FORRESTER®

FOR SECURITY & RISK PROFESSIONALS

Market Overview: Data Loss Prevention

DLP Suite Adoption Holds Steady As DLP Becomes A Feature And Managed Services Offer An Attractive Option

by Heidi Shey
May 2, 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. Today, S&R pros can source DLP capabilities in a variety of ways. This report examines the factors driving renewed interest in DLP, the state of DLP suite adoption, and the pros and cons of different approaches of bringing DLP capabilities into the enterprise.

Key Takeaways

DLP Suite Interest And Adoption Hold Steady
Compared with their North American counterparts, European enterprises are more likely to adopt a DLP suite in 2016. Globally, the manufacturing and retail sectors are leading DLP investment.

The DLP Market Landscape Has Expanded
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.

Market Overview: Data Loss Prevention

DLP Suite Adoption Holds Steady As DLP Becomes A Feature And Managed Services Offer An Attractive Option

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

May 2, 2016

Table Of Contents

Notes & Resources

Forrester interviewed 23 vendor companies: BAE Systems, Check Point, CipherCloud, CipherMail, Clearswift, CloudLock, CoSoSys, Digital Guardian, Elastica (Blue Coat Systems), Fidelis Cybersecurity, Forcepoint (formerly Raytheon|Websense), Identity Finder, Intel Security, Microsoft, Mimecast, Proofpoint, Secure Islands (Microsoft), Symantec, Trend Micro, Trustwave, Watchful Software, ZixCorp, and Zscaler.

Related Research Documents

Rethinking Data Discovery And Data Classification Strategies

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

Data Loss Prevention Enforces Policies For Sensitive Data

According to our data, of the 49% of global enterprise security decision-makers whose firms have suffered a breach of sensitive data — that they know of! — in 2015, the top three types of breached data were personally identifiable information, authentication credentials, and intellectual property.[1] What's more, 37% of these breaches were the result of an insider action — either deliberate or unintentional. DLP solutions aim to prevent both unintentional data loss and intentional exfiltration of data. Forrester defines DLP as:

> *A capability that detects and prevents violations to corporate policies regarding the use, storage, and transmission of sensitive data. Its purpose is to enforce policies to prevent unwanted dissemination of sensitive information.*

DLP Is A Capability, Not A Single Product

What is data loss prevention anyway? You could argue that it's an overarching security strategy rather than a technology solution. You could also say it's a capability rather than a product. Both are true. S&R pros create security strategies and make investments for the purpose of protecting data and preventing data loss. To do so effectively requires a combination of capabilities, from policies to tools to corporate culture. DLP tools are essentially policy enforcement engines, providing firms with the capability to enforce policies in order to prevent data loss. Forrester believes that DLP in the future — and there are already signs that we are on our way — will be a capability or feature of integrated security solutions rather than a single product.

Ongoing Security Challenges Drive Renewed Momentum For DLP Capabilities

In 2009 and 2010, DLP was a bright, shiny star: an exciting, much-hyped technology solution bursting with promise. As stories of difficult or failed implementations emerged in 2011, excitement waned.[2] Today, however, a combination of compounding challenges is driving renewed interest in DLP. The challenges include:

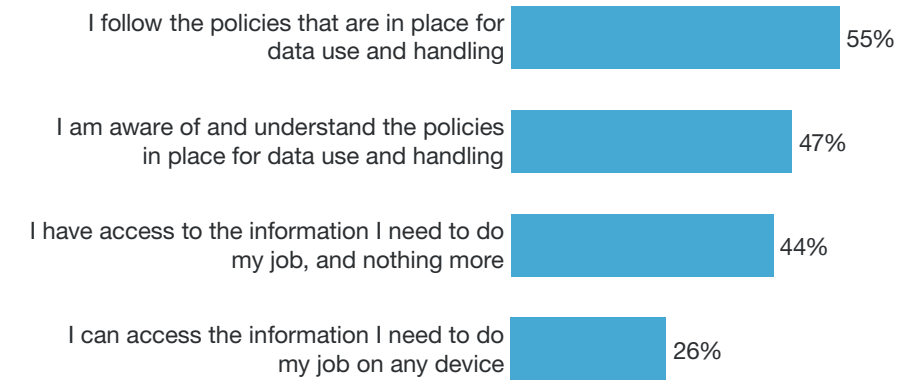
- **An inability to enforce data use and handling policies.** An inability to enforce policy is a pressing concern today given both the dire state of employee awareness of proper data handling and the array of sensitive data that employees can access from a variety of devices (see Figure 1). A firm can have a policy that prohibits employees from copying sensitive data to an external USB drive, but policy alone won't stop the workforce from doing it. DLP solutions can help S&R pros discover actions employees take that violate security or privacy policies and enforce these policies while educating the workforce.
- **The fact that addressing privacy requires more than just regulatory compliance.** Compliance with such regulations as the EU's General Data Protection Directive and various country requirements for data transfer and data sovereignty is just one facet of privacy concerns.[3] Customer insights and customer experience initiatives that raise ethical issues of internal data use

are another. Firms must align these policies and policy enforcement not just to avoid the wrath of regulators, but also to maintain and preserve customer trust.[4] DLP solutions can help enforce data-handling measures outlined in customer-facing privacy policies.

› **The demand to meet both security and business needs for using cloud services.** Whether it's information workers bringing their own preferred SaaS services and tools to work with them or enterprise-deployed SaaS applications, sensitive data is at risk (see Figure 2). There is a high demand for visibility into data movement and use, along with the capability to enforce use and handling policies of data going into and stored in the cloud.[5] DLP providers like Digital Guardian, Forcepoint, Symantec, and Trend Micro have cloud DLP capabilities to help firms restrict the movement of sensitive data to the cloud. DLP is also a capability found in cloud access security intelligence (CASI) solutions today.[6]

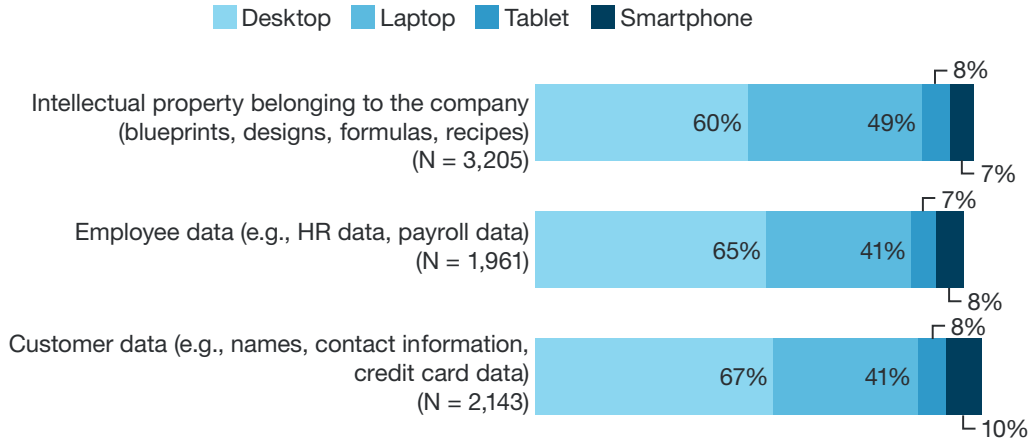
FIGURE 1 The State Of Employee Policy Awareness And Sensitive Data Access

1-1 Information workers understand but don't always follow policy for data use and handling



Base: 6,351 global information workers (20+ employees)

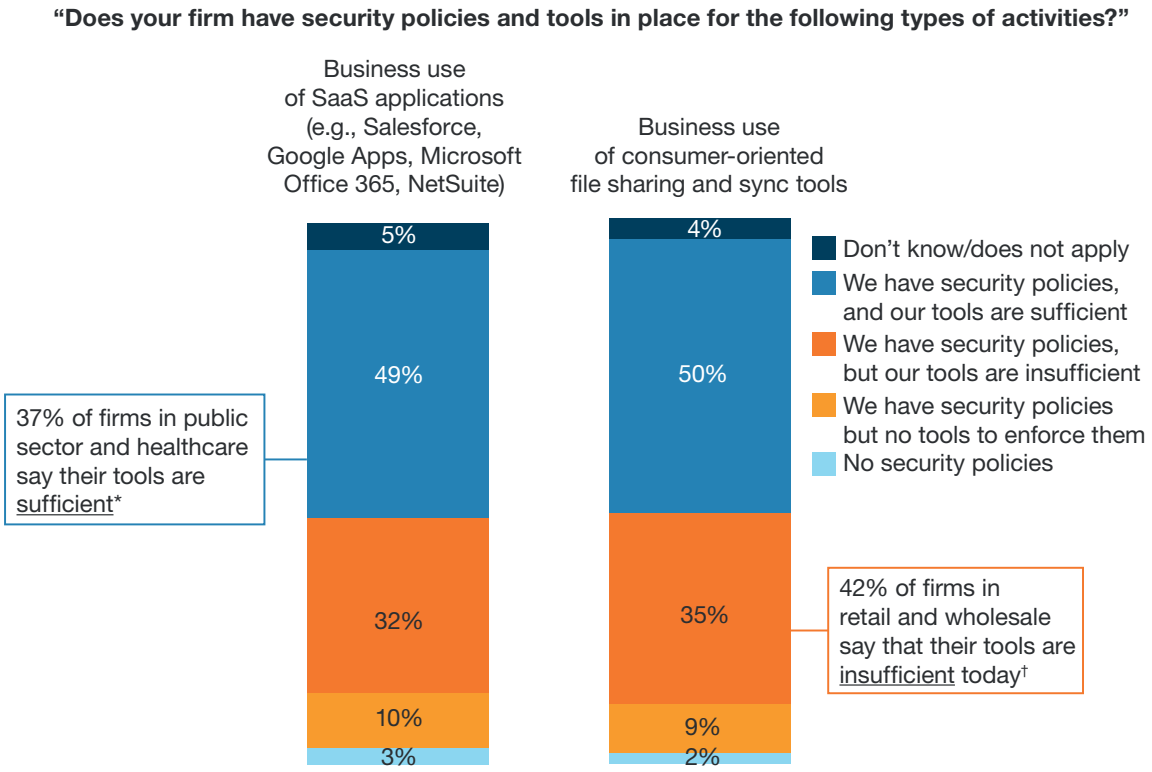
1-2 Information workers access data from a variety of devices



Base: global information workers who have access to the specified type of data (20+ employees)

Source: Forrester's Global Devices And Security Workforce Survey, 2015

FIGURE 2 One-Third Of Firms Say Their Tools For Enforcing Policy Are Insufficient



Base: 1,713 global security decision-makers (1,000+ employees)
*Base: 195 global public sector and healthcare security decision-makers (1,000+ employees)
†Base: 125 global retail/wholesale security decision-makers (1,000+ employees)

Source: Forrester's Global Business Technographics® Security Survey, 2015

Adoption Of DLP Solution Suites Remains Steady

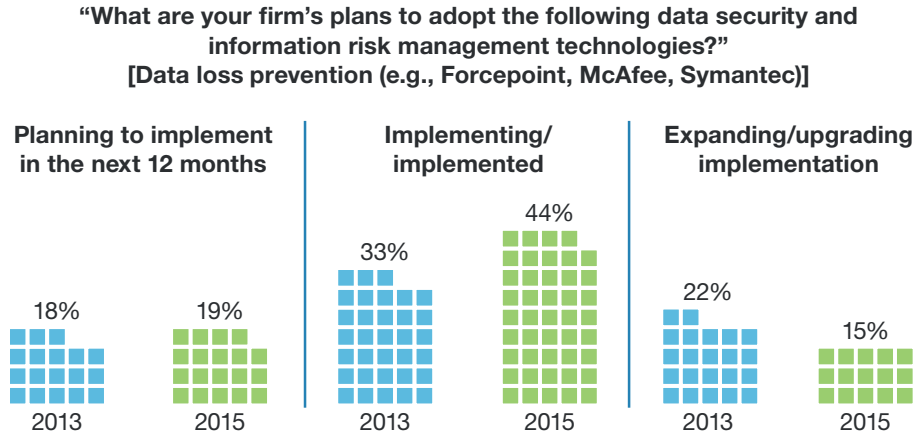
Interest in DLP suites has held steady during the past few years, and DLP suites were in use in many enterprises in 2015. Acquiring and shoring up existing DLP capabilities remains on the security agenda, and enterprises are sustaining interest and investment in DLP suites. Today, we see that:

› **DLP solution suites continue their upward trajectory.** In 2015, 44% of North American and European enterprise decision-makers had implemented or were in the process of implementing comprehensive DLP solutions and suites from vendors like Symantec, Intel Security, and Forcepoint (formerly Raytheon|Websense), while an additional 15% indicated plans to expand an existing implementation and 19% had plans to implement over the next 12 months (see Figure 3). Compared with 2013, plans to implement are holding steady, on top of a growing adopted base.

› **European enterprises are more likely to have a net new implementation in 2016.** When this survey was fielded mid-2015, 22% of European security decision-makers indicated that their firms had plans to implement a DLP suite within the next 12 months, compared with 16% of North American enterprise decision-makers (see Figure 4). Overall, indicators of interest and growth (plans to implement as well as intent to expand and upgrade existing implementations) are respectable across North America and Europe.

› **Manufacturing and retail firms lead the charge for net new DLP suite investment.** Globally, 24% of security decision-makers at manufacturing firms plan to implement a DLP suite in 2016, driven by concerns for protecting intellectual property. Twenty-three percent at retail and wholesale organizations are planning the same, driven by interest in protecting customer data (see Figure 5). Growth in public sector and healthcare, however, is less robust.

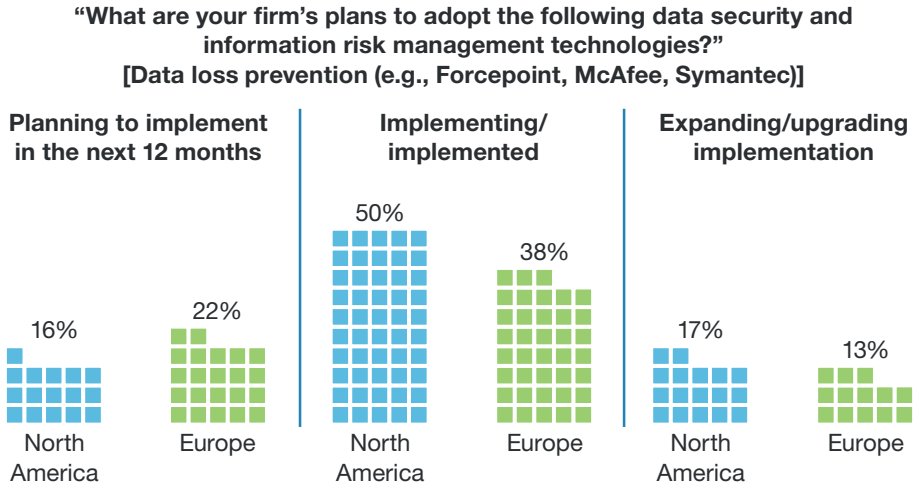
FIGURE 3 DLP Suite Interest Remains Steady



Base: 436 (2015) and 379 (2013) North American and European security decision-makers (1,000+employees)

Source: Forrester's Global Business Technographics® Security Survey, 2015 and Forrsights Security Survey, Q2 2013

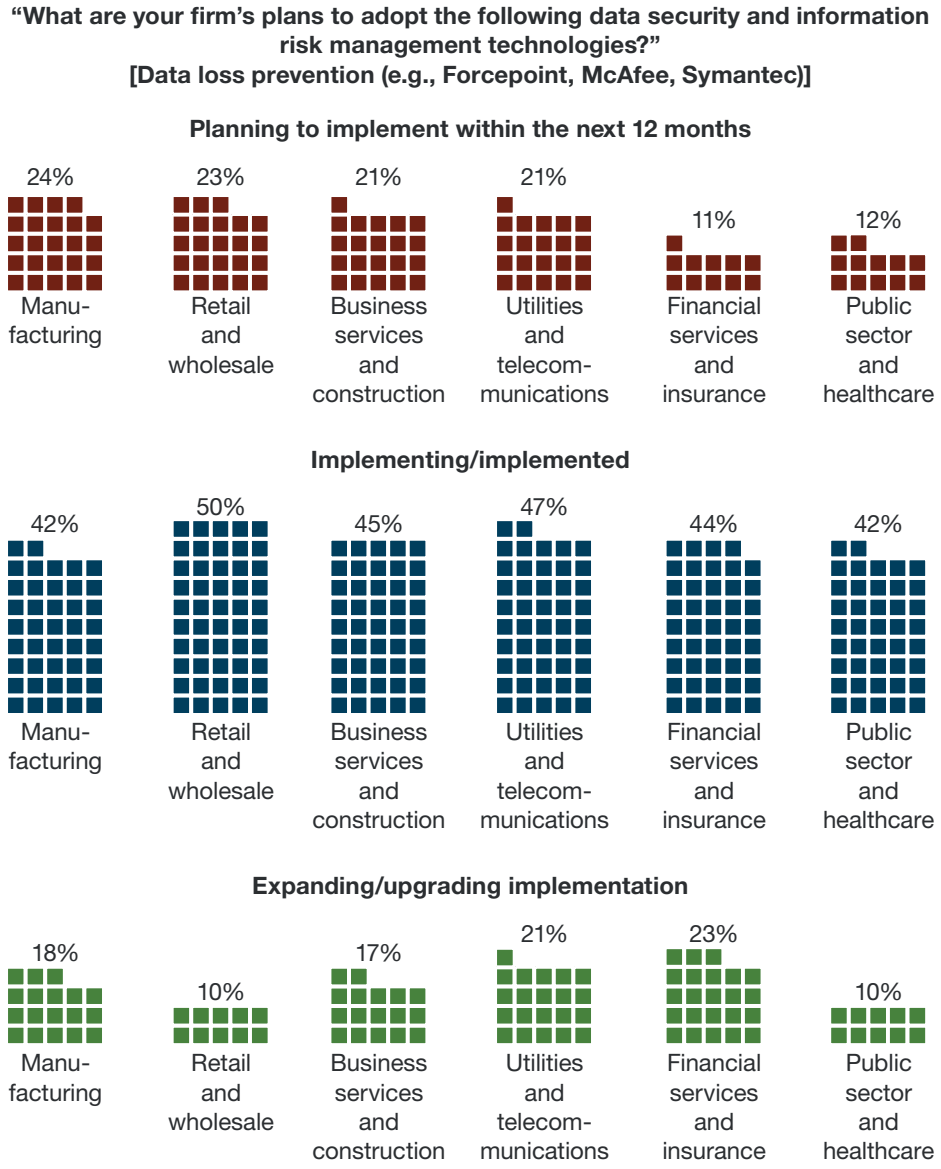
FIGURE 4 DLP Suite Adoption By Region, 2015



Base: 232 North American and 204 European security decision-makers (1,000+ employees)

Source: Forrester's Global Business Technographics® Security Survey, 2015

FIGURE 5 Global Enterprise Adoption Of DLP Suites By Industry, 2015



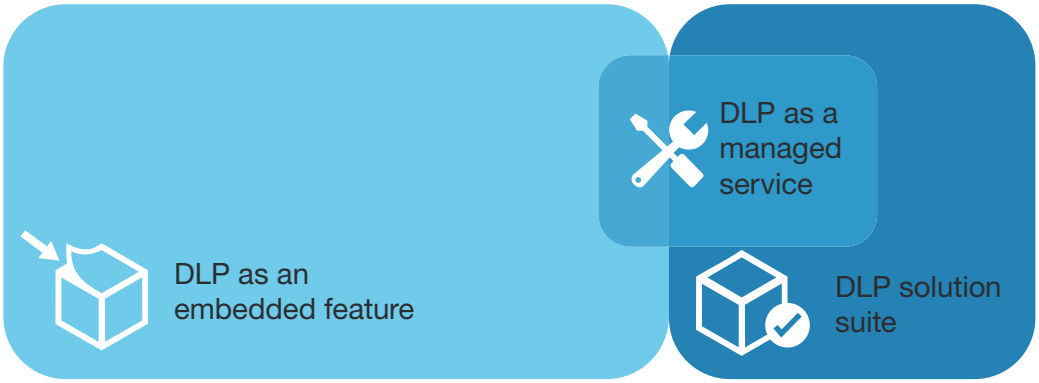
Base: 40 to 184 global security decision-makers working in the specified industries

Source: Forrester's Global Business Technographics® Security Survey, 2015

The DLP Market Expands In Three Dimensions

In the past, DLP was a distinct market with a set of well-defined vendors offering specific products, namely DLP suites. Today's DLP story is of a diverse market, as DLP evolves from a product to a feature. There are a multitude of ways for S&R pros to acquire DLP capabilities as the vendor landscape expands in three ways: 1) DLP as an embedded feature; 2) DLP solution suites; and 3) DLP as a managed service (see Figure 6).

FIGURE 6 A View Of Today's DLP Market



Embedded DLP Offers Easier Implementation But No Central Policy Management

Typically, embedded DLP will address a specific channel of data loss, such as email, with simplified management of DLP policies for that specific channel. DLP here is a feature in a next-generation firewall, cloud security solution, endpoint security solution, email security gateway, web security gateway, or other security tool. There is a diverse array of vendors with DLP as a feature in their offerings, ranging from BAE Systems to ZixCorp. In the DLP-as-an-embedded-feature approach, S&R pros:

- **Gain targeted coverage and control in a way that is relatively easy to implement.** If the DLP capabilities aren't a default native capability already, it's usually as simple as turning on DLP capabilities and selecting your required policy templates. For example, in Microsoft Office 365, DLP is a feature; setting up and configuring DLP policies takes minutes. On a Check Point security gateway, DLP is a software blade that you can activate. With DLP as a feature, subsequent customization to DLP policies is straightforward. The upfront work regarding DLP processes and policies still applies and can help to support a successful implementation of DLP capabilities.
- **But need to rely on multiple solutions to cover all of extrusion channels.** Depending on your requirements, DLP as a feature may fall in the DLP-lite camp with existing policy templates and single-channel focus. While you can take steps to cover your major channels of data loss (web,

endpoint, etc.) the way you would with a solution suite, DLP as a feature means you're using a diverse array of tools from different vendors to accomplish this, with no centralized management console across your different data loss channels. It then becomes incumbent on S&R pros to develop granular policies across multiple solutions that do more than default to policy templates that cover basic compliance obligations but not intellectual property or sensitive corporate data.

DLP Suites Offer Centralized Policy Management But Are Often Slow To Innovate

These are the solutions that S&R pros are most likely to associate with DLP, covering data at rest, in motion, and in use. These DLP solution suites can address multiple channels of data loss, such as email, endpoint, web, and cloud, and typically centralize management of DLP policies. This category is consolidating into a handful of major players, who are increasingly morphing into integrated security solutions with elements of prevention, threat detection, and response. Examples of vendors include CA Technologies, Clearswift, Digital Guardian, Forcepoint, Intel Security, Trend Micro, Trustwave, and Symantec. In the DLP suite approach, S&R pros:

- **Can source all of their DLP capabilities from a single vendor.** With a DLP suite, S&R pros can cover all of their channels of data loss and centralize management of DLP policies. These vendors also have years of experience and expertise, a valuable asset for guiding your firm through the deployment process. This expertise is important because many of the challenges that firms experience with DLP deployments arise from establishing processes and policies for an implementation rather than the technology itself.
- **But may still need another vendor for a new capability or channel.** Some firms look to these DLP suites with the intent of eventually putting together all the pieces to cover every channel of data loss, but ultimately they only utilize one part of the suite (e.g., endpoint DLP) as their DLP initiative progresses and priorities shift over the course of deployment. As the big kids on the DLP playground, these vendors may not be the most nimble with DLP-specific innovation. Take DLP for cloud apps like Box for example; specialized cloud DLP vendors (CloudLock, Netskope, and many others) met this need long before many of the big suites had the capability.

DLP As A Managed Service Offers A Flexible And Attractive Deployment Option

With DLP as a managed service, experts can help you manage processes, policies, and infrastructure. Service providers vary in their offerings here today, ranging from managing a full DLP-specific solution suite (like Symantec's) to including DLP capabilities as a part of an adjacent managed service (e.g., email security). These managed services are also distinct from consultative services offerings like those from IBM or HP that can help with the upfront process and policy work required to successfully deploy DLP, and leave the ongoing management and monitoring to you. Examples of managed service providers include Digital Guardian, EY, InteliSecure, and Wipro. With a managed services approach, S&R pros:

- **Can overcome limitations from lack of staff and staff expertise.** A DLP initiative isn't a one-time project; it's an ongoing one that needs continued attention beyond the initial setup. For some firms with staffing and resource constraints, DLP as a managed service provides much welcomed expertise in and focus on deployment and continued monitoring, especially when your service provider has the capability to also escalate and respond to alerts.
- **But can't expect providers to have in-depth contextual knowledge of your business.** Managed services providers will perform reasonably well to help you cover the usual macro use cases for DLP: establishing DLP policies for credit cards, account numbers, ID numbers, SSNs, keyword matches for intellectual property, and integration with classification solutions. Contextual issues may pose a challenge, such as changes to data access or a temporary scope of a user's role.

Recommendations

Future-Proof Your DLP Approach With Data Identity

As DLP evolves from a product to a feature, and as today's DLP suites morph into integrated security solutions and platforms (thus, also turning DLP into a feature), knowing your data (what you are trying to protect!) will no longer be an optional "good to know." Estimate for a three-to-five-year timeline before the DLP market matures into this next phase of ubiquitous DLP as a feature. Get ahead and start now to embrace coming changes, and future-proof your DLP approach by giving data an identity.

Data identity is comprised of attributes such as: 1) who created it; 2) who owns it in the business; 3) where it's located; 4) what its toxicity level is; and 5) who can consume it (read versus write). Today's security tools and DLP solutions are already starting to help make it easier for S&R pros to discover and classify sensitive data, one of the first steps to giving data an identity. User behavior analytics will surface an additional layer of context to help build data identity:

- **Data identity reduces reliance on policy templates and centralized policy management.** Data classification already helps to optimize the value gained from DLP suites today. Data identity, which includes classification and more contextual information, will in the future help to eliminate the need for centralized policy management and policy templates. DLP policy engines can rely on data identity rather than rules that use regular expressions, dictionaries, and keywords to help identify sensitive data and subsequent policy violations.
- **Data identity paves the way for accelerating DLP initiatives, addressing PII and IP.** It will reduce the chasm between using DLP for compliance use cases (like preventing loss of PII and cardholder data) and intellectual property data loss use cases. It also helps firms tackle earlier on protecting data that does not fall under compliance obligations, but is still sensitive. Examples include consumer-generated health data from wearables, biometric data that may be considered protected PII in some jurisdictions and not in others, or machine-generated data from sensors and IoT devices.

› **Data identity optimizes managed security services.** Like DLP suites, DLP as a managed service doesn't disappear. As DLP becomes a feature, it will also be a common feature within a broader managed security service offering, such as a managed email security service. Data identity will reduce the upfront work with DLP policy creation, and create more comprehensive DLP coverage while freeing up time and resources for other tasks — both operational and strategic.

What It Means

DLP As A Feature Will Feed Into Automating Breach Response

Rules of engagement define what a soldier can do or cannot do on the battlefield given a set of circumstances. This allows autonomy and a real-time reaction with an appropriate action without the need to go up the chain of command to ask for permission. In the enterprise, rules of engagement are desperately needed to empower security employees to do the same and respond to possible data breaches quickly:

› **More ubiquitous DLP increases visibility.** More-ubiquitous DLP in the enterprise environment as the result of DLP as a feature will help bring firms one step closer to enabling rules of engagement for automating breach response. While the goal of DLP is to enforce policies so as to prevent the data loss from occurring in the first place, the visibility that DLP capabilities provide is important context for determining rules of engagement.

› **Visibility for security analytics feeds a response index for automated response.** The visibility into data movement and policy violations surfaced by DLP tools is one source of data for security analytics. Firms can use security analytics to create a response index for security events such as a data breach. This response index is what kicks off rules of engagement for an automated response based on the confidence of and potential impact of the particular security event detected. For example, unusual or repeated alerts of DLP policy violations that generate a suspicious pattern when correlated with other security data and categorized as high impact could kick off ROE for a breach response.

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

Survey Methodology

Forrester's Global Business Technographics® Security Survey, 2015

Forrester conducted an online survey fielded in April through June 2015 of 3,543 business and technology decision-makers located in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Forrester's Business Technographics provides demand-side insight into the priorities, investments, and customer journeys of business and technology decision-makers and the workforce across the globe. Forrester collects data insights from qualified respondents in 10 countries spanning the Americas, Europe, and Asia. Business Technographics uses only superior data sources and advanced data-cleaning techniques to ensure the highest data quality.

Companies Interviewed For This Report

BAE Systems

Check Point

CipherCloud

CipherMail

Clearswift

CloudLock

CoSoSys
Digital Guardian
Elastica (Blue Coat Systems)
Fidelis Cybersecurity
Forcepoint (formerly Raytheon|Websense)
Identity Finder
Intel Security
Microsoft
Mimecast
Proofpoint
Secure Islands (Microsoft)
Symantec
Trend Micro
Trustwave
Watchful Software
ZixCorp
Zscaler

Endnotes

[1] Source: Forrester's Global Business Technographics Security Survey, 2015.

[2] Using client feedback, survey data, and input from security leaders in Forrester's security and risk council, we looked at DLP with a different lens to address common pitfalls and implementation challenges. S&R pros need to approach DLP as an ongoing process, not a product or even a one-time project. We designed this report to help you assess the current state of your DLP efforts against data loss vectors and process maturity. See the "Rethinking Data Loss Prevention With Forrester's DLP Maturity Grid" Forrester report.

[3] Forrester outlines the major changes to the EU General Data Protection Regulation to prepare security and risk (S&R) pros for the tough road ahead. See the "Quick Take: EU Gives The General Data Protection Regulation Some Sharp Teeth" Forrester report.

In Asia Pacific, evolving privacy laws also pose challenges for S&R pros, particularly regarding cross-border data transfer requirements. See the "Privacy, Data Protection, And Cross-Border Data Transfer Trends In Asia Pacific" Forrester report.

[4] In 2016, short-sighted firms will make the mistake of thinking that privacy is only about meeting compliance and regulatory requirements at the lowest possible cost, while enlightened ones will recognize it's actually a way to build better customer relationships — built on trust. This brief analyzes the nine most significant privacy developments ahead in 2016 and tells you what to do about them. See the "Predictions 2016: The Trust Imperative For Security & Risk Pros" Forrester report.

[5] Forrester estimates that the broader cloud security market will exceed $2 billion in annual spend by 2020. As enterprises embrace a diverse cloud ecosystem, a new generation of software is emerging to address the security requirements of highly distributed IT infrastructure. These new offerings make up for the missing features of perimeter-based security solutions in their ability to discover, analyze, and control corporate data across bare metal, virtual machines, IaaS, PaaS, and SaaS, and are rapidly maturing into an independent category Forrester calls cloud security solutions. See the "Sizing The Cloud Security Market" Forrester report.

[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.

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.