Data Loss Protection Survival Guide

By Ashley Knowles

About Me

13 Years in Cyber

15 Years in IT

Cheese Connoisseur

Board Game Collector

Unwillingly Educated in AI

GETTING STARTED

Why DLP Shouldn't Terrify You (Too Much)

You're Not Alone - Let's Demystify This Together

Manageable Approach

DLP seems overwhelming at first, but it becomes manageable when you break it down into practical steps with the right approach and tools.

Build Incrementally

Start small with quick wins, build incrementally over time, and focus on protecting what matters most to your organization.

Knowledge is Power

Understanding the threats and attack vectors helps you defend effectively and prioritize your security investments.

Actionable Guidance

Today you'll gain practical guidance to get started with confidence and build a defensible DLP program.

STEP 1

Understanding Your Data Landscape

What Data Do You Actually Have?

Structured Data

Organized information stored in databases and systems with defined schemas and relationships.

- Customer databases with PII and payment information
- Employee records including SSN, salaries, and medical data
- Financial data with reports, transactions, and forecasts

Unstructured Data

Information that doesn't fit neatly into databases, often the hardest to protect and most commonly leaked.

- Documents, spreadsheets, and presentations
- Emails with sensitive attachments
- Code repositories containing intellectual property
- Chat messages in collaboration tools

Data Classification Framework

Not All Data Needs The Same Protection

1

Public

Marketing materials, public website content, press releases—no harm if exposed.

2

Internal

General business documents, internal communications, non-sensitive project data.

3

Confidential

Customer data, financial records, employee information requiring protection.

4

Restricted

Trade secrets, M&A plans, regulated data (HIPAA, PCI-DSS) aka your crown jewels.

Pro Tip: Start simple by focusing on your "crown jewels" first. What would hurt most if leaked? You can always expand coverage later.

Where Does Your Data Live?

Mapping Your Data Estate

Endpoints

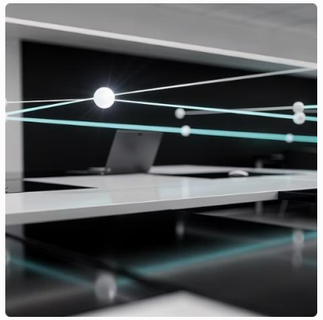
Laptops, desktops, and mobile devices with local storage and downloads folders. Should be your first line of defense.

Network Storage

File servers, NAS devices, and shared drives where teams collaborate and store critical business data.

Cloud Services

SaaS applications like Office 365, Salesforce, cloud storage providers, and custom applications with APIs.



In Transit

Email communications, file transfers, API calls. Data moving between systems and outside your network.

⚠ THREAT LANDSCAPE

Understanding Data Exfiltration

How Does Data Actually Leave?

Accidental Loss

Most data breaches aren't sophisticated attacks - they're honest mistakes that happen every day.

- Wrong recipient on email
- Misconfigured cloud storage permissions exposing files publicly
- Lost or stolen devices without encryption
- Improper disposal of old hardware

Malicious Exfiltration

- Email forwarding to personal accounts
- Uploading to personal cloud storage services
- USB drives and external devices
- Screenshots, copy/paste, and printing sensitive information

Advanced Exfiltration Methods

What Sophisticated Threats Look Like

Covert Channels

DNS tunneling hides data in DNS queries. Steganography embeds data in images. Encrypted connections to external command-and-control servers bypass traditional monitoring.

Evasion Techniques

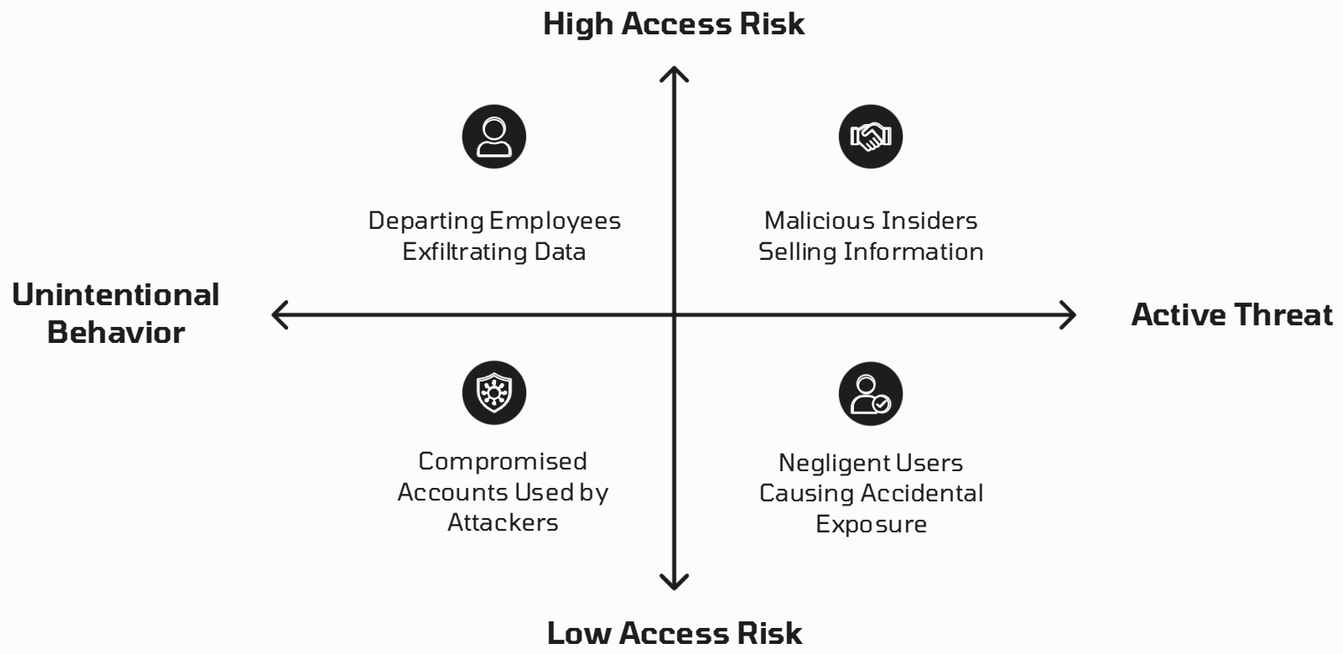
Breaking files into small pieces to avoid detection. Encrypting before sending to bypass content inspection. Using legitimate business tools maliciously. Slow exfiltration over time to blend with normal traffic.

Timing Attacks

After-hours or weekend transfers when security teams are offline. Gradual data theft over weeks or months to avoid triggering volume alerts.

The Insider Threat Reality

Not Everyone With Access Has Good Intentions



Understanding the insider threat landscape is crucial because these actors already have legitimate access to your systems and data.

Warning Signs to Monitor

Behavioral indicators often precede an actual data breach. Watch for these red flags:

- Accessing data outside normal job function or business need*
- Downloading unusually large amounts of data or documents
- Activity during odd hours, weekends, or holidays
- Use of personal devices or external accounts
- Data access spike right before resignation or termination

*Least Privilege Principle

DEFENSE STRATEGY

How to Stop Data Loss: The Basics

Building Your Foundation

01

Know Your Data

Discover where sensitive data lives across your environment. Classify by risk and sensitivity. Map who has access and why they need it.

02

Control Access

Implement principle of least privilege. Conduct regular access reviews quarterly. Remove access immediately when roles change or employees depart.

03

Monitor Activity

Log all data access and transfers comprehensively. Establish baseline "normal" behavior for users and systems. Alert on anomalies and investigate promptly.

Technical Controls That Work

Practical DLP Implementation

Email Protection

Content inspection for sensitive patterns like SSN, credit cards, and confidential labels. Block or automatically encrypt emails with sensitive data. Quarantine suspicious attachments for review.

Endpoint Controls

Monitor copy/paste to external drives and cloud services. Control USB and device access with whitelist policies. Block uploads to unapproved cloud services at the system level.

Network Controls

Web filtering with SSL inspection to see encrypted traffic. Block access to personal cloud storage domains. Monitor DNS for tunneling attempts and data exfiltration.

LAYERED SECURITY

Recommended Layered Approach

Depth in Defense for Data Protection

Network Controls

TLS-inspecting forward proxy or Next-Gen Firewall (NGFW) to monitor and block suspicious traffic flows, ensuring data doesn't leave via unauthorized network channels.

Tenant Restrictions

Implement tenant restrictions for M365/Google Cloud and leverage Cloud Access Security Brokers (CASB) for sanctioned application governance, controlling who can access what data.

Endpoint DLP Agent

Deploy DLP agents on all endpoints for comprehensive coverage of off-network devices, monitoring local activities, copy/paste functions, and USB transfers.

DNS Sinkholing

Utilize DNS sinkholing for quick wins against known malicious domains, preventing command and control communications and exfiltration to blacklisted destinations.

Cloud & Modern Workplace Protection

Securing Where Work Actually Happens

Cloud Access Security Broker (CASB)

Gain visibility into all cloud app usage, including shadow IT. Apply DLP policies consistently across SaaS applications. Detect anomalous file sharing and external collaboration risks.

Data-Centric Security

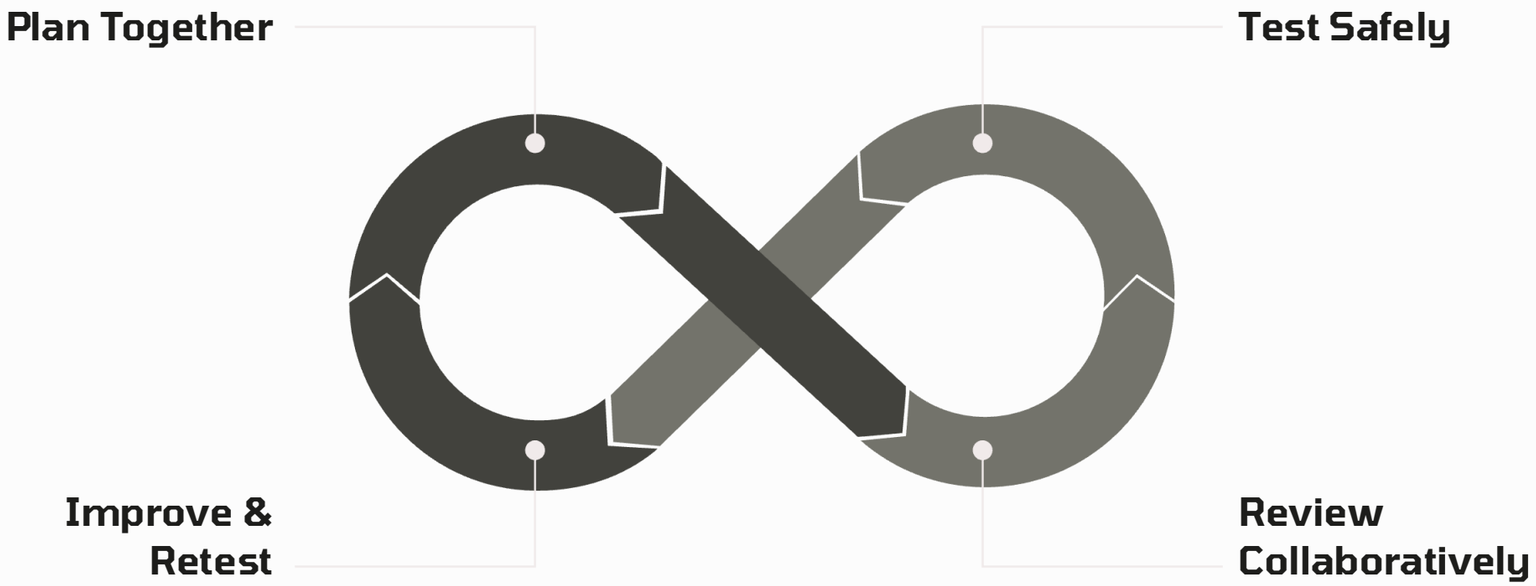
Encrypt sensitive files automatically based on classification. Apply rights management like view-only or no-download policies. Use persistent labels that follow data everywhere it goes.

User Behavior Analytics

Detect unusual patterns like large downloads or odd-hour access. Risk scoring based on multiple behavioral factors. Automatic alerts for high-risk activities requiring investigation.

The Purple Team Process

Testing, Learning, Improving Together



1. Plan Together

Agree on what to test and when. Define clear success criteria. Document expected detections and alert timing.

2. Test Safely

Use non-production sensitive data. Run in controlled environment. Document every step for reproducibility.

3. Review Collaboratively

Compare what detected versus what didn't. Analyze time to detect and alert quality. Root cause any gaps discovered.

4. Improve & Retest

Update rules and policies based on findings. Validate improvements work. Schedule next test cycle.

PURPLE TEAM

Purple Team Testing: Scenario 1

Email Exfiltration Test

The Test

Send sample sensitive data to personal email accounts. Try forwarding as attachment. Test encrypted attachments and password-protected files.

Expected Detection

DLP alert triggers on sensitive content patterns. Email blocked or decrypted automatically. Activity logged for security review even if allowed through.

Testing Objectives

- Validate email DLP rules work as configured
- Tune policies to reduce false positives
- Document gaps and create improvement plan
- Verify alert quality and investigation workflow

Success Criteria: Blue team receives actionable alerts within 5 minutes and can trace the full email path.

PURPLE TEAM

Purple Team Testing: Scenario 2

Cloud Upload Test

The Test Procedure

Upload sensitive files to personal Dropbox, OneDrive, and Google Drive. Try via web browser, desktop sync app, and mobile app. Test with renamed file extensions to evade detection.

What Blue Team Should See

- CASB or web proxy blocks upload attempt
- Endpoint DLP prevents file transfer at system level
- Alert generated for security team investigation
- User receives notification about policy violation

Validation Goals

Confirm cloud DLP coverage across all upload methods. Identify unsanctioned apps being used. Update policies for better protection.

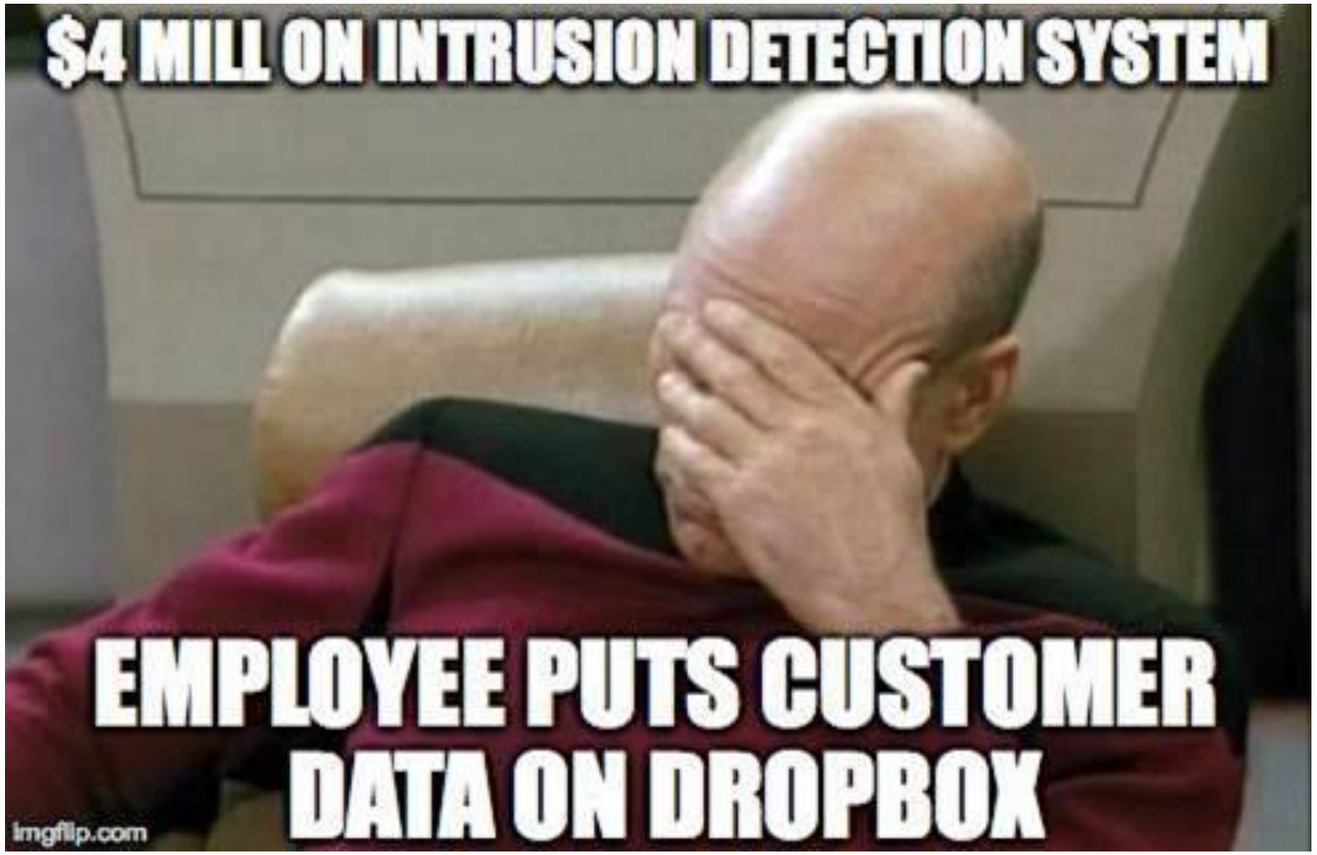
Common Gaps

Mobile apps often bypass web filters. File extension changes can evade content inspection. Personal VPN usage circumvents network controls.

PURPLE TEAM

Purple Team Testing: Scenario 3

Insider Threat Simulation



The Test

Download large volume of customer data exceeding normal patterns. Access files outside normal job function. Perform suspicious actions during after-hours or weekends.

Expected Detection

- UEBA flags unusual behavior with risk score
- Data access logs show clear anomaly
- Alert escalates based on risk score threshold
- Incident response procedures activate

Result

Validate behavioral detection works effectively. Adjust thresholds to catch real threats without alert fatigue. Test and refine incident response procedures.

PURPLE TEAM

Purple Team Testing: Scenario 4

USB & Physical Exfiltration

Test: USB Drive

Copy sensitive files to USB drive. Expected: Endpoint DLP blocks USB write operation and logs attempt.

Test: Mobile Device

Transfer files to personal mobile device. Expected: Device control policy enforces rules and prevents transfer.

Test: Printing

Print sensitive documents. Expected: Print job logging captures activity for audit trail.

Results confirm physical controls work as designed, identify printers not being monitored, and reveal gaps in device control policies that need updating.

Purple Team Testing: Scenario 5

Advanced Evasion Techniques

Test: Pre-Encryption

Encrypt files before uploading to evade content inspection. **Expected Detection:** Encryption before transfer triggers behavioral alert based on timing and pattern.

Test: DNS Tunneling

Use DNS tunneling tools to exfiltrate data covertly. **Expected Detection:** Network anomaly detection flags unusual DNS query patterns and volumes.

Test: File Fragmentation

Split large files into small pieces to avoid size-based alerts. **Expected Detection:** Behavioral analytics correlate multiple small transfers from same user.

Test: Screen Capture

Screenshot sensitive data instead of copying text. **Expected Detection:** Screenshot monitoring tools catch screen captures of sensitive applications.

Critical Insight: This scenario identifies gaps in advanced threat detection and helps prioritize next security investments.

IMPLEMENTATION GUIDE

Starting Your DLP Journey

A Practical Roadmap

Week 1-2: Discovery

1

Identify your top 5 most sensitive data types. Map where they currently live and who accesses them regularly.

2

Quarter 1: Quick Wins

Enable email DLP for obvious patterns like SSN and credit cards. Implement basic USB control on endpoints. Start logging cloud app usage.

Quarter 2-3: Build & Test

3

Deploy endpoint DLP to pilot group. Run first purple team test. Tune policies based on results and user feedback.

4

Quarter 4+: Expand & Mature

Roll out to all users gradually. Add cloud DLP and CASB capabilities. Establish regular testing cadence.

Key Takeaways & Action Items

You Can Do This - Here's Where to Start

Understand Your Data

You can't protect what you don't know. Start with understanding your data landscape, classification, and locations.

Focus on Quick Wins

Email and endpoint controls deliver immediate value. Build momentum with visible early successes.

Test Regularly

Purple team approach validates everything works as designed. Testing reveals gaps before attackers do.

Iterate Continuously

DLP is a journey, not a destination. Improve based on testing, incidents, and changing threats.

Do This Week

1. Identify your top 3 most critical data types that would cause the most damage if leaked
2. Map where they currently live across endpoints, network storage, and cloud services
3. Schedule a kickoff meeting for your DLP initiative with key stakeholders

Questions & Resources

Let's Address Your Specific Concerns

We're Here to Help

DLP doesn't have to be scary or overwhelming. Start small and build confidence through incremental wins. Focus on progress, not perfection. Every step forward improves your security posture.

> *"The best time to start DLP was yesterday. The second best time is today."*

Resources Available

- DLP implementation templates and checklists
- Purple team testing guides with scenarios
- Risk assessment worksheets
- Sample policies and incident playbooks
- Data classification frameworks
- Vendor evaluation criteria

Links/Resources

- https://ithandbook.ffiec.gov/it-booklets/information-security
- https://www.federalreserve.gov/boarddocs/srletters/2001/sr0115.htm
- https://www.endpointprotector.com/blog/federal-reserve-and-ffiec-requirements-for-safeguarding-customer-data/
- https://www.blackfog.com/what-is-data-loss-prevention/
- https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp
- https://frsecure.com/data-loss-prevention-best-practices/
- https://www.nightfall.ai/blog/data-loss-prevention-dlp-policies-guide-and-policy-template
- https://storware.eu/blog/what-are-the-best-practices-for-data-loss-prevention-dlp/