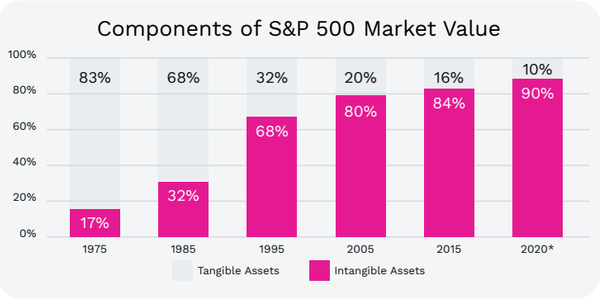
DON'T JUST MIGRATE, UPGRADE YOUR DATA LOSS PREVENTION

DIGITAL GUARDIAN®

WHY READ THIS EBOOK?

"The world's most valuable resource is no longer oil, but **data.**" *– The Economist*

Data is now more important than ever, it's the most valuable resource.



Data is evolving. Intangibles, like digital data, represent 90% of the S&P 500 value.

Number of years it took for each product to gain 50 Million Users

- Airlines: **68yrs**
- Automobiles: **62yrs**
- Telephone: **50yrs**
- Electricity: **46yrs**
- Credit Card: **28yrs**
- Televison: **22yrs**
- ATM: **18yrs**
- Computer: **14yrs**
- Cell Phone: **12yrs**
- Internet: **7yrs**
- iPods: **4yrs**
- YouTube: **4yrs**
- Facebook: **3yrs**
- Twitter: **2yrs**
- Pokémon Go: **19 days**

The pace of business is accelerating. Security solutions must evolve with your business model.

1. Outdated DLP is a liability; a successful upgrade requires planning.
2. Your new solution must extend your existing coverage.
3. You need DLP that can find all your sensitive data, drive growth, and adapt.
4. You need coverage for a work-from-anywhere world.

Read this eBook to learn how to upgrade your DLP to be a strategic element of your data protection program and migrate without complexity.

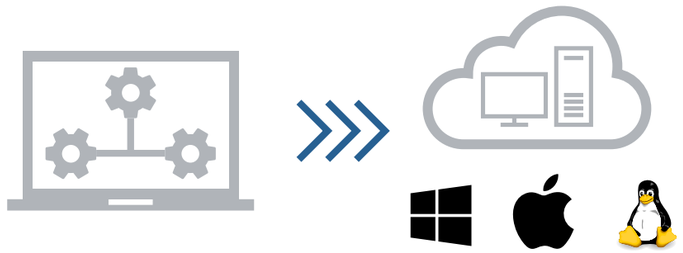
Source: *Ocean Tomo, LLC Intagible Asset Market Value Study, 2020*
**Interim Study Update as of 07/01/2020*

TABLE OF CONTENTS

ASSESING YOUR TODAY STATE AND HOW YOU EVOLVED HERE

BUSINESS EVOLUTION + TECHNOLOGY EVOLUTION + USER EVOLUTION

Your business has evolved, technology solutions have evolved, but the ways your users do their job has evolved too. You need to take into account their new found power to add complexity to any data protection program.



Single OS >>>
Multi OS, VDI, DaaS

Finite, local apps >>>
Infinite, web-based apps

Most employees in office >>>
Work From Anywhere

BUSINESS AND SECURITY NEED TO EVOLVE TOGETHER

Business and Security Goals at time of purchase → Business and Security Goals Today

How has the relative importance of IP protection vs regulated data protection shifted

- Greater reliance on IP and increased regulatory oversight means both have evolved
- Has the balance flipped? Will it flip?

What were and what are now the most common paths for data to move?

- Email, Web upload, USB, Printer, FTP, etc.
- What's now the highest risk vector?

How has the company culture evolved?

- Is the risk of false negative or a false positive greater?
- What short/medium/long term objectives may change?

BUSINESS AND SECURITY NEED TO EVOLVE TOGETHER

Business and Security Goals at time of purchase → Business and Security Goals Today

- Is PII data your only sensitive data you need to protect?
- Where does your “data at rest” reside within the organization?
- How are you monitoring data usage now?

?

- How is sensitive data used or shared?
- How does your “data in motion” flow through and out of the organization?
- How do you educate employees on data usage and how do you handle incidents?

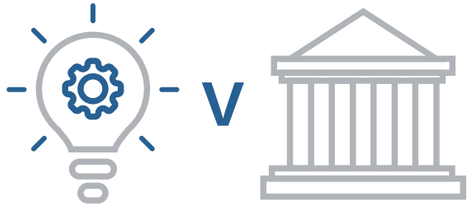
MAKING YOUR WISH LIST FOR DATA PROTECTION

BUSINESS INITIATIVES + PROTECTING DATA

- Can you still achieve the goals you set out for when your organization started its data protection program?
- What compromises due to technology limitations must you make?
- What is the impact of doing nothing?

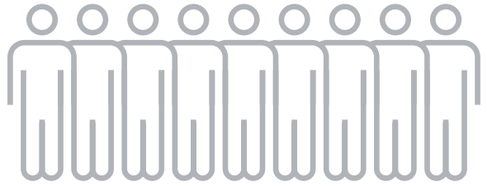
ENABLING THE BUSINESS AND PROTECTING DATA

WHEN EVALUATING YOU EXISTING DATA PROTECTION PROGRAM UNDERSTAND WHAT YOUR GOALS ARE, HOW THEY ALIGN WITH THE BUSINESS, AND HOW THEY ARE PRIORITIZED.



IP Protection vs Regulated Data Protection

Email, Web upload, USB, Printer, FTP, etc.



Culture of the company, risk of false negative vs false positive, short/ medium/long term objectives

BUSINESS INITIATIVES + PROTECTING DATA

COMMON GOALS

1. Protect sensitive data, meet compliance requirements
2. Support the business, share decision making responsibilities
3. How and where does data move?
4. Identify risks or gaps
5. Enable secure growth

THE RIGHT DLP DELIVERS THE DEEPEST VISIBILITY

An iceberg is 90% hidden under the surface of the water; like the data in your business, much of it is hidden. You need above and below the water level visibility. An effective, enterprise DLP can find, understand, and protect all your data, not just the visible.

GETTING STARTED

WHERE DO I START WITH A DLP RE-EVALUATION?

LOOK INSIDE BEFORE LOOKING OUTSIDE. GATHER THE INSIGHTS WHERE YOU HAVE EASIER ACCESS TO THE PEOPLE AND OTHER RESOURCES NEEDED TO ASK HOW AND WHY DATA MOVES THE WAY IT DOES.

Visibility First = Metrics

- Gather data to share with business units and stakeholders, data owners
- Share with them the data they need to make informed policy decisions
- Useful to track improvements and show ROI

Provide risk-based policy recommendations

- Not all data is the same
- Leverage existing experience and best practices

DLP RE-EVALUATION – STEP 2

SEEK PROFESSIONAL HELP WITH DLP VENDORS WITH THE FOLLOWING GUIDANCE:

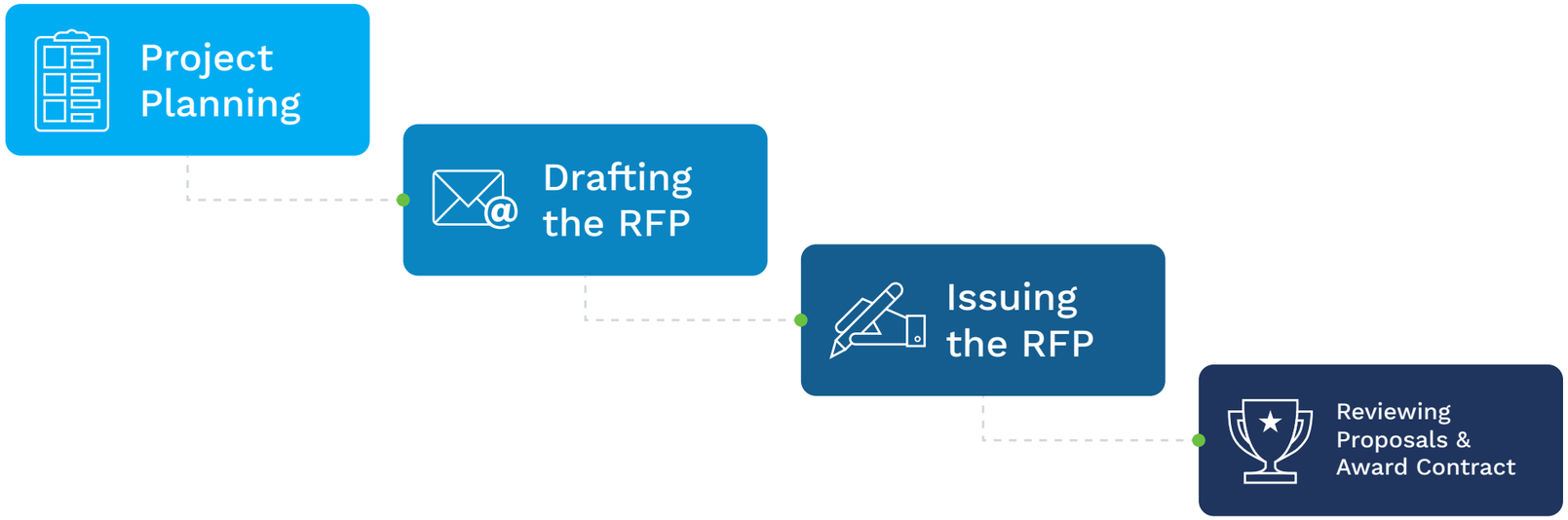
Have use cases in mind to make it real
Was there an incident that we don't want to see happen again?

- Have people become too free using webmail or USB with sensitive data
- Was there an employee departure flagged too late to stop printing of confidential information?
- Was there malicious code or ransomware that is thought to have accessed sensitive data?

If you're prepared to discuss a specific issue, you're likely to have a better experience than if you have overly generalized discussions

EXTRA CREDIT READING

Digital Guardian's CISO, Tim Bandos, authored another eBook with a section dedicated to improving your RFP process. He'll explain how best to structure your RFP process among other topics.



FREE DOWNLOAD

· Get the CISO's Guide to Enterprise Security Migration here

PROVEN ROADMAP TO DLP SUCCESS

A PHASED APPROACH FOR DLP SUCCESS

Once you've gone through your internal review, external evaluation, and selection, the deployment process begins. Here is where you need to have a well documented plan. Digital Guardian has implemented DLP programs for hundreds of organizations, the one thing they have in common is a need to protect sensitive data without a drawn-out deployment.

OUR PROVEN, 5-PHASE APPROACH DELIVERS THE ENTERPRISE DLP YOU NEED:

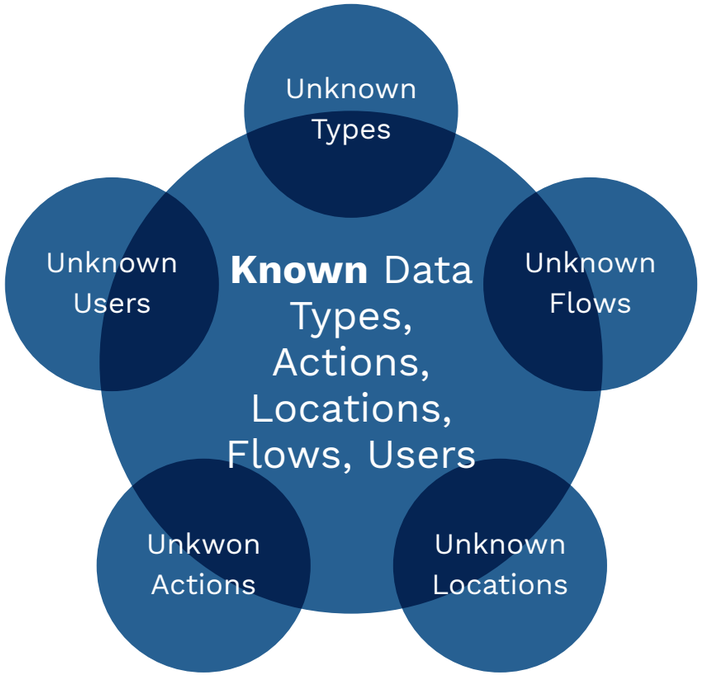
STAGE 1: INSIGHT

IDENTIFY EXISTING BEHAVIOR & DEFINE ACCEPTABLE BEHAVIOR

STAGE 1: INSIGHT

INSIGHT | BASELINE | EDUCATE | ACT | ASSESS

- During the initial "Insight" phase focus on the types of data you will need to protect and how they are moving. (Both the intended/approved and the workarounds that will inevitably occur.) Data in use, data in motion, and data at rest.
- Beyond data types and how its being manipulated, is the location of the data. You need to see, understand, and protect it across the entire extended enterprise from the endpoint to the cloud.



STAGE 2: BASELINE

DEVELOP BASELINE, MODELS, AND POLICIES

STAGE 2: BASELINE

INSIGHT | **BASELINE** | EDUCATE | ACT | ASSESS

- **Once you have a DLP deployed you need to set policies to see anything, right? A DLP that can deploy in a policy free mode simply collects data on the events that happen in the course of the normal business processes. From this you can establish a baseline of what normal looks like, then build better polices (or establish a cybersecurity training program).**

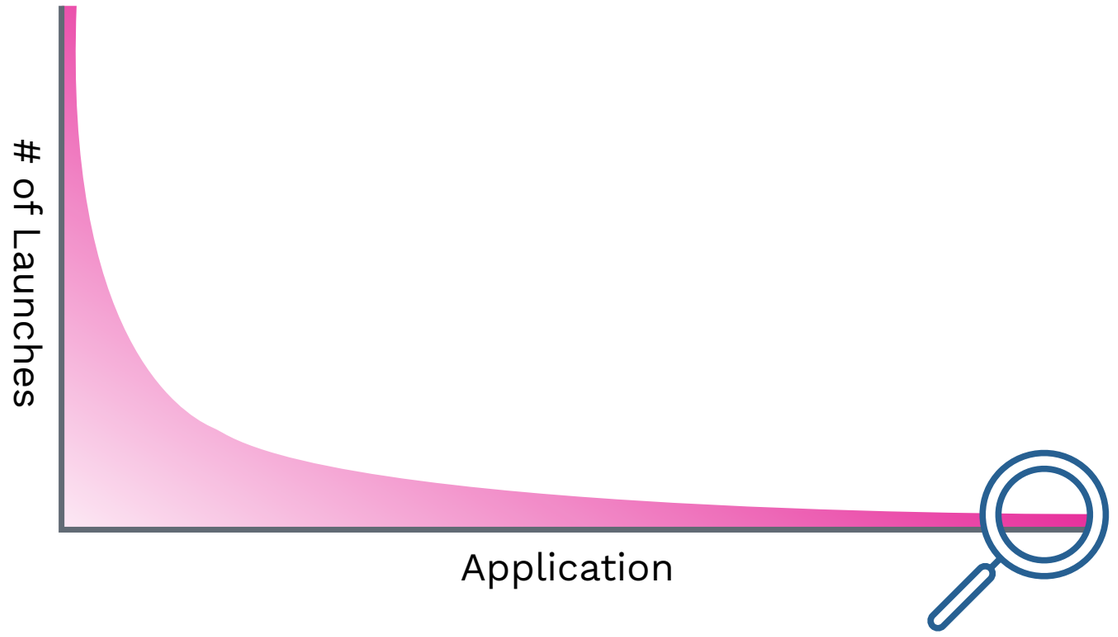
- **You will gain tremendous into the business with the unbiased data collection:**
  - Normal data flows throughout the business
  - Marketing accessing the legal and finance server at off hours
  - Sales reps encrypting, compressing, renaming excel files to look like .JPGs
  - Finance accessing and downloading customer data at 3AM
  - User attempting to access multiple inactive
  - Applications spawning other applications and making registry changes

- **With a baseline established, look for anomalies or deviation from expected, investigate, and make an informed decision about the risk to the business.**

STAGE 2: BASELINE

INSIGHT | **BASELINE** | EDUCATE | ACT | ASSESS

- How well can you see “rare processes” in your environment? In a normal day, you would expect Email apps, MS Office apps, or if you in manufacturing CAD apps to launch. But what about things you don’t expect to see, like Powershell or developer tools by a member of the HR team? Sorting these rare processes by user can give greater detail or highlight data loss risks.



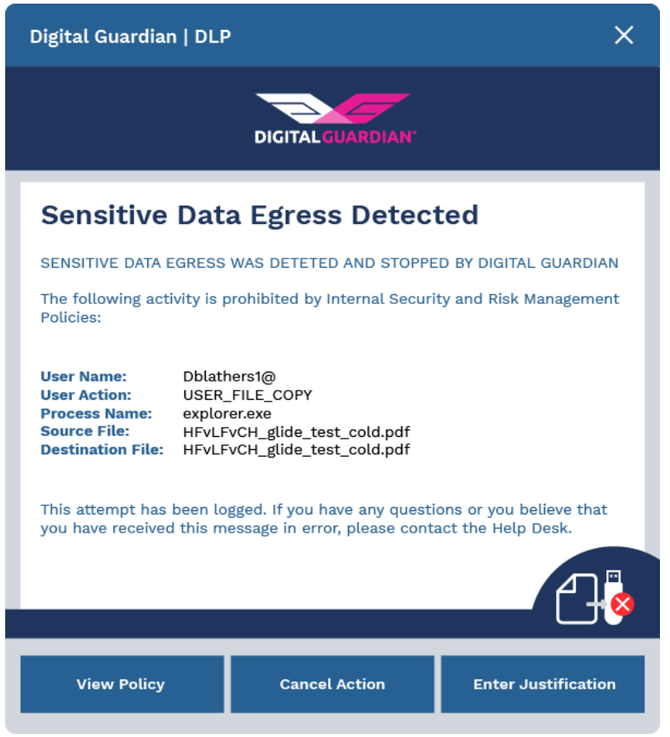
STAGE 3: EDUCATE

EDUCATE AND INFORM ON SMART DATA USE

STAGE 3: EDUCATE

INSIGHT | BASELINE | **EDUCATE** | ACT | ASSESS

- Information about data risks that lives only within the information security department doesn't deliver the full benefits it could. The end users need guidance on how to act and what behaviors could be deemed too risky by the business. Because these actions can change as the business evolves, and as security solutions evolve, it's important to provide regular feedback and education to the entire organization.

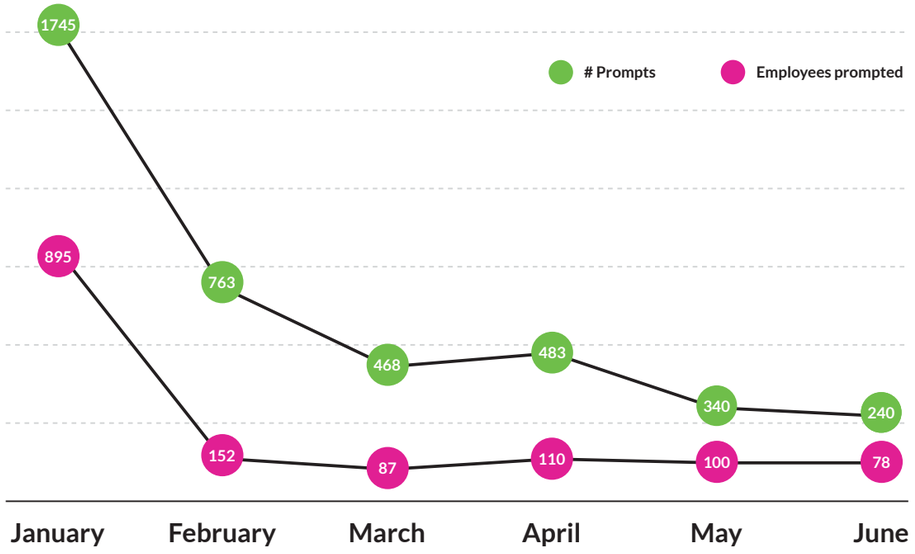


STAGE 3: EDUCATE

INSIGHT | BASELINE | **EDUCATE** | ACT | ASSESS

- **Here is an example of how user prompting can encourage better data use decisions. By prompting users about how their actions could put patient data at risk, the organization saw over 85% reduction in unauthorized PHI data transferred.**

UNAUTHORIZED TRANSMISSION OF PHI DATA



STAGE 4: ACT

ENFORCE ACCEPTABLE BEHAVIOR

STAGE 4: ACT

INSIGHT | BASELINE | EDUCATE | **ACT** | ASSESS

- **Even with the insights, baseline, and user education, there are still times that information security solutions like DLP need to take automated actions. Whether the user is ignoring the prompts, or an active and malicious user, security automation can stop data loss before it happens and give the security team the knowledge to further respond to the incident. The question is, what is the right level of action to take? That depends upon the risk profile of the business, but security teams need broad and flexible automation options.**

STAGE 4: ACT

INSIGHT | BASELINE | EDUCATE | **ACT** | ASSESS

- **To best determine the actions, security teams should rank the actions using standardized terms, then assign a risk level to the results. From that list the team can then decide the level of automated response that balances information security benefits with business process interruption. An unauthorized access by and insider might be a moderate level event that requires a justification to proceed, while improper usage by an outsider may be critical and be blocked.**

Category
- Unauthorized Access
- Potential Malware
- Improper Usage
- Unsuccessful Attempt
- Explained Anomaly

Type
- Insider Threat
- Opportunistic
- Outsider
- Broken Business Practice

Severity
- Critical Impact
- High Impact
- Moderate Impact
- Low Impact

STAGE 5: ASSESS

ONGOING REVIEW AND POLICY TUNING

STAGE 5: ASSESS

INSIGHT | BASELINE | EDUCATE | ACT | **ASSESS**

- Just as no business is static, no information security policy should be static. New target markets, new delivery options, and new risks all require a consistent review of the DLP program to ensure it still meets the intended data protection goals without impeding the business growth. Over the previous 6 months how easily can you show any changes to data egress? Are there new channels? Has a traditional data egress channel suddenly dropped? While that could mean people are moving less data (unlikely given the data explosion), it's more likely they've found a new method that the security team needs to understand and evaluate.

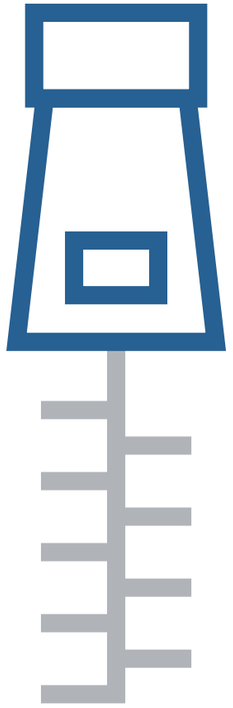
NEED TO ACT NOW?

READY TO ACT NOW?

- Have you already done your business and security assessment, or is a compelling event driving urgency?
- Migration of any enterprise technology can present challenges, here are some tips from our team of Solutions Engineers. They've engaged with a diverse range of global businesses and helped them migrate to a new DLP platform.
- Read on for how to make the migration process go smoothly.

STEPS FOR A SEAMLESS TRANSITION

- Getting exports of all the policies you have in place with your existing DLP vendor.
- Organizing a governance strategy for handling DLP related questions.
- Establishing communications with and soliciting feedback from entire organization about data protection program
- Ensuring antivirus exclusions are applied to all users to prevent solution conflicts
- Completing in-app tutorials and trainings
- Using a Project Tracker to maintain project momentum



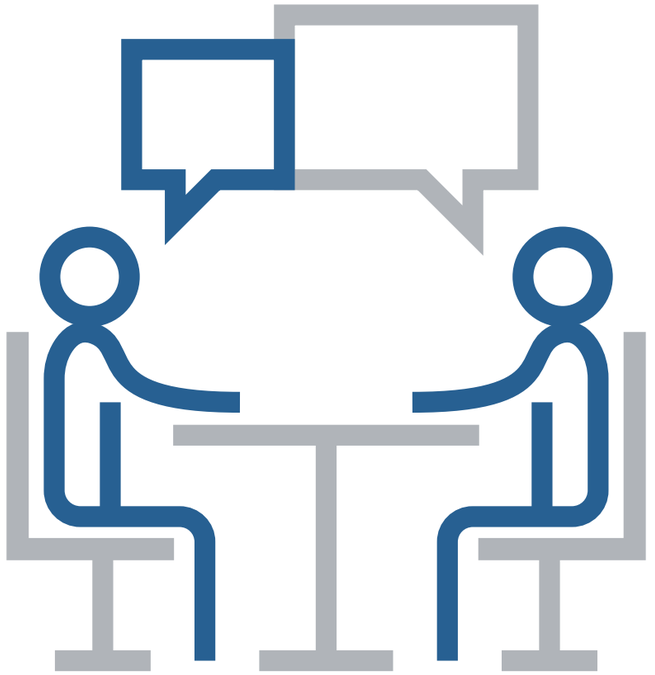
PROJECT TRACKER TEMPLATE

MAP OUT YOUR PROCESS STEPS FROM START TO FINISH. WORK CLOSELY WITH THE DLP VENDOR TO DEVELOP AND REALITY-CHECK THIS DOCUMENT. WHETHER YOU ARE A SMALL OR LARGE COMPANY, MANY STEPS WILL BE THE SAME, THE SCOPE OF EACH IS DIFFERENT.

- **Step 1 -** A/V Exclusions for All Security Products
  - (EDR and A/V)
- **Step 2 -** Allow DLP Agent Traffic to the Cloud
- **Step 3 -** Gather Existing DLP Configuration
- **Step 4 -** Map DLP Requirements to DLP Solution
- **Step 5 -** Map DLP Policy Pack Controls

STEPS FOR SUCCESS – END-USER COMMUNICATION

No one likes surprises or being force fed a solution without any chance to comment. Any data security tool can alienate the users if they're not included throughout the entire process and this lack of communication causes workflow disruptions. While there are some occasions when a stealth mode install is needed, open communication is generally the recommended process with DLP.



WHAT IS DIGITAL GUARDIAN AND WHAT DOES IT DO?

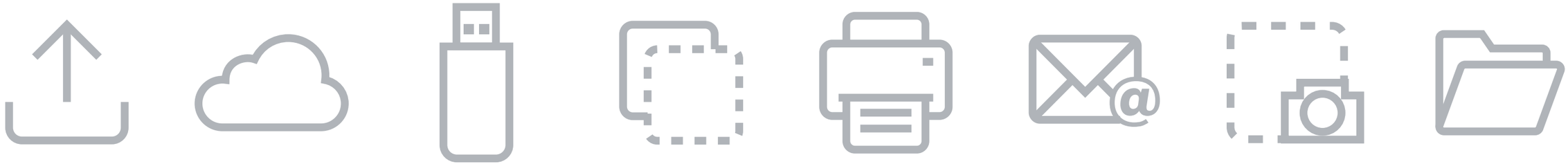
Digital Guardian (DG) platform is the leading Enterprise Information Protection solution for Global 2000 companies and is the cornerstone of a strategic information protection and risk management program.

Integrated, comprehensive, and proven, Digital Guardian uniquely solves the broadest set of information protection use cases faced by global businesses. Digital Guardian differentiators include:

- Enterprise-wide visibility into sensitive data location, usage and movement both on and offline
- Uniform policy enforcement that leverages identity, activity, context, and content analysis with actionable, multi-variable data classification
- Automated risk-appropriate controls manage user activities through warnings and blocks combined with fully integrated encryption, thus enforcing business processes and holding end users accountable
- Deterministic, continuous and accurate system that is device, channel and application agnostic
- Actionable, fully integrated decision support and reporting console that includes dashboards, drill-down capabilities, trend location-based and organizational views

MAP EXISTING REQUIREMENTS TO DLP POLICY PACK

UPGRADING DLP IS A CHANCE TO REEVALUATE POLICIES, BUT BE SURE YOU CAN EASILY MAP EXISTING, KNOWN REQUIREMENTS TO THE NEW SOLUTION. YOU SHOULD TAKE ADVANTAGE OF THE SWAP TO UPDATE AND IMPROVE DATA PROTECTION STRATEGY AND POLICIES.



Upload Cloud USB Copy Paste Print Email Print Screen Archive

CONFIGURE OUT OF THE BOX POLICIES

- Based on what you know and what the DLP solution provides out of the box, you can get your initial data protection policies in place.
- Set up the compliance policies that look for the easy to recognize data that follows a pattern – PCI, PHI, or PII.
- Establish your IP protection policies to recognize and protect the harder to protect unstructured and less predictable format common to IP.

DEPLOYMENT SCENARIOS

When **adding** DLP to an organization without anything in place a soak period where you watch and learn how the data is moving leads to a more effective deployment. You can use data about the data to make policies that match your real world.

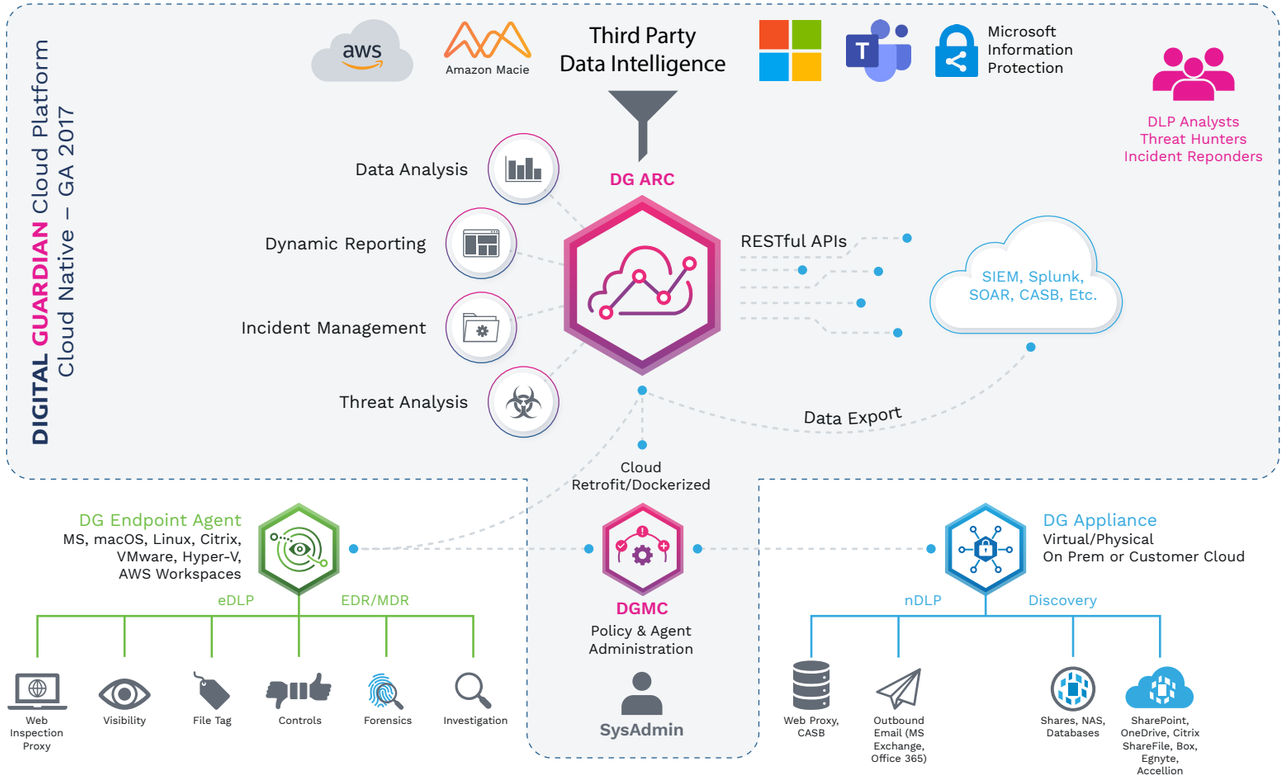
In a **displacement** scenario policy duplication is where some businesses will begin. They are confident in the existing policies but need a better platform for their data protection. Once the new solution is in place, revisiting the data flows should be done to see where your team can make improvements.

WHY DIGITAL GUARDIAN?

THE ONLY CLOUD DELIVERED DATA PROTECTION PLATFORM

Data protection is at the core of our company mission. The DG Data Protection Platform detects threats and stops data exfiltration from both well-meaning and malicious insiders as well as external adversaries.

- Data Loss Prevention
- Managed Detection & Response
- Data Discovery
- Data Classification
- Analytics
- Reporting
- System Management



FREE DOWNLOAD

· Digital Guardian Platform Technical Overview

PROVEN 5-STEP METHODOLOGY: SPEEDS MIGRATION AND ELIMINATES DATA PROTECTION GAPS

Your Digital Guardian team is with you throughout the entire process. From the initial planning stages, through build-out & testing, and ultimately production deployment, we'll combine on our team's data protection experience with your business knowledge to get you operational quickly.

NO-COMPROMISE DATA PROTECTION THAT STOPS DATA LOSS

CLOUD-DELIVERED
Powered by AWS, Digital Guardian delivers simplified deployment, low overhead, and elastic scalability for increased return on your security spend.

CROSS PLATFORM
Coverage for your Windows, macOS, or Linux operating systems and all your applications, both browser based and native.

FLEXIBLE CONTROLS
Fine-grained controls, ranging from log & monitor to automated blocking, help protect data before it's lost.

DEEPEST VISIBILITY
We see everything that happens to your organization's sensitive data.
Cross Platform

NO POLICY, NO PROBLEM
Our "unknown risk" approach enables you to see where sensitive data is located, how it flows, and where it is put at risk - all without policies.

COMPREHENSIVE CLASSIFICATION
Only Digital Guardian provides content, user, and context-based data discovery and classification.

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.

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

–John Graham, former 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.

DIGITAL GUARDIAN®

CASE STUDY

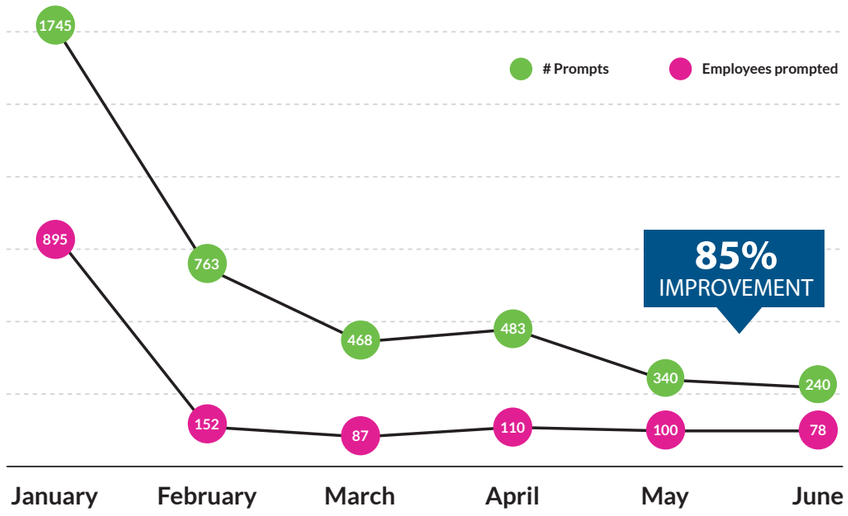
THE POWER OF REAL-TIME USER EDUCATION

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.

DON'T JUST MIGRATE, UPGRADE YOUR DATA LOSS PREVENTION

QUESTIONS?

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

DIGITAL GUARDIAN®