OVERVIEW

anchor

# DLP Is Broken. This Is Why— And How To Fix It.

Learn how to protect your data – without the DLP angst


anchormydata.com

# Breaking the Mold

As attack surfaces grow and cyber attacks become more frequent, it is more important than ever to protect information assets. These are largely comprised of data files generated from applications such as Word, Excel, and dedicated financial and human resource systems.

For certain types of information such as customer data, protection is mandated by regulations. In industrial settings, securing intellectual property and proprietary data are vital steps to preserve the organization's brand, product, and revenue and to meet compliance obligations. Data protection is now a basic requirement for supply chains, and it can cost organizations business if their security standards are not demonstrable.


But where to start? Let's take a look.

## A common approach to safeguarding data is data loss prevention (DLP). Ironically, though, DLP strategies do not offer protections for a lot of common industry and line-of-business applications that really need safeguarding – such as proprietary CAD files and sensitive electronic healthcare records.

Plus, these conventional IT controls aren't really working to deliver the desired result efficiently and effectively. They focus on locking down networks, devices, and people. Once files are moved, shared, or stolen, the data is no longer protected. And because of their inherent complexity and need for continuous monitoring and user training, more than 35% of large DLP implementations fail.[1]

The real solution is to enable data to protect itself – a new concept that is fundamentally different from DLP in philosophy and implementation. Self-protecting data "bakes" invisible protection into files of any type and from any application, allowing users to work and collaborate securely – with no changes to how they work. Best of all, self-protecting data remains secure even when it leaves the organization. The chain of custody is easily tracked through forensic logging. And if an employee or contractor leaves, file access can be revoked in seconds.

New tools are disrupting traditional data protection thinking and its inherent weaknesses. But what does that really mean?

**More than 35% of large DLP implementations fail.[1]**

**Keep reading to discover 4 ways self-protecting data flips the script on traditional DLP's inherent weaknesses.**

[1] https://www.gartner.com/en/articles/build-a-successful-data-loss-prevention-program-in-5-steps

# 1 Fast Implementation

## Days, months, and years should be minutes

Regardless of the size of the organization, developing and implementing a DLP program can be a complex process. The massive services requirement is the reason that DLP is often outsourced rather than tackled in-house.

DLP development alone is cost- and resource-intensive. It takes months – often years – to identify data sources across the organization's distributed infrastructure, inventory the data, define "sensitive" data and develop secure workflows and processes for data use, integrate with other systems and apps, and gain business leaders' commitment to enforce the developed policies.

And the work is still not done since, once implemented, DLP is not a "set and forget" solution. It needs constant monitoring for infrastructure, compliance, and business changes that may prompt adjustments to security policies and controls.

[2] https://www.proofpoint.com/us/threat-reference/dlp

## Self-Protecting Data Advantages

- Implement in minutes – no complex processes, no integrations, no monitoring required.
- Choose what you want to protect.
- Pick who gets access.
- Select how it can be accessed using existing applications and IT controls.
- Relax – changes to the infrastructure or business don't affect the data.

## The Data Security Problem Needs to Be Solved

There has been a **47% increase** in data breaches since 2020.[2]

including accidental data loss and deliberate data exfiltration by negligent or disgruntled employees.

2

# Transparent to Users

## Security is “built-in” and invisible, not as a multi-level afterthought rife with user complaints

To protect an organization’s information, DLP establishes security policies based on the content of the data as well as its context. The enforcement of these security policies can be heavy-handed to users (and frankly, twice as hard to manage for IT and security) and changes how they access and interact with the data. As a result, users must be trained on the new workflows, DLP security policies, and in some cases, new applications and interfaces.

But DLP security controls get in the way of work and collaboration. Frustrated users complain to IT and to the executives, and intentionally find ways to work around these controls. By doing so, though, they negate the intended protection and increase risk.

## Self-Protecting Data Advantages

- Protection is invisible to users (similar to antivirus software) and doesn’t impact user experience.
- Authorized users can access and share files freely and securely.
- Workflows are familiar through Word, Outlook, Excel, and other existing business applications.
- Self-protecting data is lightweight and unobtrusive, so users aren’t motivated to work around it.

## DLP Complexity Is a Barrier in Modern Environments

**84%**
of IT leaders say DLP is more difficult with a remote workforce.[2]

which adds risks compared to keeping data internally on corporate and controlled devices.

[2] https://www.proofpoint.com/us/threat-reference/dlp

# 3 Data Protected in All States

## Data use is free and unencumbered – but secure

A DLP strategy uses technologies and processes to protect proprietary and sensitive data from unauthorized access and use. DLP restricts confidential data and locks it in behind the organization's firewalls, preventing users from sending it outside of the organization.

At endpoints and in applications, DLP secures data while it is in use. DLP encrypts data to protect it while it is in transit across a network. And it protects data that is stored – in databases, in backups, on devices, or in the cloud.

But data is unprotected – and vulnerable – until DLP acts upon it. So, when DLP fails, as it often does, data is leaked as plain text instead of ciphertext.

## Self-Protecting Data Advantages

- Secured data is encrypted in all states – in transit, in use, and at rest – so a data breach does not result in a data leak.
- Access rules include continuous multifactor access controls.
- Self-protecting data leaves a digital chain of custody that includes file sharing.
- If an employee leaves, data access can be revoked immediately – so any files they have are worthless.
- Protects industry and line-of-business application data including CAD files and electronic healthcare records.

## Access Controls Are Lacking

**76%**
of U.S. employees have inappropriate access to sensitive data.[3]

[3] https://www.varmour.com/press-release/new-varmour-research-reveals-76-of-u-s-employees-have-inappropriate-access-to-applications-and-data/

# 4 Affordable Data

## Security doesn't have to come at a big cost

Depending on whether the services are outsourced or in-house, the cost of a DLP program implementation can be significant. There is also a significant investment of time required by resources – including data owners and other key stakeholders, and technical and specialized resources (e.g., for system integrations).

As we mention in Advantage #1, DLP frontloads teams with a lot of detail-intensive tasks that require significant time and resource commitments – from project scoping and data mapping to use-case and workflow development.

Even after DLP implementation, resources are needed for the continuous monitoring of infrastructure and business changes, fine-tuning, and user training.

[4] https://phoenixnap.com/blog/data-loss-prevention-best-practices

## Self-Protecting Data Advantages

- The cost to acquire is a fraction of a DLP investment.
- Fast and significantly less work to implement, so time and resource commitments are minimal.
- Does not impact the user experience – no training for new workflows and no user workarounds.
- No fine-tuning needed – files are protected even as your business and infrastructure evolve.

## Data Security Must Protect on Multiple Fronts

### 3 CAUSES OF DATA LOSS[4]

**Negligence**
e.g., system misconfigurations

**Infiltration**
e.g., criminal attacks

**Insider Threats**
e.g., disgruntled employees

# The Advantages Are Clear

| | | Self-Protecting Data Solution | Data Loss Prevention |
|---|---|---|---|
| IMPLEMENTATION | Fast implementation speed | ✓ minutes | ⊖ month/years |
| | Simple for companies of any size | ✓ no discovery, integration, or policies needed | ⊖ |
| | No user training needed | ✓ | ⊖ |
| | Protects any type of file | ✓ e.g., CAD, source files, custom, video, etc. | ⊖ |
| TRANSPARENCY | Invisible as antivirus to the end user | ✓ | ⊖ |
| | Feature-rich for enterprises | ✓ | ✓ |
| | No outsourcing or services required | ✓ set-up is easy | ⊖ |
| ACCESS | Continuous multifactor access controls | ✓ | ⊖ |
| | Simple file-sharing and collaboration | ✓ | ⊖ |
| | No required workflow changes | ✓ | ⊖ |
| | Digital chain of custody | ✓ including sharing | ⊖ |

# The Anchor Advantage

Existing DLP solutions focus on locking down networks, devices, and people. All of this is done in the name of protecting data. But, once files are moved, shared, or stolen, the data is no longer protected. Solutions that enable data to protect itself are the holy grail for data security initiatives.

Here's how the Anchor SaaS Platform flips the script on DLP:

- Anchor makes data protection simple and affordable, securing data in less than 60 minutes and without the cumbersome policies and workflows of traditional DLP solutions.
- Anchor bakes transparent protection into the data so it becomes self-protecting, freeing business users to work unobstructed – and securely.
- Anchored data is transparent for users and allows them to use existing and familiar apps, storage, and cloud providers.
- Each Anchored file is individually military-grade encrypted at rest, in motion, and even while in use (saving does not generate plain text).
- Even if the files are stolen, they are never more than unreadable ciphertext.

**See How Easy It Is To Anchor YOUR Data.**
**BOOK A DEMO**

> ***"It really wasn't that difficult to choose Anchor over the other options. It felt like a very easy to use, lightweight product that could get the job done. The Microsoft [Zero Trust] solution was going to be very expensive. Anchor has a more reasonable price point."***
>
> -BRYANT CHERRY, RESIDENT GURU, EMERSION DESIGN



8000 Walton Parkway
Suite 224
New Albany, OH 43054

Hello@AnchorMyData.com
www.anchormydata.com

anchor

## Our Vision

Information is the result of work and is valuable property. Its owner has the right to realize its benefits while maintaining absolute control of it.

## Our Mission

To empower organizations to easily and affordably realize the benefits of their information by confidently using and sharing it as needed to do business without fear of it being lost, stolen, or abused.