# THE DEFINITIVE GUIDE TO DATA LOSS PREVENTION

## 2019 EDITION


DIGITAL GUARDIAN®

# TABLE OF CONTENTS

# WHY READ THIS GUIDE?

## WHAT'S OLD IS NEW AGAIN

A number of macro trends are driving the wider adoption of DLP. But as we looked at the resources out there, we couldn't find one source that could provide all the essential information in one place. So we created this guide to provide answers to the most common questions about DLP - all in an easy to digest format.

## HOW TO USE THIS GUIDE

| IF YOU ARE INTERESTED IN LEARNING... | GO TO... |
|---|---|
| **What does DLP look like today** | Five reasons why over 35 vendors now offer DLP<br>Top DLP use cases |
| **How DLP has matured** | The top myths of DLP that could hold you back |
| **How to evaluate DLP providers to find the best fit for your firm** | Evaluating DLP technology providers – the big three criteria<br>DLP managed service provider evaluation checklist<br>DLP deep dive evaluation toolkit |
| **How to streamline internal approval for your DLP project** | How to make a value-based business case<br>How to align DLP with company growth and innovation initiatives<br>Positioning DLP to executives |
| **Why you should consider Digital Guardian for your short list** | Why choose Digital Guardian<br>How we're different<br>Our proven data protection framework<br>Case studies |

DIGITALGUARDIAN®

# PART ONE
# THE STATE OF DLP IN 2019

# 5 REASONS WHY OVER 35 VENDORS NOW OFFER DLP

Google Microsoft

One of the first things that jumps out from Forrester's report, Now Tech: Data Loss Prevention, Q1 2019, is that over 35 vendors (37 to be exact) now claim to offer some form of data loss prevention.

Contrast this with the 12 vendors in the most recent Gartner Magic Quadrant for Enterprise Data Loss Prevention, published in 2017

Let's look at the 5 primary reasons why DLP remains in high demand.


*Forrester estimate

# #1 DATA SECURITY AND PRIVACY IS A GROWTH DRIVER

> At a time when the biggest source of competitive differentiation comes from how businesses use data and insights to create new value for customers, increase their operational agility to serve customers, and form digital ecosystems that generate entirely new revenue streams, data security and privacy is so much more than cost reduction and compliance. **It is, in fact, a driver of revenue and growth.** If S&R leaders can't protect this data, these advantages disappear.

FORRESTER®

*Protect Your Intellectual Property and Customer Data From Theft and Abuse, Forrester Research, July 2018*

# #2 GARTNER RECOMMENDS DLP TO STRENGTHEN GDPR COMPLIANCE

Even if the EU GDPR doesn't directly impact your organization, privacy regulations are coming (as demonstrated by the new California Consumer Privacy Act of 2018) that will affect your organization. **Forward thinking security pros are proactively taking action now.**

> The General Data Protection Regulation (GDPR) 2016/679, among other principles, requires that enterprises have purposeful and effective industry-standard data security capabilities that mitigate the risks presented to the individual. **Some of the most effective data security tools that enterprises choose to support GDPR compliance are data loss prevention (DLP) tools.**

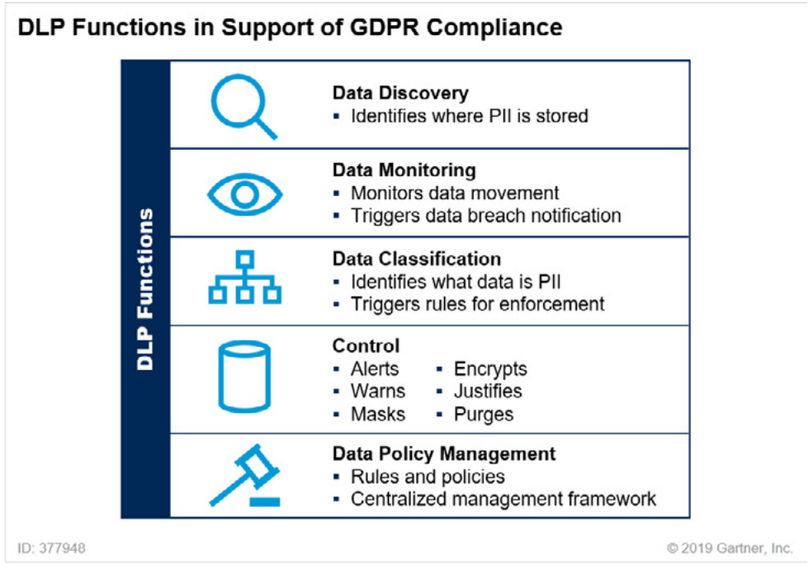
Gartner®

*How Data Loss Prevention Can Strengthen GDPR Compliance, Gartner, Jan 2019*

# #2 GARTNER RECOMMENDS DLP TO STRENGTHEN GDPR COMPLIANCE (CONT.)

DLP functions inherently support compliance with GDPR through a detailed inventory of where personal data is, how it is used and how to best manage its access and movement.

Figure 1. DLP Functions in Support of GDPR Compliance




Source: Gartner (January 2019)

**Figure 1, states that:**

- **Data discovery** is the preliminary action taken by organizations to identify what data is stored, and where. This capability is a prerequisite for addressing GDPR.
- **Data classification** furthers GDPR compliance by grouping data to define varying levels of permissions for end users. Classification allows for better organization and oversight of data, and triggers rules to enforce GDPR compliance over various means (such as network, application and email). Some vendors in the DLP market will automatically classify and track data and restrict access to data.
- **Data policy management** is based on a centralized management framework and the creation of rules and policies to enhance the monitoring and security of personal data.
- **Control features in DLP** products include alerting, warning, masking, encrypting, justifying and purging data. These control features support the GDPR requirement to protect personal data in use and in motion.
- **Data monitoring** keeps a constant eye on data in motion and works best as network components monitor network communications. The real-time monitoring of data alerts security and risk management leaders of potential data breaches, prompting immediate review and investigation.

# #3 NATION STATE IP THEFT IS A MAJOR RISK TO COMPANIES OF ALL SIZES & INDUSTRIES

China is trying to "to get secret information about our trade, our ideas, and innovations," Wray said, using "an expanding set of unconventional methods each time to achieve their goals." He warned that the threat of **economic espionage from China "affects companies in all regions and in all sectors of the US economy."**

"We have economic-espionage investigations in every state, all 50 states, that trace back to China. **It covers everything from corn seeds in Iowa to wind turbines in Massachusetts and everything in between.** So the volume of it, the pervasiveness of it, the significance of it, is something I think this country cannot underestimate."

*"CBS This Morning" co-host Norah O'Donnell interview with FBI Director Christopher Wray at FBI headquarters in Washington, DC, Sept 13 2018*

**Worth Noting:**

China's IP theft is most frequently executed by an insider or an outsider who has stolen credentials of an insider. DLP suites are proven to be among the best technologies for preventing this type of IP theft.

# #4 "AS THE BUSINESS BECOMES DIGITAL, SECURITY MUST BECOME DATA-CENTRIC"

In a digital business, processes are rarely, if ever, confined to the infrastructure of the company. Customers engage across numerous digital channels, business applications live in data centers and in the cloud, and there are dozens of third-party relationships critical to operations. This exposes a fatal flaw in the main assumption underpinning perimeter-based security — that there is a trusted internal network where data is safe and an untrusted external network where data is unsafe. This implicit trust assumption is both naive and untenable in a digital enterprise.

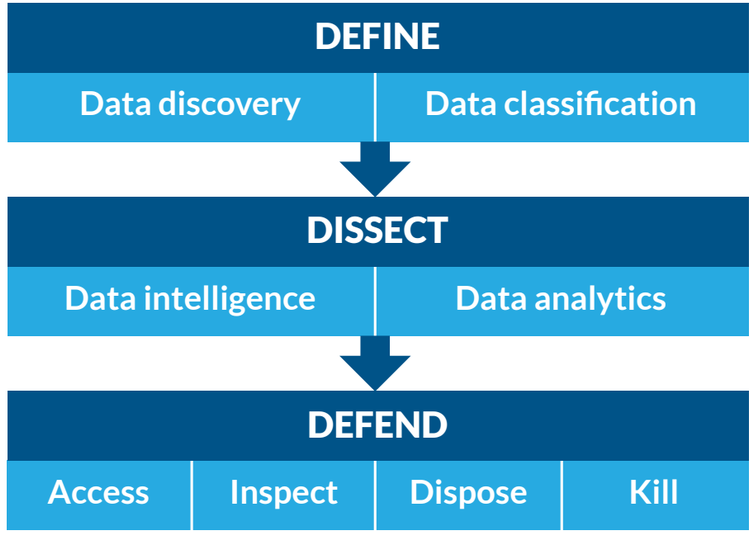
Security leaders must abandon traditional perimeter-based security and focus on the data with a Zero Trust security architecture and approach.

FORRESTER®

*The Future of Data Security and Privacy: Growth and Competitive Differentiation, Forrester Research, August 2018*

# A DATA-CENTRIC SECURITY FRAMEWORK

Forrester has created a framework to help security and privacy leaders implement a security strategy focused on the data. Their data security and control framework breaks down the problem of controlling and securing data into three areas: 1) defining the data; 2) dissecting and analyzing the data; and 3) defending and protecting the data.




**DEFINE:** This involves data discovery and data classification.

**DISSECT:** This involves data intelligence (extracting information about the data from the data, and using that information to protect the data) and data analytics (analyzing data in near real-time to protect proactively toxic data).

**DEFEND:** To defend your data, there are only four levers you can pull — controlling access, inspecting data usage patterns for abuse, disposing of data when the organization no longer needs it, or "killing" data via encryption to devalue it in the event that it is stolen.

### Worth Noting:

A DLP suite that integrates data discovery, data classification, data loss prevention and encryption can enable the framework across all three areas.

*The Future Of Data Security And Privacy: Growth And Competitive Differentiation, Forrester Research, August 2018.*

# #5 DLP NOW OFFERED IN THREE DISTINCT MODES

Data loss prevention is now available in three distinct modes that enable organizations to implement DLP based on their risk profile and security resources. Here is Forrester's description of the three modes.

**Feature/channel provides targeted coverage and simplified implementation.**

- Capabilities come as a part of another security solution, as an embedded feature or a functionality that you enable within another security offering
- Addresses a specific channel of data loss (e.g., DLP functionality within an email security solution or a cloud security gateway).
- Organizations typically rely on this segment for compliance-driven use cases.

**Suite covers all data loss channels and offers more robust capabilities.**

- Typically an integrated technology offering that specifically addresses data loss prevention.
- Should include native data classification capabilities and some form of centralized policy management.
- Greater functionality in a suite to support intellectual property protection and insider threat use cases in addition to compliance.
- Components of the suite may also be available for standalone purchase (e.g., endpoint DLP).

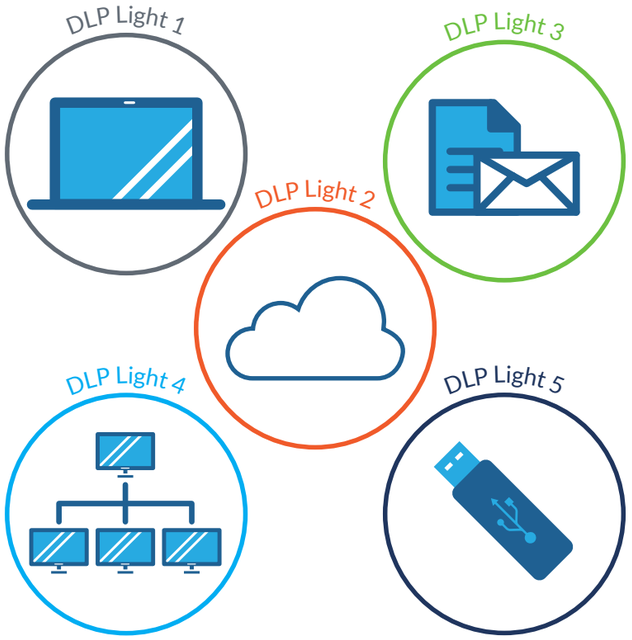
**Managed service alleviates staffing limitations with external expertise to manage entire DLP program.**

- Service offerings can involve deploying and managing a DLP suite for you or including DLP capabilities as a part of an adjacent managed service (e.g., email security).
- Managed services providers can help you manage processes, policies, and infrastructure for DLP.

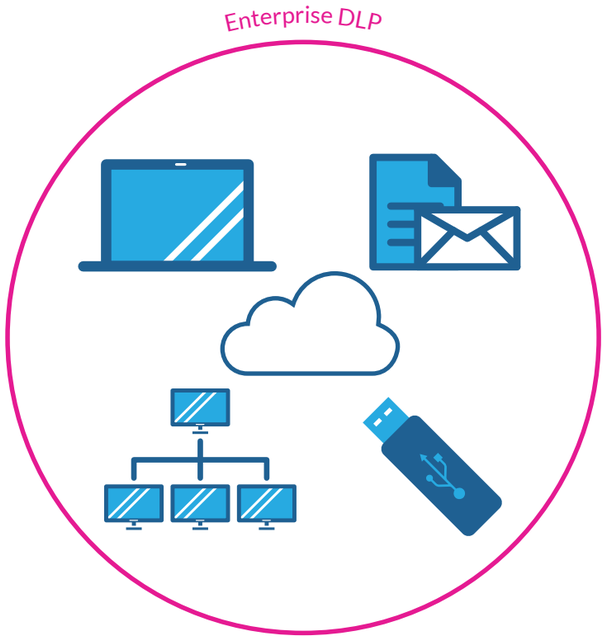
*Now Tech: Data Loss Prevention, Q1 2019, Forrester Research, Inc JAN 2019*

# DLP MODES VISUALIZED

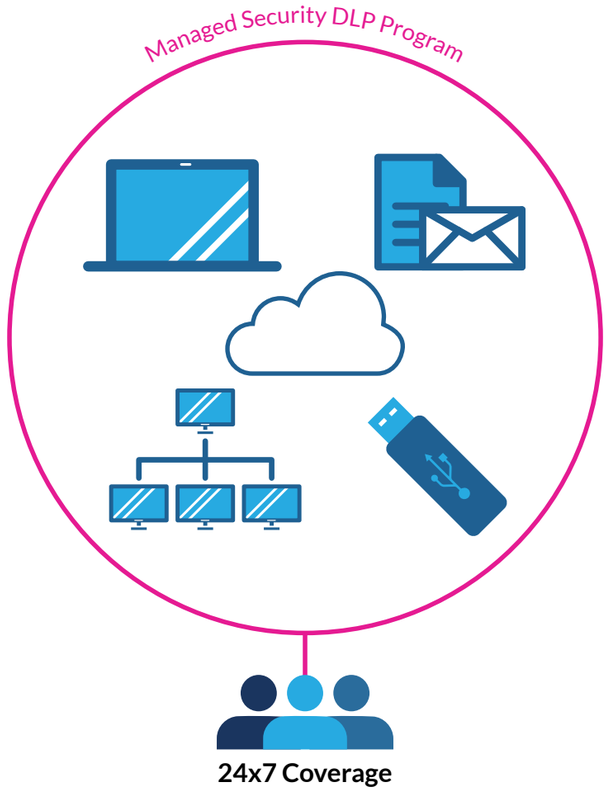
**DLP Lite**
Each vector may require an independent DLP




**Enterprise DLP**
Single solution for all vectors




**Managed Security Program DLP**
Single solution for all vectors + security expertise to manage entire program



# MAPPING DLP MODES TO REQUIREMENTS

How do you weigh the tradeoffs of the three types? Use the chart to get started with the process.

| | DLP Lite | Enterprise DLP | Managed Security DLP Program |
|---|---|---|---|
| Breadth of Coverage | ●○○ | ●●● | ●●● |
| Deployment Options | ●○○ | ●●● | ●●● |
| IP Protection | ●○○ | ●●● | ●●● |
| Regulatory Compliance | ●●○ | ●●○ | ●●○ |
| Data Classification | ●○○ | ●●● | ●●● |
| Remediation Options | ●●○ | ●●● | ●●● |
| Content Analysis | ●●● | ●●● | ●●● |
| Context Analysis | ●○○ | ●●● | ●●● |
| Implementation Ease | ●●○ | ●○○ | ●●● |
| Resources Required | ●●○ | ●●● | ●○○ |
| Vendor Support | ●●○ | ●●○ | ●●● |

**Segment Functionality**

- ●○○ Low
- ●●○ Moderate
- ●●● High

# TOP DLP USE CASES

| OBJECTIVE | SITUATION |
|---|---|
| **Personal Information Protection / Compliance** | Your organization is required by national or local regulations to ensure protection and confidentiality of your customers' information such as General Data Protection Regulation (GDPR), Personally Identifiable Information (PII), Protected Health Information (PHI), or payment card information (PCI). |
| **Intellectual Property (IP) Protection** | Your organization has valuable intellectual property, trade secrets or state secrets that, if lost or stolen by a malicious employee or accidentally shared by an unwitting employee, would cause significant monetary or brand damage.<br><br>Your organization is the target of industry competitors or nation states who are trying to break into your networks and pose as legitimate insiders to steal sensitive data. |
| **Business Visibility** | Your organization has an established process by which data is created; there are storage repositories where it lives; there are policies on who can access specific sensitive data; there are policies on what can be transmitted and any safeguards. Often times, the reality is in contrast to the ideal or originally documented policy.<br><br>Deep data visibility shows you the actual data map to your organization and allows you to compare to the desired. |

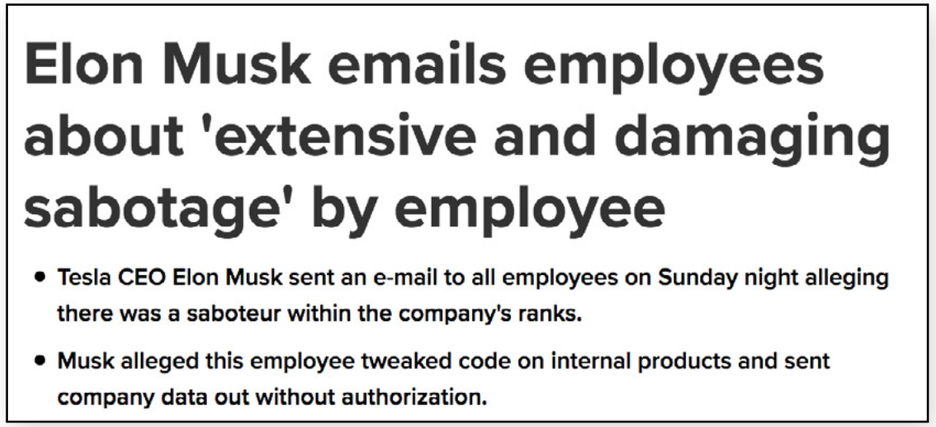
**CASE STUDY**
Compliance: St. Charles Health System

**CASE STUDY**
IP Protection: F50 Energy Company

**CASE STUDY**
Data Visibility, IP Protection, and Reduced IT Complexity

# NATION STATE IP THEFT

Intellectual Property fuels growth; as millions upon millions are poured into R&D, the temptation and payback to steal it increases. Nation state attacks are some of the most difficult to defend against given the imbalance in resources between a well funded nation and even a large enterprise.



**Elon Musk emails employees about 'extensive and damaging sabotage' by employee**

- Tesla CEO Elon Musk sent an e-mail to all employees on Sunday night alleging there was a saboteur within the company's ranks.
- Musk alleged this employee tweaked code on internal products and sent company data out without authorization.

*https://www.cnbc.com/2018/06/18/elon-musk-email-employee-conducted-extensive-and-damaging-sabotage.html*

Hyperdrive

**Second China-Bound Apple Car Worker Charged With Data Theft**

*https://www.bloomberg.com/news/articles/2019-01-30/apple-worker-charged-with-secrets-theft-for-china-robocar-firm*

DIGITALGUARDIAN®

# PART TWO

# TOP 5 MYTHS ABOUT DLP

# TOP 5 MYTHS OF DATA LOSS PREVENTION

DLP is too complex, too expensive, breaks business processes, too resource intensive, too limited… Not anymore.

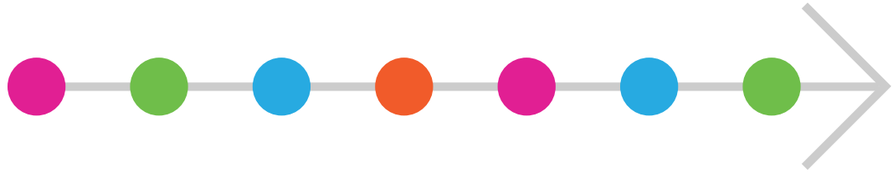
Today's DLP is effective, automated and within the reach of more enterprises than ever. Despite the ability to stop data theft and support multiple compliance regulations, DLP's history has been one of hype and disillusionment, resulting in a few myths that need to be dispelled to further illustrate why there are 35+ vendors offering DLP and why you need DLP if you don't already have it!

Whether for compliance, data protection or a blend of both, see how DLP has evolved.

# MYTH 1: DLP ALWAYS REQUIRES LOTS OF INTERNAL RESOURCES

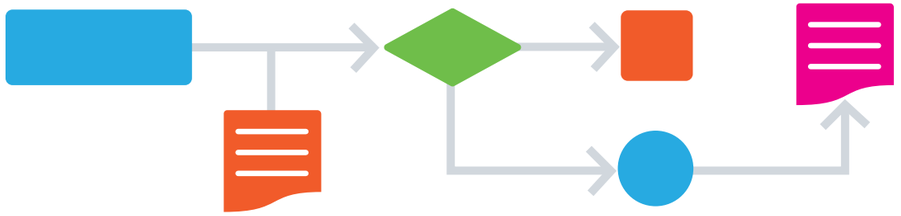
While this was true in the past, new DLP options require no dedicated internal resources to manage and maintain and no on-site infrastructure. The introductions of automation and managed security services have eased what was perceived as the "heavy lift" of DLP: hosting, setup, ongoing monitoring, tuning and maintenance. Further, fully hosted SaaS DLP options remove the additional cost, complexity, and general overhead of yesterday's server-intensive DLP.

# MYTH 2:DLP REQUIRES 18+ MONTHS TO DELIVER VALUE



DLP implementations are no longer a “big bang” that take years to return measurable value. Organizations can see results in days rather than months or years. With DLP delivered via a SaaS model, no longer do you need an additional procurement project of servers, databases, and other technology along with the staffing to manage and maintain all that iron. Today’s SaaS DLP solutions can be turned on quickly, are modular and allow for iterative deployment as part of a continuously evolving, ongoing data protection program.

# MYTH 3: DLP REQUIRES POLICY CREATION FIRST



Even the best policy wizard in the world can't fix a fundamentally flawed policy, one based on an idealistic or incomplete view of your organization's data map.

Today's DLP does not depend on a policy driven approach to get started. Context-aware DLP enables you to automatically collect information on data usage and movement in and out of the extended enterprise, and then work with the business unit leader to define the right policies based on data, not speculation.

# MYTH 4:DLP PROVIDES TOO MANY ALERTS AND FALSE POSITIVES

DLP, like any security solution, does what it is told, for good or for bad. Overly broad policies lead to alert overload, even within those alerts too many of them are false positives. Analysts waste their time investigating, end users are frustrated when business critical processes are blocked or slowed.

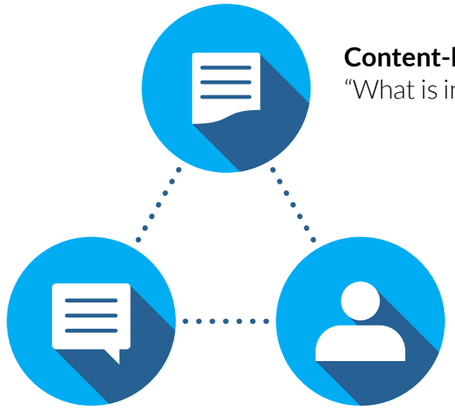
Data classification, specifically fully automated data classification, delivers the prioritization of these alerts enabling analysts to focus on what matters, attacks targeting sensitive data.

What about actions that may appear innocuous, but are really part of a larger attack? Enter User & Entity Behavioral Analysis (UEBA). By profiling normal behavior, DLP with integrated UEBA understands when behaviors deviate from the norm and can trigger alerts. Add in the data classification and the actions that target sensitive data bubble to the top for immediate action.

# THE POWER OF DATA CLASSIFICATION

Organizations generate volumes of data. This comes as no surprise, but what might be surprising is the accelerating volume at which the data is being created. As an InfoSec professional responsible for protecting digital data, you're going to need a new approach to stay ahead of the data deluge. Data Classification allows you to prioritize your data protection efforts, ensuring you focus on the most critical events, those targeting sensitive data.

Understand the three core classification methods and how they align to your data types, then evaluate the vendors' classification solutions for a match.



**Content-based** answers "What is in the document?"

**Context-based** answers "How is the data being used," "Who is accessing it," "Where are they moving it," "When are they accessing it"

**User-based** relies on user knowledge and discretion at creation, edit, or review to flag sensitive documents.

**LEARN MORE**

Read how Digital Guardian Delivers the most complete data classification solution in the industry

# MYTH 5: DLP IS ONLY FOR STOPPING DATA THEFT

DLP is called Data Loss Prevention for a reason, but that is not all it can do.

Data can be misused without ever leaving the extended enterprise, DLP can assist with internal investigations such as to prevent insider trading and to document compliance status for audit purposes.

DLP is a valuable too for an exit interview when employees do transition out. It can reinforce privacy conditions as part of many employment agreements.

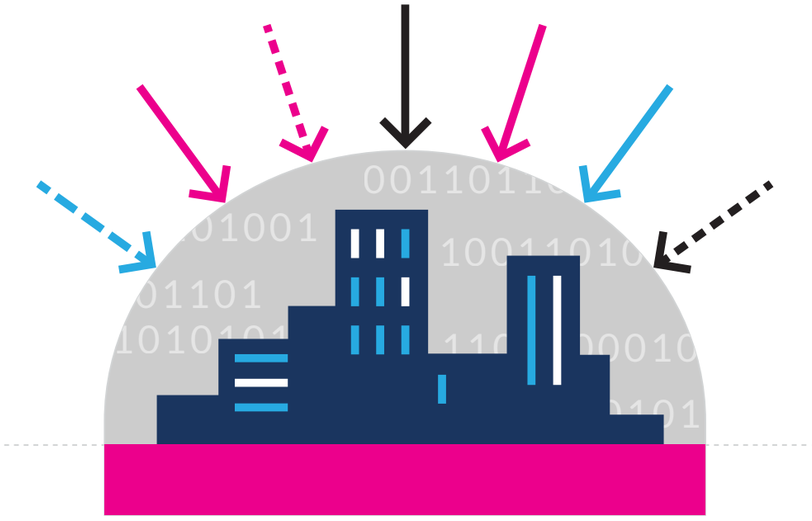
# PART THREE
# EVALUATING DLP

# THE FIRST STEP IS DISCOVERY

Before reaching out to vendors, engage business leaders informally on what data exists and how it's used. Engage with the end users too, understand how they do their jobs, what frustrations they face, what would change about existing data security policies and programs.

From these discussions you can learn:

- What pockets of information exist in your business?
- Who uses the data, who shouldn't use it?
- How does sensitive information move?
- How could your data be lost, compromised, or abused?
- Compare these insights with how perception differs from reality.



## THE PURPOSES OF THESE DISCUSSIONS ARE:

**1.** They should provide you with the details needed to create a strategic data protection plan.

**2.** They will make business leaders aware of the program and begin the process of gaining buy-in from critical constituencies.

**3.** End users will feel included in the process and more likely to understand and support the solution.

# HOW TO EVALUATE DLP SOLUTIONS

## KEY STEPS FOR ENTERPRISE DLP VENDOR EVALUATION:

1. **Research initial vendor set.** Thousands of vendors offer some form of data protection. Identify and apply filters to narrow down your organization's choices. One common filter is identifying whether the vendor supports all of your OSs. In addition to peer research many organizations is the Gartner Magic Quadrant report for Enterprise DLP.

2. **Reach out to vendors with a plan.** After you create the short list, it is time to contact the vendors. Have a list of use cases or critical business needs.

3. **Consolidate responses.** Gather the key stakeholders and seek to build consensus around which vendors have the best ability to solve your problems.

4. **Narrow choices down to two vendors.** Based on RFP scores or rankings, you should be able to eliminate all but two vendors for presentation and risk assessment.

5. **Conduct pilot tests.** Request pilots from both vendors, or from a single finalist as selected from onsite meetings.

6. **Select, negotiate, purchase.** After pilot testing has concluded, take the results to the full selection team. Begin negotiating with your top choice.

# THE BIG 3 VENDOR EVALUATION CRITERIA

Your environment ultimately decides which DLP variant and vendors makes sense to deploy. To simplify the process, here are the big three filters

1. **What Do the Analysts Say?** Sometimes it's nice to make sure someone has your back, in this case the analysts community is a great resource. They've invested thousands of hours to research, dissect, and then disseminate their knowledge about what works for who. Look to these reports to see what are the strengths and gaps of each vendor to how they align to your needs.

2. **OS Coverage:** This is often a forgotten element, if you have a pocket of key knowledge that lives on Mac or Linux machines, you need a vendor that provides full protection for these. Dive in to understand what, if any, differences in coverage exist.

3. **Delivery Models:** DLP used to have one option, on-site deployment, this is no longer the case. With the global move to the cloud, DLP is no exception. Understand how the vendor can deploy can guide your decision. If your business has said "we don't want a data center" or "we are not allowed to put sensitive data in the cloud" the vendor should be able to fulfill that. Don't forget to ask about managed programs if staffing is a concern.

**FREE DOWNLOAD**

· Get the Data Protection Vendor Evaluation Tool Kit (includes RFP template and Vendor Evaluation Scorecard)

# MANAGED SECURITY SERVICES EVALUATION CHECKLIST

Functionality or deployment options; where do you start the evaluation? If you know you need a fully managed offering, understand what is included in the service first, before the technical evaluation begins and your team falls in love with something you can't have.

**01** Does the MSP have any of the following security certifications, and if so, which ones? Asking about all of these, not only about the standards and regulations of your industry, is one way to demonstrate the vendor's depth and breadth of DLP knowledge:

- ☐ Statement on Standards for Attestation Engagements (SSAE) 16 (SOC 1)
- ☐ Audited Cloud Security Alliance Cloud Controls Matrix (CCM)
- ☐ Information Technology Infrastructure Library ITIL v3
- ☐ Payment Card Industry Data Security Standard (PCI-DSS)
- ☐ Department of Defense Information Assurance Certification (DIACAP) Federal Information
- ☐ Security Management Act (FISMA)
- ☐ Health Insurance Portability and Accountability Act (HIPAA)
- ☐ Health Information Technology for Economic and Clinical Health (HITECH)
- ☐ Security Clearance Level (U.S. Federal Government)

**02** What steps does the MSP take in cloud DLP delivery to ensure that your sensitive data is protected?

- ☐ Data collection and dissemination
- ☐ Metadata collection and dissemination
- ☐ Data residency
- ☐ Tamper proof agents
- ☐ Secure communication protocols

**SEE OUR BLOG**

Read how to hire & evaluate Managed Security Service Providers (MSSPs).

# PART FOUR
# BUSINESS CASE FOR DATA PROTECTION

# HOW TO MAKE A VALUE-BASED BUSINESS CASE

Data protection makes sense to you, how do you pitch that idea internally to get the financial and political support you need? The key is to make a value-based business case by positioning DLP initiatives in terms that executives recognize.

## WHAT'S A VALUE-BASED BUSINESS CASE?

| | |
|---|---|
| **Demonstrates alignment with business priorities** | Shows how security contributes to growth and revenue |
| **Encourages a focus on understanding data** | Supports data classification, proper data use and handling |
| **Sends a message that security and privacy are business differentiators** | Supports view that security is a business partner and enabler |

A value-based business case demonstrates alignment between business priorities and data protection initiatives. There are two different approaches to identifying value:

- **QUALIFY** how security aligns with the business.
- **UNDERSTAND** the value of information security.

# UNDERSTAND THE VALUE OF INFORMATION SECURITY

## WHAT'S THE TRUE COST OF A BREACH? IT DEPENDS...

There are multiple studies that attempt to quantify, down to the cost per record in case of PII breaches of a data loss incident. The problem is they vary, and when it comes to your business, might not be close enough to base a business decision on it, such as purchasing cyber insurance. Below are some tips to help with the specifics to your organization:

And many fail to include IP theft in their analysis further impacting the applicability to your business.

**Are you most concerned with losing PII, PCI, PHI, GDPR type information?**
In the case of hospitals, retail banks, retail, and hospitality businesses customer records and the information associated with it is the crown jewels. If you fail to protect it, you risk fines and customer churn.

- **Fines:** GDPR cites the 4% of global revenue as the big stick, what is your global revenue, how would a fine of that magnitude impact your annual earnings?
- **Churn:** What is your average customer acquisition cost? What would the impact on your organization be if, post-breach, your churn rate went up 5%, 10%?

**Are you most concerned with losing intellectual property?**
Intellectual property is a staple in organizations from manufacturing to pharmaceutical, but it lives in virtually every organization. It is hard to value, often only at liquidation can a value be determined, and this intellectual property comes with a shelf life, such as patent protection limits. To help put numbers that apply to your business:

- **Patents:** What is the R&D budgeted to patent development? How many patents per year are you awarded? What is the expected revenue from that patent? What would the impact be if one of those patents was stolen?
- **Algorithms:** In Financial Services complex trading and pricing models are closely guarded as each firm seeks to outperform the market. What would the impact to your organization if your models leaked?

# ALIGN DLP WITH COMPANY GROWTH AND INNOVATION INITIATIVES

## "DATA SECURITY AND PRIVACY IS A SOURCE OF GROWTH AND DIFFERENTIATION"

Data is the new (insert your favorite valuable item here)! It may sound cliché, but data is what fuels businesses. It is one of the biggest sources of sustainable competitive advantage. According to Forrester, here is how data protection can benefit your business growth and innovation initiatives.

**Build trusted customer relationships that drive loyalty and retention.** Firms must give customers assurance and additional reasons to do business — and continue to do business — with them.

**Elevate data security and privacy as a corporate social responsibility.** Behind every compromised customer record is a person who must deal with the consequences, and this makes data protection an ethical and moral imperative.

**Capitalize on risk.** Workforce mobility, internet of things, big data analytics, artificial intelligence, automation, and more all give firms plenty of ways to carve out new opportunities to drive growth. All come with varying levels of security, privacy, and ethical risks that you must address, including data collection, appropriate use, and data access. Security and privacy pros must help manage and mitigate the risks.

**Protect future revenue streams.** Research and development efforts, corporate secrets, and intellectual property can hold the key to a company's future growth and direction. Safeguard this data against cyberespionage, theft, and careless compromise.

**Thrive in a post-EU General Data Protection Regulation (GDPR) world.** With GDPR readiness out of the way, S&R and privacy professionals must focus on sustaining compliance over time. From managing third-party risk to reporting data breaches in a timely manner and addressing privacy by design, GDPR requires ongoing compliance.

*The Future Of Data Security And Privacy: Growth And Competitive Differentiation, Forrester Research, August 2018.*

# ALIGN DLP WITH COMPANY GROWTH AND INNOVATION INITIATIVES

## TEMPLATE

Using the growth and innovation opportunities from the previous page, determine which ones you can tie your DLP project with to make a growth oriented business case

| GROWTH OPPORTUNITY | DESCRIBE HOW YOUR DLP PROJECT CAN SUPPORT (IF APPLICABLE) |
|---|---|
| **Build trusted customer relationships that drive loyalty and retention** | |
| **Elevate data security and privacy as a corporate social responsibility** | |
| **Capitalize on risk** | |
| **Protect future revenue streams** | |
| **Thrive in a post GDPR world** | |

# A WORD ABOUT CYBER INSURANCE COVERAGE

A KPMG study estimated the cyber insurance market will grow between 20-25% annually and by 2025 reach $20b in premiums, up from $2.5b in 2015. Despite this growth, in insurance terms the industry is still in it's infancy with only ~40% of the Fortune 500 carrying cyber insurance coverage. The industry is learning, both the insured and the carriers, and sometimes it can cause tension. Zurich Insurance is claiming the attack was as "act of war" and denying coverage to Mondelez, who is appealing that decision.

*https://assets.kpmg/content/dam/kpmg/za/pdf/2017/12/17383MC-cyber-insurance.pdf*

**NotPetya Victim Mondelez Sues Zurich Insurance for $100 Million**

**Mondelez files lawsuit after Zurich rejects claim for damages from massive ransomware attack.**

Mondelez, US food distributor and owner of major brands Ritz and Nabisco, has filed a lawsuit against Zurich Insurance Group after its claim seeking $100 million for NotPetya damage was denied.

*https://www.darkreading.com/attacks-breaches/notpetya-victim-mondelez-sues-zurich-insurance-for-$100-million/d/d-id/1333640*

# POSITIONING DLP TO THE BUSINESS

DLP is not just a security decision, more titles within the organization are involved in data protection projects.

- **CEO and Board**
- **CISO**
- **CFO**
- **CMO**
- **CRO/CCO**
- **Director of InfoSec**
- **Business Unit Lead**

Build allies with the business at multiple levels. Business unit executives are data owners, users create and consume data. Engage with them on their key business processes and routine data flows. Identify how they would be impacted by a data breach (besides your security team).

## CEO

**PAIN POINTS**

- Business growth
- Market perception
- Future prospects

**LINK DATA PROTECTION TO ADDRESSING PAIN POINTS**

- Flexibility to expand organization globally, seek new business partners, securely outsource
- Proactive stance on security shows position as industry leader and advanced cybersecurity posture

## CISO

**PAIN POINTS**

- Securely enabling the business to grow
- Scalable solutions that don't overly burden the team

**LINK DATA PROTECTION TO ADDRESSING PAIN POINTS**

- Managed DLP offerings allow rapid deployment and limit ongoing internal resources
- Event-based solutions don't require lengthy policy creation projects
- Accuracy enables team to resolve the high risk threats first

## CFO

**PAIN POINTS**

- Profitable growth
- Efficient use of assets

**LINK DATA PROTECTION TO ADDRESSING PAIN POINTS**

- Managed offerings eliminate need for additional staff, CapEx to deploy and maintain
- Managed offerings deliver predictable expenses
- SaaS DLP deployments reduce need for on-site infrastructure and reduce staffing needs

## CRO/CCO

**PAIN POINTS**

- Support and document compliance stance against evolving regulations

**LINK DATA PROTECTION TO ADDRESSING PAIN POINTS**

- Managed DLP delivers compliance reporting without needing additional staff
- Discovery and classification locates and tags sensitive data

# POSITIONING DLP TO THE BUSINESS

## DIR. OF INFOSEC

**PAIN POINTS**

- Business process security
- Efficient use of resources
- Advance cybersecurity maturity

**LINK DATA PROTECTION TO ADDRESSING PAIN POINTS**

- Data-centric security protects the targeted assets – data!
- Managed offerings eliminate need for additional staff
- Integrations to 3rd party security and analytics partners increase visibility and speed incident response

## BUSINESS UNIT LEAD

**PAIN POINTS**

- Outpacing the market for my business unit
- Collaborating enterprise wide to drive company growth
- "How can I get to be the CEO?"

**LINK DATA PROTECTION TO ADDRESSING PAIN POINTS**

- Pursue creative business growth initiatives, securely
- Share data across company, securely
- Use security as a competitive advantage to gain new business

## CMO

**PAIN POINTS**

- Drive customer experience, satisfaction, and growth
- Outpace the market
- Customer churn, customer acquisition cost

**LINK DATA PROTECTION TO ADDRESSING PAIN POINTS**

- Protect the brand by reducing likelihood of customer data leaking out
- Effectively share strategic growth plans across enterprise securely

## USER

**PAIN POINTS**

- Doing job effectively, without unnecessary burdens
- Protecting me from unintentional leaks

**LINK DATA PROTECTION TO ADDRESSING PAIN POINTS**

- Solutions only intervene when risky behavior is identified, otherwise invisible to the user
- Real time user education and prompts helps users do the right thing

PART FIVE

# WHY SHORT LIST DIGITAL GUARDIAN

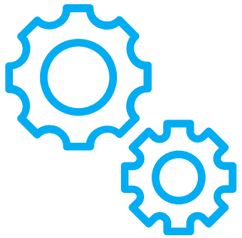
# WHY CHOOSE DIGITAL GUARDIAN

## Deepest Visbility

You need to see and correlate all data events throughout your organization; these include system, user, and data events at the endpoint, on the network, and in the cloud. Combining these three types of events gives you the context into data movement to understand and reduce risky behavior from either internal or external actors.

## Real-Time Analytics

You can aggregate and analyze millions of system, user, and data events with a big data, cloud services architecture and intuitive UI. Your analysts see human digestible and actionable intelligence in real time and can respond to threats, both internal and external, faster and more efficiently.



## Flexible Controls

Flexible and scalable controls let you control data movement on Windows, Linux, or Mac machines across the entire enterprise. With these controls you can log, alert, prompt, block, and encrypt files, delivering the situational granularity you need without getting in the way of legitimate business.

With automated controls you can prevent a data breach before it happens. You can control data everywhere it lives in your extended enterprise - on the network, in database servers or endpoints, even in the cloud.

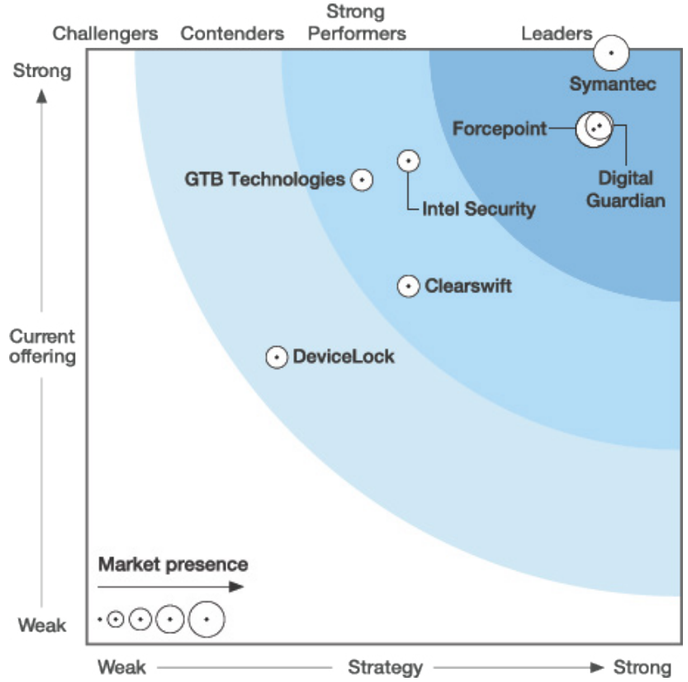
# GARTNER AND FORRESTER DLP LEADER

"The Digital Guardian endpoint covers DLP, advanced threat protection, and endpoint detection and response (EDR) in a single agent form factor installed on desktops, laptops and servers running Windows, Linux and Mac OS X, as well as support for VDI environments..."

*Gartner Magic Quadrant for Enterprise Data Loss Prevention, February 2017*


"Digital Guardian brings together two in-demand enterprise security capabilities today: DLP and endpoint visibility and control (EVC). A strong focus on strategic partnerships augments the company's information management capabilities. It also has a popular DLP-as-a-managed-service offering that now includes local UK and EU hosting options."

*Forrester Wave™: for Data Loss Prevention Suites, Q4 2016*

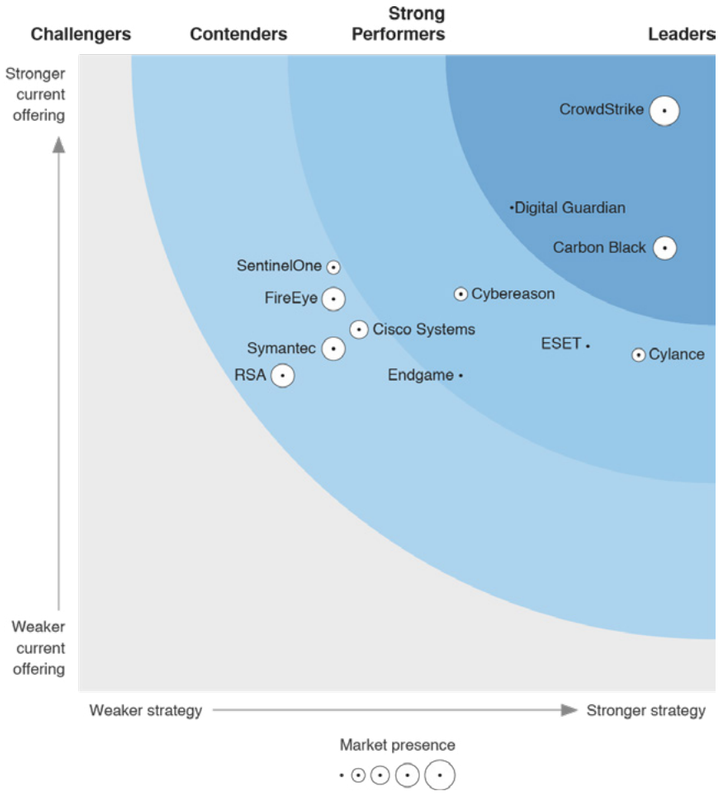


# WE'RE ALSO AN EDR LEADER – USING THE SAME AGENT

> Digital Guardian is a newer entrant into the space and has built an extremely exciting EDR solution on top of its data loss prevention (DLP) technology. While there have been many criticisms of the effectiveness of DLP from an enforcement perspective, file analytics capabilities solve one of the biggest challenges for security teams in identifying sensitive data within their environments. Digital Guardian differentiates itself by using these file analytics to help you understand the sensitivity of data that has been accessed as part of detection and alerting.

FORRESTER®

*The Forrester Wave™: Endpoint Detection and Response, Q3 2018*



# PROVEN DATA PROTECTION FRAMEWORK


**Understand**
- What data you need to protect
- When sensitive data is at risk

**Build**
- Smart policies & controls
- Based on REAL data usage
- Enterprise wide knowledge how business operates

**Enforce**
- Flexible & Automated controls

**Educate**
- Real-time prompts increase employee awareness and educate users on proper usage

**Assess**
- Advanced analytics & reporting

**Improve**
- Determine next level data protection

Our four part data protection program framework has proven successful for hundreds and hundreds of our customers.

- **UNDERSTAND.** It's essential to understand what data you need to protect and when that data is at risk. We help you do this with a combination of enterprise data discovery, data classification, data loss prevention, and endpoint detection & response.
- **BUILD**. With the understanding of how data is used, where it flows, where it's at risk, instead of guessing, you can build smart polices and controls based on the real data usage.
- **ENFORCE AND EDUCATE.** Our solution enables you to educate users in real-time, making them aware of when they might be violating polices. This can be a game changer. We also help you apply enforcement controls that can stop bad actors before the data gets out.
- **ASSESS & IMPROVE.** You can't improve what you don't measure. We give you the mechanisms to continuously assess, iterate and improve your security policies and procedures.

# USE DATA VISIBILITY INSIGHTS TO ENGAGE BUSINESS LEADERS

Anyone with DLP experience will tell you that DLP isn't just a security or IT initiative. Success depends on support and sponsorship from the business leaders. This is pure common sense. But we have a unique view on how to engage them.

The standard process is to sit down with the business leaders to define all data classification schemes and protection policies in advance. What do we recommend instead?

Start by sharing real discoveries from your "Quick Win" about where sensitive data resides and how it's being used. This will get the attention of your enterprise's business leaders. It will make it much easier for them to understand the risks to the business. And it will make it much easier to collaborate with them. That's exactly what John Graham, former CISO of Jabil did. Read on to learn more.

**"Digital Guardian [Data Loss Prevention] helped us changed the conversation with business unit leaders."**

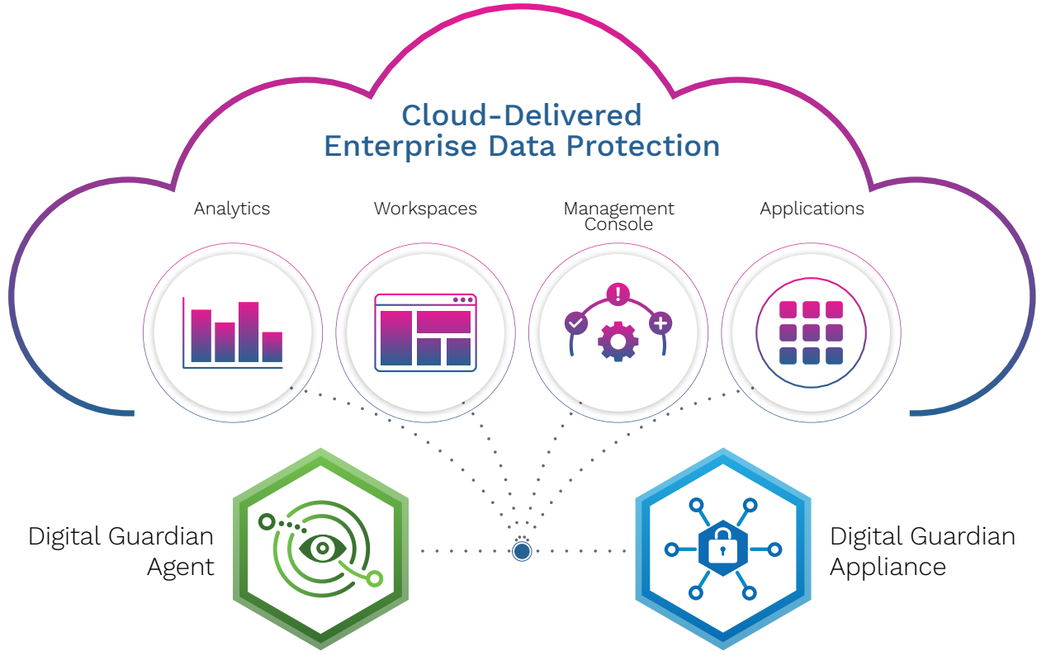
*–John Graham, former Chief Information Security Officer, Jabil*

JABIL

# THE ONLY CLOUD DELIVERED DATA PROTECTION PLATFORM

Data protection is at the core of our company mission. Our data protection platform is purpose built to stop data theft from all threats.

- Data Loss Prevention
- Endpoint Detection & Response
- User & Entity Behavior Analytics
- Data Discovery
- Data Classification
- Analytics
- Reporting
- Management




**FREE DOWNLOAD**

· Digital Guardian Platform Technical Overview

# HOW WE'RE DIFFERENT

Data protection is at the core of our company mission. Our data protection platform is purpose built to stop data theft from all threats. This platform is designed to:

**Broadest Endpoint DLP Operating System and Browser Coverage**
Only Digital Guardian offers the broadest endpoint OS and browser coverage of any DLP vendors, covering Windows, Mac, and Linux (multiple versions supported for SUSE, Red Hat, Ubuntu, Debian), VMware and Citrix virtual machines. Content inspection and policy enforcement for Google Chrome v68 and on ensures full visibility into all web traffic.

**No Policy, No Problem**
Only with Digital Guardian can you deploy DLP even before you have policies in place to get a complete understanding of how sensitive data is actually being accessed and used within your organization, then add the polices based on your real-world.

**SaaS Delivery Model**
Only Digital Guardian offers a Software as a Service (SaaS) solution fully hosted by DG. Our SaaS offering includes everything in the subscription – provisioning and support for all back-end infrastructure, application monitoring, backups, upgrades, etc. This cuts costs and eliminates the complexity of patching, updating and maintaining on premise server infrastructure.

**FREE DOWNLOAD**

· Digital Guardian Platform Technical Overview

# HOW WE'RE DIFFERENT

Data protection is at the core of our company mission. Our data protection platform is purpose built to stop data theft from all threats. This platform is designed to:

**Vendor-Delivered DLP as a Service**
Only Digital Guardian delivers a DLP solution that is available as a managed service directly from the technology vendor. This eliminates finger-pointing between the technology vendor and the managed service provider. Pair with our Managed Security Program for EDR to protect your most sensitive data from all threats.

**Greater Context for Enhanced Data Protection**
Only Digital Guardian delivers the context into your data security alerts to allow more informed DLP, EDR, and UEBA decisions. Alerts include the sensitivity of the documents accessed allowing better prioritization of alerts and immediate action when sensitive data is at risk.

**Single Agent for DLP, EDR & UEBA**
Only DG addresses insider threats, advanced threats and compliance with a single agent and a single platform. Only Digital Guardian's solution is recognized as both a "Leader" in the latest (2017) Gartner Magic Quadrant for Enterprise Data Loss Prevention AND a "Leader" in the 2018 Forrester Wave for Endpoint Detection and Response.

**FREE DOWNLOAD**

· Digital Guardian Platform Technical Overview

**FREE DOWNLOAD**

· Digital Guardian Managed Security Program Technical Overview

## CASE STUDY

# ENABLING EMPLOYEES TO PROTECT SENSITIVE CLIENT INFORMATION

**SITUATION:** The company collects and maintains confidential information on candidates and salaries, including Personally Identifiable Information (PII) subject to regulatory requirements. Protecting this information from attackers and inadvertent disclosure required a comprehensive, but flexible security solution. The  task was complicated by separate IT infrastructure and differing privacy requirements in each of 1,000+ offices. In addition, they operated with a lean IT team and capital budget, therefore could not take on workload for deploying and managing new tools.

**SOLUTION:** Digital Guardian's Managed Security Program (MSP) provided the full-service deployment and support the company's staff required, along with automated classification and enforcement options. Digital Guardian worked to understand appropriate policies for different data classifications and transform those into rules that could be enforced automatically, or provide reminders to users of policies. Digital Guardian automatically classified data based on the source (HR systems) and the content (social security numbers and other PII).

**RESULTS:** Starting with deployment in a single office, Digital Guardian's MSP team monitored the company's activities to identify those which violated policies. Digital Guardian allowed the company to identify and deter activity not in alignment with acceptable use policies, while treating individuals as the valued employees they were.

**MORE INFO**

Read the full case study here.

## CASE STUDY

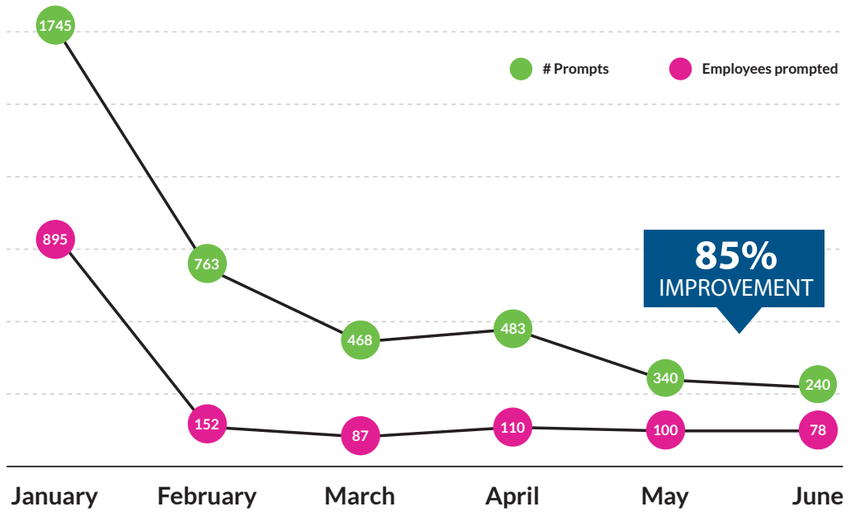
# THE POWER OF REAL-TIME USER EDUCATION

**SITUATION:** The company is one of the largest managed healthcare providers in North America. Despite spending more than $1M annually on HIPAA compliance training, an internal audit identified a significant risk of non-compliance. The training had failed because it was a specific event not reinforced through ongoing processes. Users were not diligent about using the company's VPN, where data protection controls were enforced. Remote users routinely traveled with the sensitive data they needed to do their jobs.

**SOLUTION:** The company's auditors recommended stricter controls, both on and off the corporate network. The company needed to change user behavior when interacting with sensitive data, reinforce existing policies as data was used, and create a culture that held users accountable for their actions. Digital Guardian helped by enforcing connections through the company's VPN, applying policies in real time based on network awareness, and prompting users who violated data use policies. Users are presented with a prompt screen that requires them to acknowledge the appropriate company policy and provide justification to continue.

**RESULTS:** Within six months, the healthcare provider reported an 85% decrease in prompts to users, indicating a significant increase in both policy awareness and secure employee behavior.

### UNAUTHORIZED TRANSMISSION OF PHI DATA




**WATCH A VIDEO**

Watch a video on driving security using real-time user education.

## CASE STUDY

# PROTECTING INDUSTRIAL AUTOMATION IP

**SITUATION:** Research and development is the lifeblood of the industrial automation market. The company's Chief Information Security Officer, began looking for a solution to protect their critical IP after becoming increasingly concerned about industrial espionage from both domestic and foreign sources.

**SOLUTION:** After an extensive selection process, the company determined that Digital Guardian provided the best mix of visibility to IP, control over information movement, and low impact on the endpoints and users

**RESULTS:** Digital Guardian was deployed across 5,000 endpoints. The CISO gained the visibility into the risks to the company's IP and applied controls to policies that had previously been unenforceable. Digital Guardian's MSP provided the support the company desired without the overhead of additional IT staff.

**MORE INFO**

Read the full case study here.

## CASE STUDY

# JABIL'S QUICK WIN

**SITUATION:** Jabil is a Fortune 100 contract manufacturer. The company was at risk of large financial penalties if customer NDAs were violated due to a security incident.

**SOLUTION:** Within 30 days of DLP deployment, Jabil's security team gained visibility into all data access and usage across 52,000 workstations. They immediately realized that users copying large data files to USB drives was far more common than anyone expected. Digital Guardian's detailed egress reporting on the data leakage from USBs enabled Jabil's security team to have more productive conversations with business unit leaders. These exchanges focused not on defining what data was considered sensitive, but rather on how data from specific servers was being used (in this case copied to USBs) by users.

**RESULTS:** By providing business leaders real-world information on how data was being used (or misused), Jabil was able to identify and classify their most sensitive data faster and more efficiently. This was a dramatic improvement over a more traditional discovery and classification approach.

Within 30 days of DLP deployment, Jabil's security team gained visibility into all data access and usage across 52,000 workstations.

**MORE INFO**

Read the full case study here.

## CASE STUDY

# IP PROTECTION AT A GLOBAL INVESTMENT BANK

**SITUATION:** A global investment firm needed to protect the proprietary source code that powers their financial platform.

**SOLUTION:** Using Digital Guardian Data Loss Prevention, they can monitor users as they check out code, make changes on a local machine, and then check it back in again. The solution tracks each and every event – including when, where and how source code is used as well as how it is changed. This visibility prevents users from downloading all or part of the source code via removable devices or uploading it to the web. All events are logged and audited to streamline compliance, forensics and incident response.

**RESULTS:** Digital Guardian allowed the organization to maintain its culture of "open access," while improving security over critical intellectual property. Once the value of Digital Guardian was established in the Investment Banking business, use then expanded into other business units.

## CASE STUDY

# SECURING PII SHARED WITH THIRD PARTY VENDORS

**SITUATION:** A regional bank needed to protect its sensitive customer data, which was being shared with thirty party vendors for IT management. The firm realized that failure to secure its PII and PCI could result in regulatory penalties, class action lawsuits, or loss of credibility.

**SOLUTION:** Digital Guardian's Data Base Record Matching allowed deep inspection into the bank's customer databases and created mathematical hashes of the data. Outgoing traffic to external vendors is now inspected for any matches to regulated data, while also preventing unauthorized data access. Our solution's data protection capabilities protect on and off the network as well as across virtual environments.

**RESULTS:** Digital Guardian enables the bank to maintain it's competitive advantage of "safety and soundness.". They understand what data is shared with partners and control where and how data is distributed.

**CASE STUDY**

# MANAGED DETECTION & RESPONSE AT A MULTINATIONAL BANK

**SITUATION:** A leading multinational bank needed to protect sensitive financial records from advanced cyber-attacks. Stolen financial data is coveted by criminals because it can be quickly monetized in underground marketplaces. The firm realized that failure to secure these records could not only damage its bottom line but also hurt its customers. The bank found it challenging to hire cybersecurity professionals qualified to protect against evolving cyber threats.

**SOLUTION:** The bank turned to Digital Guardian's Managed Security Program to detect and remediate threats quickly and efficiently using a proven combination of people, process and technology. Our cybersecurity experts have more than 20 years of experience in threat hunting, incident response, threat research, threat intelligence, investigation and mitigation, protecting the bank from advanced cyber attacks.

**RESULT:** The bank has upgraded their incident response and threat hunting programs faster than they ever could have with internal resources.

**Managed Security Program For**
Endpoint Detection & Response

# THE DEFINITIVE GUIDE TO DATA LOSS PREVENTION

## 2019 EDITION


QUESTIONS?

1-781-788-8180
info@digitalguardian.com
www.digitalguardian.com




DIGITAL GUARDIAN®