FORTRA

The Definitive Guide to Data Loss Prevention

Hybrid Work Edition

Table of Contents

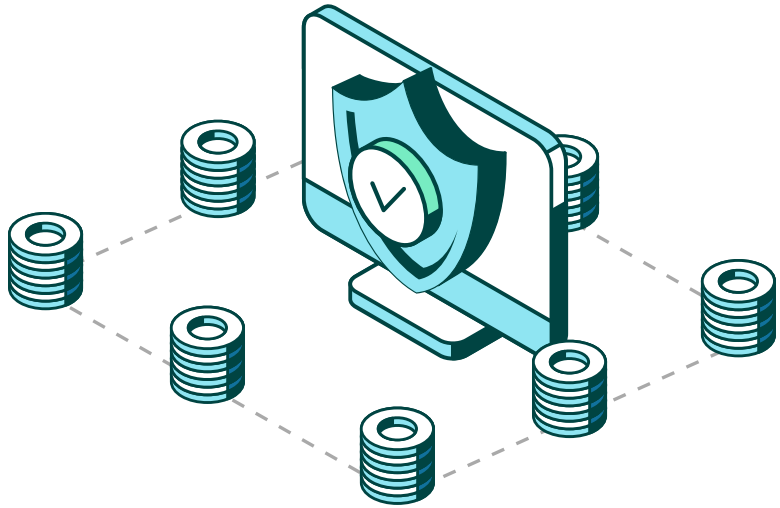
PART ONE

Top Two Reasons to Consider a DLP Solution

Approach Compliance with Confidence

Organizations are handling more sensitive data than they ever have before, and as a result, data privacy is taking center stage. Gartner predicts that by the end of 2024, 75% of the world's population will have its personal data covered under modern privacy regulations. And according to IBM's 2022 Cost of a Data Breach Report, compliance failures were one of three factors associated with the highest net increase in the average cost of a breach.

With pressure mounting to comply with these regulations, it's important that organizations find and implement a modern DLP solution that will provide immediate value and can adapt to changing regulations. And if your organization spans multiple countries, a modern DLP solution can help employees handle data properly in an uneven regulatory landscape.



Begin to Combat Costly Data Breaches

If your organization is looking to mature its data protection journey, implementing a DLP solution (or replacing one you've outgrown) is a wise step. Modern solutions do not depend on a policy-driven approach to get started. Rather, context-aware DLP enables you to automatically collect information on data usage and movement in and out of the extended enterprise, giving your organization valuable insight and visibility over its data and preventing costly breaches.

Today's SaaS DLP solutions can also be turned on quickly, are modular, and allow for iterative deployment as part of a continuously evolving, ongoing data protection program that integrates other data protection solutions.

PART TWO

Key Steps Before You Talk to Any DLP Vendors

TIPS from the Experts

Enterprise security is not about deploying and maintaining tools. It is **about knowing how your business runs**, what data and apps are vital for it to add value to its customers, while fostering a strong risk management strategy to protect those assets.

Process First, Technology Second

Getting your process in order first helps you focus on what matters most – what you and your business need – not what a vendor has
to offer.

Due to the pandemic, **33% of buyers** spent more time researching products before making a purchase this year.

49% of buyers spent time doing extra research because of data security concerns.

Almost 9 out of 10 of buyers want to self-serve part or all of their buying journey.

Source: TrustRadius - The 2021 B2B Buying Disconnect

Process First, Technology Second

- 30% of organizations deploy more than 50 cybersecurity-related tools on their networks, and nearly a quarter of those organizations deploy more than 100 tools.
- Deploying more solutions does not always lead to greater cyber resiliency, however, as 37% of organizations believe they have too many security solutions in place.
- Meanwhile, 33% of organizations believe they don't have enough security solutions in place, while only 30% believe they have the right number of solutions to achieve cyber resiliency.
- Rather than fixating on the number of security solutions your organization deploys, focus your organization's efforts on the decision-making process instead.

Source: *IBM Cyber Resilient Organization Study 2021*

"Mature security teams are investing heavily in a couple key categories. So as an organization, I would ask, "Where am I not investing, and why?" Understand your points of weakness and your risk in those areas, and get a strategic plan around trying to solve those gaps."

Cary Hudgins, Director of Product Management, Fortra's PhishLabs
CISO Perspectives:
Data Security Survey 2022

What to do Before You Contact Any Vendors

The list of things to do before contacting a vendor can seem daunting, but it will prove beneficial and prevent the "changing the tire while driving" scenario that leads nowhere good.

1. Define the problem you are trying to solve and the criteria you intend to use to judge the solution
2. Establish what matters to the various stakeholders – what the CISO cares about and what the VP of Sales cares about may be very different, but you need a common language to evaluate
3. Create a scoring system on functionality that allows people to adjust weightings
4. Set milestones for the internal process and the external process
5. Create a cross functional project team
6. Seek guidance from peers. Look to similar and dissimilar roles/industries
7. Look to online reviews
8. Seek industry analyst guidance, many of whom are regularly briefed by vendors
9. Make a short list of vendors you're interested in
10. Develop an RFP (Request for Proposal) document

TIPS from the Experts

Having a ton of market leader security tools will not make your enterprise secure or prevent a breach if they're not deployed properly.

You need to first arm yourself with knowledge of where your critical data resides and the systems that store it in order to fully utilize these solutions for maximum protection.

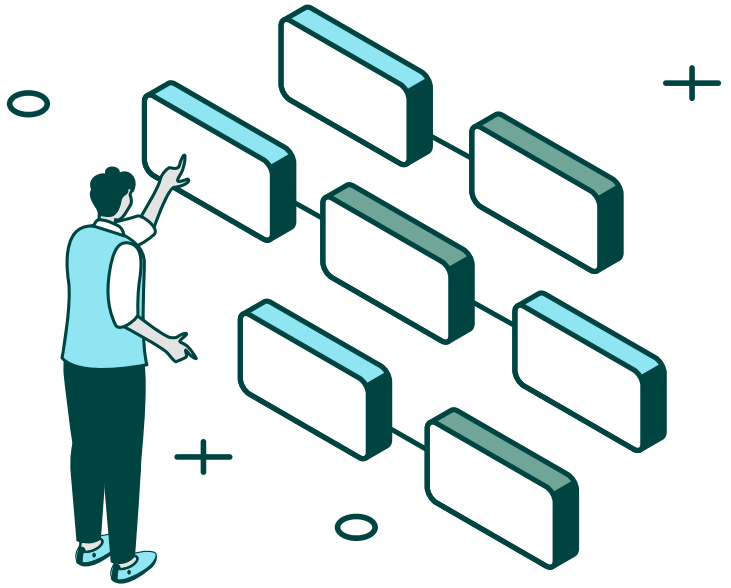
PART THREE

How to Improve Your DLP RFP Process

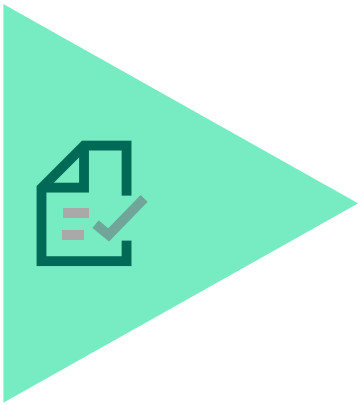
An RFP is a Lot of Work... It Doesn't Have to Be

Bite off as much as you can, whatever prep you do will pay dividends to the business and improve the overall decision-making process.

1. RFPs help meet organizational needs & forces you to define requirements
2. Allows for comparison of one system/solution to another using consistent criteria
3. Gets control of product demonstrations
4. Gets you to think about return on investment
5. Produces an organized selection methodology



Structure Your RFP Process for Success



PROJECT PLANNING

DRAFTING THE RFP

ISSUING THE RFP

REVIEWING PROPOSALS & AWARD CONTACT

Project Planning

1. **Requirements scope** - Start by examining the features of the existing software that are used and rewriting them into requirements. Look to the broad base of people within the business to ensure you get the full picture. From the admins to the end users, each has a role to play in defining the scope This process of reverse engineering requirements from the existing features is critical to ensure you don't regress on functionality when you see something new and exciting in a potential replacement platform and ignore what you use today.

2. **Alignment with business strategy** – How does your business operate today? What are the things that make it unique? Are you a highly seasonal, retail business where even a few minutes of downtime during the holiday shopping crunch can mean millions? Align the project with the business goals, calendar, and future plans. Are there any major shifts planned? Be aligned with the leadership team and use security solution as a growth accelerator!

3. **Budget** – You never have enough time or money but knowing how much you have sets the guardrails on the project. Don't evaluate a $100mm solution when you have a $100k budget. It wastes your time and creates unrealistic expectations. Understand how that money can be spent too. Opex vs Capex can drastically change budgeting.

PROJECT PLANNING

"Software selection is like painting a building. The real work is in the preparation, not the selection."

Unknown

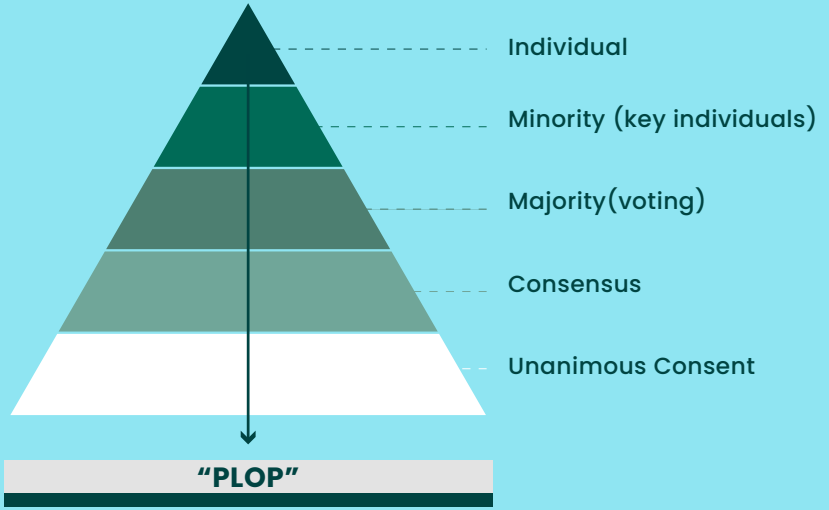
Project Planning

1. **Timeline** – What compelling event, if any, is driving the evaluation and how can you respond as quickly as needed to address it. If you've been breached, the timeline may be accelerated, if a business peer has been breached, there may be even higher urgency. Transparency throughout the business will avoid nasty surprises. Timelines should be set up front but be realistic about them and allow for slippage when the inevitable happens.

2. **Stakeholders and review panel** - Who is going to be part of the evaluation process and the decision process. More input is good, to a point. You need technical and non-technical people involved. Each party should know what their level of involvement is and how the final decision will be made. The RACI model can help organize the roles and keep the order. Get them on board and involved early.

3. **Scoring criteria and review process** – How will the points be assigned and how will the weighting work? Who wants what, and how important is that to them? Does anyone have override authority? Who breaks the tie if it happens? How will you document the procedure so that when the time comes all know what to do and stay to a consistent process? A blend of quantitative/yes/no and qualitative questions allows for objective and subjective data and will give you a more complete picture of capabilities.

The Six Types of Team Decisions



Drafting The RFP

1. **Introduction**
2. **Statement of purpose**
3. **Background information**
4. **Scope of Work**
5. **Project Schedule**
6. **Contract Terms and Conditions**
7. **RFP Timeline and Review Process**
8. **Requirements for Proposal**

DRAFTING THE RFP

Set the stage for the RFP with the details that you and the team already agreed upon, but that the potential vendors have no insights into, yet. The more thorough you are here, the better tailored the responses will be. You'll also eliminate vendors that can't compete.

- Who is the lead, who else is involved
- Why is this happening and why now?
- What's important for the vendors to know?
- How do you box in the project?

The nuts and bolts of an RFP, such as schedule, T's & C's, and other requirements are a great filter. The last thing you want is to invest time with a vendor, award them the business, and have them tell you that their delivery timelines are well outside your window.

Issuing The RFP

1. **Creating the Shortlist of Vendors**
2. **Distribution to Networks**
3. **Take 60 Seconds for Yourself**
4. **Coordinate Responses and Answer Questions**
5. **Receive Submissions**

DRAFTING THE RFP

Getting a proper response means delivering the RFP to the right selection of vendors. You need to make the list manageable, but comprehensive enough to get a feel for the breadth of capabilities. Be sure to give a reasonable and equitable time to respond. Once it's out there, you can take a breath for a minute before the questions come back from the vendors and the responses come in.

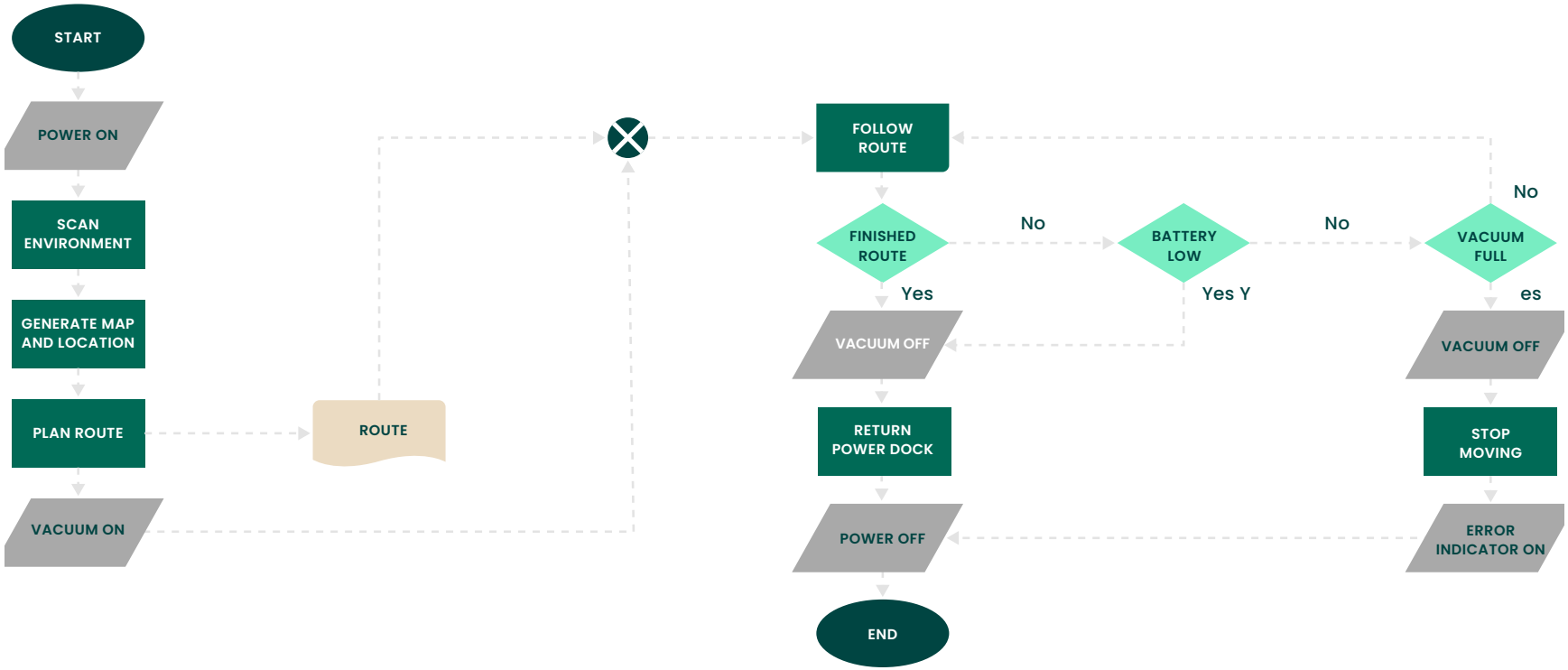
TIPS from the Experts

Use conferences and exhibitions you attend intelligently. InfoSec conferences can be beneficial if used in the right direction. Arrive with a plan to view each product you're interested in.

Virtual events add a new wrinkle. They can be helpful given most are now free and none require the time away, but the lack of face-to-face conversations adds new challenges.

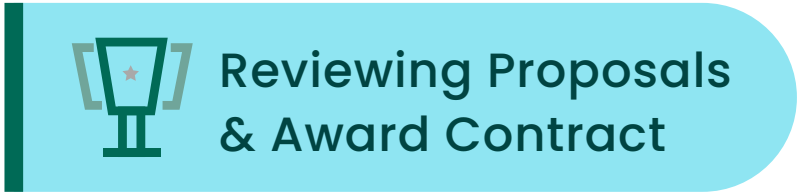
Don't Get Stuck in Analysis Paralysis

The reason you invested time up front in the RFP process was to have a plan ready to go when the responses came in. Now you can execute (and refine if needed) on that plan. Even if you need to modify, you have something to start with and that the other stakeholders provided input on and bought into early in the process.



Reviewing Proposals & Award Contract

1. **RFPs Scored**
2. **Finalists Selected**
3. **Interviews & Reference Checks**
4. **Best and Final Offers Submitted**
5. **Contracts Awarded**
6. **Final Legal Clarifications Complete**
7. **Other Bidders Notified**



Refer to your scoring matrix you created early on and begin the process of scoring, then ranking each of the vendors based on their submitted answers. How do the vendors rank relative to what's most important to your business needs? If you want to eliminate some bias, you can have a neutral party in your business receive and anonymize the responses. Any questions back to the vendors should be aggregated then submitted together.

Once you're happy with the scoring, you rank them and select the finalist(s). Depending on the scope of the project reference checks, interviews, price negotiations, etc are all the final stage before awarding the winner.

The vendor's provided references are good, but use your own personal network to find unofficial references to boost comfort level.

Once you and the selection committee are satisfied with all the responses and have decided on the winner, you get to make one of the teams happy. Depending on the breadth of the contract, some final legal work may be needed, but given the time invested thus far, both sides should be eager to come to an agreement on any issues and get down to business.

Alas, with any competitive situation, there are those that didn't win the bid. Common courtesy suggests you notify them all in a timely manner. Some may request a feedback call with you to inquire areas they needed to improve. The decision about that rests with the team, though it does help the vendor learn what gaps they have and if they can even address them.

PART FOUR

Integrated Vs. Enterprise DLP

Integrated Vs. Enterprise DLP

When a vendor embeds a feature or functionality to address a specific channel of data loss, this is referred to as Integrated DLP. For example, many secure email gateway providers these days have an added functionality that protects against leaks of data via email. Enterprise DLP on the other hand, is an integrated technology that protects against data loss from all channels and offers more robust data detection and control capabilities.

There are advantages and disadvantages to both Integrated and Enterprise DLP. The right choice depends on the nature of your company's data and risk tolerance.

Integrated Vs. Enterprise DLP

The Upside of Integrated DLP

- Allows you to leverage your existing security investments
- Gives you high fidelity alerts for a specific channel, such as email, and can be effective for whichever channel your organization selects

The Downside of Integrated DLP

- Compared to Enterprise DLP, it has less sophisticated capabilities to detect sensitive data
- Usually siloed by channel, with no integration and no consistent policy across integrated products
- Harder to coordinate for incident investigation and response because you need a console for each integrated product. This can lead to coverage gaps as your DLP will only cover specific egress vectors

The Upside of Enterprise DLP

- Much greater depth and breadth of sensitive data detection methodologies, which translates into meaningful increases in DLP effectiveness
- A central management console that eliminates the need for multiple management interfaces and significantly reduces the management overhead of a comprehensive DLP program
- In combination with CASB it can provide coverage across the complete spectrum of data leakage vectors

The Downside of Enterprise DLP

- Considerably more resource intensive to deploy and manage. DLP as a managed service has grown dramatically in the past few years in response to this challenge.

When Integrated DLP Makes the Most Sense

- If your existing security tools have DLP for specific channels built in, then integrated DLP can be a cost and resource effective interim solution for companies that aren't in heavily regulated industries, don't have lots of valuable IP to protect, and/or have a higher risk tolerance.

When Enterprise DLP Makes the Most Sense

- Although Enterprise DLP is more resource intensive, it provides the level of data protection that regulated, IP-intensive organizations need. Done right, it can drive changes in business processes that reduce risks to your organization's most sensitive data. For resource-challenged companies, Enterprise DLP as a service is an increasingly popular option.

Managed Security Services Evaluation Checklist

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

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

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

See Our Blog

Read about Managed Security Service Providers (MSSPs), why you should use their services, and how to select a provider.

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

PART FIVE

Making the Business Case for DLP

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?

What's a Value-based Business Case?

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

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

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

Understand the Value of Information Security

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

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

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

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

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

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

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

Align DLP With Company Growth and Innovation Initiatives

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

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

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

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

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

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

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

Align DLP With Company Growth and Innovation Initiatives

TEMPLATE

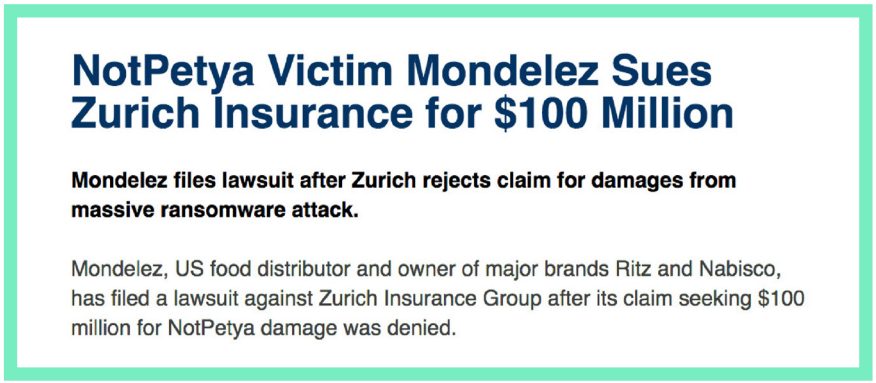
Using the growth and innovation opportunities from the previous page, determine which ones you can tie your DLP project with to make a growth oriented business case.

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

A Word About Cyber Insurance Coverage

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

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



NotPetya Victim Mondelez Sues Zurich Insurance for $100 Million

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

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

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

Positioning DLP to the Business

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

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

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

CEO

PAIN POINTS

- Business growth
- Market perception
- Future prospects

LINK DATA PROTECTION TO ADDRESSING PAIN POINTS

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

CISO

PAIN POINTS

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

LINK DATA PROTECTION TO ADDRESSING PAIN POINTS

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

CFO

PAIN POINTS

- Profitable growth
- Efficient use of assets

LINK DATA PROTECTION TO ADDRESSING PAIN POINTS

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

CRO/CCO

PAIN POINTS

- Support and document compliance stance against evolving regulations

LINK DATA PROTECTION TO ADDRESSING PAIN POINTS

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

Positioning DLP to the Business

DIR. OF INFOSEC

PAIN POINTS

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

LINK DATA PROTECTION TO ADDRESSING PAIN POINTS

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

BUSINESS UNIT LEAD

PAIN POINTS

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

LINK DATA PROTECTION TO ADDRESSING PAIN POINTS

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

CMO

PAIN POINTS

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

LINK DATA PROTECTION TO ADDRESSING PAIN POINTS

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

USER

PAIN POINTS

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

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 SIX

A 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.

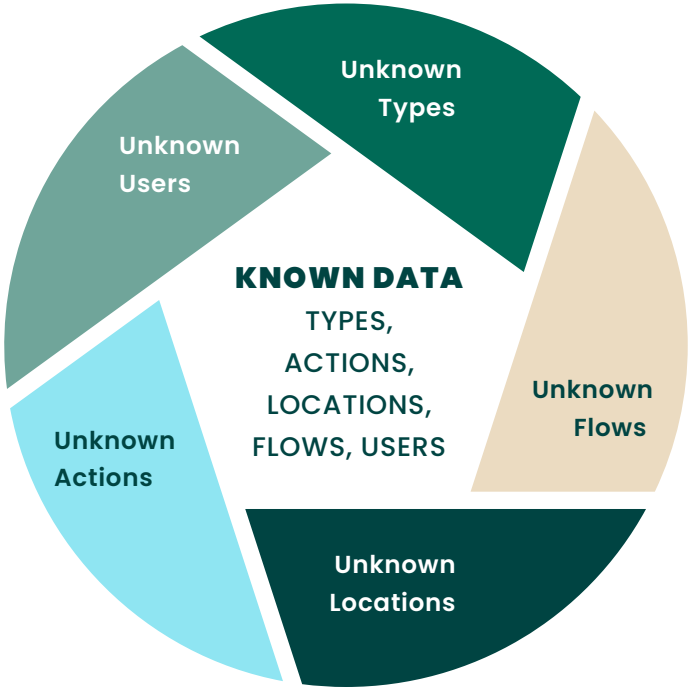
OUR PROVEN, 5-PHASE APPROACH DELIVERS THE ENTERPRISE DLP YOU NEED:

Stage 1: Insight

INSIGHT | BASELINE | EDUCATE | ACT | ACCESS

- 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

INSIGHT | **BASELINE** | EDUCATE | ACT | ACCESS

- **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).**

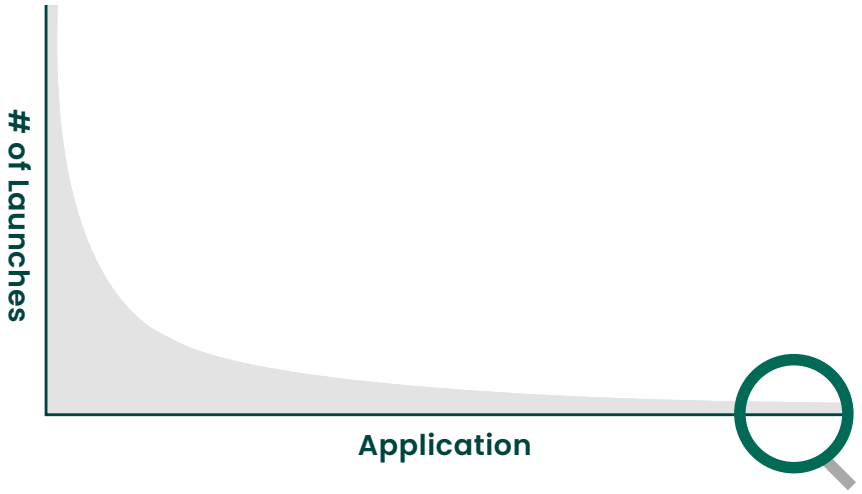
- **You will gain tremendous into the business with the unbiased data collection:**
  - Normal data flows throughout the business
  - Marketing accessing the legal and finance server at off hours
  - Sales reps encrypting, compressing, renaming excel files to look like .JPGs
  - Finance accessing and 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 | ACCESS

- 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

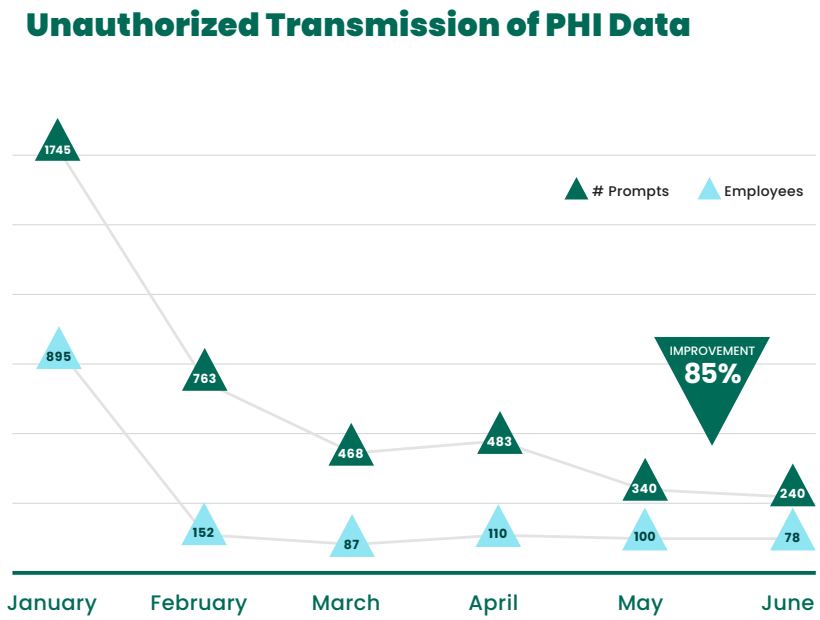
INSIGHT | BASELINE | **EDUCATE** | ACT | ACCESS

- **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 | ACCESS

- 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.



Stage 4: Act

- **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

- **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 4: Access

- **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.**

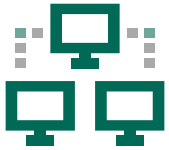
PART SEVEN

Why Fortra's Digital Guardian

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

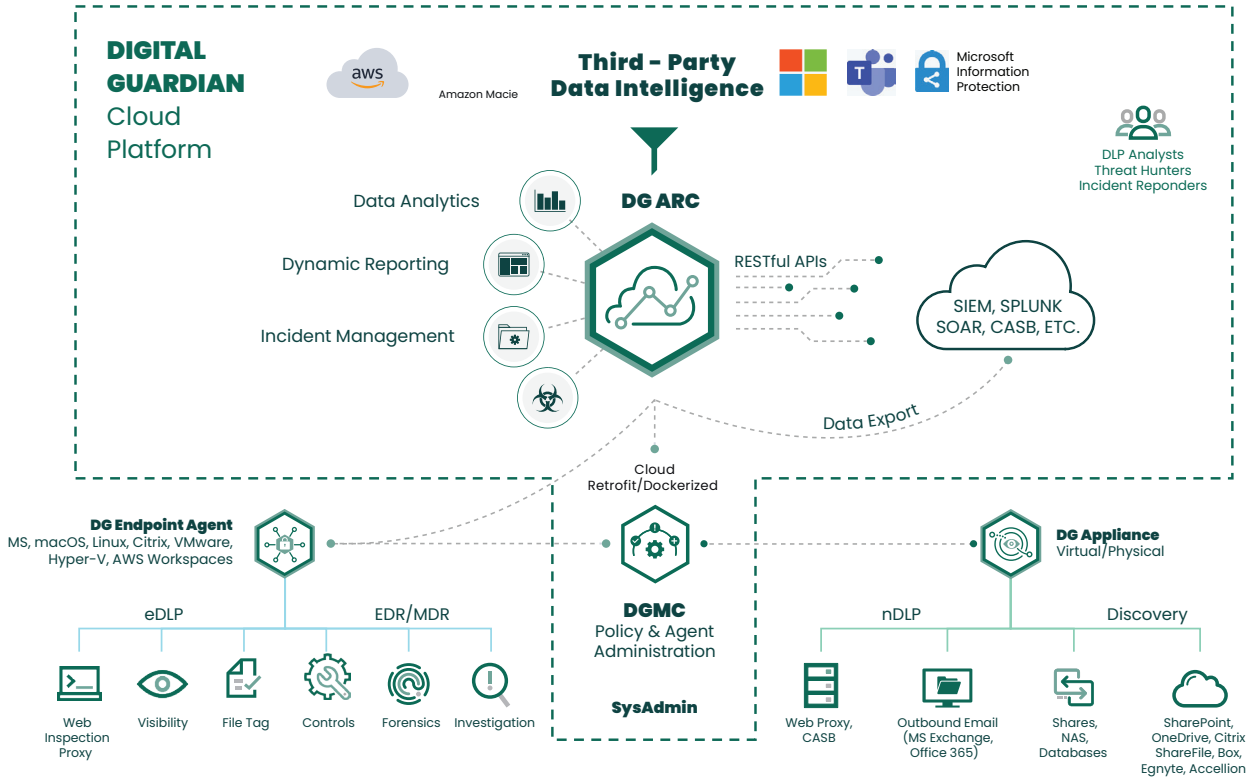
Only Digital Guardian provides content, user, and context-based data discovery and classification.

The Only Cloud Delivered Data Protection Platform

Free Download
Fortra's Digital Guardian Corporate Overview

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



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?

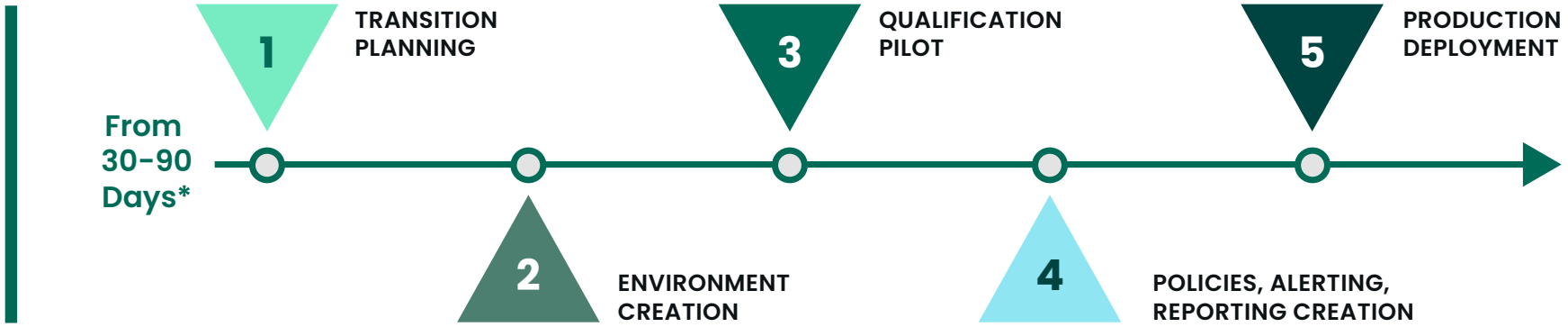
Start by sharing real discoveries from your "Quick Win" about where sensitive data resides and how it's being used. This will get the attention of your enterprise's business leaders. It will make it much easier for them to understand the risks to the business. And it will make it much easier to collaborate 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

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.



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.

JABIL

MORE INFO

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

Read the full case study here.

CASE STUDY

Enabling Employees to Protect Sensitive Client Information

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

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

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

MORE INFO

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

Read more case studies here.

CASE STUDY

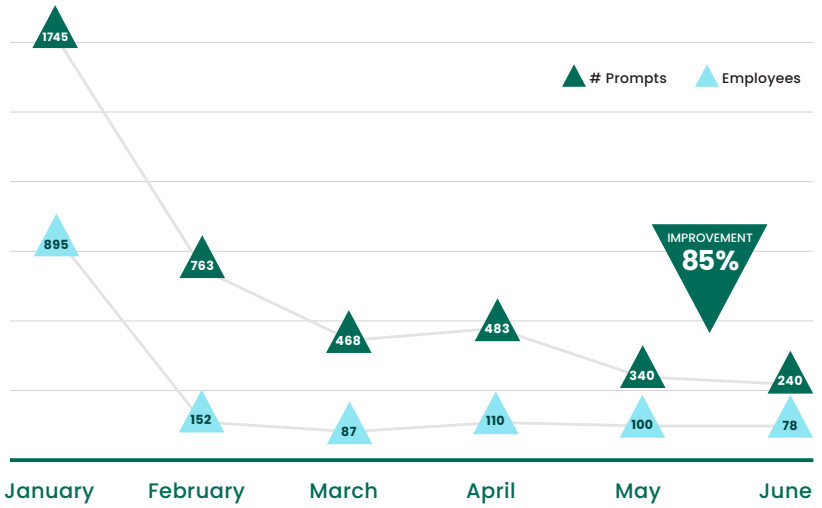
The Power of Real-Time User Education

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

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

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

Unauthorized Transmission of PHI Data



WATCH A VIDEO

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

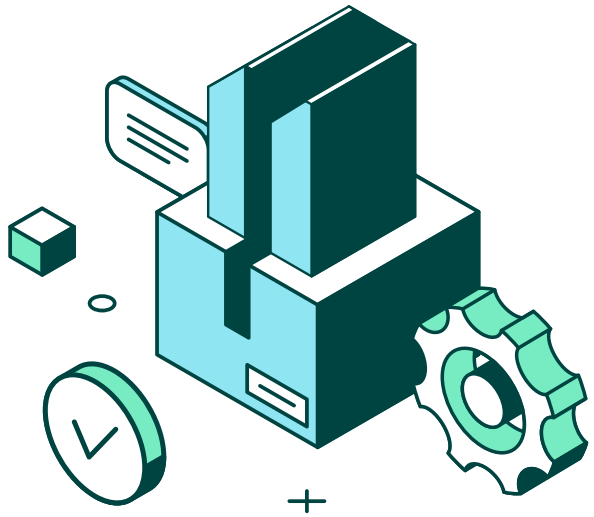
CASE STUDY

Protecting Industrial Automation IP

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

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

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



MORE INFO

Read more case studies here.

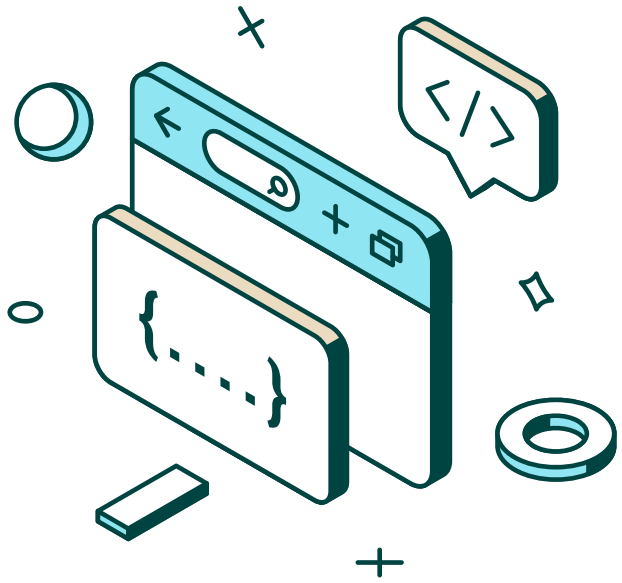
CASE STUDY

IP Protection at a Global Investment Bank

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

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

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



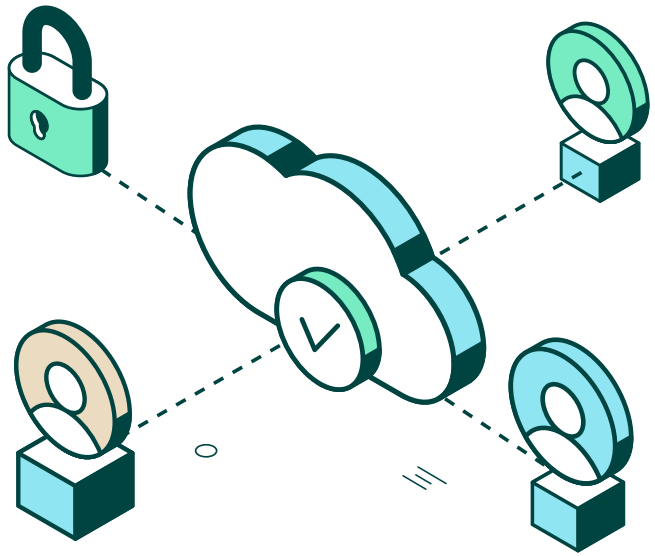
CASE STUDY

Securing PII Shared With Third Party Vendors

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

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

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



CASE STUDY

Managed Detection & Response at a Multinational Bank

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

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

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

DIGITAL GUARDIAN
Managed Detection & Response

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

(fta-dg-gd-0223-r2-as)