cyberhaven

DATA PROTECTION CHECKLIST:

DLP Blueprint

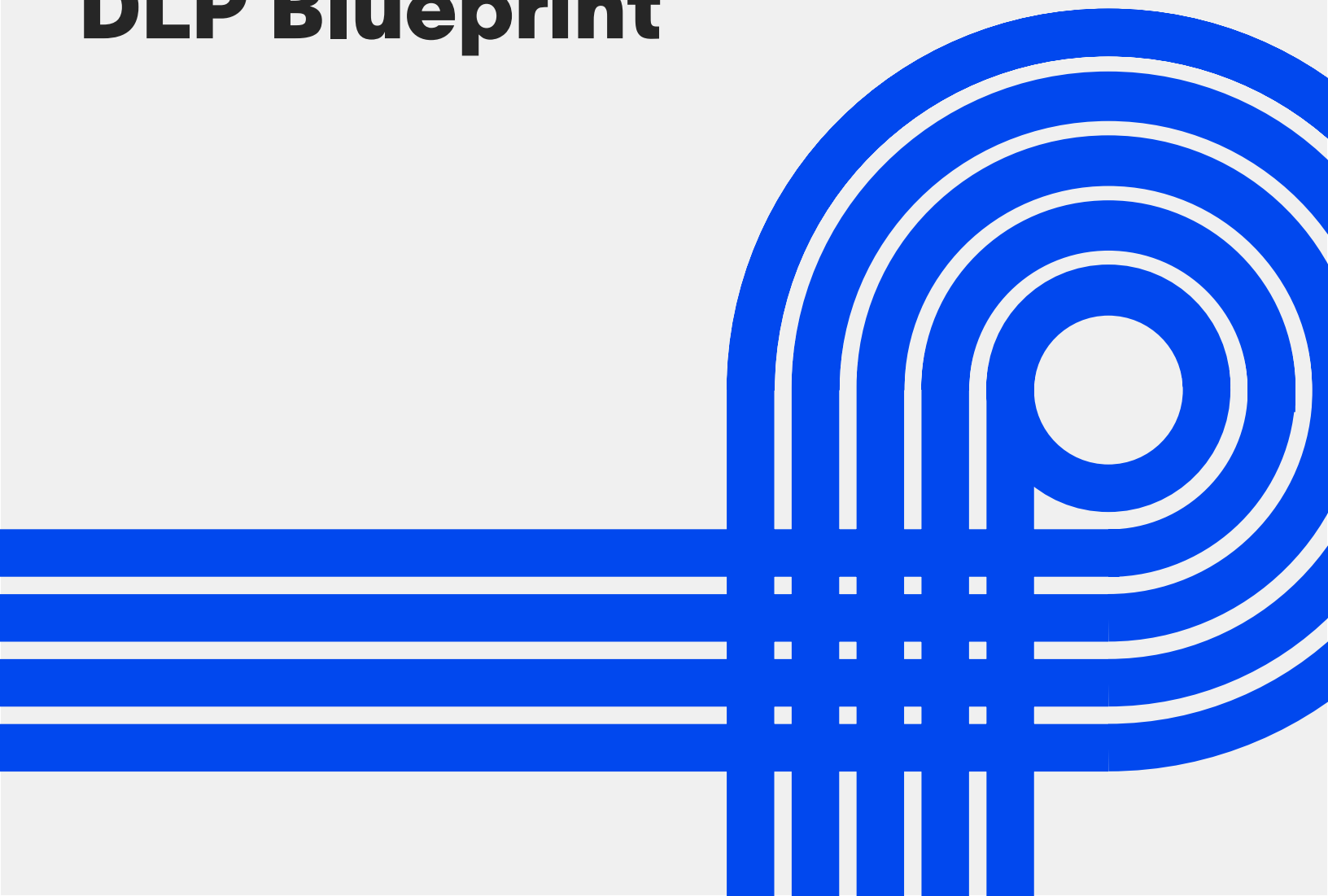


Table of Contents

Who we are 3

Executive Summary 4

Days 0–30: Clarity & Visibility 5

Days 31–60: Enforcement & Protocols 7

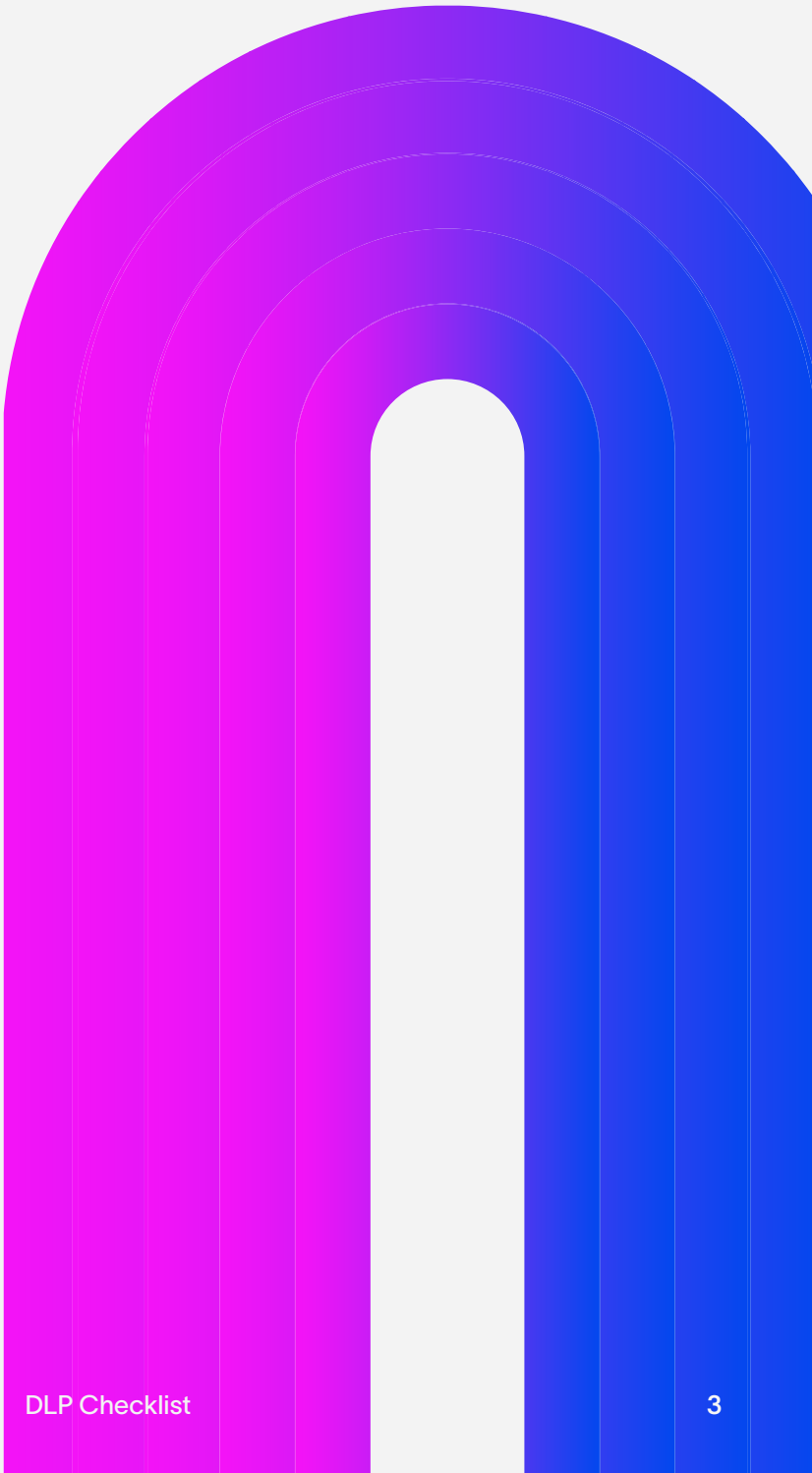
Days 61–90: Scale & Prove 9

90-Day Outcome Targets 10

Who We Are

Cyberhaven is reimagining data security. Until now, data security products have been limited to scanning data content or looking for specific user actions. Our AI-enabled data lineage technology analyzes billions of workflows to understand every piece of data within an organization, identify when it's at risk, and take action to protect it.

To learn more, visit
cyberhaven.com



Executive Summary

The blanket use of blocking turns out to be an outdated, ineffective approach to DLP and IRM. In the AI era, business leaders who can sleep well at night, knowing their data is truly secure, will be those who can implement upgraded protocols with speed and precision, enforce those protocols with full employee buy-in, and demonstrate continuous, on-going value.

Days 0–30: Clarity & Visibility

1. Establish cross-functional governing body

- [ ] Form core working group drawn from Security, IT, HR, Legal, Finance, Engineering, etc. and including data owners/stewards and an executive sponsor.
- [ ] Define communications channels and cadences (weekly standups, Slack/Teams channel, escalation paths, etc.).
- [ ] Publish program charter covering DLP/IRM objectives, scope, roles, decision rights, etc. CIS Control 3 governance; NIST SP 800-53 PM/RA families. (CSF Tools)

2. Understand your organization's objectives and risk appetite

- [ ] Document top business objectives and how data security supports them (revenue, customer trust, compliance, etc.).
- [ ] Define risk tolerance statements for data loss vs productivity impact (e.g., when to coach vs block).

3. Identify and classify sensitive data

- [ ] Identify **crown jewels** of sensitive data (PII, financials, contracts, code, trade secrets, etc.).
- [ ] Devise a classification scheme (Public/Internal/Confidential/Restricted) and map to the data. CIS Control 3. (CIS Security)

Days 0–30: Clarity & Visibility

4. Map data flows & risky vectors

- [ ] Use the Linea AI platform for ongoing **data lineage** capture across endpoints, SaaS, browsers, cloud drives, and AI tools. Document flows to consider include email, cloud sync, personal email, USB, print/screenshot, gen-AI prompts, repo pushes, and tickets/wikis.

- [ ] Capture **shadow AI** usage: require registration and review of all AI tools used.

- [ ] Secure **procurement/change policies** so vendors cannot silently enable AI features. NIST AI RMF (Govern). (NIST Publications)

5. Telemetry & integrations

- [ ] Integrate DLP with IdP/SSO, EDR, SIEM, M365/Google, ticketing, and HRIS (for joiner/mover/leaver). NIST SP 800-53 IR/AU/AC families. (NIST Publications)

- [ ] Establish evidence retention policies for audits and for handling of incidents. NIST SP 800-61. (NIST Computer Security Resource Center)

Days 31–60: Enforcement & Protocols

6. Begin graduated enforcement (coach→contain→block)

- [ ] Configure **just-in-time** (JIT) coaching for common risky actions (e.g., "Don't paste customer data into ChatGPT").
- [ ] Define precise conditions for containment actions (quarantine file, pause transfer, require justification).
- [ ] Establish blocking protocols for high-risk events (bulk PII exfil to personal cloud, code to public repository).

7. Publish a DLP/IRM runbook

- [ ] Detail triage workflows, severity tiers, and SLAs. NIST SP 800-61. (NIST Computer Security Resource Center)
- [ ] Outline steps for evidence handling and maintaining chain-of-custody. NIST SP 800-61. (NIST Computer Security Resource Center)
- [ ] Establish thresholds for HR/Legal escalation (for discrimination/harassment, IP theft, privacy breach, etc.).

8. Publish a policy starter set (targeted, high signal)

- [ ] PII → personal email / cloud drive (coach → block on repeat)
- [ ] Source code → public repositories; secrets leakage; tokens/keys detection
- [ ] Bulk CRM exports (USB, cloud); payroll/financials to untrusted domains
- [ ] Sensitive content in **AI prompts;** ban high-risk AI domains until reviewed. NIST AI RMF (Map/Measure). (NIST Publications)

Days 31–60: Enforcement & Protocols

9. Monitor leavers and movers

- [ ] Auto-elevate monitoring (two weeks before termination) of USB, email forwarding, cloud uploads, AI pastes, etc.
- [ ] Establish HR/Legal **self-service dashboards** for look-backs to minimize security bottlenecks.
- [ ] Document privacy and employee-notice policies to ensure fairness and transparency. CISA Insider Threat guidance. (CISA)

10. Control map & automation

- [ ] Build a **control crosswalk** linking policies to frameworks (CIS 3, NIST 800-53) and business objectives. CIS/NIST. (CIS Security)
- [ ] Give preference to controls that **automate** detection and enforcement and that provide strong visibility/remediation without administrative overload.

Days 61–90: Scale & Prove

11. Role-based hardening

- [ ] Confirm policies for Engineering (source code, secrets, build artifacts, etc.), Finance (payroll/GL), Sales (CRM exports), and executives (M&A).
- [ ] Require break-glass justification and auto-expire for exceptions.

12. AI governance in production

- [ ] Operationalize NIST **AI RMF:** Govern/Map/Measure/Manage; maintain a reviewed list of allowed AI tools with risk scores. NIST AI RMF. (NIST)
- [ ] Continue **JIT nudges** and carry out periodic AI safety awareness measures.

13. Tabletop exercises & red team (insider and AI-exfil)

- [ ] Monthly exercise covering email → cloud → AI prompt → external sharing.
- [ ] Based on lessons learned, update runbooks and policies. NIST SP 800-61; tabletop guidance. (NIST Computer Security Resource Center)

14. Compliance & executive scorecard

- [ ] Auto-generate audit packs (ISO 27001/SOC 2/PCI/privacy) and map to controls.
- [ ] Deliver an **Executive Scorecard** that assesses risk reduction metrics, including # and type of incidents, % coached vs blocked, false-positive rate, hours saved by automation, and AI-risk trend.

15. Communicate program value

- [ ] Communicate updates via regular stakeholder touchpoints and broader avenues (newsletters, Q&A, etc.).
- [ ] Tell the **business story** associated with your organization's data security (revenue retention, increased customer trust, sales acceleration via faster security reviews).

90-Day Outcome Targets

- **Broad visibility** established across all endpoints, SaaS, browsers, and AI tools
- **6–8 high-confidence policies** with <2% false positives
- **Automated offboarding monitoring** with HR/Legal self-service look-backs
- **Executive scorecard delivered,** demonstrating coverage, incidents, and ROI
- **AI-associated risks governed** under an approved tool list with JIT coaching and measurable reductions. NIST AI RMF. (NIST)

cyberhaven