensure that the policies are appropriate.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

Ask a question related to our research; a Forrester analyst will help you put it into practice and take the next step. Schedule a 30-minute phone session with the analyst or opt for a response via email.

Learn more about inquiry, including tips for getting the most out of your discussion.

Analyst Advisory

Put research into practice with in-depth analysis of your specific business and technology challenges. Engagements include custom advisory calls, strategy days, workshops, speeches, and webinars.

Learn about interactive advisory sessions and how we can support your initiatives.

Supplemental Material

Companies Interviewed For This Report

BAE Systems
Check Point
CipherCloud
CipherMail
Clearswift
CloudLock
CoSoSys
DeviceLock
Digital Guardian
Elastica
Fidelis Cybersecurity
Forcepoint (formerly Raytheon/Websense)
Intel Security
Microsoft
Mimecast
Netskope
Proofpoint
Somansa
Spirion
Symantec
Trend Micro
Trustwave

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

Watchful Software

Zscaler

ZixCorp

Endnotes

[1] Today, enterprises can acquire DLP capabilities and tools in a variety of ways. This report looks at the factors driving renewed interest in DLP, the state of DLP suite adoption today, and the pros and cons of different approaches of bringing DLP capabilities into the enterprise. See the "Market Overview: Data Loss Prevention" Forrester report.

[2] Note that these services are distinct from other security services offerings that help with the upfront process and policy work to deploy DLP, and leave the ongoing management and monitoring to you.

[3] Data discovery and classification is the first part of Forrester's Data Security And Control Framework, which breaks data protection into three areas: 1) defining data; 2) dissecting and analyzing data; and 3) defending data. Classification enables the creation of attributes for data identity, which helps determine how to treat and secure data. See the "Rethinking Data Discovery And Data Classification Strategies" Forrester report.

[4] Data discovery solutions differ along several dimensions: 1) whether they are software- or appliance-based; 2) their support of resources as discovery targets; 3) their granularity of indexing and classification capabilities; and 4) their post-classification capabilities and integrations (potentially including functions such as deletion, migration, archival, encryption, and masking).

[5] These more advanced capabilities are more commonly found in a DLP suite.

[6] To support their firms' cloud strategy without compromising security or compliance, security and risk (S&R) pros need to develop a number of important capabilities. They need the capability to: 1) discover sanctioned and unsanctioned cloud app adoption; 2) prevent the unauthorized transfer of sensitive data to the cloud; 3) protect and encrypt sensitive data in the cloud; and 4) identify suspicious employee behaviors and threats in cloud services. This report examines the vendor landscape for cloud access security intelligence (CASI) solutions that provide some or all of these capabilities. See the "Vendor Landscape: Cloud Access Security Intelligence (CASI) Solutions" Forrester report.

[7] The advantage of endpoint-resident OCR compared with server-based OCR is its ability to prevent leakage of sensitive data in images via local data channels on the endpoint as well as from mobile computers used outside of the corporate network control structure.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research (Nasdaq: FORR) is one of the most influential research and advisory firms in the world. We work with business and technology leaders to develop customer-obsessed strategies that drive growth. Through proprietary research, data, custom consulting, exclusive executive peer groups, and events, the Forrester experience is about a singular and powerful purpose: to challenge the thinking of our clients to help them lead change in their organizations. For more information, visit forrester.com.
119808