G00277565

Critical Capabilities for Enterprise Data Loss Prevention

Published: 25 April 2016

Analyst(s): Brian Reed, Neil Wynne

IT security leaders deploy enterprise DLP for three major use cases: regulatory compliance, intellectual property protection and visibility into how users treat sensitive data. This research evaluates DLP products for the three use cases, based on nine critical capabilities.

Key Findings

- In the ongoing second wave of adoption, enterprise data loss prevention has become a key component of a broader data life cycle process supported by technology, as opposed to simply being another technology buying decision.
- When added to secure email gateways and secure Web gateways, integrated DLP can address basic regulatory compliance requirements; however, more comprehensive regulatory compliance requirements are better addressed through the unified workflow of enterprise DLP.
- Enterprise DLP is typically adopted for intellectual property protection and broader data visibility and monitoring, particularly in large multinational organizations.

Recommendations

- Engage and involve business units and data owners to improve the odds of success of a DLP deployment.
- Identify the lead use case for your DLP initiative to address regulatory compliance, IP protection, or data visibility and monitoring.
- Start with data in use at the endpoint for DLP initiatives driven by IP protection, then implement advanced detection features, such as image analysis, machine-learning and other data-matching techniques.
- Deploy data in motion (i.e., network DLP on outbound email) for DLP initiatives driven by regulatory compliance to meet the requirements for the Payment Card Industry, the Health Insurance Portability and Accountability Act and other compliance standards.

- Evaluate vendors for their integrations with other data security technologies, such as data classification, user and entity behavior analytics, cloud access security brokers, and incident response and forensics products.

Strategic Planning Assumption

By 2020, intellectual property (IP) protection will be the primary enterprise data loss prevention (DLP) use case for 80% of organizations, which is an increase from today's 25%.

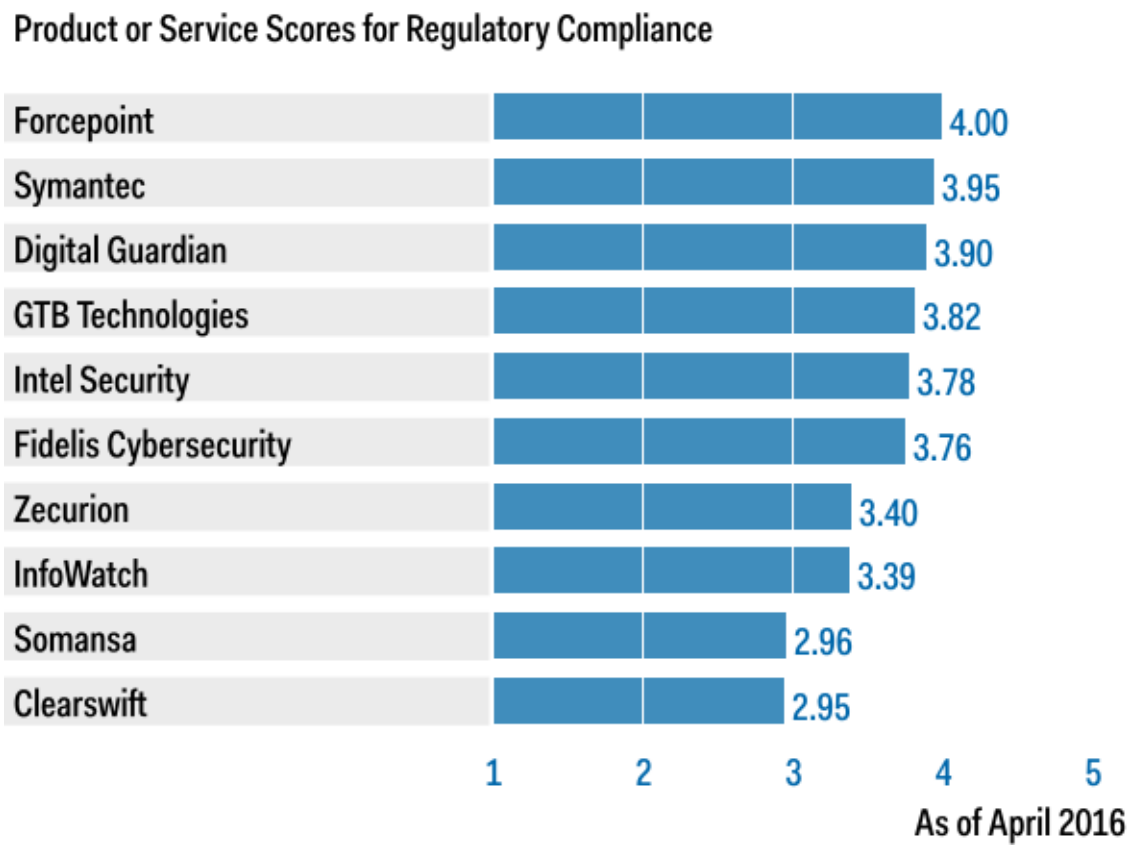
What You Need to Know

This Critical Capabilities research is intended for clients looking to adopt enterprise DLP and map their organization-specific DLP deployment to one of the three most common use cases for DLP. This research should be used as a starting point to better understand the appropriate use cases and critical capabilities that enterprise DLP vendors can address. It should be used in conjunction with the analysis provided by the "Magic Quadrant for Enterprise Data Loss Prevention."

Analysis

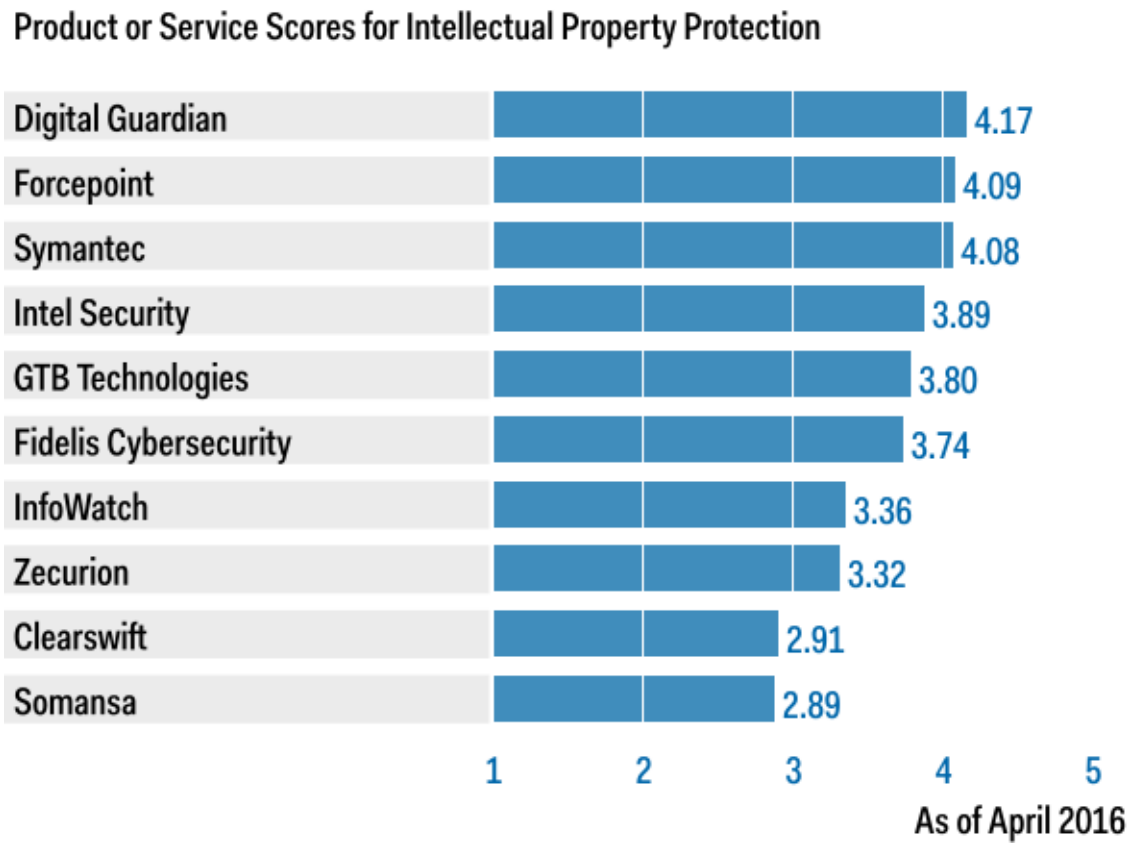
Critical Capabilities Use-Case Graphics

Figure 1. Vendors' Product Scores for the Regulatory Compliance Use Case



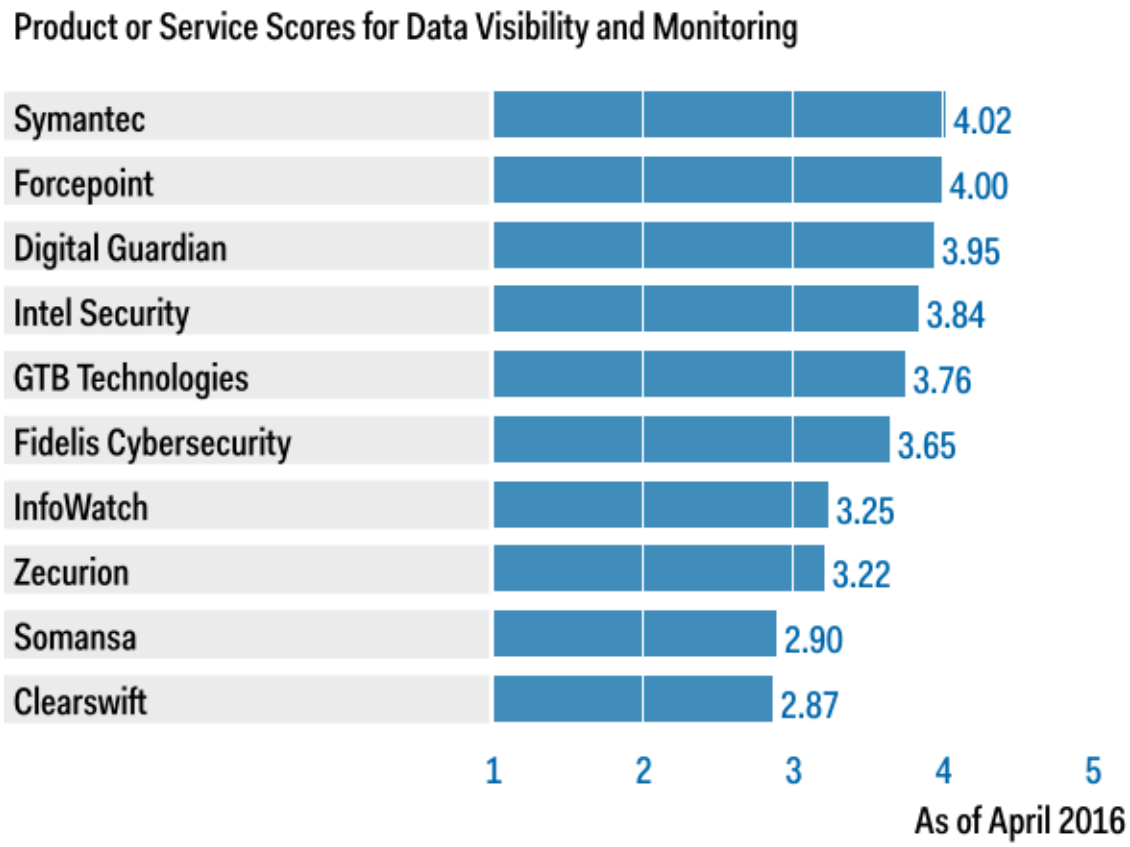
Source: Gartner (April 2016)

Figure 2. Vendors' Product Scores for the Intellectual Property Protection Use Case



Source: Gartner (April 2016)

Figure 3. Vendors' Product Scores for the Data Visibility and Monitoring Use Case



Source: Gartner (April 2016)

Vendors

Clearswift

Clearswift is a new entrant to the Enterprise DLP Critical Capabilities research, and has strong name recognition in the secure email gateway (SEG) market in the U.K. The Clearswift Adaptive DLP (A-DLP) product is new in 2015, and results from two earlier acquisitions and a significant development effort to get the product to market in early 2015. Clearswift's strong redaction and sanitization capabilities and its business focus in the U.K. and Europe makes it a compelling DLP contender in European markets, as well as worthy of global consideration.

Product: Adaptive Data Loss Prevention

DLP Endpoint

The Clearswift DLP Endpoint supports all major versions of Windows, and performs standard DLP endpoint functionality, such as copy/move/save as and clipboard activity restrictions, as well as a

complete set of granular USB control options. The DLP Endpoint works online and offline and does not require any phone home capabilities to the DLP Management server or cloud instance. Document-matching (either partial or exact) detection techniques are not supported at the endpoint.

DLP Discovery

Clearswift DLP Discovery is limited to Windows file systems. Discovery policy includes full regular expression matching, keyword matching and lexicon analysis. The DLP Discovery agent can scan only files stored on the local file system, network drives and local folders that are synced to cloud services; there are no native API capabilities with cloud services.

DLP Network

Clearswift DLP Network is available as a hardware appliance, a software installation or a virtual appliance deployed in VMware ESXi or Microsoft Hyper-V. Clearswift integrates with existing email and Web proxy architectures through the interception of content via SMTP, HTTP/S and Internet Content Adaptation Protocol (ICAP).

Ease of Deployment

DLP Endpoint and agent-based DLP Discovery are straightforward to deploy. DLP Network also integrates with email and Web proxy deployments.

Configuration Flexibility

Clearswift can operate cloud hosted and on-premises, based on an organization's Web (including ICAP) and SMTP architecture for visibility and content inspection of Web and email traffic.

DLP Advanced Detection

Clearswift has many DLP detection capabilities; however, it does not support optical character recognition (OCR) image analysis, statistical analysis or have coverage for instant messaging (IM). Clearswift supports full file fingerprinting and subfile (information-based) fingerprinting for use in its DLP product. Clearswift has strong industry recognition for its adaptive redaction capabilities, and it's able to redact and/or sanitize the sensitive parts of a file, while not interrupting delivery to its destination. Adaptive redaction is supported for Microsoft Office files, OpenOffice, PDF, plain text and HTML content.

Internationalization Support

Clearswift supports scanning text encoded in the major standard character encoding schemes, including UTF-8, UTF-16 and UTF-32, and the administration interface is localized in English and Japanese. The end-user interface is localized in English, French, German, Japanese, Chinese, Italian, Spanish and Portuguese.

DLP Management System

The management system is straightforward and usable, with good reporting capabilities, and can be deployed on-premises or cloud-hosted.

DLP Vendor Integrations

Clearswift has a few external vendor partnerships to enhance its DLP product line at this time: Echoworx, Linoma Software and SecureMySocial. Clearswift also supports Titus data classification.

Digital Guardian

Founded as Verdasys in 2002 and rebranded in 2014, Digital Guardian is headquartered in Waltham, Massachusetts. Digital Guardian's approach to enterprise DLP has been primarily through endpoint DLP, with strong product integration partnerships to cover network DLP and discovery DLP until its acquisition of Code Green Networks in October 2015. Gartner received separate vendor questionnaires and supporting research information from Digital Guardian and Code Green; however, we are evaluating them here as one organization.

Product: Digital Guardian 7.1.2 and Code Green Networks TrueDLP 9.1

DLP Endpoint

Digital Guardian offers its DLP Endpoint for Windows, Mac OS X and Linux OSs. The DLP agent is a kernel-level agent, which requires thorough testing of client OSs and any custom applications deployed to endpoints.

DLP Discovery

Digital Guardian has both agent-based discovery and DLP discovery through the acquisition of Code Green Networks. Discovery capabilities exist through Code Green for the discovery of data over Accellion, Citrix ShareFile and Box, using native-API integrations.

DLP Network

Digital Guardian partners with Fidelis for DLP Network capabilities; however, this Critical Capabilities research rates the functionality of the Code Green Networks product that was acquired in 2015. Code Green Networks for Network DLP CI-Appliance can act as a network sniffer for data monitoring, as well as integrate with email and Web proxy products to inspect content.

Ease of Deployment

The Digital Guardian endpoint is highly configurable, and can be tuned based on endpoint DLP requirements. The CI-Appliance deploys just like any other network appliance for DLP: It integrates with proxy or mail MTA, or it can take a data-monitoring role by using an additional network interface as a monitoring port.

Configuration Flexibility

Digital Guardian offers considerable deployment flexibility, and has integrations and add-on modules at the endpoint for forensics, email encryption and encrypted file support.

DLP Advanced Detection

Digital Guardian covers most advanced detection capabilities. Structured data fingerprinting is not directly supported, but this is covered by contextual variables and data tagging. Unstructured data fingerprinting, such as form data, is covered as part of the product capabilities of Code Green.

Internationalization Support

Digital Guardian and Code Green Networks have wide language support, including language support for single-byte and double-byte character sets, including Chinese, Japanese and Korean, as well as support for Arabic and Hebrew.

DLP Management System

The Digital Guardian management system is flexible in deployment and functionality, and, through the Hybrid Managed Services Platform (MSP), it can be cloud-hosted or reside on-premises.

DLP Vendor Integrations

Digital Guardian has several key partnerships with other security technologies, most notably the longstanding partnership with Fidelis, and Blue Coat Systems, which integrates with the Code Green product line. Other notable technology partnerships include FireEye, Imperva, Palo Alto Networks and Splunk.

Fidelis Cybersecurity

Fidelis was founded in 2002, acquired by General Dynamics in August 2012, and spun back out as an independent, private company through an investment by Marlin Equity Partners in 2015. Fidelis and Digital Guardian have a joint technology integration partnership that has been in place for several years, in which the DLP offering from Fidelis is integrated within the management console offered by Digital Guardian, providing a full-suite DLP product. Due to Digital Guardian acquiring Code Green Networks, and Fidelis focusing on broader threat detection, Gartner anticipates Fidelis expanding beyond DLP to compete more broadly for opportunities in network security, advanced threats, and the endpoint detection and response markets. Fidelis' DLP technologies will remain a core capability of the overall Fidelis XPS platform.

Product: Fidelis XPS 8.0 (now called Fidelis Network)

DLP Endpoint

Fidelis does not offer its own DLP Endpoint; however, it provides this functionality via a longstanding partnership with Digital Guardian. It received a base score of 3.0, due to meeting this criterion; however, consult the Digital Guardian vendor section for further details.

As noted in the "Magic Quadrant for Enterprise Data Loss Prevention," the relationship between Fidelis and Digital Guardian is likely to change significantly in 2017, due to the acquisition of Code Green Networks by Digital Guardian and the acquisition of Resolution1 by Fidelis

DLP Discovery

Fidelis does not offer its own DLP discovery product, and provides this functionality via a longstanding partnership with Digital Guardian. It received a base score of 3.0, due to meeting this criterion; however, consult the Digital Guardian vendor section for further details.

As noted in the DLP Magic Quadrant, the relationship between Fidelis and Digital Guardian is likely to change significantly in 2017, due to the acquisition of Code Green Networks by Digital Guardian.

DLP Network

Fidelis XPS is the most fully featured network DLP product in the Enterprise DLP market, and operates at speeds of 20Gbps and above. The strength of this product is its wide range of deployment and throughput options, as well as port and protocol independence, and no reliance on a proxy architecture. Fidelis XPS goes beyond just network DLP capabilities, and provides wider threat prevention with payload analysis, intrusion detection and prevention features, and threat intelligence capabilities to identify malicious traffic and content.

Ease of Deployment

Fidelis XPS deployment is comparable to other security appliances, such as intrusion prevention systems (IPSs) and next-generation firewalls, and requires moderate knowledge of the networking environment where deployed.

Configuration Flexibility

Fidelis XPS can be deployed in-line or as a network tap or SPAN, and can be delivered in hardware appliance or virtual appliance form factors.

DLP Advanced Detection

Fidelis XPS covers all of the common DLP detection capabilities, and can also analyze metadata content. Fidelis XPS has additional features to better determine content, such as payload analysis and sandboxing of files.

Internationalization Support

Fidelis XPS provides native Unicode support (UTF-8, UTF-16 and UTF-32) for any language in all document formats. Fidelis XPS supports detection and prevention without restriction, using all 15 of the character sets enumerated in ISO/IEC 8859, as well as dozens of additional legacy single- and double-bytecode pages used in Latin, Cyrillic, Greek, Hebrew, Arabic, Thai and Japanese languages.

DLP Management System

Fidelis XPS CommandPost is feature-rich with advanced configuration options, logical event tracking and alert options.

DLP Vendor Integrations

Fidelis has numerous integrations to help with its threat detection strategy, notably integrations with multiple threat intelligence vendors and Cisco ThreatGRID for payload analysis and file inspection. Fidelis' own Endpoint product (formerly Resolution1 Endpoint) supports deep threat detection, visibility, investigation and response capabilities.

Forcepoint

In 2015, Raytheon and Vista Equity Partners completed a joint venture that combined Websense, a Vista Equity portfolio company, and Raytheon Cyber Products. This created a new company called Forcepoint. Raytheon owns a majority share of Forcepoint, whereas Vista Equity Partners maintains a minority interest.

The AP-DATA product line is part of its TRITON architecture, and includes TRITON AP-DATA Discover, TRITON AP-DATA Gateway and TRITON AP-ENDPOINT DLP.

Product: TRITON AP-DATA 8.1 and TRITON AP-ENDPOINT DLP 8.1

DLP Endpoint

TRITON AP-ENDPOINT DLP provides the ability to monitor and enforce DLP policies on Windows, Mac OS X and Linux endpoints using a range of data inspection points and endpoint controls. Uniquely, TRITON AP-ENDPOINT supports full DLP policy enforcement, including the protection of structured and unstructured data, when Windows and Mac endpoints are disconnected from the corporate network.

DLP Discovery

TRITON AP-DATA Discover provides the ability to discover and remediate critical business data stored throughout data centers (file servers, databases, Microsoft SharePoint, Microsoft Exchange, etc.) and in enterprise cloud applications (e.g., Exchange Online, SharePoint Online and Box).

DLP Network

TRITON AP-DATA Gateway provides the ability to monitor and enforce DLP policies across several channels of communication including Web, email and mobile. Protector is a multifunction DLP appliance (software or hardware) that analyzes SMTP, HTTP, FTP, plain text and IM traffic (e.g., Yahoo, MSN, chat and file transfer). The protector can act as a mail transfer agent (MTA) to block sensitive email and can enforce DLP policies via third-party products that support ICAP, such as Citrix ShareFile and Blue Coat Web proxies. Email Gateway for Microsoft Office 365 is a virtual appliance that provides DLP policy enforcement for outbound Exchange Online email traffic. It can be deployed from Microsoft's Azure Marketplace.

Ease of Deployment

Forcepoint supports a wide variety of deployment options. It can be deployed entirely on-premises; via a hybrid deployment of management on-premises and content inspection components deployed in a hosted cloud environment; and by a full cloud deployment, in which management and content inspection components are deployed in a hosted cloud environment. Forcepoint users can start a full enterprise DLP deployment program via integrated DLP provided in AP-WEB and AP-EMAIL, and use the same set of policies already in place for scaling up to AP-DATA deployments.

Configuration Flexibility

Forcepoint has a large library of predefined classifiers, policies and attributes, providing a wide range of context logic capabilities to meet specific customer use cases. Data Theft Risk Indicator policies provide the ability to combine content classifiers with context logic, which is designed to identify high-risk data transactions.

DLP Advanced Detection

Forcepoint has strong DLP detection capabilities and also supports structured data fingerprinting from data stored in Salesforce. Forcepoint employs policy and detection consistency to apply a cohesive set of policies and detection techniques across data in motion, at rest and in use from a single console. Support for OCR to allow embedded text to be identified in image-based documents, including faxes, scanned documents and photographs, is included. Forcepoint machine learning has algorithms that support the creation of machine-learning classifiers, without the need to supply a negative document set. This significantly lowers the barrier to machine-learning adoption. Cumulative DLP (Drip DLP) is an advanced detection technique focused on low and slow data exfiltration. Accurate name detection recognition capabilities in 13 languages is a strong detection method for personally identifiable information (PII) and other regulatory compliance use cases.

Internationalization Support

Forcepoint has been deployed in more than 80 countries. Although the management user interface is available in English only, end-user email notifications and endpoint agent notifications can be customized and localized.

DLP Management System

All TRITON products (AP-DATA, AP-ENDPOINT DLP, AP-WEB, and AP-EMAIL) are managed and configured via a unified management console, the TRITON Manager. AP-DATA uses the TRITON management system to provide a single location to orchestrate policies across DLP, Web and email products, as well as endpoint, gateway, cloud and discovery components.

DLP Vendor Integrations

Forcepoint has multiple vendor integrations, most notably licensing the cloud application database from Imperva Skyfence and using that in on-premises, hybrid and cloud AP-WEB (secure Web gateways [SWG]) and AP-DATA Gateway products. Forcepoint also partners with its own SureView Insider Threat (IT) to integrate DLP and user and entity behavior analytics (UEBA) capabilities for its customers.

GTB Technologies

Founded in 2004 and headquartered in Newport Beach, California, GTB Technologies' enterprise DLP suite supports network DLP, endpoint DLP and discovery DLP, as well as information rights management (IRM).

Product: GTB Data Loss Prevention 15.0

DLP Endpoint

Advanced Endpoint Protector is multifunctional DLP system that supports local discovery; network scanners; device control, including printers and faxes; application control; and user activity monitoring. Advanced Endpoint Protector supports 32-bit and 64-bit Windows. Options are available for local fingerprinting detection, which means there's no requirement to have an Internet connection or check in with the DLP Management server to verify a database or file fingerprint.

DLP Discovery

GTB Discovery system is designed to discover on- and off-premises data. Available on-premises targets include local PCs, file shares, structured databases, Outlook PST and OST files, Exchange, and SharePoint. For off-premises (cloud) data, GTB Discovery uses native-API integrations for discovery scanning of Box, Dropbox, Azure, Microsoft OneDrive, Google Drive and its own Exchange API for Hosted Microsoft Exchange scans. GTB Discovery optionally classifies files automatically by mapping predefined classification levels to DLP policies. GTB integrates with Seclore to provide enterprise digital rights management (EDRM) capabilities and enforce file-level access controls.

DLP Network

GTB Inspector is port- and protocol-agnostic. It supports all TCP channels, but has specific filters for the most common traffic types, such as POP3, IMAP, WBXML (active-sync), NNTP, Secure RDP, VNC, HTTP Server, FTP Server, SSH, HTTP Tunnel, Secure Sockets Layer (SSL), P2P, Gtalk, MS IM, Yahoo Messenger (including file transfers), IRC, Outlook, Yahoo Mail, and Gmail. All other protocols and ports are recorded as TCP incidents. The GTB Inspector is capable of inspecting outbound and inbound traffic. It has a built-in MTA, and it also serves as a smart host. GTB provides its own SSL proxy and is able to accept ICAP hand-offs from any other Web proxy or firewall, such as Blue Coat, Cisco, Forcepoint, Intel Security proxy products or the Palo Alto firewall.

Ease of Deployment

GTB Central Console is a straightforward, Linux-based management platform, deployed on hardware or virtual appliances. The GTB Endpoint for Windows is deployed as a multisourcing service integration installation package. It can be deployed through system management tools or installed interactively.

Configuration Flexibility

GTB's hybrid offering of cloud-based or on-premises architecture enables operations teams to manage policies from a single console in both directions — cloud to on-premises and on-premises to the cloud. All detection engines are available when deployed in the cloud or on-premises, and the GTB Inspector can also be deployed to a cloud instance, such as Microsoft Azure or Amazon AWS.

DLP Advanced Detection

GTB has several advanced detection capabilities, including exact document matching, partial document matching, structured data fingerprinting, unstructured data fingerprinting of patent forms and other content types with combinations of text and images, as well as statistical analysis. The OCR functionality supports 75 languages, as well as upside-down scanned documents. Sensitive data inside images may optionally be redacted. The system is capable of detecting encrypted data and true file types, including binary files.

Internationalization Support

GTB supports UTF-7, UTF-8, UTF-16 and UTF-32 encodings, and it has specific language support for English, Chinese Traditional, Chinese Simplified, Japanese, Russian, Polish, Spanish, German and Portuguese.

DLP Management System

GTB Central Console Server can be deployed as a software install or as a virtual machine (VM) instance, most commonly through VMware ESXi. The Central Console deploys policies to all GTB components and is used for complete workflow (incident response), reporting and email alerts.

DLP Vendor Integrations

Although GTB has been deployed with some other technologies for specific use cases for clients — such as HPE Security and ZixCorp for email encryption, Titus and Boldon James for data classification, and an OEM relationship with Seclore for IRM — there is currently no formalized partnership program with other technology vendors.

InfoWatch

InfoWatch was founded as an initial project by Kaspersky Lab, and has a strong market presence in Russia/Commonwealth of Independent States (CIS), the Asia/Pacific (APAC) region and Latin America.

Product: Traffic Monitor Enterprise 6.0

DLP Endpoint

InfoWatch Device Monitor, the Endpoint DLP product, supports Windows systems; however, Mac and Linux are not yet supported.

DLP Discovery

InfoWatch Crawler is a module of Traffic Monitor for network-based discovery; agent-based discovery is also supported.

DLP Network

Traffic Monitor is available as a hardware appliance, software install and VM. Traffic Monitor integrates with ICAP and SMTP proxies. However, to decrypt traffic, an endpoint agent is required.

Ease of Deployment

Installation for InfoWatch is relatively straightforward, with network DLP integrations with ICAP and SMTP.

Configuration Flexibility

Traffic Monitor supports any ICAP-enabled proxy. Web traffic decryption requires an endpoint agent.

DLP Advanced Detection

InfoWatch supports many advanced detection capabilities, including specific policies for detecting passport documents, database detection (data extracted from business systems) and filled forms detection.

Internationalization Support

InfoWatch includes a Character Set Decoder that support all UTF-8, UTF-16 and UTF-32 character sets.

DLP Management System

InfoWatch has separate management consoles for Traffic Monitor and Device Monitor.

DLP Vendor Integrations

InfoWatch does not yet have significant external vendor partnerships that enhance its DLP product line.

Intel Security

McAfee was founded in 1987, acquired by Intel in 2010 and rebranded as Intel Security. The Intel Security DLP technology comes primarily from two past McAfee acquisitions — Onigma in 2006 for endpoint DLP, and Reconnex in 2008 for network DLP and discovery DLP.

Product: Data Loss Prevention Version 9.4 (v.9.3 for DLP Monitor and DLP Prevent)

DLP Endpoint

Intel Security significantly improved the DLP policy engine in the DLP v.9.4 release. However, there is still only device control support for Mac OS X, and there is no Linux endpoint support.

DLP Discovery

Intel Security improved the agent-based DLP Discover product significantly in v.9.4. The DLP Capture database remains a powerful feature to further verify and tune the DLP Network products, particularly for the creation of dynamic filters based on scanned content. Intel Security does not offer native-API-based integrations with cloud storage providers or the discovery of sensitive data in the cloud in hosted email providers or cloud storage products.

DLP Network

The DLP Monitor and DLP Prevent products have strong capabilities. However, the management system configuration for DLP Network is separate from DLP Endpoint, though the events can be viewed together. Endpoint and network incidents are unified under the Incident Manager tab in ePolicy Orchestrator (ePO).

Ease of Deployment

For existing ePO clients, DLP Endpoint is relatively straightforward to install and deploy. The DLP network and DLP discovery products present administrators with a wide variety of deployment options.

Configuration Flexibility

DLP Network products can operate in-line (DLP Prevent) or in an out-of-band configuration, such as network tap or SPAN port (DLP Monitor).

DLP Advanced Detection

DLP Advanced Detection features include exact document matching, partial document matches, file fingerprinting, and abstract forms of nontext data, such as computer-aided design (CAD) drawings.

Internationalization Support

Intel Security has significant support for a wide variety of languages, including single- and double-byte character-set languages.

DLP Management System

Intel Security has enhanced the manageability of the DLP Endpoint and DLP Discover in v.9.4. The DLP Monitor and DLP Prevent products still use a separate management system, with some event linkage between ePO and the DLP Manager. All network DLP events and incidents are now viewed in ePO. DLP Manager is still required for policy management and configuration tasks for DLP Network and the appliance-based DLP Discovery.

DLP Vendor Integrations

Intel Security has the most extensive ecosystem of partnerships via Security Innovation Alliance (SIA), which includes partnering and providing specific integrations with data classification, EDRM, incident response and UEBA products to enhance the contextual value of its DLP product line.

Somansa

Somansa is a new entrant to the 2016 enterprise DLP Critical Capabilities research. Founded in 1997, Somansa first released its network data loss detection (DLD) products in 1999. Somansa has a strong APAC presence, with considerable operations located in its main headquarters in Seoul, South Korea.

Product: Network DLP and Endpoint DLP

DLP Endpoint

Privacy-i DLP Endpoint supports only Windows systems, Linux and Mac endpoints are supported only in Discovery DLP.

DLP Discovery

Somansa uses native-API support for discovering sensitive data on multiple cloud services, including Box, Google Drive and Microsoft OneDrive.

DLP Network

Network DLP can support throughput as high as 3Gbps, and can integrate with ICAP for HTTP/HTTPS, SMTP, as well as IM protocols.

Ease of Deployment

Deployment of DLP Endpoint product components is relatively straightforward — it does not alter network or browser configurations, except proxy autoconfiguration (PAC) files, if needed. Auto-update capabilities are only available for network DLP.

Configuration Flexibility

Multiple in-line and proxy deployment options are available for network DLP. However, limitations include explicit proxy and the use of PAC files on end-user systems. Some advanced configuration options are flexible and customizable, based on geography, language or customer.

DLP Advanced Detection

Somansa is missing partial document matching, statistical analysis and unstructured data fingerprinting (useful for form data). OCR image analysis is available in Endpoint DLP and Discovery DLP.

Internationalization Support

Somansa has specific language support for English, Chinese, Spanish, Korean, Japanese and Portuguese.

DLP Management System

DLP+ Center provides a centralized Web-based console for all administration tasks of the various network, endpoint, cloud and mobile DLP components.

DLP Vendor Integrations

Somansa provides integrations with EDRM products, including Microsoft RMS, Samsung SDS, Softcamp, Fasoo and MarkAny.

Symantec

Headquartered in Mountain View, California, Symantec has been in the DLP market since its acquisition of Vontu in 2007. Symantec released its Symantec Data Loss Prevention 14.0, which was made generally available in June 2015.

Product: Symantec Data Loss Prevention 14.0

DLP Endpoint

The DLP Endpoint Agent supports Windows and Mac systems. Although the Mac OS X agent does not have full feature parity with Windows, some key improvements were made in v.14.0, including browser upload monitoring on Mac OS X, removable storage support, support for VMware Fusion, and file-sharing support between Windows VM guests and the Mac OS X host system.

DLP Discovery

DLP Discover and Protect is a software installation for Windows or Linux, includes support for VMware ESXi, Microsoft Hyper-V and can be deployed as an Amazon Web Services EC2 AMI. DLP Discovery supports scanning several collaboration platforms, databases, file servers, and API-based scanning of Box cloud storage. The DLP Data-Insight and Self-Service Remediation Portals enable administrators to effective identify file owners and to fan out remediation to end users.

DLP Network

DLP Network Prevent and Monitor can be deployed as a software installation, virtual appliance and hardware appliance through partners such as InteliSecure and infoLock Technologies, which also offer DLP Managed Services. DLP Network Monitor can passively monitor network traffic at egress points (TAP and SPAN), and DLP Network Prevent integrates with ICAP and SMTP proxy architectures for Web and email DLP inspection and prevention. DLP Cloud Service for Email is a fully hosted service that provides comprehensive protection for Office 365 and Gmail.

Ease of Deployment

Symantec DLP v.14.0 has improved ease of deployment significantly over the previous versions by allowing for a Single Server Installation, which enables customers to deploy the Enforce platform, detection servers and the Oracle Database on a single physical server for branch offices or smaller organizations. DLP detections servers and the DLP Enforce platform can also be hosted in environments, such as Amazon and Azure.

Configuration Flexibility

Symantec offers a wide variety of configuration and deployment options, and can readily scale from midsize to large global organizations. Network and storage solutions can be deployed as a software installation, a virtual instance or cloud services, with integrations into numerous Web proxy and email infrastructures and cloud services (e.g., Box, Office 365 and Gmail).

DLP Advanced Detection

Symantec supports a wide variety of advanced detection capabilities, including Vector Machine Learning (VML), Indexed Data Matching (IDM) and fingerprinting. Clients specifically mention Exact Data Matching (EDM) feature as a key capability, reporting that EDM greatly increases the fidelity of inspected data and reduces false positives. Prebuilt policies for detecting Competitor Communications, Financial Information, Offensive Material, Job Hunting and DLP Avoidance are also provided.

Internationalization Support

Symantec DLP has been deployed in more than 100 countries, with the DLP Management System and DLP Endpoint Agent localized for more than 25 languages.

DLP Management System

Enforce Management is used to define, deploy and enforce DLP and security policies across endpoint, network, storage and the cloud. The Enforce Server administration console provides a centralized, Web-based interface for deploying detection servers, authoring policies, remediating incidents and managing the system, all with role-based access controls. The console's advanced reporting module includes user risk-based reporting to prioritize incident response.

DLP IT Analytics is an advanced reporting and analytics module that enables DLP program managers to easily create reports, dashboards and KPI scorecards. It provides deep analysis via pivot tables and custom filters, and it can explore DLP data without knowledge of database schema or query languages.

DLP Vendor Integrations

Symantec DLP has a wide variety of integrations with EDRM, IT GRC tools, UEBA, mobile security, cloud-based hosted services, SSL visibility devices, encryption, data classification and data-archiving solutions. Symantec DLP offers a rich set of APIs for development of custom response actions, workflows, unique in-house proprietary file types and enterprise issue-ticketing systems.

Zecurion

Zecurion offers enterprise DLP through Zlock (endpoint), Zgate for network DLP and Zdiscovery for data-at-rest scanning, as well as Mobile DLP for iOS and Android devices. Although it is based in Moscow, Russia, Zecurion has a presence in the U.S., with an office in New York City.

Product: Zecurion DLP — Zlock, Zgate and Zdiscovery

DLP Endpoint

Zlock has strong Windows support, with full archiving capabilities of all data interactions on Windows. However, the Mac endpoint is limited in features, and there is no agent support for Linux.

DLP Discovery

Zdiscovery can scan SMB and NFS file shares, Microsoft Exchange, SharePoint, and Microsoft Dynamics CRM content repositories, as well as Microsoft SQL Server and Oracle Databases for structured data.

DLP Network

Zgate can monitor traffic out-of-band, function in-line via ICAP and SMTP proxy integration, or function as its own MTA and Web proxy. HTTPS decryption is also supported as a part of the Zgate Web proxy.

Ease of Deployment

Zecurion can be deployed as an appliance, software installation or virtual appliance via VMware.

Configuration Flexibility

Zecurion has wide ICAP and SMTP proxy support, as well as its own Zgate proxy for mail and Web.

DLP Advanced Detection

Zecurion supports many advanced detection capabilities, including linguistic analysis, SmartID (a self-training technology based on Bayesian methods), analysis of transliterated and masked text and image file fingerprinting, and OCR support.

Internationalization Support

Zecurion recognizes 190 different language types, with support for English, Russian, Czech, Slovak, Greek, German, Spanish, French, Italian, Arabic, Turkish, Malaysian, Korean and Hindi, among other regional and localized dialects.

DLP Management System

The Zecurion management system supports centralized policy configuration and can provide reports and event data to administrators.

DLP Vendor Integrations

Zecurion does not have significant external vendor partnerships to enhance its DLP product line at this time.

Context

DLP is experiencing a renaissance through a "second wave" of adoption. As noted in the "Hype Cycle for Data Security, 2015," DLP has moved out of the Trough of Disillusionment and is climbing toward the Plateau of Productivity. There are several reasons this has taken place during the past two years.

First, breach activities have engulfed organizations in nearly every sector of the global economy. Although DLP is not designed to stop data theft in every conceivable scenario (and was never intended to do so), it can provide a key element of data security when used in concert with other detect and respond technologies. Few data security controls can delineate between users with deliberate intent to exfiltrate sensitive data and those who inadvertently disclose it. This has created an environment in which organizations are scrambling for security tools that can provide any additional visibility and context to aid in the detection of and response to data security incidents.

The first wave of DLP adoption that drove the market into the Trough of Disillusionment focused on DLP as a data security "silver bullet." It was often marketed as a way to identify and stop every case of accidental data loss and purposeful data theft. The market has since matured and evolved. Buyers and sellers in this market have become aware that enterprise DLP is a key piece of a broader data life cycle process supported by technology, as opposed to DLP simply being another technology buying decision.

Specifically, the most-significant use cases for enterprise DLP have emerged as:

- Regulatory compliance
- IP protection
- Data visibility and monitoring

Each use cases requires emphasis (and thus weighting) on a different combination of critical capabilities for the products, as detailed below. This means that versatility and strength in many areas is critical, as IT security leaders are forced to grapple with data security across a wider range of use cases in their organizations. The critical capabilities for enterprise DLP defined in this research represent the most important of these functional characteristics, based on the data security trends in the market during the next several years.

Product/Service Class Definition

Enterprise DLP tools enable the dynamic application of policy based on the assessment of content determined at the time of an operation. Enterprise DLP describes a set of technologies and inspection techniques used to classify information content contained within an object, such as a file, an email, a packet, an application or a data store while at rest (i.e., data at rest), in use (i.e., data in

use on an endpoint system) or in transit over the network (i.e., data in motion). In addition, it describes the ability to dynamically apply a policy action, such as logging, redaction of sensitive content, report, classify, relocate, tag, encrypt and apply EDRM protections to data. Organizations should understand the use of DLP technologies to develop, educate and enforce better business practices concerning the handling and transmission of sensitive data.

DLP is a nontransparent control, which means it can be intentionally visible to an end user, with the primary value proposition of changing user behavior. This is different from transparent controls, such as firewalls and antivirus programs, which are unseen by end users. Nontransparent controls represent a cultural shift for many organizations, so it's critical to have business involvement in the requirements for planning and implementing a DLP initiative.

Critical Capabilities Definition

DLP Endpoint

Commonly called "data in use," DLP endpoint is defined as software that resides on an endpoint system to determine how sensitive data is being used or manipulated by end user activity. Copy, paste, save, open, and print operations and screen captures are common DLP endpoint capabilities.

DLP endpoint solutions prevent users from transferring confidential data to removable storage; copying and pasting data into documents; printing data, sending data outbound over communication protocols or through third-party applications (e.g., Skype, Jabber and WebEx) even when disconnected from the corporate network. DLP endpoint can also monitor when sensitive data is copied to a client's machine.

DLP Discovery

Commonly called "data at rest," DLP discovery is defined by the ability to discover data in unstructured or semistructured content types. The discovery of on-premises data repositories and cloud storage locations via native-API integrations with cloud services are increasingly important.

DLP discovery is able to scan a wide variety of on-premises and cloud-hosted content repositories for the discovery of sensitive data. On-premises content repositories typically include local file shares, such as Server Message Block (SMB) and Network File System (NFS); Microsoft Exchange; Microsoft SharePoint; EMC Documentum; intranet websites and Web-based repositories, including content management systems and wikis; and Lotus Notes/Domino. Cloud-hosted content repositories typically include Box, Dropbox, Google Drive, Microsoft OneDrive for Business, Microsoft Exchange Online and Microsoft SharePoint Online.

DLP Network

Also called "data in motion," DLP network is defined by the ability to monitor sensitive data over network protocols (e.g., email, Web, FTP and IM). DLP network is critical for organizations that can't deploy endpoint DLP to every system, and it's often a starting point for regulatory compliance.

DLP network solutions provide the ability to scan for sensitive data over a wide range of network communication protocols — most commonly, HTTP, HTTPS, FTP, email and IM. More-sophisticated products can operate beyond that of a Web or email proxy to analyze data movement over any port or protocol that it can accurately decode, decrypt and understand. DLP network products are delivered as either physical appliances or in a virtual appliance form factor, and can be deployed in-line, as a proxy for network traffic, or out-of-band using a network tap, SPAN port, or other means to redirect and replay network traffic.

Ease of Deployment

Easy of deployment assesses the simplicity of the initial installation and ongoing operations. This is inversely related to the critical capabilities of configuration flexibility and DLP advanced detection, which afford high degrees of customization.

Regulatory compliance extends from large to small organizations, and often requires easy-to-implement prebuilt policies that are specifically focused on financial data, HIPAA, PCI and PII data types. Use cases for IP protection, as well as data visibility and monitoring, place a lower priority on ease of deployment, because, in many complex network and end-user computing environments, sensitive data is difficult to track or monitor accurately.

Configuration Flexibility

Configuration flexibility includes the ability to granularly tune DLP system operations and multiple options for DLP deployment. Deployment of the system as software, hardware or a virtual appliance, as well as supported operating environments and policy options, is evaluated.

Large organizations that have diverse requirements and deployment environments value configuration flexibility. Predefined policies and default system configurations are usually a starting point for tailoring DLP solutions to fit their precise requirements. These organizations require policy configuration interfaces; remediation; quarantine; notification; user justification; a blend of network, endpoint and discovery DLP; platform support (such as Microsoft Windows, Mac, Linux and Unix); special use cases (such as social media); system tools that support precise configurations of system operational parameters; and third-party integration with proxy services, mail transfer agents, identity and access management (IAM), security information and event monitoring (SIEM), and EDRM. Smaller organizations and organizations that are not looking to address complex DLP use cases (such as IP protection or monitoring complex environments) typically do not require a high degree of configuration or remediation flexibility.

DLP Advanced Detection

DLP advanced detection includes a diverse range of powerful detection techniques, such as partial document matching, structured data fingerprinting, machine learning, lexicons and watermarking, along with various techniques used to reduce false positives.

DLP advanced detection capabilities go beyond basic string and pattern matching of sensitive data to include semistructured content (such as form data and handwritten data), as well as OCR and

other types of image recognition. DLP advanced detection also uses integrations with file encryption and decryption capabilities (on DLP endpoint, DLP discovery and DLP network), as well as recognizing how content may be packed or compressed, encryption algorithms have been used or electronic digital rights have been applied.

Internationalization Support

Internationalization support includes the ability to deploy to users in multiple countries or geographies, and provides localized end-user and management interfaces, support for a variety of languages and character sets, separation of duties by geographic location and localized DLP policies.

Internationalization support ultimately means enabling the deployment of a DLP system to users located in more than one country, and providing the user interfaces in multiple languages. Critical capabilities include user and management interface localization; DLP engines that support non-English languages; support for left-to-right and right-to-left text; UFT8/16/32, double-byte character support (e.g., Chinese, Japanese and Korean); separation of duties and distinct management roles with obfuscation of sensitive data based on role (e.g., first-level triage, second-level event remediation and third-level compliance oversight); geographic reach (e.g., sales, system integration and support); support for multiple concurrent policies that may be applied differently in different countries; and support for complex case management across different policy jurisdictions.

DLP Management System

DLP management system includes the configuration of policies and remediation mechanisms, the definition of management and user roles, triage, and the identification of events and logical administrative workflows. The DLP management system should be easy for administrators to read, interpret and use.

The deployment of the DLP management system should include options such as software installation, hardware appliance and virtual appliances. DLP management systems often support deployment and operation in a cloud-hosted environment, such as Amazon Web Services or Microsoft Azure. The workflow and ongoing operation of the DLP management system must be logical and flexible enough to meet the needs of the three primary use cases of regulatory compliance, IP protection and data visibility.

DLP Vendor Integrations

Enterprise DLP solutions integrate with security products, such as SIEM for event management, EDRM for content protections, and cloud access security brokers (CASBs) for visibility and control of data in motion to cloud services, as well as UEBA for context awareness for users of sensitive data.

DLP vendor integrations should provide users with compelling reasons to use two different types of security technologies together, to achieve added value not recognized from each product deployed on its own. Many DLP vendors can share DLP network policy via ICAP with CASB or SWG products. UEBA products can provide deeper analytics and context-awareness to supplement the

content-awareness that enterprise DLP products offer natively. Events, incidents and evidence from DLP management systems must be exportable and consumable by products such as SIEM and log management platforms, as well as incident response products for the remediation of issues. Integrations with SIEM vendors to provide more than just an export capability for events is a key integration point for enterprise DLP products.

Incident response tools, particularly those that can provide remediation, are another integration point where DLP systems can contribute event-specific data about file access by a specific user on a system. This event data can be linked with incident response tools as part of remediation to provide a better understanding of the user activities related to data loss.

Use Cases

Regulatory Compliance

Data controlled by governing regulations, such as payment card, employee or customer personal data; medical records; or other legally regulated information.

Regulations do not explicitly mandate the use of enterprise DLP to protect data, although there are many instances in which data protection requirements lead organizations to deploy enterprise DLP products. For example, the Payment Card Industry Data Security Standard (PCI DSS) has stringent requirements for inventorying where cardholder data resides, tracking how it's accessed and determining how it moves around environments. Although much of the focus of PCI DSS data protection is on encryption, DLP network capabilities are frequently used to ensure that cardholder data is transmitted securely via approved channels, rather than outbound email and Web traffic, which are typically an organization's most significant points of egress. Although DLP is not explicitly mentioned in PCI DSS, it is obvious where it, or something like it, is being implied.

Two mentalities are typically observed around regulatory compliance and DLP:

- The "checking the box" mindset
- Data-centric protection

It is universally held that the checking-the-box mentality is not very useful, and, because enterprise DLP is not explicitly required, auditors are unlikely to be persuaded that its presence in an environment infers full compliance with requirements. In the latter case, data protection can be demonstrated through a well-architected approach, although effectiveness will often hinge on the specific detection techniques used and whether the data is structured or unstructured. Regulatory compliance extends from large enterprises to small organizations. It often requires prioritizing ease of deployment to implement prebuilt policies that most vendors include as part of the enterprise DLP products that are specifically focused on financial data, HIPAA, PCI and PII data types.

Intellectual Property Protection

This organization-specific data includes contract or settlement, product/marketing, service manual, formulary, and engineering data (CAD/computer-aided manufacturing [CAM]).

Organizations are increasingly sensitive to the need to maintain the value of their IP by controlling access to it, as well as its distribution and use. This has become a more important, because of the growing complexity of the digital business environment and particularly because of global supply chains, which frequently include operations in regions without strong IP protections. IP can take many forms, including negotiated contracts or settlements, product specifications, service manuals, analyses, chemical formulas, patent applications and CAD/CAM files. Enterprise DLP is a critical element in organizations' strategies for IP protection. IP protection frequently begins with DLP endpoint for data in use, applying DLP advanced detection to these endpoint agents to handle the need for complete content inspection at the point of data use.

Data Visibility and Monitoring

DLP is used as a tool to observe and monitor the decisions that users make with specific types of data, without notifying end users in the event of data policy violations.

Although enterprise DLP is a technology designed to intercept and remediate the unauthorized use of sensitive data, organizations can choose to deploy enterprise DLP products in a "monitor only" mode. Some organizations leverage this use case for monitoring and discovery before migrating to other use cases that involve automated action and protection. Other organizations have no intent to remediate, but rather seek the ability to measure and analyze the collected data for insight into the existence of sensitive data within the organization and how it is being treated. Given this requirement for the broad visibility of data flowing through the organization, all three components of enterprise DLP (endpoint, network and discovery) will need to be deployed.

Vendors Added and Dropped

Added

Clearswift and Somansa are new to the Critical Capabilities research this year. Digital Guardian (formerly Verdasys), Intel Security (formerly McAfee) and Forcepoint (formerly Websense) were added due to name changes and acquisitions.

Dropped

Absolute Software, CA Technologies, Palisade Systems, Safend, Trend Micro and Trustwave were not evaluated for this Critical Capabilities research.

Code Green Networks (acquired by Digital Guardian), McAfee (now Intel Security) and Websense (now Forcepoint) were dropped due to name changes and acquisitions.

EMC (RSA) has been dropped due to its announcement of the end-of-life status of its DLP product business.

Inclusion Criteria

The inclusion criteria represent the specific vendor attributes analysts believe to be necessary for inclusion in this research:

- $8 million in annual revenue specifically for enterprise DLP products.
- The ability to detect sensitive content in network traffic, without the need for an endpoint agent.
- The ability to detect sensitive content in either discovery scans (data at rest) or endpoint (data in use) — Products that can solve for all three scenarios of network, endpoint and data discovery will be viewed as more complete.
- A relatively sophisticated, centralized policy and event management console.
- The ability to detect sensitive content using at least three of the following content-aware detection techniques: partial and exact document matching, structured data fingerprinting, statistical analysis, extended regular expression matching, and conceptual and lexicon analysis.
- The ability to support the detection of sensitive data content in structured and unstructured data, using registered or described data definitions.
- The ability to block, at minimum, policy violations that occur via email communications.
- General availability as of 30 September 2015.

Gartner analysts consider that some aspects of the company's product execution and vision merit inclusion.

Table 1. Weighting for Critical Capabilities in Use Cases

Critical Capabilities	Regulatory Compliance	Intellectual Property Protection	Data Visibility and Monitoring
DLP Endpoint	11%	22%	15%
DLP Discovery	11%	11%	15%
DLP Network	22%	11%	15%
Ease of Deployment	15%	5%	10%
Configuration Flexibility	5%	15%	10%
DLP Advanced Detection	10%	15%	10%
Internationalization Support	7%	7%	7%
DLP Management System	17%	10%	10%
DLP Vendor Integrations	2%	4%	8%
Total	**100%**	**100%**	**100%**
As of April 2016			

Source: Gartner (April 2016)

This methodology requires analysts to identify the critical capabilities for a class of products/services. Each capability is then weighed in terms of its relative importance for specific product/service use cases.

Critical Capabilities Rating

Each of the products/services has been evaluated on the critical capabilities on a scale of 1 to 5; a score of 1 = Poor (most or all defined requirements are not achieved), while 5 = Outstanding (significantly exceeds requirements).

Table 2. Product/Service Rating on Critical Capabilities

Critical Capabilities	Clearswift	Digital Guardian	Fidelis Cybersecurity	Forcepoint	GTB Technologies	InfoWatch	Intel Security	Somansa	Symantec	Zecurion
DLP Endpoint	2.8	4.8	3.0	4.0	3.5	3.3	3.7	2.7	3.8	3.4
DLP Discovery	2.7	3.7	3.0	4.2	4.3	3.4	3.6	3.2	4.2	3.1
DLP Network	2.9	3.7	4.9	4.2	4.0	3.5	3.9	2.7	4.0	3.6
Ease of Deployment	3.1	2.7	2.7	3.0	3.2	3.0	3.0	3.2	3.0	3.2
Configuration Flexibility	3.0	4.4	4.4	4.1	3.9	3.2	4.0	3.0	4.4	3.0
DLP Advanced Detection	3.1	4.3	4.3	4.3	3.9	3.8	4.1	2.7	4.3	3.6
Internationalization Support	3.0	4.3	4.3	4.7	4.3	4.4	4.7	3.0	4.7	4.4
DLP Management System	3.1	4.3	3.6	4.1	3.9	3.3	3.8	3.3	4.0	3.4
DLP Vendor Integrations	2.1	3.1	2.7	3.3	2.5	1.0	4.3	2.3	4.0	1.0
As of April 2016										

Source: Gartner (April 2016)

Table 3 shows the product/service scores for each use case. The scores, which are generated by multiplying the use case weightings by the product/service ratings, summarize how well the critical capabilities are met for each use case.

Table 3. Product Score in Use Cases

Use Cases	Clearswift	Digital Guardian	Fidelis Cybersecurity	Forcepoint	GTB Technologies	InfoWatch	Intel Security	Somansa	Symantec	Zecurion
Regulatory Compliance	2.95	3.90	3.76	4.00	3.82	3.39	3.78	2.96	3.95	3.40
Intellectual Property Protection	2.91	4.17	3.74	4.09	3.80	3.36	3.89	2.89	4.08	3.32
Data Visibility and Monitoring	2.87	3.95	3.65	4.00	3.76	3.25	3.84	2.90	4.02	3.22
As of April 2016										

Source: Gartner (April 2016)

To determine an overall score for each product/service in the use cases, multiply the ratings in Table 2 by the weightings shown in Table 1.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Magic Quadrant for Enterprise Data Loss Prevention"

"Hype Cycle for Data Security, 2015"

"How to Choose Between Enterprise DLP and Integrated DLP Approaches"

"Data Loss Prevention in Microsoft Office 365"

"Anticipating and Overcoming the Five Key Obstacles to Success in Enterprise DLP Deployments"

"Overcome the Limitations of DLP for Mobile Devices"

"Market Guide for Cloud Access Security Brokers"

"Market Guide for User Entity Behavior Analytics"

"How Products and Services Are Evaluated in Gartner Critical Capabilities"

Evidence

Vendor surveys and recorded product demos from vendors represented in this Critical Capabilities research.

Vendor briefings with vendors represented in this Critical Capabilities research.

More than 370 Gartner client inquiry calls centered on DLP from March 2015 to March 2016.

Customer reference surveys — delivered in an online survey to 48 customers, and live interviews with 10 customers of vendors represented in the "Magic Quadrant for Enterprise Data Loss Prevention."

Gartner secondary research related to company financials and market-size metrics.

Critical Capabilities Methodology

This methodology requires analysts to identify the critical capabilities for a class of products or services. Each capability is then weighted in terms of its relative importance for specific product or service use cases. Next, products/services are rated in terms of how well they achieve each of the critical capabilities. A score that summarizes how well they meet the critical capabilities for each use case is then calculated for each product/service.

"Critical capabilities" are attributes that differentiate products/services in a class in terms of their quality and performance. Gartner recommends that users consider the set of critical capabilities as some of the most important criteria for acquisition decisions.

In defining the product/service category for evaluation, the analyst first identifies the leading uses for the products/services in this market. What needs are end-users looking to fulfill, when considering products/services in this market? Use cases should match common client deployment scenarios. These distinct client scenarios define the Use Cases.

The analyst then identifies the critical capabilities. These capabilities are generalized groups of features commonly required by this class of products/services. Each capability is assigned a level of importance in fulfilling that particular need; some sets of features are more important than others, depending on the use case being evaluated.

Each vendor’s product or service is evaluated in terms of how well it delivers each capability, on a five-point scale. These ratings are displayed side-by-side for all vendors, allowing easy comparisons between the different sets of features.

Ratings and summary scores range from 1.0 to 5.0:

1 = Poor or Absent: most or all defined requirements for a capability are not achieved

2 = Fair: some requirements are not achieved

3 = Good: meets requirements

4 = Excellent: meets or exceeds some requirements

5 = Outstanding: significantly exceeds requirements

To determine an overall score for each product in the use cases, the product ratings are multiplied by the weightings to come up with the product score in use cases.

The critical capabilities Gartner has selected do not represent all capabilities for any product; therefore, may not represent those most important for a specific use situation or business objective. Clients should use a critical capabilities analysis as one of several sources of input about a product before making a product/service decision.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp