FORTRA™

**WHITE PAPER** (Digital Guardian)

# How To Overcome Pitfalls That Sabotage DLP Initiatives

## Challenge – Many DLP Deployments Don't Deliver Expected ROI

Done right, a data loss prevention (DLP) implementation can play an essential role in protecting an organization's sensitive data from accidental or malicious incidents. By providing visibility to sensitive information, tracking its use, and blocking misuse DLP can quickly pay for itself. But while most companies have seen some benefit from their DLP solutions, only 18% have seen transformational business benefits [Forrester Research, It's Time for Next-Generation DLP, May 2019].

The key to getting a high return on investment from DLP is avoiding six common pitfalls that slow adoption of DLP and limit its effectiveness:

1. **Insufficient Business Sponsorship** – A DLP program requires executive support for success. If business leaders don't understand and embrace the need for a DLP initiative, they are likely to view it as an impediment to productivity.

2. **Policy Creation Quagmire** – DLP implementations often get bogged down by analysis paralysis that results from trying to capture and think through every use case prior to rolling out the DLP solution.

3. **Inflexible Policies That Impede Employee Productivity** – Most DLP solutions take a binary approach to policy enforcement; every action must either be allowed without limits or blocked entirely. This ignores how businesses operate and how information is used. Strict controls may be justified for some actions, but strict rules can also block legitimate use of data by employees and partners, harming productivity and unnecessarily slowing down DLP adoption.

4. **Onerous to Setup, Maintain, and Scale** – Shortages of security, compliance, and technical staff are found in organizations of all sizes. Enterprise DLP solutions that require extensive configuration and setup to "train" the solution on classification and usage rules can take months or more to create value. After implementation, these solutions can burden security and IT teams trying to triage and prioritize critical findings from false positives, update policies, and build exceptions. In response, many companies end up limiting the rollout to select groups or departments.

5. **Missing Egress Vectors** – Some DLP solutions are geared to specific solutions and egress channels. These so-called "Integrated DLP" solutions cover single egress vectors like email or removeable media with no integration or consistent policy across other channels and products. Enterprise DLP solutions typically cover all egress vectors but can leave gaps in coverage for non-Windows operating systems as well as less commonly used browsers and applications.

6. **Violating Employee Privacy Regulations** – DLP solutions are designed to track data and user actions. In some jurisdictions this can violate workers' rights, including Workers' Council mandates for employee privacy.

## How Digital Guardian DLP Delivers High ROI

### Rapid Time to Value is Achievable

While these pitfalls do not necessarily prevent successful deployments over time, each is a hinderance to adoption and return on investment. Fortra™'s Digital Guardian® is designed to avoid these obstacles to success; simplifying adoption, getting buy-in from the business leaders, protecting sensitive information across all egress vectors, and respecting user privacy while enabling unfettered access to data by authorized users.

### Overcoming Pitfall 1 (Insufficient Business Sponsorship & Pitfall 2: Policy Creation Quagmire)

Standard enterprise DLP supports a "Top-Down" or "Known Risks" approach to protecting your sensitive data. This approach requires that you already know what data you need to protect, where it resides in the organization, and how it is used. In a Top-Down approach, you focus on a specific data type (e.g., PHI) or a group of users (e.g., engineers), then create policies dictating how to handle known sensitive data types in identified locations and users. Digital Guardian can do this, and if your organization is just trying to meet a basic compliance requirement, this may be enough. But given the volume of digital data generated in most companies, focusing just on the compliance requirement can leave your organization exposed to risks you are not even aware of.

**Known Risks: Top-Down visibility & analysis**

- Use-case based approach
- Compliance or IP protection
- Secure and enable existing business processes
- Focus on known data types, flows, groups & risks

< Continuous Risk Management >

**Unknown Risks: Bottom-Up discovery & quantification**

- No policy, no problem
- Know what you don't know
- Understand non-sanctioned activities
- Focus on unknown data types, repositories, flows, groups & risks

Digital Guardian's unique ability to do contextual classification of data means that you can add a "Bottom Up" or "Unknown Risks" approach and learn all the places where sensitive data is located, how it flows in the organization, and where that data is at risk (e.g., identifying – with evidence – the predominant egress channels).

**The benefits of this approach are:**

- **It eliminates the need to create policies up front.** Instead, you can deploy the Digital Guardian endpoint agent and it will immediately start identifying sensitive data and collecting the data movement and usage patterns across the organization to inform better policy creation.
- **You discover previously unknown risks.** For example, instead of simply looking at email attachments or USB downloads, you can see exactly how data is currently exfiltrated – whether maliciously or by well-meaning but careless employees. This could include employees uploading sensitive data to unsanctioned cloud apps, copying sensitive data into new documents, or simply printing data that can be slipped out in a briefcase.
- **It more effectively identifies sensitive, unstructured data.** Not all sensitive data resides in databases. Word documents, emails, presentations, and commercial or proprietary applications can create and store sensitive but unstructured data, including organizational IP. Tracking that data to prevent loss is also important.
- **A bottom-up approach is a real-world approach.** Business leaders want a fact-based approach to security. The information gathered from an initial data discovery allows security, IT, and business sponsors to develop very granular policies based on how the data is actually used and how it flows within the organization. More granular policies are less likely to impede standard employee workflows, while still protecting the data. Once deployed you can use the ongoing data usage patterns to refine and optimize policies for better data governance that reduces risks without impacting business productivity.

Many large enterprises will use a combination of the Top-Down and Bottom-up approaches. You can only do that with Digital Guardian.

> ***"The insights from this bottom-up approach make it much easier to engage the business sponsors; you can give them concrete examples that they can understand and relate to instead of abstract policies."***
>
> **John Graham**
> *Former CISO, Jabil*

## Overcoming Pitfall 3 (Inflexible Policies that Impede Employee Productivity)

Closely related to Pitfall 2, Pitfall 3 is the logical outcome when organizations neglect to account for real world data usage. When a solution only considers data and users, it can result in obstacles to established, legitimate usage patterns. For example, while it may not be the norm, at times it may be necessary for engineering to view a customer contract to understand required deliverables, or for sales to view invoices.

**Digital Guardian considers users, actions, and data in context.** Whether the data is structured or unstructured, Digital Guardian always knows where it is and how it is being used. DG understands the context of how sensitive data is used, seeing at the system, user, and data level. When data is used safely, Digital Guardian is invisible to end users, allowing unfettered access and use of data. When use policies are violated, or actions are attempted that could out sensitive data at risk, DG DLP can apply a wide range of controls, from hard blocks or warnings to forced encryption and exception handling.

## Overcoming Pitfall 4 (Onerous to Setup, Maintain, and Scale)

Traditional approaches to DLP, where internal employees set up, manage, and monitor solutions can be effective in organizations with sufficient resources and skills. Increasingly, however, organizations recognize the value in outsourcing portions of their security to dedicated and skilled service providers. Powered by AWS, Digital Guardian's cloud-delivered enterprise DLP provides simplified deployment, low overhead, and elastic scalability for accelerated time-to-value on your security spend. It is available as SaaS, or a managed service based on your resources.

### SaaS Security for Enterprise DLP

Our purpose-built SaaS DLP infrastructure enables you and your team to focus more time, energy, and resources on identifying and mitigating risks to your sensitive data and less time on acquiring, building, and maintaining the infrastructure. The benefits include:

- **Immediate Time to Value** – Digital Guardian hosts and manages all hardware and software. No upfront investment in staff is required – we work with your team to identify and protect your most critical assets without disrupting your operations.
- **Lower Costs and Maintenance Cycles** - You cut costs and the complexity of patching, updating, and maintaining on premises hardware and software. Digital Guardian hosts and manages a big data security architecture for you.
- **Scalability** - Instead of ordering new hardware, testing updates in a development environment, rebalancing servers, and training new personnel, the DG cloud scales on demand. Adding endpoints anywhere in the world is simple. We can instantly scale up to meet your demand and provide sufficient storage and compute power to drive world class data protection at lower cost and with reduced complexity.

### Managed Security Program for DLP

With our Managed Security Program, you can focus on strategic imperatives while our security experts take care of all aspects of DLP: hosting, setup, ongoing monitoring, analyzing, tuning and maintenance. Our team of DLP experts will administer, analyze, and guide your DLP program for faster time to value and peace of mind.

Our experts have 10+ years of experience in designing and executing DLP projects across industries such as manufacturing, financial services, healthcare, and technology. The benefits include:

- **Fill Your Security Talent Gap** - Leverage our DLP experts and InfoSec analysts with 10+ years' experience implementing and improving mission-critical data visibility, IP protection, compliance, and governance programs.
- **Accelerate Time-to-Value** - Our MSP customers repeatedly tell us that they were able to improve their data visibility and data security risk posture faster than they ever could have done by themselves, or with any other vendor.

- **Leverage Programmatic Best Practices** – MSP for DLP customers gain the benefit of our insights, experiences, and processes protecting the most critical information for hundreds of customers across a range of industries.

## Overcoming Pitfall 5 (Missing Egress Vectors)

Few organizations have a monolithic technology stack, and the work from anywhere movement has broadened the security challenges. Workers now run a variety of devices and operating systems, browsers, and cloud applications. Disgruntled workers may download customer lists, product plans, and other IP to bring to a competitor. Careless but well-meaning employees may upload files to private cloud accounts for easier access from home. In many cases, an insider may simply print sensitive information.

**Digital Guardian covers all egress vectors and the broadest range of operating systems, browsers, and applications.** Digital Guardian provides companies with the broadest coverage and control, including Windows, macOS, and Linux endpoints. Digital Guardian integrates with leading cloud storage providers to scan repositories, enabling encryption, removal, or other automated remediation of sensitive data before the file is shared in the cloud.

Digital Guardian's protection travels with the data, on and off the corporate network. This includes the ability to monitor and control web browser, copy/paste, email, removeable media, printing, and archiving activity. Our DLP solution offers the industry's broadest endpoint coverage, including Windows, macOS, and Linux endpoints as well as VDI support, recognizing both structured and unstructured files across all platforms. With Digital Guardian, you have complete data visibility and control regardless of what users are running, what they're running it on, and on or off the network.

Integration with Microsoft Information Protection (MIP) enables our platform to read MIP Labels and map them to internal policies, controls, and actions to ensure users cannot bypass traditional DLP controls. It can review data classified by MIP to validate that classification, and encrypt, log, and/or block sensitive information egress in outbound email messages, cloud uploads/downloads, or files being copied to external/removable storage across Linux, MacOS, Firefox, Safari, and the thousands of other apps that are used by organizations.

## Overcoming Pitfall 6 (Violating Employee Privacy Regulations)

Digital Guardian is a proven data protection platform that enables companies operating in Europe to protect employee rights while maintaining effective data security. Digital Guardian makes it easier for corporate security and legal officers to engage with Workers' Council members by offering visibility into data risk without compromising privacy. It provides flexibility in implementing mitigation controls that protect both employees' and sensitive enterprise information. **Digital Guardian has been deployed successfully, with Workers' Council approvals, in Germany, Austria, Switzerland, Italy, and France**.

Digital Guardian can enforce controls while protecting user privacy. Our agents capture activity on endpoints, including descriptive data about events, but not the actual content of a file or email. Flexible control responses to risky activities include real-time user warnings, prompts, encryption, and action blocking.

Digital Guardian can be deployed so that all collected data sources are anonymized. Anonymizing data results in no direct association between users' identities and collected or reported activities. Digital Guardian also controls access to the anonymized data. In the event of an incident, Digital Guardian supports procedures for controlled unlocking of a computer or user's account. This includes the use of split passwords, requiring two logins to unlock a user's identity. Security, Department Managers, and Workers' Council representatives can work together to define procedures that offer protection to all employees, while enabling effective incident response and escalation.

**Other privacy related features include:**

- All communications from agent to console are encrypted
- Agents are not transferring sensitive data to DG console
- Agents collect event details (metadata) of user, system, application events

- Events collected may be increased/decreased to address privacy concerns
- Identifying details can be pseudo-anonymized based on RBAC
- Tokenize or hide details like user, computer, file path, file name
- Files may optionally be collected, but are transferred to customer repositories
- File is encrypted with public key. Customer maintains private key
- Link to encrypted, collected file is available in DG console
- Activities in the console are logged and reportable
- Centrally define policies to comply with local laws and privacy regulations
- Enforce controls without collecting the PII data of individuals or group

## Summary

Today's organizations face a variety of internal and external threats to sensitive data. A strong DLP solution will identify sensitive data throughout the enterprise and protect it through logical and consistent policies. However, not all solutions are prepared to help organizations overcome common pitfalls and achieve value from their DLP implementations.

Digital Guardian helps organizations establish successful DLP programs by overcoming the common pitfalls. Whether it is using our unique combination of "Top-Down" and "Bottom-Up" DLP for identifying, classifying, and protecting sensitive data or taking advantage of Digital Guardian's managed security services, our customers are able to achieve and maintain executive buy-in, quickly establish and enforce policies that protect information without hampering employee productivity, cover all egress vectors, and protect employee privacy – to drive a high ROI for your DLP initiative.

FORTRA™

Fortra.com

**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.