

# THE DEFINITIVE GUIDE TO DATA LOSS PREVENTION



# TABLE OF CONTENTS

- 03** Introduction
- 04** Part One: What is Data Loss Prevention
- 08** Part Two: How DLP Has Evolved
- 11** Part Three: The Resurgence of DLP
- 24** Part Four: The Shift to Data-Centric Security
- 28** Part Five: Determining the Right Approach to DLP
- 39** Part Six: Business Case for DLP
- 46** Part Seven: Buying DLP
- 52** Part Eight: Getting Successful with DLP
- 61** Part Nine: Digital Guardian—Next Generation Data Protection
- 65** Conclusion
- 66** Resources at a Glance

# WHY READ THIS GUIDE?

## WHAT'S OLD IS NEW AGAIN

As security professionals struggle with how to keep up with non-stop threats from every angle, a 10+ year old technology, data loss prevention (DLP) is hot 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...   | GO TO...  |
|---|---|
| New to DLP  | Part One: What is Data Loss Prevention                        |
| Familiar with DLP, but want to learn what's new                     | Part Two: How DLP has Evolved                                 |
| Not sure where to start?  | Part Four: A Data Centric Security Framework                  |
| Trying to determine the best DLP architecture for your organization | Part Five: Determining the Right Approach to DLP              |
| Looking to buy DLP  | Part Six: Buying DLP  |
| Looking for a quick win deployment                                  | Part Eight: Getting Successful with DLP                       |
| Looking to understand what makes Digital Guardian different         | Part Nine: Digital Guardian's Next Generation Data Protection |

## PART ONE

# WHAT IS DATA LOSS PREVENTION?

# DLP DEFINED

“DLP [Data Loss Prevention] is a system that performs real-time scanning of data at rest and in motion, evaluates that data against existing policy definitions, identifies policy violations and automatically enforces some type of pre-defined remediation actions such as alerting users and administrators, quarantining suspicious files, encrypting data or blocking traffic outright.”

—451 Research, “The Data Loss Prevention Market by the Numbers,” July 2015

## DLP BASICS

**WHAT:** In short, DLP is a set of technology tools and processes that ensure sensitive data is not stolen or lost.

**HOW:** DLP detects and protects your organization’s sensitive data by:

- Scanning data in motion, in use and at rest
- Identifying sensitive data that requires protection
- Taking remedial action—alert, prompt, quarantine, block, encrypt
- Providing reporting for compliance, auditing, forensics and incident response purposes

**WHY:** accidental (i.e. employee error) or malicious actions (i.e. cyber criminal breach) put your organization's data at risk.

## WHO USES DLP?

**COMPANY SIZES:** Large enterprises in the Fortune Global 500 have invested in DLP for almost 15 years. Today’s DLP puts this critical security strategy within the reach of mid-size enterprises.

**INDUSTRIES:** Historically DLP has been heavily utilized in regulated industries such as financial services, healthcare, manufacturing, energy, even government. But new and motivated adversaries aren’t limiting themselves; services companies across a wide range of industries are a major target for example.

50%  
OF ORGANIZATIONS




have some form of DLP in place, but Gartner predicts that will rise to 90% by 2018. (source: Gartner “Magic Quadrant for Enterprise Data Loss Prevention”, 1 February, 2016 , Brian Reed and Neil Wynne)



# DO WE NEED DLP?

Take a look at these common situations. If any of them apply to your organization, DLP will almost always make sense.

## DLP OBJECTIVES CHECKLIST

| OBJECTIVE   | SITUATION   | Check if this applies to you |
|---|---|------------------------------|
|  <b>Personal Information Protection / Compliance</b> | Your organization is required by national or local regulations to ensure protection and confidentiality of your customers' information such as Personally Identifiable Information (PII), Personal Health Information (PHI), or payment card information (PCI). | <input type="checkbox"/>     |
|  <b>Intellectual Property (IP) Protection</b>       | 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.                         | <input type="checkbox"/>     |
|   | 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.  | <input type="checkbox"/>     |
|  <b>Business Partner Compliance</b>                | Your organization is contractually obligated to ensure that your customers' intellectual property is protected. Failure to do so would require you to pay a large financial penalty to the customer.  | <input type="checkbox"/>     |
|   | Your corporate clients are auditing you to determine that you have the ongoing security mechanisms necessary to protect the sensitive data they have entrusted with you.  | <input type="checkbox"/>     |



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



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



**CASE STUDY**  
Business Partner  
Compliance: Jabil

# THE GREAT BRAIN ROBBERY

Intellectual property  
is increasingly being  
compromised.

## DID YOU KNOW?



In January 2016, 60 Minutes ran a feature, "The Great Brain Robbery," by Lesley Stahl that covered China's wide-scale attack on U.S. companies to steal their intellectual property. Rather than competing with the U.S. economy through innovation and development, the 60 Minutes report shows how China is committed to stealing IP through acts of cyber-espionage.

The Justice Department declared that China's espionage activities are so wide in scale that they constitute a national security emergency, as China targets almost every sector in U.S. business. According to 60 Minutes, this activity is costing U.S. companies hundreds of billions of dollars in losses and more than 2 million jobs.



## SEE OUR BLOG

To learn more we  
recommend, WIPOut:  
The Devastating  
Business Effects of  
Intellectual Property  
Theft on our blog.

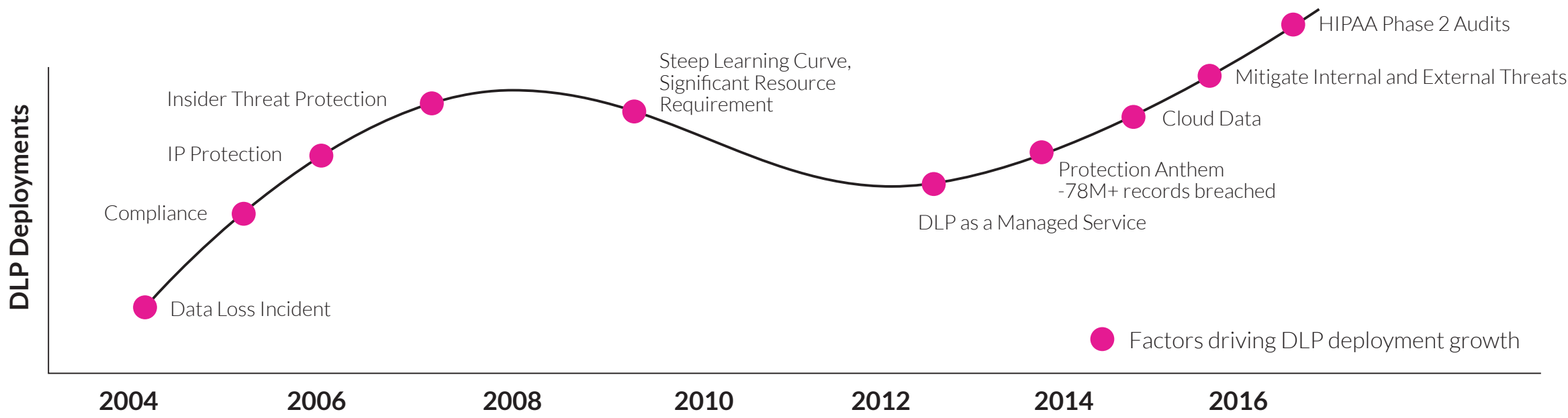
# PART TWO

# HOW DLP HAS EVOLVED



# DLP BACK IN THE LIMELIGHT

DLP came to market with big interest and bigger expectations. Demand softened as organizations struggled with the cost and complexity of deploying first generation DLP software. The dramatic increase in big breaches, coupled with factors such as DLP as a service, DLP functionality extending into the cloud and advanced threat protection, have put DLP back into the limelight.



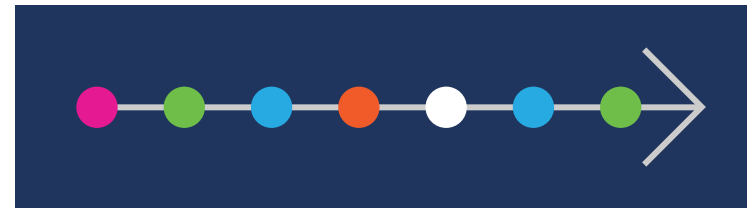
# 3 MYTHS OF DATA LOSS PREVENTION

Today's DLP is sophisticated, automated and within the reach of more enterprises than ever. DLP's history has been one of hype and disillusionment, resulting in a few myths that need to be dispelled up front.



## MYTH 1: DLP REQUIRES SIGNIFICANT INTERNAL RESOURCES TO MANAGE AND MAINTAIN.

While this was true in the past, new DLP options require no dedicated internal resources to manage and maintain. 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.



## MYTH 2: DLP REQUIRES AT LEAST 18 MONTHS TO DELIVER VALUE.

DLP implementations are no longer a "big bang" that take up to two years to return measurable value. Organizations can see results in days rather than months or years. Today's DLP solutions are modular and allow for iterative deployment as part of a continuously evolving, ongoing data protection program.



## MYTH 3: DLP REQUIRES POLICY CREATION FIRST.

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

# PART THREE

# THE RESURGENCE OF DLP

DLP is no longer exclusively for the largest enterprises in the most data-dependent industries. A number of macro trends such as cloud computing and big data are driving the wider adoption of DLP. Let's examine them...

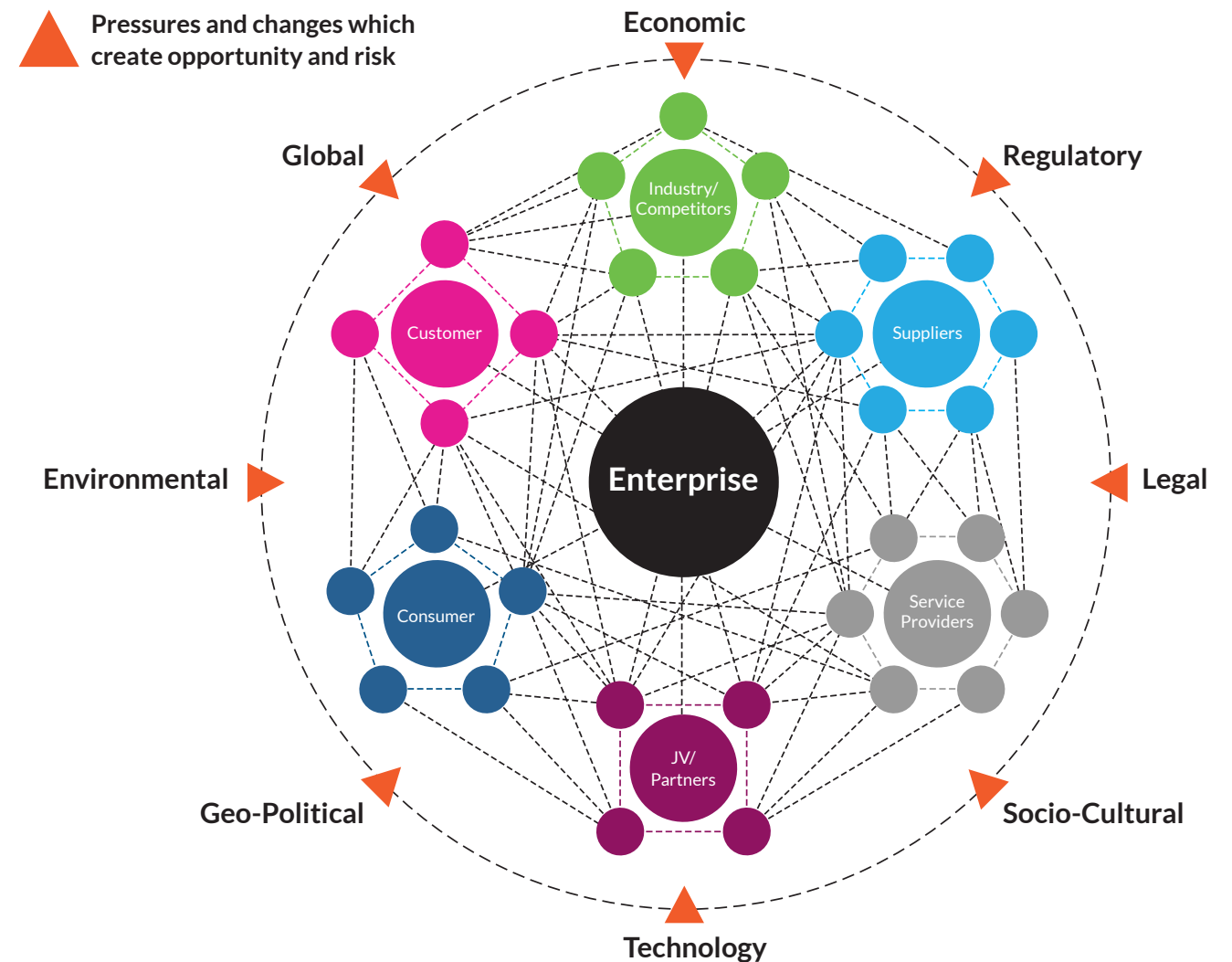
## TREND #1

# WELCOME TO A PERIMETER- LESS WORLD

### TRADITIONAL BOUNDARIES HAVE SHIFTED

- The information ecosystem is built around a model of open collaboration and trust—the very attributes being exploited by an increasing number of global adversaries.
- Constant information flow is the lifeblood of the business ecosystem. Data is distributed and disbursed throughout the ecosystem, expanding the domain requiring protection.
- Adversaries are actively targeting critical data assets throughout the ecosystem—significantly increasing exposure and impact to businesses.

### TODAY'S GLOBAL INFORMATION ECOSYSTEM



(source: Best Practices for Data Security & Data Breach Protocol, PwC, 2015)



## TREND #2

# THERE ARE MORE PLACES TO PROTECT YOUR DATA

Cloud computing creates complexity as data increasingly leaves corporate boundaries and flows essentially unchecked across networks and devices you no longer control. The use of cloud services in the enterprise is at a tipping point.

**5400%**

Growth in number of health records compromised from 2011 to 2015.

**91%**

of healthcare organizations reported at least one data breach in the last two years.

**112M**

Number of healthcare records lost or compromised in the US in 2015.

**253**

Number of healthcare breaches in the US affecting 500 individuals or more in 2015.

**I FULLY 1/3** of health care recipients will be the victim of a data breach in 2016.

**5 OF 8** of the largest healthcare security breaches over the last five years happened during the first six months of 2015.

TREND #3

# BAD GUYS ARE AFTER YOUR DATA

Let’s face it: the bad guys are probably already on your networks and endpoints. These new and varied adversaries include cybercrime, nation states, hacktivists, and employees ...all chasing your sensitive data. They differ in motive and target, but they represent big risks to your organization.

| A WIDE RANGE OF ADVERSARIES...   | WHO ARE HIGHLY MOTIVATED...  | ARE TARGETING YOUR SENSITIVE DATA...   | CREATING UNPRECEDENTED RISKS FOR YOUR ORGANIZATION   |
|--|--|--|--|
|  <b>Nation State</b>      | <ul style="list-style-type: none"><li>· Economic, political, and/or military advantage</li></ul>   | <ul style="list-style-type: none"><li>· Trade secrets</li><li>· Business information</li><li>· Emerging technologies</li><li>· Critical infrastructure</li></ul>                         | <ul style="list-style-type: none"><li>· Loss of competitive advantage</li><li>· Disruption to critical infrastructure</li></ul>  |
|  <b>Cyber Criminals</b> | <ul style="list-style-type: none"><li>· Immediate financial gain</li><li>· Collect information for future financial gains</li></ul>                | <ul style="list-style-type: none"><li>· Financial / Payment situations</li><li>· PII, PCI, PHI</li></ul>   | <ul style="list-style-type: none"><li>· Direct financial loss</li><li>· Regulatory inquiries and penalties</li><li>· Lawsuits</li><li>· Loss of confidence</li></ul>         |
|  <b>Hacktivists</b>     | <ul style="list-style-type: none"><li>· Influence political and/or social change</li><li>· Pressure businesses to change their practices</li></ul> | <ul style="list-style-type: none"><li>· Corporate secrets</li><li>· Business information</li><li>· Information about key executives, employees, customers</li></ul>                      | <ul style="list-style-type: none"><li>· Disruption of business activities</li><li>· Damage to brand and reputation</li><li>· Loss of consumer confidence</li></ul>           |
|  <b>Insiders</b>        | <ul style="list-style-type: none"><li>· Personal advantage, monetary gain</li><li>· Professional revenge</li><li>· Patriotism</li></ul>            | <ul style="list-style-type: none"><li>· Sales, deals, market strategies</li><li>· Corporate secrets, IP, R&amp;D</li><li>· Business operations</li><li>· Personnel information</li></ul> | <ul style="list-style-type: none"><li>· Trade secret disclosure</li><li>· Operational disruption</li><li>· Brand and reputation</li><li>· National security impact</li></ul> |

## TREND #3 (CONT.)

## BAD GUYS ARE AFTER YOUR DATA

**AND THERE IS A BIG "DETECTION DEFICIT" BETWEEN THEIR ATTACKS AND YOUR DETECTION.**

"Figure 5 offers a new twist on one of our favorite charts from the 2014 DBIR. It contrasts how often attackers are able to compromise a victim in days or less (orange line) with how often defenders detect compromises within that same time frame (teal line). Unfortunately, the proportion of breaches discovered within days still falls well below that of time to compromise. Even worse, the two lines are diverging over the last decade, indicating a growing "detection deficit" between attackers and defenders. We think it highlights one of the primary challenges to the security industry."

*—Verizon 2015 Data Breach Investigations Report*

## VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

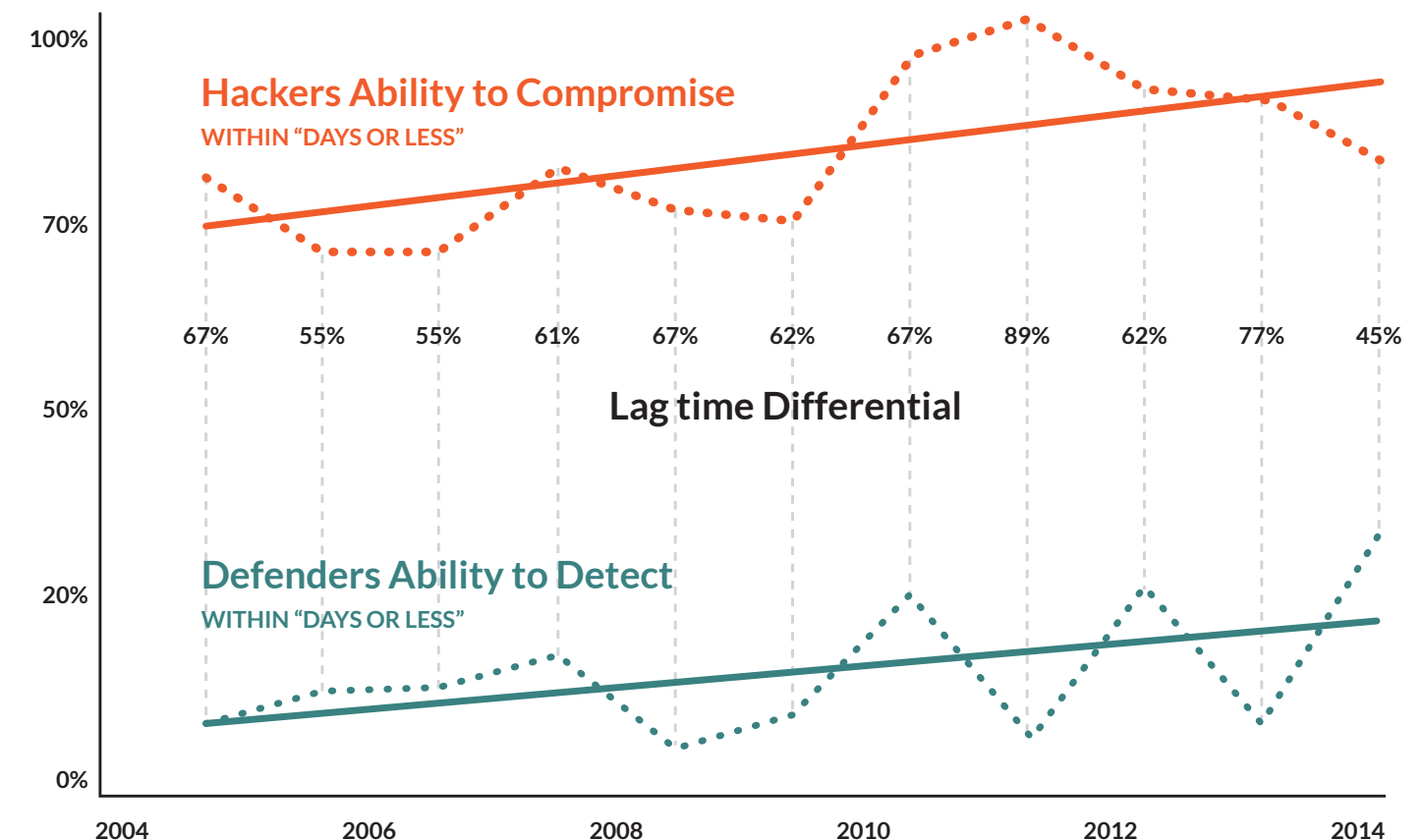


Figure 5

**TREND #4**

# DATA BREACHES ARE FREQUENT AND LARGE

Show this page to any data owner who might be skeptical of the need for better data protection.

**79,790**  
**SECURITY  
INCIDENTS**

—an “incident” is any event that exposes and compromises the confidentiality, integrity or availability of an information asset

**2,122**  
**DATA BREACHES**

—the frequency of breaches, defined as incidents that result in confirmed data disclosure to unauthorized parties, is growing

**1 BILLION**  
**RECORDS LOST**

**\$3.79 MILLION**  
—the average cost of recovering from a single data breach

**\$154.00**  
—the average cost per lost/stolen record

**+56%**  
—the increase in theft of “hard” intellectual property over 2014



TREND #4 (CONT.)

# DATA BREACHES ARE FREQUENT AND LARGE

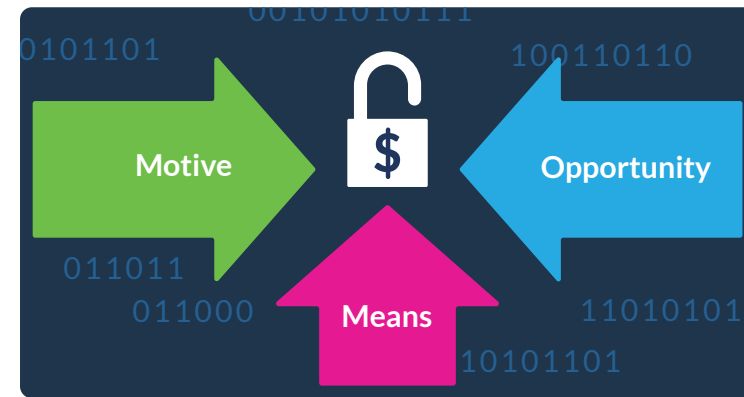
The size of data breaches is growing. 2015 was yet another year of massive data breaches, with an increase of 193 reported incidents from 2014’s total. Here’s a roundup of the ten biggest data breaches last year, by total records lost.

|    | ORGANIZATION                      | # RECORDS BREACHED |
|----|-----------------------------------|--------------------|
| 10 | Excellus BlueCross BlueShield     | 10 million         |
| 9  | Premiera                          | 11 million         |
| 8  | VTech                             | 11.3 million       |
| 7  | MacKeeper                         | 13 million         |
| 6  | T-Mobile                          | 15 million         |
| 5  | US Office of Personnel Management | 21.5 million       |
| 4  | Ashley Madison                    | 37 million         |
| 3  | Securus Technologies              | 70 million         |
| 2  | BCBS Anthem                       | 80 million         |
| 1  | Database of US Voters             | 191 million        |



**SEE OUR BLOG**  
Get more details about these breaches at our blog.

# ANATOMY OF A DATA BREACH



**MEANS** Tools, resources, and skills provide adversaries capability to dominate the Kill Chain, while remaining completely undetected.

**MOTIVE** State Sponsored: Acquire intelligence for military, political or economic advantage. Cyber criminals: Make money using any means necessary. Hacktivists: Promote their own political agenda.

**OPPORTUNITY** Timing and knowledge of the target increases the chances of a successful intrusion. Attackers leverage this information to achieve their objectives.

## HACKED CUSTOMER DATA CAN ERASE MILLIONS IN PROFITS WITHIN WEEKS

The UK telecommunications firm TalkTalk was the victim of a cyber-attack in late 2014. The attack resulted in the theft of personal data on 150,000 customers, including names, addresses, phone numbers and TalkTalk account numbers. According to the company the cost to the company was around £60 million, or \$88 million at current exchange rates.



## STOLEN INTELLECTUAL PROPERTY CAN ERASE COMPETITIVE ADVANTAGE AND ERODE SHAREHOLDER VALUE

American Superconductors Corporation (AMSC) was targeted by Chinese economic espionage. AMSC created the code and controls to operate large wind turbines and partnered with a Chinese-government backed private company, Sinovel Wind Group. Co, to manufacture the turbines themselves. After a booming business launch that saw AMSC grow revenue from \$50 million to \$500 million, ASMC eventually lost over a billion dollars in share value as Sinovel stole all of its intellectual property and began creating and selling its own turbines. ASMC is suing Sinovel for over \$1.2 billion dollars in Chinese courts, and has been in litigation with them for years.



## PRIVACY ABUSES CAN BRING UNWANTED SCRUTINY AND FINES FROM REGULATORS WHILE INFLICTING REPUTATIONAL DAMAGE

The US HHS Office for Civil Rights recently closed a pair of HIPAA breach settlements:

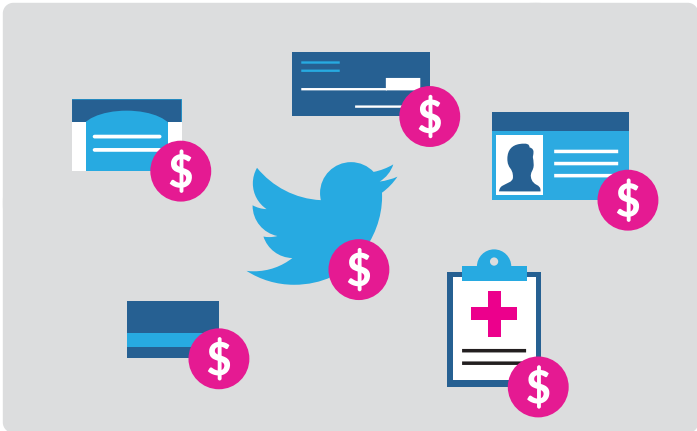
- \$3.9 million fine—Feinstein Institute for Medical Research
- \$1.55 million fine—North Memorial Health Care of Minnesota



TREND #5

# YOUR ORGANIZATION'S STOLEN DATA IS WORTH MORE

The underground economy profiting from cyber crime has sophisticated pricing and packaging models for selling your stolen data. The "Dark Web" of limited-access sites is used for illegal or criminal activity, offering any would be cyber thief global marketplaces in which to buy and sell stolen information.



The breadth of products now available for sale on the "Dark Web" has evolved to include almost every type of data as part of a formal and an efficient value hierarchy. Every bit of stolen information has value, anywhere from \$.55 to \$1,200 per record.

The massive amount of private data traded in this complex underground has transformed the economics of DLP.

|  |  |
|--|--|
| Counterfeit driver's license   | \$100-150                                  |
| Social media account credentials   | \$50                                       |
| Basic payment card data (including primary account number, card verification code, expiration date)...                                 | \$5-12 per individual (US)<br>\$25-30 (EU) |
| ...plus billing address, PIN, SSN, DOB   | \$30 (US)<br>\$45 (EU)                     |
| Bank account credentials (username & password) to an account with a \$2,000 balance...   | \$190 per compromised account              |
| ...to an account with a \$6,000 balance  | \$500                                      |
| ...to an account with a \$20,000 balance   | \$1,200                                    |
| Patient medical records or health insurance account info (including SSN, history, prescriptions, member ID number, claims information) | \$50 per individual record                 |
| Counterfeit Social Security cards ready-to-use   | \$250-400                                  |
| Complete identity profile plus a matching utility bill   | \$350                                      |

(source: Dell SecureWorks)

# WHAT HAPPENS TO STOLEN MEDICAL PATIENT DATA?

Cyber criminals monetize healthcare data in a different way than financial data, because it has a longer shelf life. Healthcare fraud may go undiscovered for months or years, making stolen medical identities among the most valuable. Medical identity fraud takes the form of either fraudulent billing by unethical providers or misuse of another person's medical records to obtain care. Criminals have become incredibly adept at monetizing stolen identities on a massive scale.

**\$363** Average cost of a  
lost/stolen data record  
for healthcare companies

**136%  
HIGHER**  
than the global average cost  
of a data breach per lost or  
stolen record

**\$154**  
Average cost of a  
lost/stolen data  
record for other  
organizations

(source: IBM/Ponemon Institute)



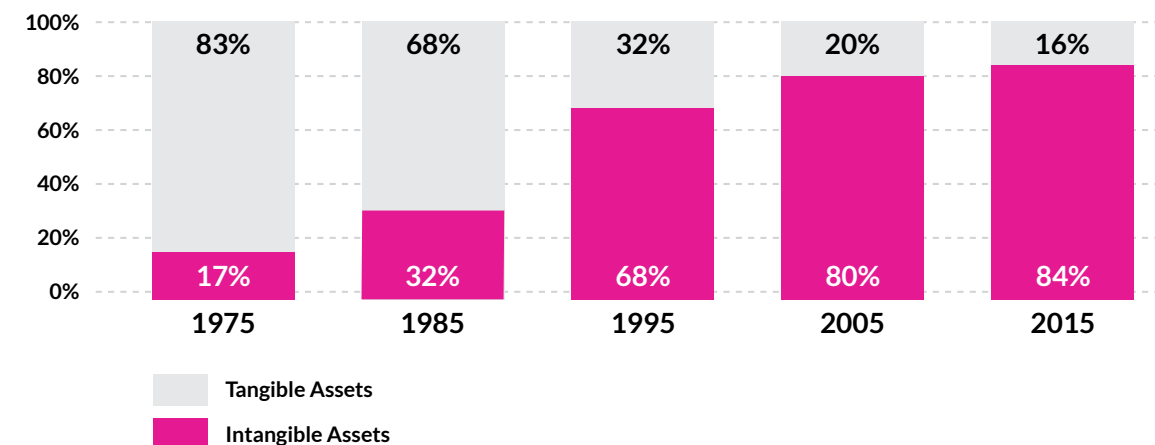
## TREND #6

# THERE'S MORE DATA THAT'S WORTH STEALING

The definition of what constitutes sensitive information has vastly expanded. It's no longer enough just to protect personally identifiable information (PII) and traditional intellectual property. Sensitive data includes all kinds of intangible assets such as pricing model or business methodologies that are pivotal drivers of competitive advantage and shareholder value.

**INTANGIBLE ASSETS (SUCH AS IP) HAVE GROWN FROM 17% OF THE S&P 500'S MARKET VALUE IN 1975 TO 84% IN 2015**

Components of S&P 500 Market Value



(source: Ocean Tomo, Annual Study of Intangible Asset Market Value)

## TREND #7

# THE SECURITY TALENT SHORTAGE IS HERE TO STAY

Cybersecurity has become a big business. As a result, it's become an IT specialty that can't find qualified practitioners fast enough to address the growing threats. Maybe you've already felt this pinch in your IT group. As an organization, you should be betting that this trend continues, because the security talent shortage is not going away anytime soon.

**209,000**

Number of cybersecurity jobs in the U.S. that remained unfilled at the start of 2016.

**ONE  
MILLION**

Number of cybersecurity job openings worldwide, a backlog that could take up to 20 years to fill.

**53%**

Growth in demand for information security professionals expected over the next two years.

**74%**

Rise in the number of job postings over the past five years.

**6 MILLION**

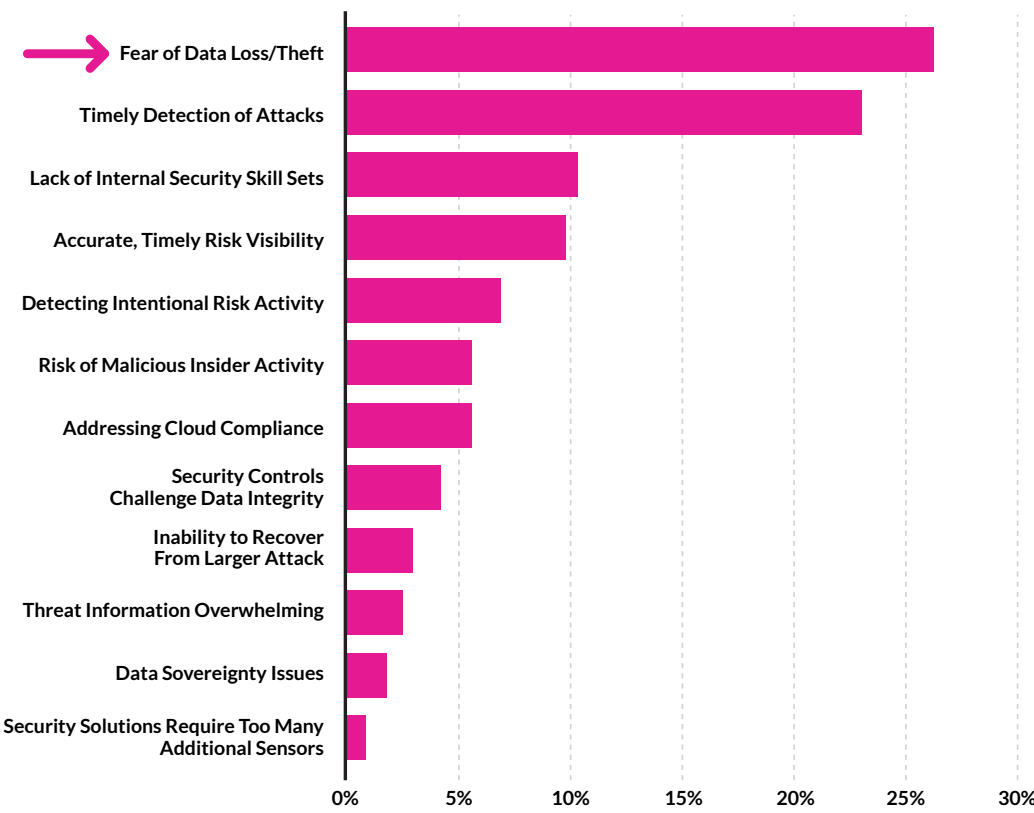
Number of information security professionals needed globally by 2019, with a projected shortfall of 1.5 million.

# DLP BY THE NUMBERS

“FEAR OF DATA LOSS OR THEFT” RANKED AS THE TOP SECURITY CHALLENGE OVER THE NEXT 12 MONTHS...

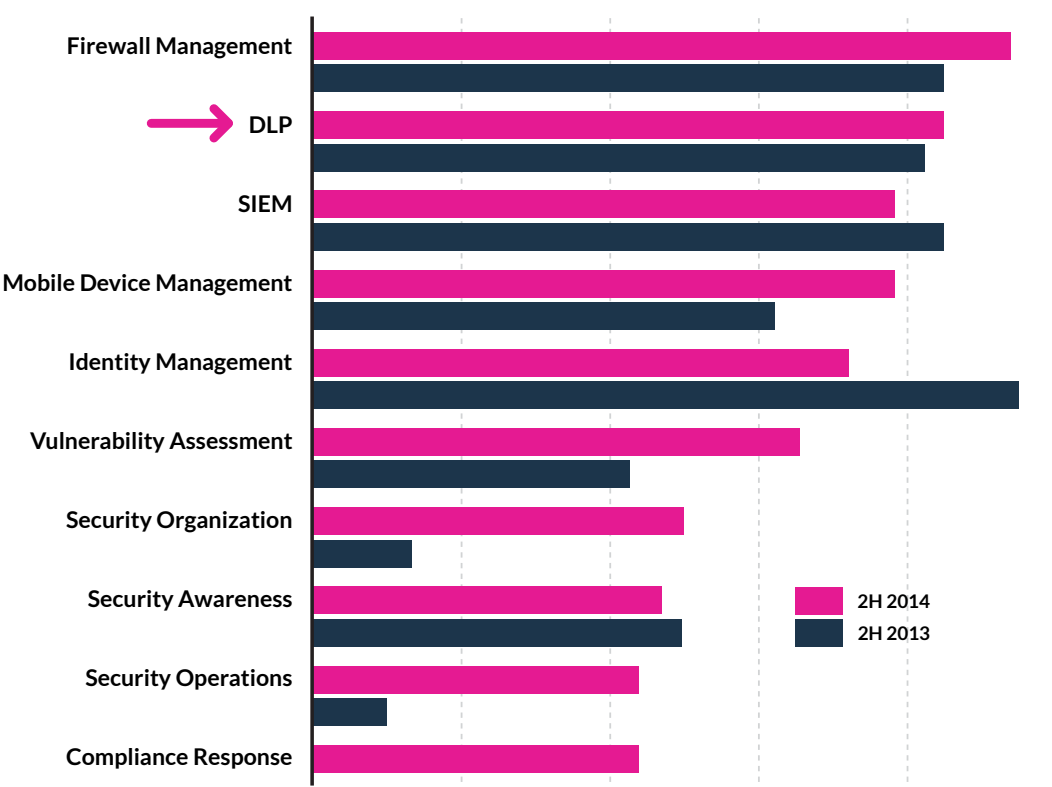
## BIGGEST SECURITY CHALLENGE—NEXT 12 MONTHS

Q: What is your top information security challenge for the next 12 months?



DLP RANKED #2 AMONG PLANNED INFORMATION SECURITY PROJECTS ACROSS MORE THAN 20 CATEGORIES...

## INFORMATION SECURITY PROJECTS—TOP CATEGORIES



 **FREE DOWNLOAD**

To learn more, download the 451 Research report, "The Data Loss Prevention Market by the Numbers," 2015

## PART FOUR

# THE SHIFT TO DATA-CENTRIC SECURITY

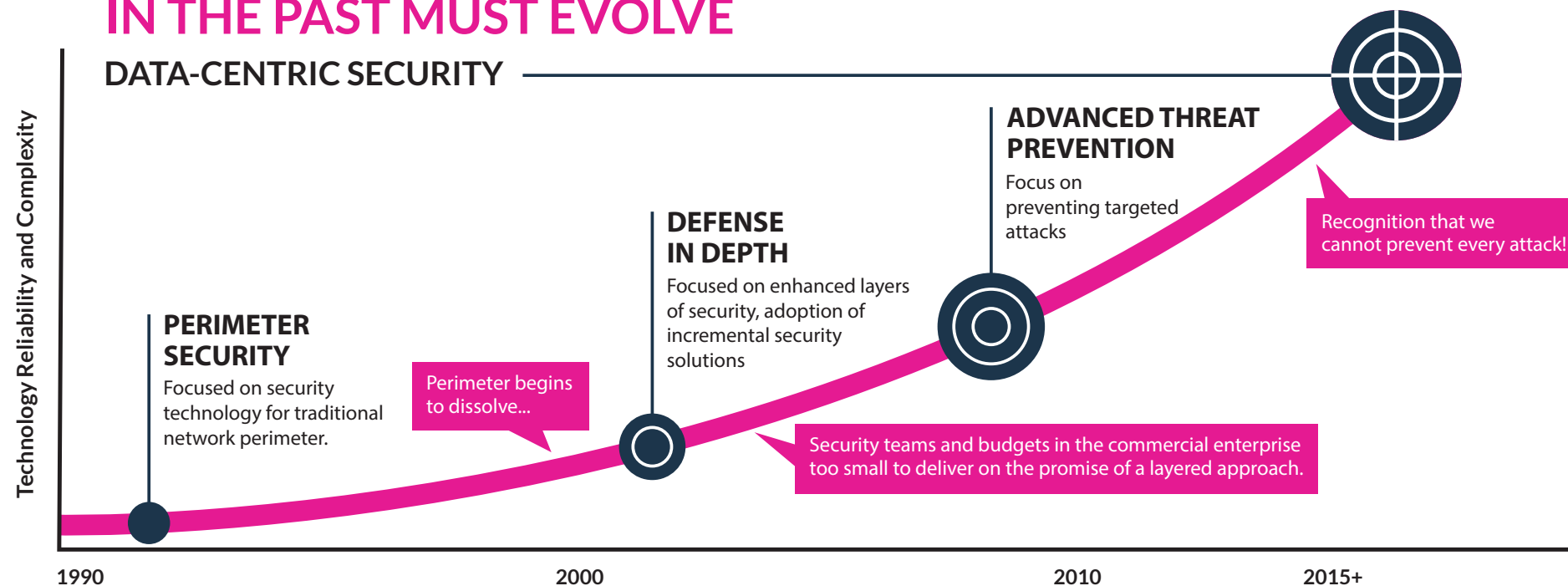
“S&R pros must take a data-centric approach that ensures security travels with data regardless of user population, location, or even hosting model.”

–*The Future Of Data Security And Privacy: Growth And Competitive Differentiation*, Forrester Research, Inc., July 10, 2015



# ALL THE TRENDS LEAD TO DATA-CENTRIC SECURITY

THE SECURITY PARADIGMS THAT SERVED IN THE PAST MUST EVOLVE



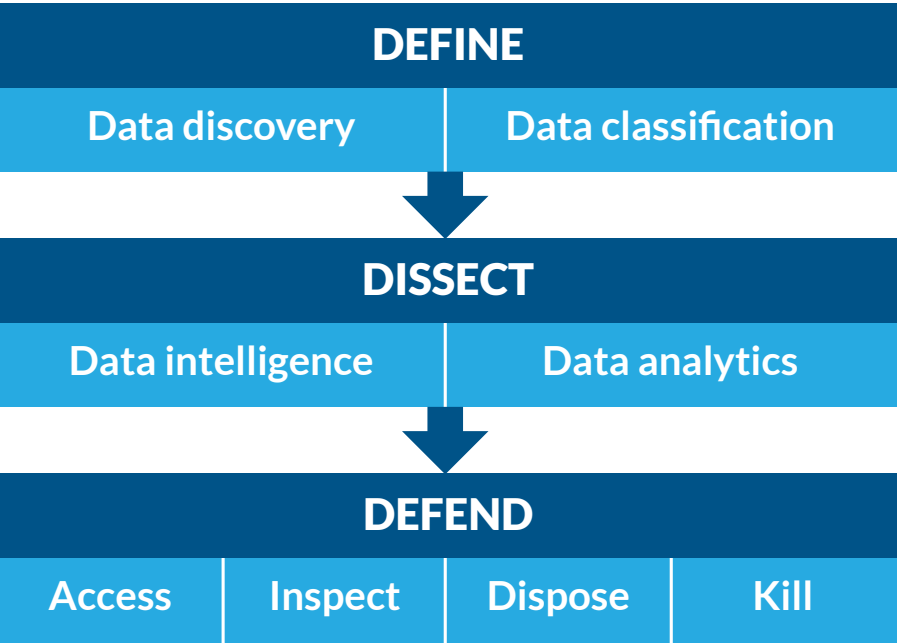
Simply stated, DLP is the foundation for data-centric security.

# “DIGITAL BUSINESSES REQUIRE A DATA-CENTRIC APPROACH.”

“In this new reality, traditional perimeter-based approaches to security are insufficient. S&R pros must take a data-centric approach that ensures security travels with the data regardless of user population, location, or even hosting model.”

# A DATA-CENTRIC SECURITY FRAMEWORK

Many organizations need help getting started. Forrester has created a framework to guide you on this journey. Their “Data Security & Control Framework” (figure below) breaks the problem of controlling and securing data into three steps: Define, Dissect, Defend. With these steps completed organizations better understand their data and can then allocate resources to more efficiently protect critical assets.



**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.



· To learn more about data-centric security, get Dan Geer's "5 Myths Holding Your Security Program Back" eBook

(source: The Future Of Data Security And Privacy: Growth And Competitive Differentiation, Forrester Research, Inc., July 10, 2015)

## PART FIVE

# DETERMINING THE RIGHT APPROACH TO DLP

## STEP 1

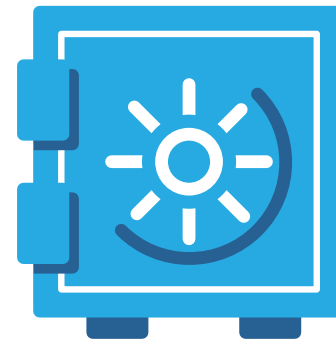
# DETERMINE YOUR PRIMARY DATA PROTECTION OBJECTIVE

The most important consideration before undertaking a DLP project is to determine your organization's primary data protection objective. Traditionally, organizations adopt DLP to achieve one of three objectives:

### COMPLY WITH REGULATIONS



### PROTECT INTELLECTUAL PROPERTY



### COMPLY WITH BUSINESS PARTNER





## STEP 1 (CONT.)

# DETERMINE YOUR PRIMARY DATA PROTECTION OBJECTIVE

### COMPLY WITH REGULATIONS

Compliance has long been and remains a primary driver of DLP demand. Starting more than 15 years ago, regulatory requirements mandated controls for handling sensitive data and helped drive a surge of “checkbox DLP” purchases by large, compliance-bound enterprises. Heavily regulated industries, such as financial services, retail, government and healthcare, tend to invest most in DLP when compliance is the primary objective.

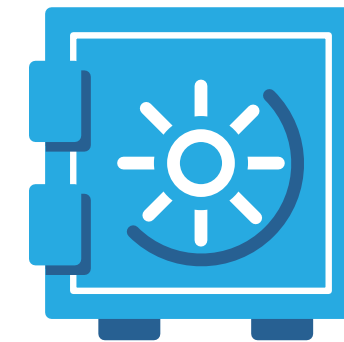


## STEP 1 (CONT.)

# DETERMINE YOUR PRIMARY DATA PROTECTION OBJECTIVE

### PROTECT INTELLECTUAL PROPERTY

The loss of IP can result in a permanent loss of competitive advantage. IP tends to skew towards unstructured data. DLP tools must be trained to understand which unstructured information constitutes your organization's critical IP, meaning the solution must be able to discern unstructured data's content and context.



# PII VS. IP

Forrester Research makes the case for IP protection as the top DLP objective as compared to securing personal cardholder information (PCI), personal health information (PHI) or personally identifiable information (PII).

|                              | PCI, PHI, PII (75% of use cases)  | IP   |
|------------------------------|---|--|
| <b>Creator/owner</b>         | <ul style="list-style-type: none"> <li>• Business partners</li> <li>• Customers</li> </ul>  | <ul style="list-style-type: none"> <li>• Enterprise</li> </ul>   |
| <b>Relationship to data</b>  | <ul style="list-style-type: none"> <li>• Custodian</li> </ul>   | <ul style="list-style-type: none"> <li>• Owner</li> </ul>  |
| <b>Examples</b>              | <ul style="list-style-type: none"> <li>• Customer PII</li> <li>• Credit card numbers</li> <li>• Government identifiers</li> </ul> | <ul style="list-style-type: none"> <li>• Trade secrets</li> <li>• Strategic plans</li> <li>• Sales forecasts and financials</li> </ul> |
| <b>Source of value</b>       | <ul style="list-style-type: none"> <li>• External: determined by regulators and criminals</li> </ul>                              | <ul style="list-style-type: none"> <li>• Internal</li> </ul>   |
| <b>Compulsion to protect</b> | <ul style="list-style-type: none"> <li>• Controlled by regulation, statute, or contract</li> </ul>                                | <ul style="list-style-type: none"> <li>• Loss would cause strategic harm</li> </ul>  |
| <b>Consequences</b>          | <ul style="list-style-type: none"> <li>• Cleanup, notification costs</li> </ul>   | <ul style="list-style-type: none"> <li>• Revenue losses</li> </ul>   |
| <b>Key question</b>          | <ul style="list-style-type: none"> <li>• Why is the data circulating?</li> </ul>  | <ul style="list-style-type: none"> <li>• Who needs to know?</li> </ul>   |
| <b>Priorities</b>            | <ul style="list-style-type: none"> <li>• Stop circulation</li> <li>• Reduce use</li> </ul>  | <ul style="list-style-type: none"> <li>• Control circulation</li> <li>• Reduce abuse</li> </ul>  |
| <b>Domain experts</b>        | <ul style="list-style-type: none"> <li>• IT security, legal</li> </ul>  | <ul style="list-style-type: none"> <li>• Business units</li> </ul>   |

(source: Rethinking Data Loss Prevention With Forrester's DLP Maturity Grid, Forrester, April 18, 2016)

## STEP 1 (CONT.)

# DETERMINE YOUR PRIMARY DATA PROTECTION OBJECTIVE

### BUSINESS PARTNER COMPLIANCE

The globalization of the supply chain means that manufacturers of goods and services rely on global relationships to deliver value to their customers. To facilitate this an unimpeded data flow is needed, often this stream contains sensitive data. Global relationships requires an unimpeded data flow necessitating robust data protection.

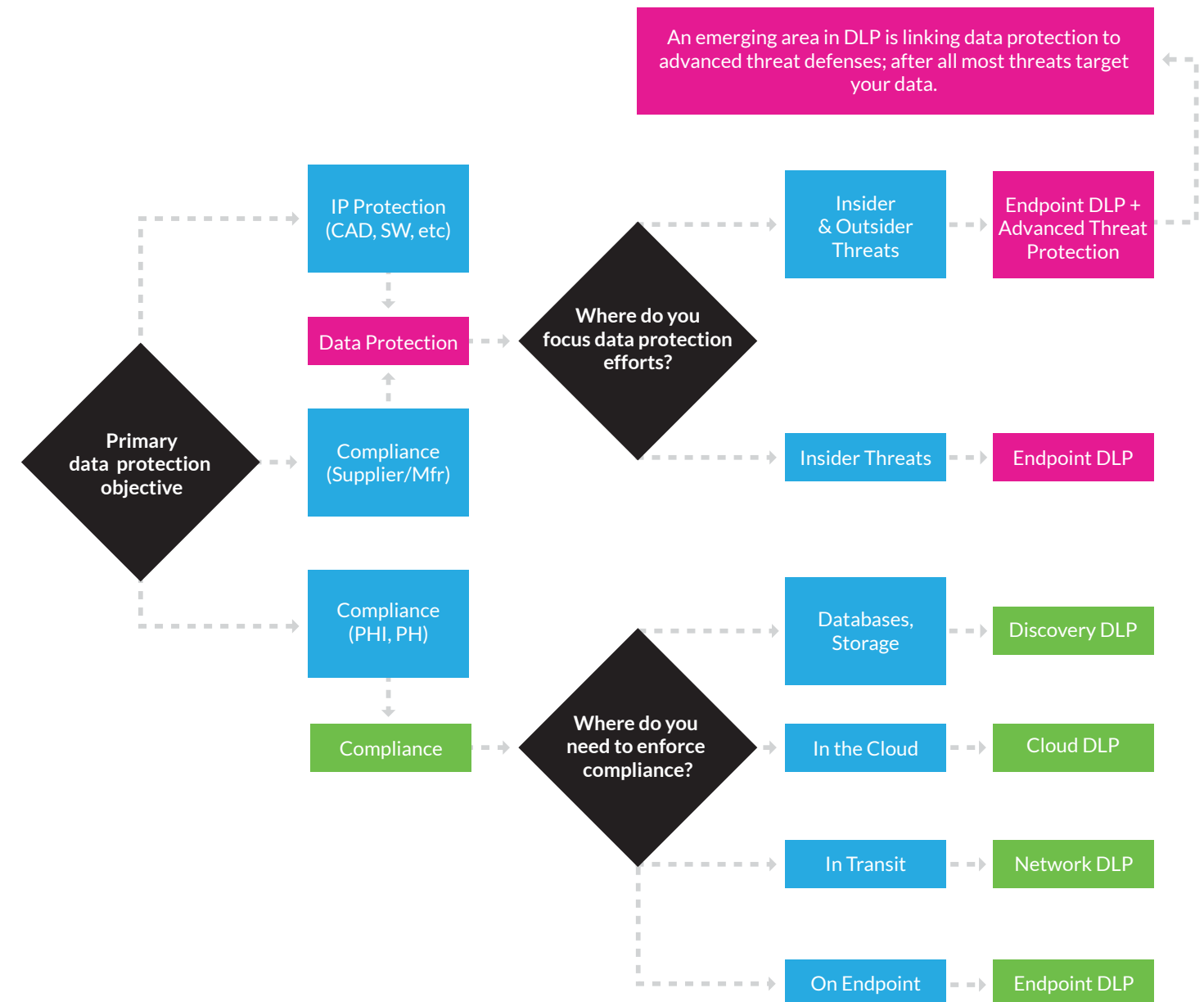


## STEP 2

# DETERMINE ARCHITECTURE

With your data protection objective defined (IP protection, regulatory compliance or business partner compliance) let's explain your DLP deployment architecture options. Use the chart on the right to map your objectives to the deployment model that best aligns. A growing number of organizations leverage multiple DLP solutions to best cover their evolving business.

The following pages detail each of the four architectures: Endpoint, Network, Discovery, and Cloud.

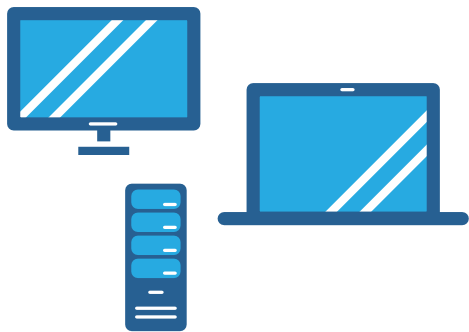


## STEP 2 (CONT.)

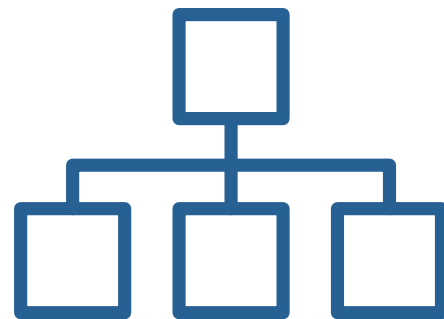
# DETERMINE ARCHITECTURE

Here are the four primary DLP deployment architectures:  
Endpoint, Network, Discovery, and Cloud.

### ENDPOINT DLP



### NETWORK DLP



### DISCOVERY DLP



### CLOUD DLP





## STEP 2 (CONT.)

# DETERMINE ARCHITECTURE

Most data protection programs begin with either endpoint-based or network-based DLP. What's the difference?

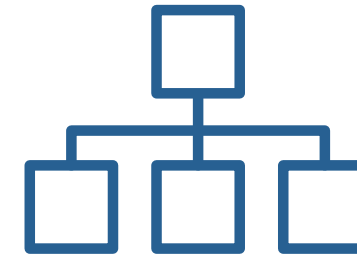
### ENDPOINT DLP

Endpoint DLP relies primarily on purpose-built software agents, that live on endpoints - laptops, desktops, servers, any device that runs on Microsoft Windows, Linux, or Apple OS X. The agent delivers visibility and, if desired, control over data. Deployment involves installing the agent on machines where protections is desired. No agent means no coverage.



### NETWORK DLP

Network DLP, often referred to as agentless DLP, delivers visibility and control of traffic that passes across the network. A physical or virtual machine inspects all traffic, such as mail, web, IM and can then enforce data policies. Deployment is either via a physical appliance or a virtual machine then configuring network traffic to pass through for the inspection.



## STEP 2 (CONT.)

# DETERMINE ARCHITECTURE

The other two variants of DLP, Cloud and Discovery, complete the data protection story and further protect your sensitive data in storage, either local or cloud based.

### DISCOVERY DLP

Discovery DLP proactively scans your network, including laptops, servers, file shares, and databases to deliver a comprehensive analysis of where sensitive data resides on all these devices. To perform the data discovery some solutions require an agent to also be installed on the machine being scanned.



### CLOUD DLP

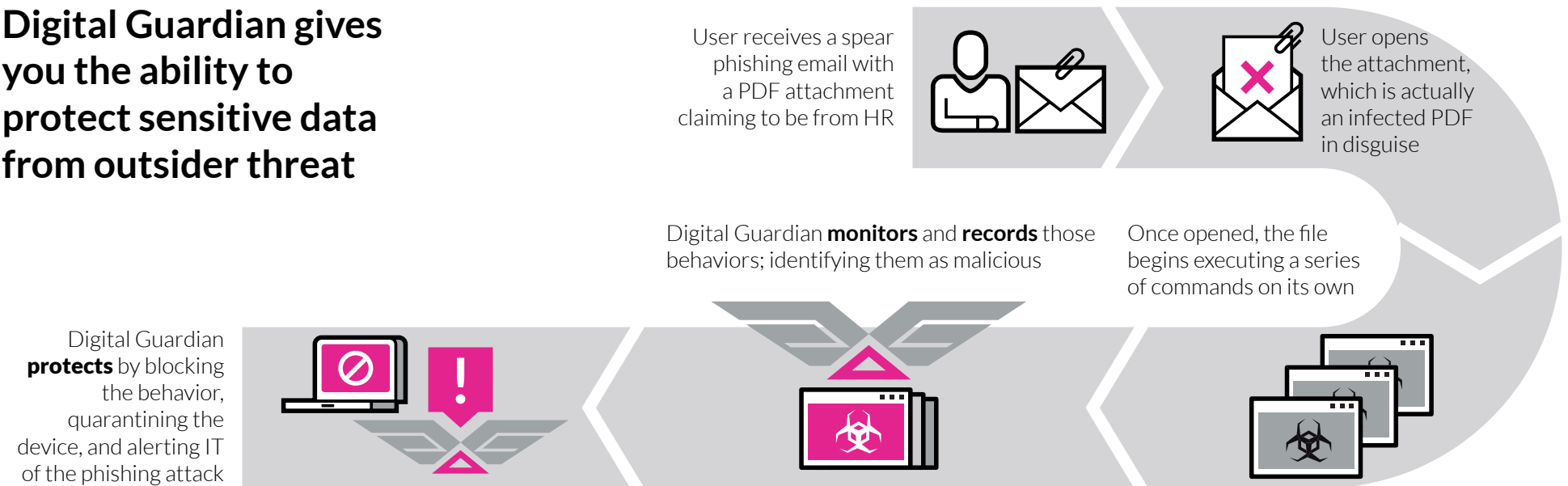
Cloud DLP, much like Discovery DLP, scans storage repositories and delivers an accurate picture of where sensitive data lives, though as its name suggests Cloud DLP focuses on your data that lives in the cloud. Cloud DLP relies on an API (Application Program Interface) to connect with the cloud storage service (Box, OneDrive, etc.) then scan the content. Cloud DLP sees data as it is being put into the cloud and can perform a cloud storage audit or remediation.



# DATA PROTECTION AND ADVANCED THREAT PROTECTION

## ATTACKS DON'T ALWAYS HAVE TO MEAN BREACHES

**Digital Guardian gives you the ability to protect sensitive data from outsider threat**



Attacks are inevitable. With the proper protocols and tools in place, you can spot and contain breaches before sensitive data gets out. Digital Guardian for Advanced Threat Protection is uniquely focused on understanding and preventing threats targeting your data and placing your systems at risk.

Digital Guardian takes a data-centric approach to advanced threat detection, incident response and prevention that ensures security travels with the data.



**WATCH  
THE VIDEO**  
DG Revokes  
Phishing Licenses.

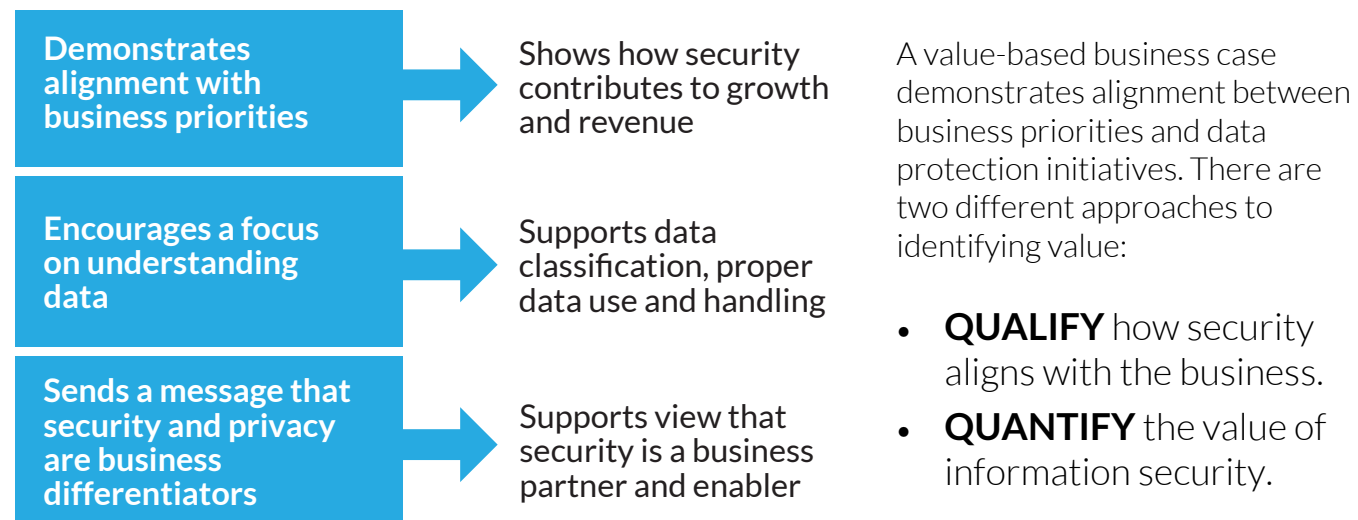
## PART SIX

# 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?



# QUALIFY HOW SECURITY ALIGNS WITH YOUR BUSINESS

This value-based approach highlights how security initiatives support or enable key business imperatives or initiatives, which aids strategic discussions and executive visibility. Here are two tips to keep in mind:

## **TIP #1**

Use the right language for the right audience. Attack surface reduction, OS X coverage, and technology integrations work well with the CISO. CapEx reduction, no additional FTEs, and reduced TCO appeal to the CFO.

## **TIP #2**

Tie data security to the right top-line goals and timelines. Your security team might talk in terms of only a 3-6 month plan, but line-of-business management plans out a full 12 months, while the corporate office gazes at a 3-5 year picture.



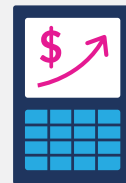
# QUANTIFY THE VALUE OF INFORMATION SECURITY

## CALCULATE THE BENEFIT OF PROTECTING INFORMATION ASSETS.



### CALCULATE THE REVENUE AN INFORMATION ASSET PRODUCES TODAY

Consider the market value of your organization's trade secrets, formulas, proprietary methodologies, and other IP that keep you in business. Protect what's most important: the information assets that actually make your organization money.



### CALCULATE ADVANTAGE FOR TOMORROW

Don't stop at the data that produces revenue today. What IP will help drive market share tomorrow? Quantify how a strong data protection regime would affect business growth over the next 3-5 years.

POSITIVE BUSINESS OUTCOMES

# A WORD ABOUT CYBER INSURANCE COVERAGE

Insurers that issue coverage against losses from cyberattack assess your security tools to determine risk and calculate rates. With the increased frequency of well-publicized breaches, cyber insurance premiums have been volatile—especially in regulated industries like retail and healthcare.

There are a number of pitfalls and exclusions to watch out for when it comes to cyber insurance policy coverage.

**1.** Be sure you know what is covered and what isn't covered. Intellectual property is often excluded due to the difficulty in determining its valuation and the complexity, or in many cases, inability to recover from loss or repair the damage.

**2.** Insured organizations face heightened due diligence from underwriters. They may ask about your formal incident response plan, deployment of encryption technology, compliance regime for impending regulations, or the security of vendor networks.

# POSITIONING DLP TO EXECUTIVES

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

- CEO and Board
- CISO
- CFO
- Director of InfoSec
- Business Unit Lead
- CMO

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

# POSITIONING DLP TO EXECUTIVES

## 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

### 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

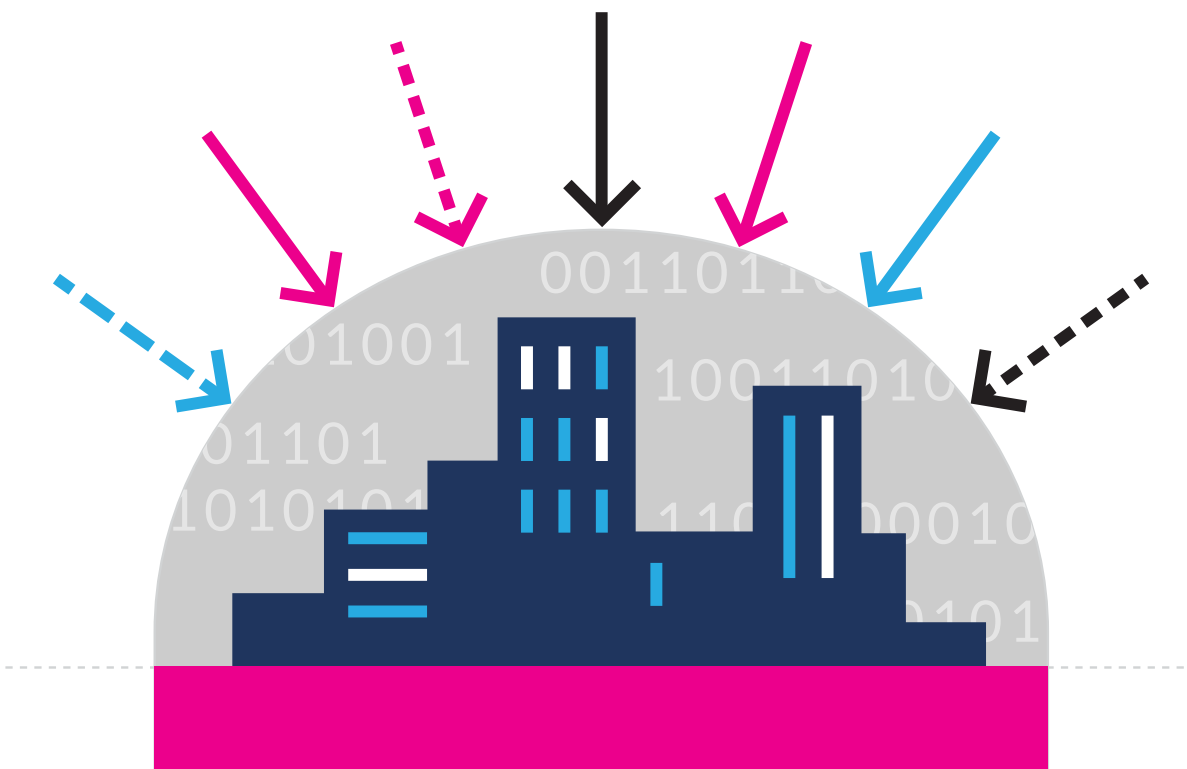
# PART SEVEN

# BUYING DLP

To guide you in your data protection journey, this section offers some tips and then a detailed evaluation matrix that can serve as a starting point for your decision making process.

# THE FIRST STEP IS DISCOVERY

Before reaching out to vendors, engage business leaders informally on what data exists and how it's used. 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.



# HOW TO EVALUATE DLP SOLUTIONS

## HERE ARE THE STEPS WE COMMONLY SEE AS ENTERPRISES EVALUATE DLP VENDOR SOLUTIONS:

1. **Research initial vendor set.** Hundreds of vendors offer some form of data protection. We recommend identifying and applying a set of filters to narrow down your organization's choices. One common filter is identifying whether the vendor supports all of your operating environments. Another guide used by many organizations is the Gartner Magic Quadrant report for Enterprise DLP. Peer research is a valuable source of information.
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. This process can be as structured as you need it to be to satisfy your internal organization.
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 that can be engaged for onsite 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.

**Gartner®**



- Get a complimentary copy of the 2016 Gartner MQ for Enterprise DLP.



- View webinar recording on 2016 Gartner MQ for Enterprise DLP.

# VENDOR EVALUATION CRITERIA

Your environment ultimately decides which of the 4 DLP variants to deploy. Within each one there are key criteria to consider.

1. **Breadth of Offerings.** Are Network, Endpoint, Cloud, and Discovery all offered from the potential vendor?
2. **Platform Support.** Are Windows, Linux, and OS X all supported with feature parity?
3. **Deployment Options.** Are on-premises or managed options offered?
4. **Internal and External Threats.** Do you need to defend against one or both?
5. **Content vs Context.** How do you intend to perform data inspection and classification?
6. **Structured vs Unstructured.** What types of data are you most concerned with protecting?
7. **Policy Based vs Event Based.** How do you plan to see and enforce data movement?
8. **Technology Alliance Partners.** What parts of your ecosystem do you wish to integrate with your DLP?
9. **Timeline.** How quickly do you need to be operational?
10. **Staffing Needs.** What additional, if any, staffing will the solution require?



**FREE  
DOWNLOAD**

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

# DLP DELIVERY OPTIONS

Data Loss Prevention used to be delivered solely via licensed software and hardware appliances. The emergence of data protection as a managed service puts DLP in the reach of more organizations looking to control costs while optimizing data protection.

## **BENEFITS OF DLP MANAGED SERVICES**

- Accelerated time-to-value—eliminating complexity and maximizing IT efficiency
- Access to a team of expert data analysts—professionals trained to identify risk, assist with policy creation, and provide incident response
- Leverage operating expense budget

## **BENEFITS OF DLP ON-PREMISES**

- Leverage existing security staff expertise and investment
- Control over all aspects of the day-to-day management, deployment, and upgrades

“...because I wanted to make sure that I utilize the talent that your team has because that’s your bread and butter; your team knows, sleeps with it, breathe it, and dreams of it every day.”

–Digital Guardian MSP customer

“We have a deep bench of security people, but I need them to be chasing threats, not ghosts. Digital Guardian shows me the threats linked to my critical data.”

–Digital Guardian on-premises customer



### **WATCH THE VIDEO**

Alleviate the talent shortage with Managed Security.

# MANAGED SECURITY SERVICES EVALUATION CHECKLIST

Managed services for DLP can be evaluated the same way you evaluate any managed service. Standard criteria such as service level agreement or global coverage still apply. However, consider these two additional questions of the prospective MSP for DLP:

**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) Type II
- ☐ 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 EIGHT

# GETTING SUCCESSFUL WITH DLP

# START WITH A CLEARLY DEFINED “QUICK WIN”

When enterprise DLP deployments stall or fail it's often due to overly complex initial rollout plans; they try to tackle too many data types or use cases. You can achieve a quick win by defining your initial approach and setting objectives that are fast and measurable. We have seen two initial approaches that have worked across hundreds of successful deployments. If you have a clear mandate to protect a specific sensitive data set, take the project approach. If not, we recommend the data visibility approach.



## PROJECT APPROACH

With the project approach you're narrowing in on a specific compliance requirement or a group of specific users. It is focused on known sensitive data types in identified locations and users. The quick win objective here is initially focusing on just one specific data type.

- **Driven by specific compliance or IP protection project**
- **Focus**
  - Known sensitive data types and locations
  - Specific user groups
  - Enabling secure business process



## DATA VISIBILITY APPROACH

The goal here is to learn where sensitive data is located, how it flows in the organization and where that data is at risk. The focus is on discovery and automated classification of sensitive data and the predominant egress channels. A quick win objective here is just concentrating on controlling the egress of sensitive data.

- **Driven by need to learn**
  - Where sensitive data is located
  - How it flows in the organization
  - Where it is put at risk
- **Focus**
  - Discovery and classification
  - Egress channels
  - Quick-win ROI by controlling egress first



## WATCH THE VIDEO

Simplify your data protection program for quick wins.

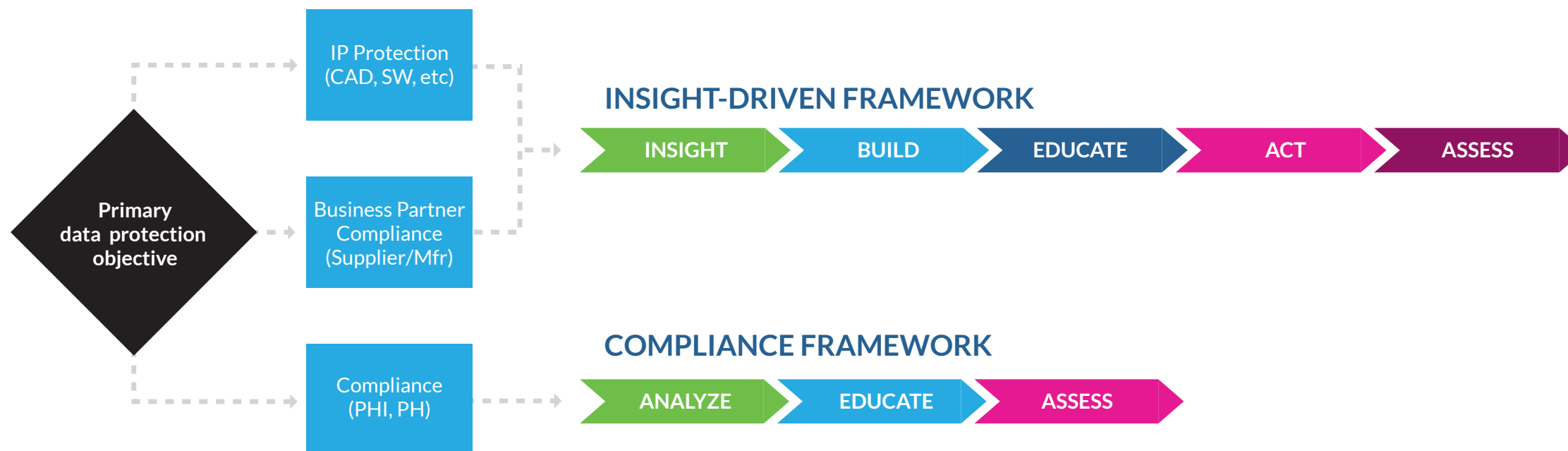


# STEAL OUR FRAMEWORKS

There are many sophisticated DLP frameworks from which to choose. But many DLP projects fail or stall because the security and risk team tries to execute a complex framework from the start. We have two simple frameworks that provide an efficient path to protecting sensitive data, mitigating risk and affecting change across your entire organization.

**“You don’t need a sophisticated framework to get high impact results.”**

*John Graham, CISO, Jabil*



# A PROVEN COMPLIANCE FRAMEWORK

Done right, DLP can provide the foundation for a straightforward compliance framework that combines people, processes, and technology to prevent breaches.



## FIRST STAGE: ANALYZE & CONTROL RISKS TO REGULATED DATA

Compliance and protection start with understanding your risks. Deploy Discovery DLP and Network DLP to identify, analyze and control risks to regulated data such as PII, PHI, PCI.

Discover, monitor and control PII/PHI/PCI that is being:

- Emailed out of your organization
- Transferred out of your organization in unencrypted FTP
- Copied to USB devices or burned to CDs or DVD
- Uploaded to the cloud

## SECOND STAGE: TRAIN EMPLOYEES ON SECURITY POLICIES IN REAL TIME

Employees are your biggest risk. Use DLP to prevent user actions that put your organization's data at risk and educate users in real time on the appropriate handling of regulated data.

When users attempt to violate policies:

- Display prompts
- Request justification
- Educate with positive reinforcement (Gamification)

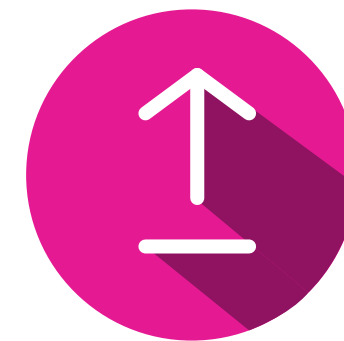
## THIRD STAGE: ASSESS & ITERATE SECURITY POLICIES

You can't improve what you don't measure. DLP provides a mechanism to continuously assess, iterate and improve security policies and procedures.

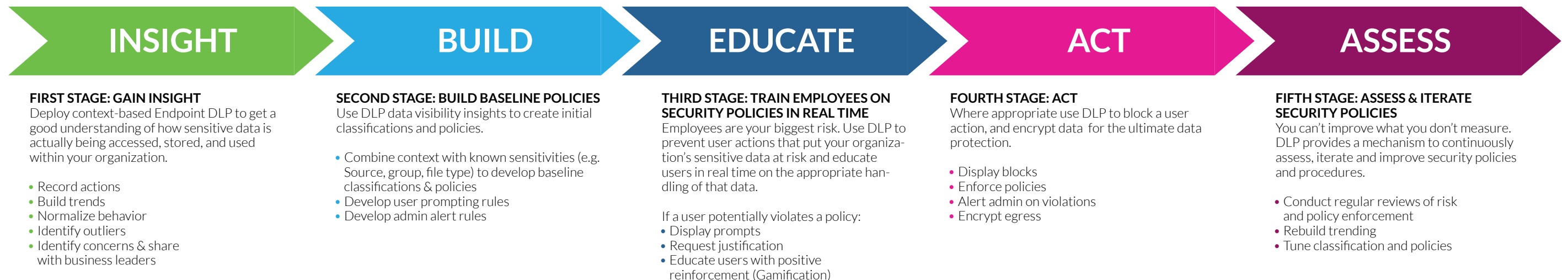
- Regular review of risk and policy enforcement
- Rebuild trending
- Tune classification and policies

# A PROVEN INSIGHT-DRIVEN FRAMEWORK

Context-based DLP is not dependent on a policy-driven approach for success. Instead you can use this proven, insight-driven framework. The key to success is that instead of dealing with abstractions, you bring real insights about how sensitive data is actually used to business leaders, then build policies from the ground up. Continue to use insights to tune. Rinse and repeat.



**WATCH THE VIDEO**  
Getting to data visibility and insights quickly.



## CASE STUDY

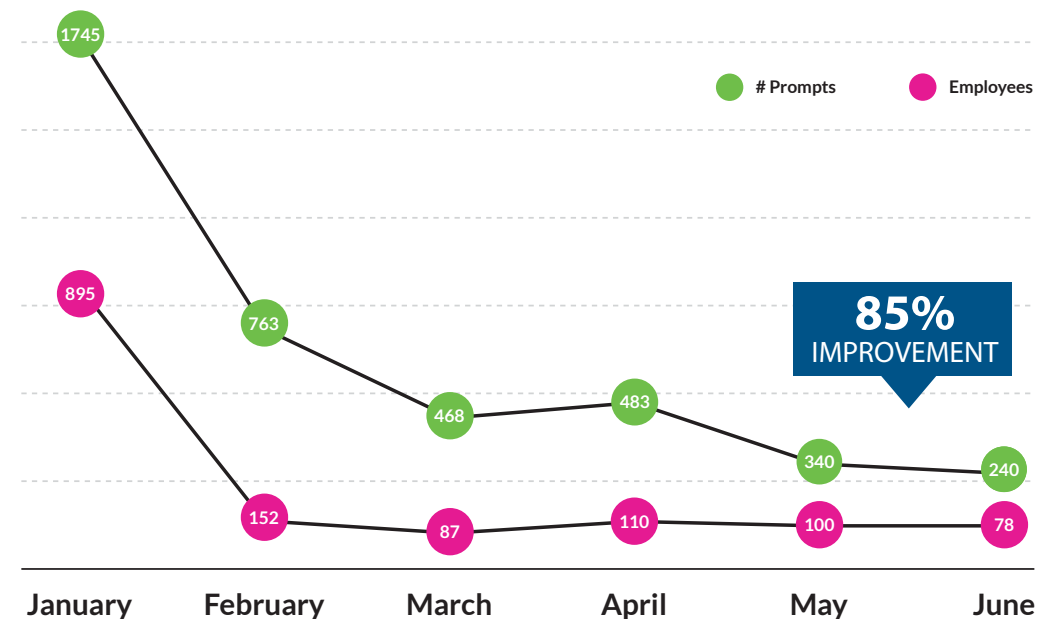
# THE POWER OF REAL-TIME USER EDUCATION

**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.

# 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, 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, Chief Information Security Officer, Jabil*

**JABIL**

## 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.

# POLICY: THERE’S NO ONE RIGHT WAY

One thing we’ve learned when it comes to patterns in data protection strategies is there are no patterns. What we often see is that the DLP strategy is more closely aligned to corporate culture than anything else. A culture focused on employee workflow leads to a “monitor only” deployment, while on the other end of the spectrum a heavily regulated company may implement strict prompting and blocking rules.

| Removable Storage | Mobile Devices | Outlook Email | CD/ DVD | Home Network | Uploads & Webmail | Outlook Data File | Cloud Uploads |                           |
|-------------------|----------------|---------------|---------|--------------|-------------------|-------------------|---------------|---------------------------|
| MONITOR           | MONITOR        | MONITOR       | MONITOR | MONITOR      | MONITOR           | MONITOR           | MONITOR       | “Monitor” Only Company    |
| MONITOR           | MONITOR        | MONITOR       | MONITOR | MONITOR      | PROMPT            | PROMPT            | BLOCK         | Balanced Company          |
| PROMPT            | PROMPT         | PROMPT        | PROMPT  | PROMPT       | BLOCK             | BLOCK             | BLOCK         | Heavily Regulated Company |



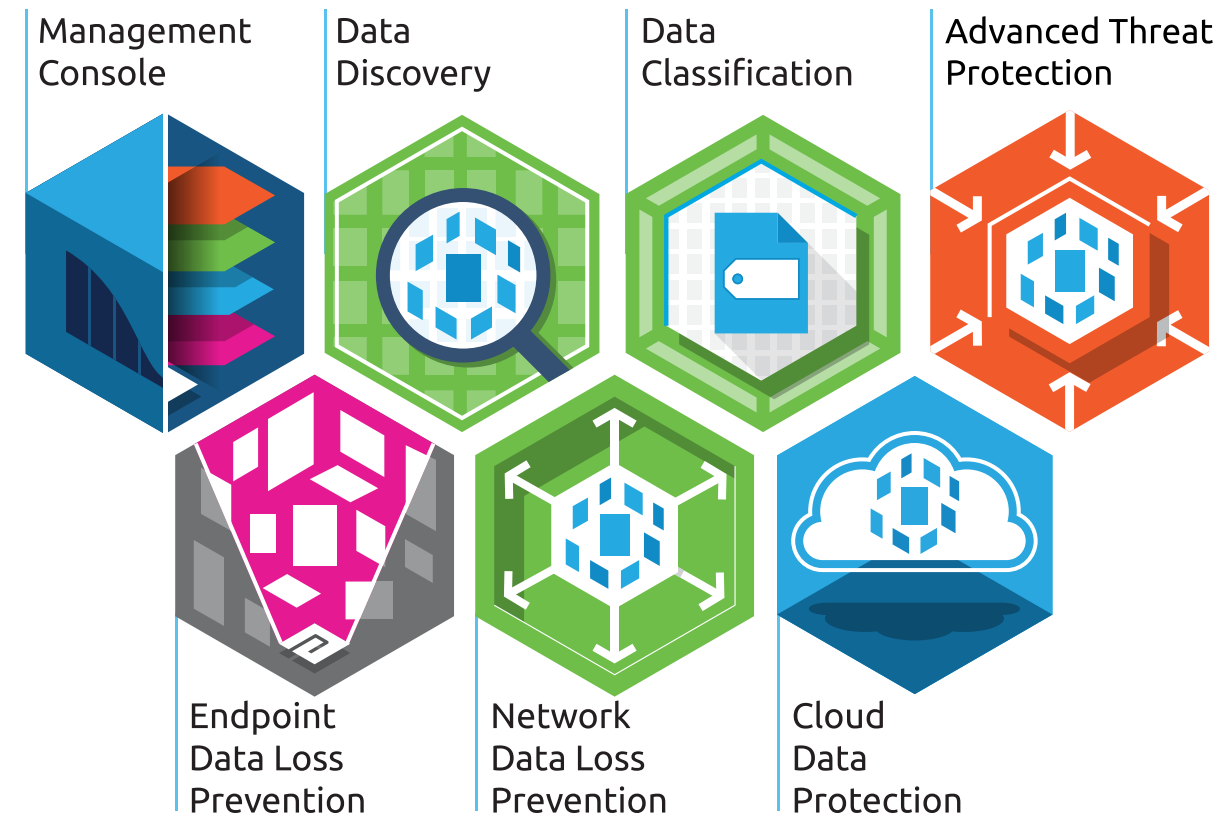
## PART NINE

# **DIGITAL GUARDIAN: NEXT GENERATION DATA PROTECTION**

# NEXT GENERATION DATA PROTECTION

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

- Discover and protect sensitive data throughout the data lifecycle and across the enterprise
- Protect sensitive data on the network at the endpoint, in storage and in the cloud
- Provide automated classification
- Provide integrated advanced protection to protect data from external threats
- Provide flexible deployment options including a managed security service manned by our peerless analyst team with deep, real-world expertise



Digital Guardian  
Platform Technical  
Overview



Digital Guardian  
Managed Security  
Program Technical  
Overview

# A LEADER IN THE GARTNER MAGIC QUADRANT

- “Digital Guardian offers one of the most advanced and powerful endpoint DLP agents due to its kernel-level OS integration. In addition to Windows, both Apple OS X and Linux are supported.”
- “The Digital Guardian solution for endpoint covers DLP and endpoint detection and response (EDR) in a single agent form factor...”
- “...Digital Guardian [is one of] two vendors most frequently mentioned by clients looking for a managed services option.”

**Gartner 2016 Magic Quadrant for Enterprise Data Loss Prevention, 1 February, 2016, Brian Reed and Neil Wynne.**

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Digital Guardian.



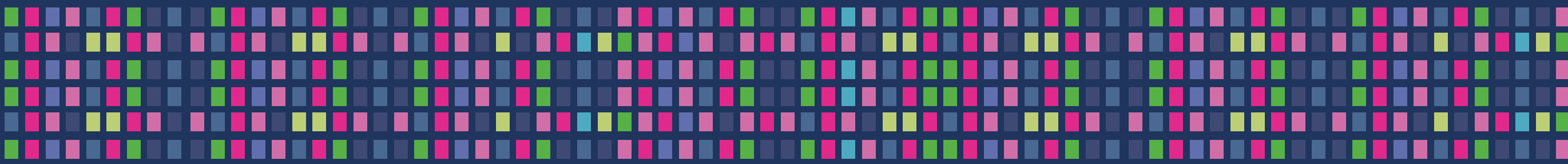
• Gartner 2016 MQ  
for Enterprise DLP

## 2016 GARTNER MAGIC QUADRANT FOR ENTERPRISE DATA LOSS PREVENTION



# 60 MILLION TERABYTES

OF SENSITIVE DATA IS PROTECTED DAILY BY DIGITAL GUARDIAN AGENTS



OVER **2.5 MILLION** AGENTS DEPLOYED WORLDWIDE

TRUSTED DAILY BY MORE THAN **450** OF THE LARGEST BRANDS IN THE WORLD

ACROSS **54** COUNTRIES

...ONE OF THE LARGEST AND MOST RESPECTED COMPANIES IN THE WORLD HAS DEPLOYED OVER **300,000** AGENTS

INCLUDING...

**7** OF THE **TOP 10** PATENT HOLDERS

AND **7** OF THE **TOP 10** AUTO COMPANIES

THE ONLY AGENT-BASED TECHNOLOGY COVERING **250,000 EMPLOYEES** USING A SINGLE MANAGEMENT SERVER

WE ARE THE **DATA PROTECTOR OF CHOICE** IN

- ENERGY
- FINANCIAL SERVICES
- GOVERNMENT
- TECHNOLOGY
- HEALTHCARE & LIFE SCIENCES
- MANUFACTURING

BECAUSE WE'RE FOCUSED ON PROTECTING **ONE THING:**

**DATA**

# WHAT DLP MUST DO

Today’s Data Loss Prevention solutions must protect against insider threats, external attacks, and outsiders posing as insiders. DLP must protect enterprise data no matter where it resides and how it is used. It must protect financial information, customer data, and intellectual property. DLP technologies provide valuable context that can help enterprises recognize the sensitivity of potentially compromised data, and then focus remediation and incident response efforts accordingly.

Success with DLP depends on setting reasonable data protection priorities, correctly evaluating vendor solutions, and selecting a deployment method. Presenting a compelling business case to business and technical executives will prevent the risk of delaying DLP initiatives. DLP can then be implemented using a simple framework that focuses on realizing “quick wins” to provide rapid return on investment and protect your sensitive data.

Data Loss Prevention is constantly evolving. We’ll continue to stay on the forefront of data protection trends and technologies and keep you up to date with our web site, blog and resources: [www.digitalguardian.com](http://www.digitalguardian.com)

And if you’d like to speak with a representative from Digital Guardian, call one of the numbers below or email [info@digitalguardian.com](mailto:info@digitalguardian.com) today.

**If you are business manager who values the data you own, demand a DLP solution.**

**If you lead IT security, make DLP a priority initiative for 2016.**

## OFFICE LOCATIONS

|  |  |  |   |   |   |
|--|--|--|---|---|---|
| <b>CORPORATE HQ</b><br>860 Winter Street, Suite 3, Waltham, MA 02451 USA<br><b>Phone</b> 781-788-8180<br><b>Fax</b> 781-788-8188 | <b>WASHINGTON DC</b><br>12030 Sunrise Valley Drive, Suite 110 Reston, VA 20191 USA | <b>CALIFORNIA</b><br>385 Moffet Park Drive, Suite 105, Sunnyvale, CA 94089 USA<br><b>Phone</b> 408-716-4200<br><b>Fax</b> 408-716-4201 | <b>EUROPE</b><br>11 Leadenhall Street EC3V 1LP London United Kingdom<br><b>Phone</b> +44 (0) 207-469-0940 | <b>JAPAN</b><br>Shiodome Plaza Bldg., 9F 2-11-4, HigashiShimbashi Minato-ku, Tokyo, 105-0021, Japan<br><b>Phone</b> +81-3-6435-6207<br><b>Fax</b> +81-3-6435-6204 | <b>INDIA</b><br>Stone Ridge Centre, 4th Floor, Survey No: 12 & 13 Opp. Google, Kondapur Main Road, Hyderabad - 500084, India<br><b>Phone</b> +91-40-4868-7872 |
|--|--|--|---|---|---|



# RESOURCES AT A GLANCE

| Title  | Type                | Link  |
|--|---------------------|---|
| St. Charles Health Case Study  | Case Study          | <a href="https://info.digitalguardian.com/rs/768-OQW-145/images/case-study-st-charles-healthcare.pdf">https://info.digitalguardian.com/rs/768-OQW-145/images/case-study-st-charles-healthcare.pdf</a>   |
| Fortune 50 Energy Company Case Study   | Case Study          | <a href="http://info.digitalguardian.com/rs/digitalguardian/images/energy-division.pdf">http://info.digitalguardian.com/rs/digitalguardian/images/energy-division.pdf</a>   |
| Jabil Managed Security Program Case Study  | Case Study          | <a href="http://info.digitalguardian.com/rs/digitalguardian/images/Jabil-manufacturing-MSP-case-study.pdf">http://info.digitalguardian.com/rs/digitalguardian/images/Jabil-manufacturing-MSP-case-study.pdf</a>   |
| Data Breaches are Frequent and Large   | Blog Post           | <a href="https://digitalguardian.com/blog/top-10-biggest-data-breaches-2015">https://digitalguardian.com/blog/top-10-biggest-data-breaches-2015</a>   |
| DLP by the Numbers, 451 Group  | Analyst Report      | <a href="https://info.digitalguardian.com/451-data-loss-prevention-market-by-numbers.html">https://info.digitalguardian.com/451-data-loss-prevention-market-by-numbers.html</a>   |
| Data-Centric Security - Why You Need It, How to Get Started., Featuring Forrester Research | Webinar             | <a href="https://info.digitalguardian.com/webinar-forrester-research-john-kindervag-why-you-need-data-centric-security.html">https://info.digitalguardian.com/webinar-forrester-research-john-kindervag-why-you-need-data-centric-security.html</a>           |
| WIPOut: The Devastating Business Effects of Intellectual Property Theft                    | Blog Post           | <a href="https://digitalguardian.com/blog/wipout-devastating-business-effects-intellectual-property-theft">https://digitalguardian.com/blog/wipout-devastating-business-effects-intellectual-property-theft</a>   |
| What Type of Data Loss Prevention is Right for Your Organization?                          | Video               | <a href="https://youtu.be/EwTKG3GB3RI">https://youtu.be/EwTKG3GB3RI</a>   |
| Digital Guardian Revokes Phishing Licence  | Video               | <a href="https://info.digitalguardian.com/whitepaper-digital-guardian-for-advanced-threat-protection.html">https://info.digitalguardian.com/whitepaper-digital-guardian-for-advanced-threat-protection.html</a>   |
| How to Make a Value-Based Business Case, Featuring Forrester Research                      | Webinar             | <a href="https://info.digitalguardian.com/webinar-forrester-tips-to-build-your-data-protection-business-case.html">https://info.digitalguardian.com/webinar-forrester-tips-to-build-your-data-protection-business-case.html</a>                               |
| 2016 Gartner Magic Quadrant for Enterprise Data Loss Prevention, Gartner                   | Report Download     | <a href="https://info.digitalguardian.com/gartner-2016-data-loss-prevention-magic-quadrant-analyst-report.html">https://info.digitalguardian.com/gartner-2016-data-loss-prevention-magic-quadrant-analyst-report.html</a>                                     |
| Gartner on the 2016 Enterprise DLP Magic Quadrant Report, Featuring Gartner                | Webinar rebroadcast | <a href="https://info.digitalguardian.com/webinar-on-demand-gartner-2016-data-loss-prevention-magic-quadrant-analyst-report.html">https://info.digitalguardian.com/webinar-on-demand-gartner-2016-data-loss-prevention-magic-quadrant-analyst-report.html</a> |
| Data Protection Vendor Evaluation Toolkit  | Evaluation tool kit | <a href="https://info.digitalguardian.com/data-protection-vendor-evaluation-toolkit.html">https://info.digitalguardian.com/data-protection-vendor-evaluation-toolkit.html</a>   |
| Alleviate the Talent Shortage with Managed Security  | Video               | <a href="https://youtu.be/h9a6qRxBWl8">https://youtu.be/h9a6qRxBWl8</a>   |
| How to Hire & Evaluate Managed Security Service Providers (MSSPs)                          | Blog Post           | <a href="https://digitalguardian.com/blog/how-hire-evaluate-managed-security-service-providers-mssps">https://digitalguardian.com/blog/how-hire-evaluate-managed-security-service-providers-mssps</a>   |
| Simplifying Your Data Protection Program for Quick Wins                                    | Video               | <a href="https://youtu.be/VFWKTj9-V2E">https://youtu.be/VFWKTj9-V2E</a>   |
| Getting to Data Visibility and Insights Quickly  | Video               | <a href="https://youtu.be/NsZooBqyVJI">https://youtu.be/NsZooBqyVJI</a>   |
| Data Visibility, Remote Communication and Increased Compliance                             | Case Study          | <a href="http://info.digitalguardian.com/rs/digitalguardian/images/managed-healthcare-provider.pdf">http://info.digitalguardian.com/rs/digitalguardian/images/managed-healthcare-provider.pdf</a>   |
| Driving Security Using Real-Time Education   | Video               | <a href="https://youtu.be/Hq9G1Wt6vg8">https://youtu.be/Hq9G1Wt6vg8</a>   |
| Jabil - Data Visibility, IP Protection and Business Unit Adoption in less than 120 Days    | Case Study          | <a href="http://info.digitalguardian.com/rs/digitalguardian/images/Jabil-manufacturing-MSP-case-study.pdf">http://info.digitalguardian.com/rs/digitalguardian/images/Jabil-manufacturing-MSP-case-study.pdf</a>   |
| Digital Guardian Platform Technical Overview   | White paper         | <a href="https://info.digitalguardian.com/digital-guardian-technical-overview-whitepaper.html">https://info.digitalguardian.com/digital-guardian-technical-overview-whitepaper.html</a>   |
| Digital Guardian Managed Security Program Technical Overview                               | White Paper         | <a href="https://info.digitalguardian.com/managed-security-program-technical-overview-whitepaper.html">https://info.digitalguardian.com/managed-security-program-technical-overview-whitepaper.html</a>   |

# THE DEFINITIVE GUIDE TO DATA LOSS PREVENTION

QUESTIONS?

1-781-788-8180

[info@digitalguardian.com](mailto:info@digitalguardian.com)

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



©2016 Digital Guardian. All rights reserved.

