

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
- 40** Part Six: Business Case for DLP
- 47** Part Seven: Buying DLP
- 53** Part Eight: Getting Successful with DLP
- 62** Part Nine: Digital Guardian—Next Generation Data Protection
- 66** Conclusion
- 67** 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
 Personal Information Protection / Compliance	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"/>
 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.	<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"/>
 Business Partner Compliance	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.

ENTERPRISE DLP OR INTEGRATED DLP?

THOUGHT LEADER INSIGHT: JARED THORKELSON, PRESIDENT DLP EXPERTS

DG: Because of the increased interest and the demand for DLP, more security vendors are adding DLP functionality into their products in what is referred to as integrated DLP. So we asked Jared Thorkelson of DLP Experts, to explain the difference between Enterprise DLP and Integrated DLP.

JT: Enterprise or Full Suite DLP technologies, are focused on the task of preventing sensitive data loss and providing comprehensive coverage. They provide coverage across the complete spectrum of leakage vectors. Significantly, Full Suite DLP addresses the full range of network protocols, including email, HTTP, HTTPS, FTP and other TCP traffic. Another critical distinction of most Full Suite DLP solutions is the depth and breadth of their sensitive data

detection methodologies, which translates into meaningful increases in DLP effectiveness. Another unique and critical feature of Full Suite DLP solutions is a central management console. This eliminates the need for multiple management interfaces and significantly reduces the management overhead of a comprehensive DLP initiative.

Integrated DLP or Channel DLP solutions were designed for some function other than DLP then were modified to add some DLP functionality. Common Channel DLP offerings include email security solutions, device control software and secure web gateways. In each case, Channel DLP solutions are limited in their coverage and detection methodologies.



**FREE
DOWNLOAD**

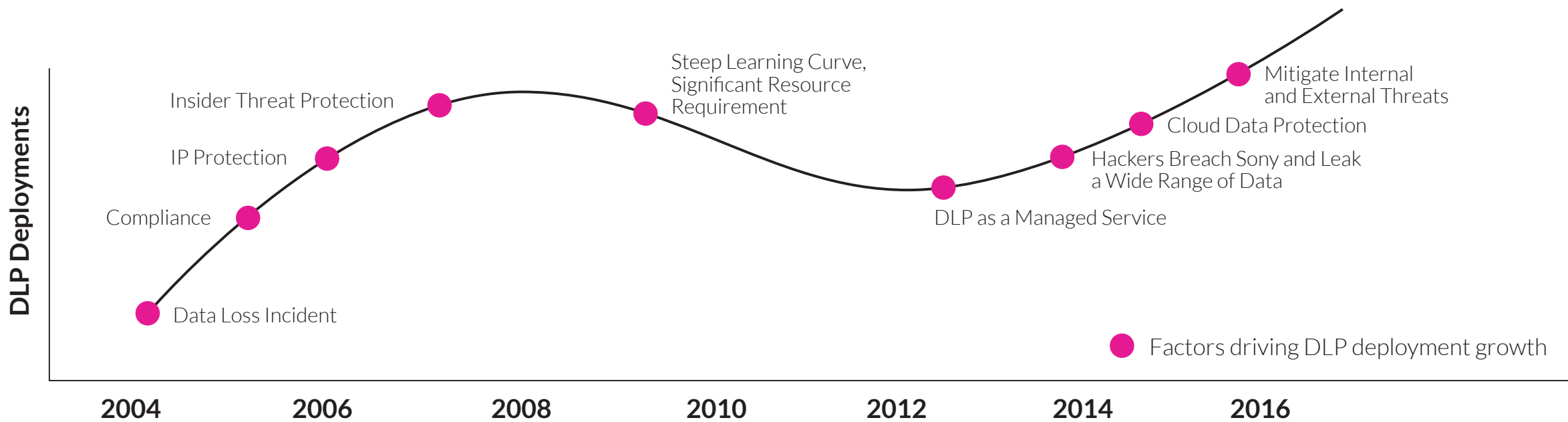
- Get the DLP Experts 2016 DLP Vendor Review Report.

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.



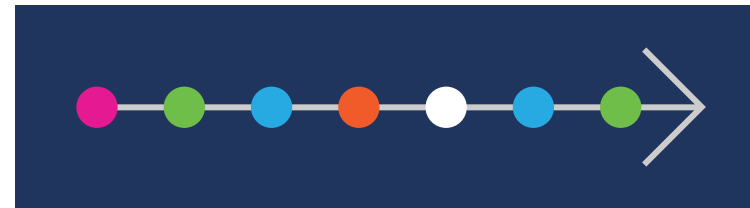
3 MYTHS OF DATA LOSS PREVENTION

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.

WE HOPE YOU ENJOYED THIS SAMPLE!

TO READ ON, CLICK HERE & DOWNLOAD THE COMPLETE GUIDE

THE FULL GUIDE INCLUDES INSIGHTS FROM 451 RESEARCH, DLP EXPERTS, FORRESTER RESEARCH AND OUR SECURITY ANALYSTS TO HELP YOU:

- 1** Select the right DLP for your organization.
- 2** Make the case for DLP to your executive team.
- 3** Get fast wins. Build from there.

TO READ ON, FILL OUT OUR SHORT FORM AND DOWNLOAD THE COMPLETE GUIDE NOW >>

