DYNAMICAL

COMPLEXITY UNDERSTOOD. SOLUTIONS SIMPLIFIED.

From “Oops” to “Never Again”: Your 90-Day DLP Action Plan

A Practical Guide to Data Loss Prevention for Modern Businesses

The 90-Day Roadmap Summary

Phase	Focus Area	Key Goal	Primary Metric
Days 1–30	**The Foundation**	Stop immediate leaks and secure the "crown jewels."	% Reduction in external sensitive shares.
Days 31–60	**Visibility**	Discover hidden data and audit third-party access.	% of sensitive data accurately classified.
Days 61–90	**Resilience**	Automate defenses and train for worst-case scenarios.	Average time to revoke access (MTTR).

Implementation Checklist

Phase 1: Stop the Bleeding (Month 1)

- [ ] **Identify the "Crown Jewels":** Define your top 5 most sensitive data classes.
- [ ] **Harden Cloud Defaults:** Disable "Anyone with the link" permissions globally in your SaaS apps.
- [ ] **Plug Email Leaks:** Deploy DLP rules to scan outgoing mail for SSNs, Credit Cards, and PII.
- [ ] **Enforce MFA:** Ensure 100% Multi-Factor Authentication for all sensitive applications.
- [ ] **Clean Up Offboarding:** Audit ex-employee access and revoke orphaned API tokens.

Phase 2: Close the Visibility Gaps (Month 2)

- [ ] **Audit Shadow SaaS:** Identify third-party apps with high-level "Read/Write" access.
- [ ] **Automate Classification:** Set up rules to auto-label sensitive docs (e.g., "Confidential").

- [ ] **Monitor Boundary Transfers:** Flag large data movements to personal cloud storage (Dropbox, etc.).
- [ ] **SaaS-to-SaaS Review:** Re-evaluate OAuth scopes for all integrated business tools.

Phase 3: Build Resilience (Month 3)

- [ ] **Test Your Defenses:** Conduct a simulated data exfiltration "fire drill."
- [ ] **Establish Shadow AI Policy:** Create guardrails for pasting data into public LLMs.
- [ ] **Automate Remediation:** Connect DLP alerts directly to your IT ticketing system (Jira/Slack).
- [ ] **Audit Simulation:** Run automated evidence collection to prep for your next compliance audit.

📁 Reference: The "Top 10" Data Types to Inventory First

Data Category	Examples to Search For
1. PII	Social Security Numbers, Home Addresses, Personal Emails.
2. PCI	Credit Card Numbers, Bank Account Details, CVVs.
3. PHI	Medical Records, Insurance IDs, Health Screenings.
4. Credentials	API Keys, Clear-text Passwords, SSH Keys, Secret Tokens.
5. Source Code	Proprietary algorithms, GitHub repositories, internal scripts.
6. Legal Docs	Signed contracts, NDAs, litigation hold documents.
7. Financials	Tax returns, payroll files, quarterly earnings drafts.
8. Strategic IP	Product roadmaps, M&A docs, patent applications.
9. Customer Lists	CRM exports, lead lists, partner contact info.
10. AI Inputs	Sensitive data used to train or prompt internal/external AI models.

"DLP is not a product; it is a culture of sensitivity. Start small, secure the defaults, and build momentum."