BROADCOM®

EXECUTIVE SUMMARY

Building a High-Impact, Future-Ready Data Loss Prevention Program

Key Topics

The Business Case for DLP	Key Principles for a Successful DLP Program	Core Steps to Standing Up a DLP Program	Overcoming Common Objections
Embedding DLP into the Organization	Communicating with End Users	Continuous Improvement Through Governance	Bottom Line for Executives

The Business Case for DLP

A well-structured DLP program empowers organizations to detect and prevent data breaches by understanding where sensitive data lives, how it flows, and how it's used. The goal is not simply compliance—it's enabling secure business growth.

Key Principles for a Successful DLP Program

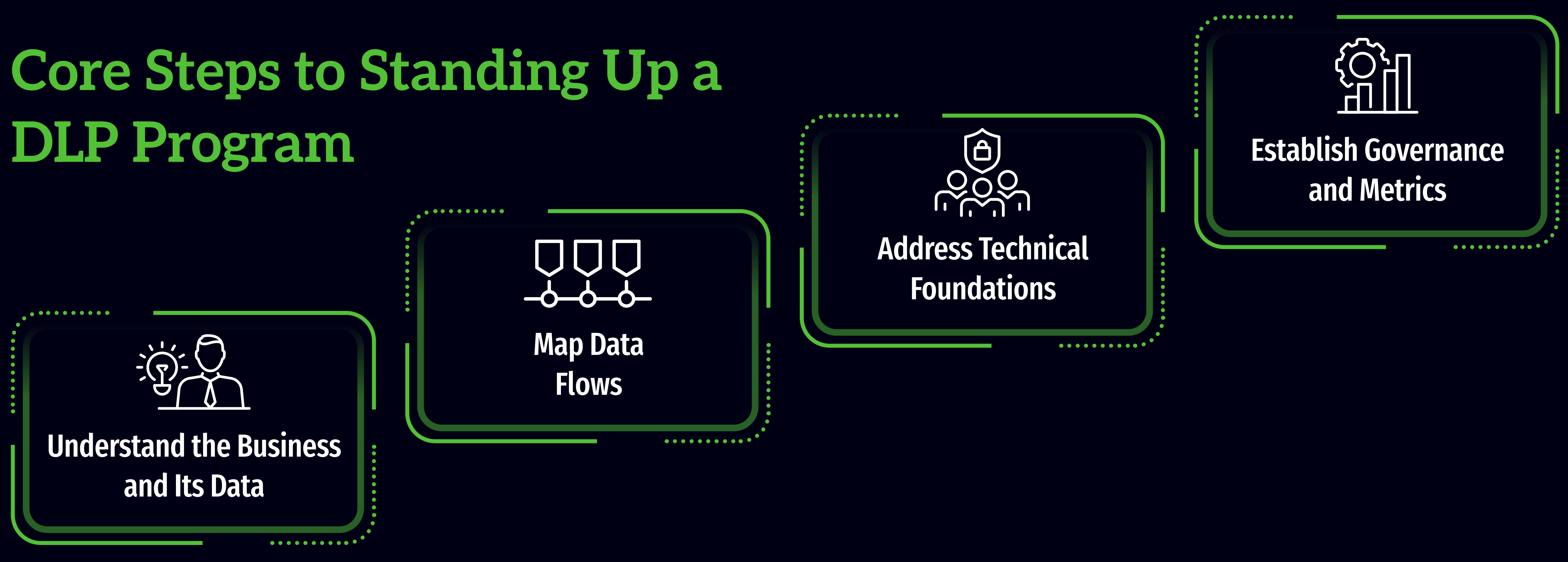
Identify and Protect High-Value Data for Quick Wins.

Build Incrementally.

Executive Buy-In Is Non-negotiable.

Tailor the Program to Your Business.

Core Steps to Standing Up a DLP Program



Understand the Business and Its Data

Map Data Flows

Address Technical Foundations

Establish Governance and Metrics

Overcoming Common Objections

Organizations often face hesitation due to DLP's perceived complexity or cost:

No Clear Owner
Place the program under compliance, security, or risk functions most aligned with the organization's data priorities.

Innovation vs. Protection
Position DLP as an enabler of innovation by securing proprietary data and ensuring safe AI and large language model (LLM) usage.

Already Using Cloud/SaaS
Cloud services do not automatically protect sensitive data. DLP must account for data at rest, in use, and in transit across third-party platforms.

Too Expensive
Compare the cost of DLP with the potential loss from data breaches, including fines, lawsuits, and reputational harm.

Too Complex
Demonstrate how phased implementation and targeted use cases mitigate complexity while delivering fast results.

Embedding DLP into the Organization

To mature the program, DLP must become part of the organization's DNA:

People
Invest in skilled professionals or managed security service providers (MSSPs).

Process
Define clear policies, alert handling procedures, and escalation paths.

Technology
Select scalable tools that can integrate across environments.

Communicating with End Users

End-user buy-in is vital. Without it, users may circumvent controls, creating risk:

Explain the rationale ("the why") behind DLP initiatives.

Customize communications by audience—technical vs. business users.

Implement feedback loops to identify and fix friction points.

Establish a steering committee to drive cross-functional alignment.

Continuous Improvement Through Governance

An effective DLP program isn't static. Governance ensures ongoing improvement:

- Use tailored metrics to measure outcomes relevant to security, compliance, legal, and risk teams.
- Report on alert volume, response times, coverage, and incident impact.
- Align metrics to key risk indicators (KRIs) that influence board-level risk reporting.

Bottom Line for Executives

DLP is not merely a technical safeguard—it's a business enabler. By following a pragmatic, iterative approach, organizations can build DLP programs that reduce risk, support regulatory compliance, and protect their most valuable asset: data.

BROADCOM®

SANS | Research Program