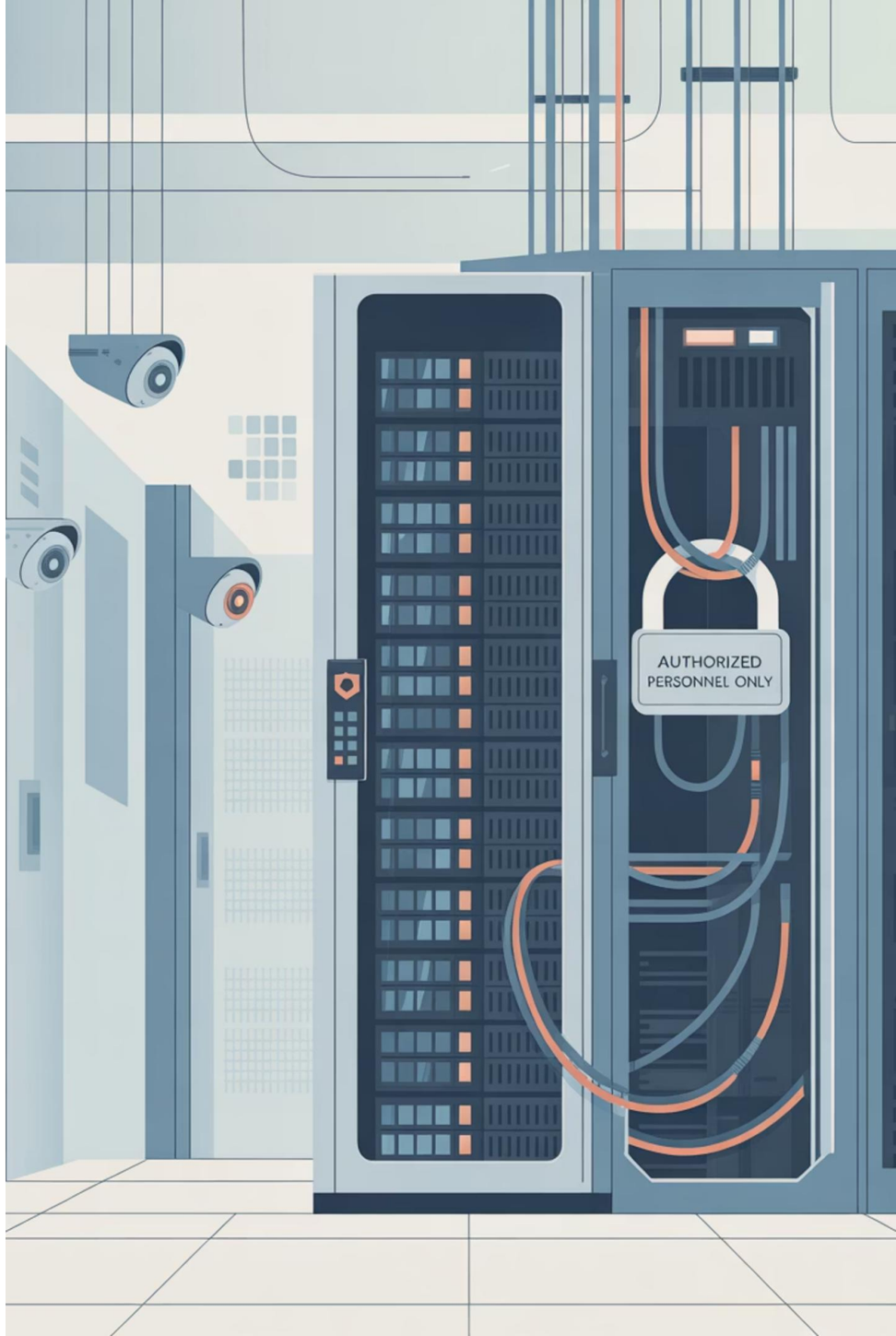
Data Integration and Governance

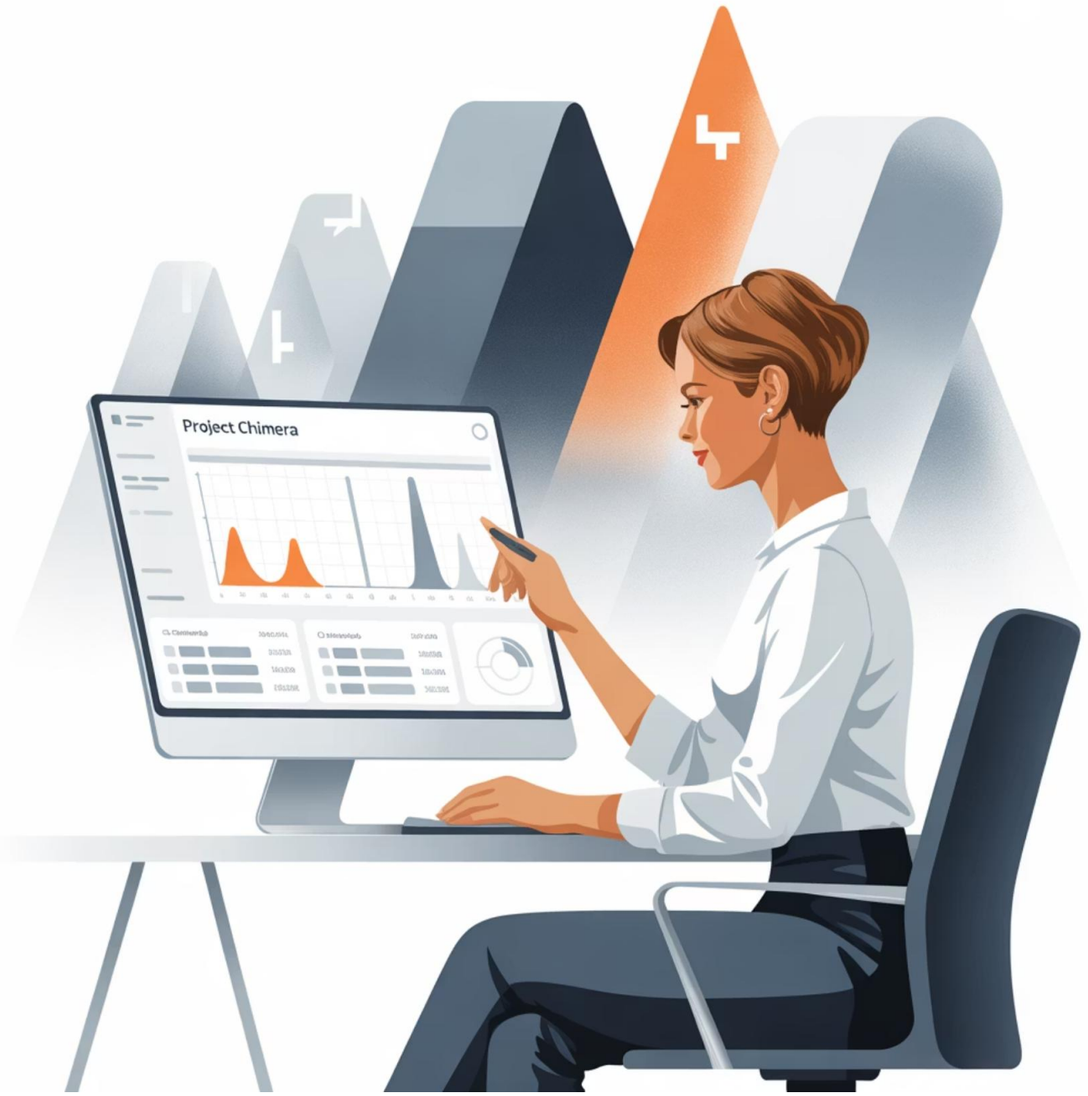
Mastering Power Platform's Connection Management and Security Framework



Module Overview: Building Secure Data Foundations

This module covers the critical foundations of data integration and governance within Microsoft Power Platform. You'll learn to configure secure connections, implement protective policies, and establish governance frameworks that scale across your organization.

By mastering these concepts, you'll be equipped to manage complex data landscapes while maintaining security, compliance, and operational efficiency. These skills are essential for any administrator responsible for enterprise Power Platform deployments.



What We'll Cover Today

01

Data Connectors Deep Dive

Explore the extensive library of available connectors and understand their capabilities, limitations, and security considerations.

02

Gateway Configuration

Master the setup and management of on-premises data gateways for secure hybrid connectivity.

03

Data Loss Prevention

Implement and configure DLP policies to protect sensitive information across Power Platform applications.

04

Connection Management

Learn best practices for managing connections, sharing permissions, and maintaining security.

05

Governance Strategies

Develop comprehensive governance frameworks using Power Platform Admin Center tools and capabilities.

Understanding Data Connectors

Power Platform offers over 400 pre-built connectors that enable seamless integration with various data sources and services. These connectors fall into different categories based on their functionality and data access patterns.

Standard Connectors

Included with most licenses, these provide access to popular cloud services like Office 365, SharePoint, and common databases.

Premium Connectors

Require premium licenses and offer advanced functionality for enterprise systems like SAP, Oracle, and specialized business applications.

Custom Connectors

Built by developers to connect to proprietary systems or services not covered by standard offerings.

Gateway Architecture

The Bridge Between Cloud and On-Premises

On-Premises Data Gateway Configuration

The on-premises data gateway acts as a secure bridge, enabling Power Platform services to access data that resides in your local network. Proper configuration is crucial for both security and performance.

Installation Planning

Choose appropriate hardware, network positioning, and service account configuration for optimal performance.

Configuration Setup

Register the gateway, configure data sources, and establish secure authentication methods.

Security Hardening

Implement encryption, access controls, and monitoring to ensure secure data transmission.

Gateway Best Practices and Architecture

1

High Availability Setup

Deploy gateway clusters with multiple nodes to ensure business continuity. Configure load balancing and failover mechanisms to handle hardware failures or maintenance windows.

- Minimum of two gateway nodes per cluster
- Regular health monitoring and alerting
- Automated failover configuration

2

Network Optimization

Position gateways strategically within your network topology to minimize latency and maximize throughput. Consider bandwidth requirements and network segmentation.

- Direct connection to data sources when possible
- Sufficient bandwidth allocation
- Network security group configurations

3

Monitoring and Maintenance

Implement comprehensive monitoring solutions to track gateway performance, identify bottlenecks, and maintain optimal operation through regular updates and maintenance.

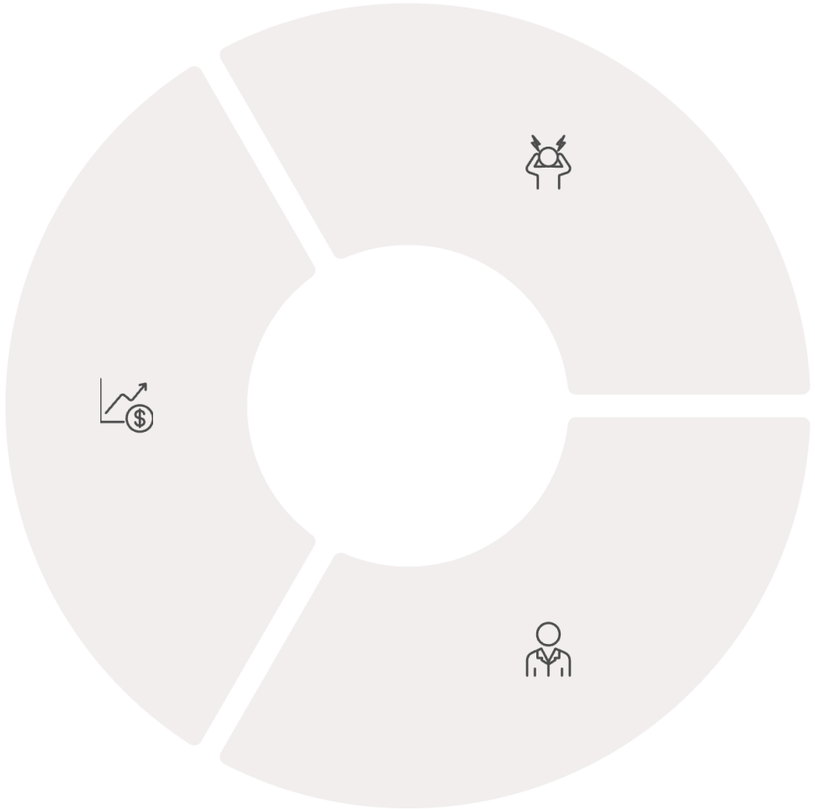
- Performance counter monitoring
- Regular software updates
- Capacity planning and scaling

Data Loss Prevention (DLP) Policies

DLP policies in Power Platform provide essential protection against unauthorized data sharing and help maintain compliance with organizational security requirements. These policies control how data flows between different connectors and services.

Business Data Group

Contains connectors that house company data requiring protection, such as SharePoint, SQL Server, and Dynamics 365.



Blocked Connectors

Connectors that are completely prohibited from use within the organization for security or compliance reasons.

Non-Business Data

Personal productivity connectors like Twitter, Facebook, or personal OneDrive accounts that shouldn't mix with business data.

Implementing Effective DLP Strategies

1 Policy Design

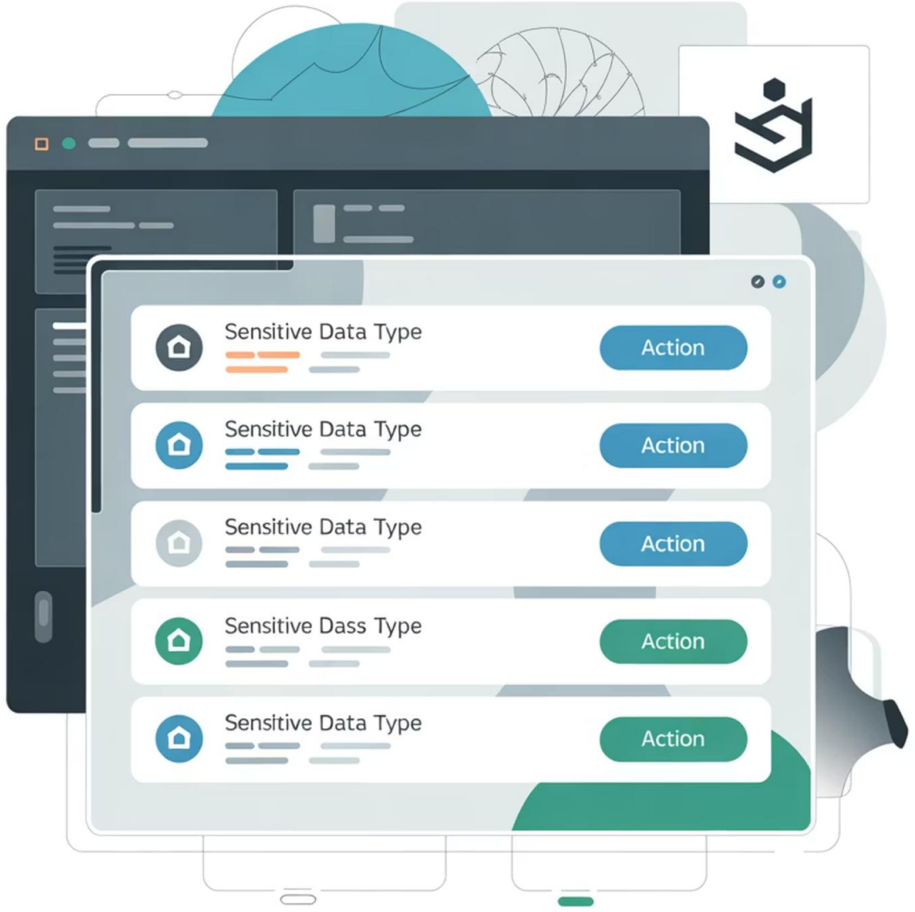
Start with a clear understanding of your data classification requirements and regulatory compliance needs. Map connectors to appropriate data groups based on sensitivity levels.

2 Phased Rollout

Implement DLP policies gradually, beginning with high-risk scenarios and expanding coverage. Use audit mode initially to understand impact before enforcement.

3 Exception Management

Establish processes for handling legitimate business requests that require exceptions to standard DLP policies. Document and regularly review approved exceptions.



Pro Tip: Always test DLP policies in a development environment before applying them to

Connection Management

Securing and Optimizing Data Access

Managing Connections and Connectors

Effective connection management ensures secure, reliable access to data sources while maintaining proper governance and user permissions. This involves both technical configuration and organizational processes.

Connection Creation

Establish secure connections using appropriate authentication methods. Consider service accounts for shared connections and individual accounts for personal use cases.

Permission Management

Control who can create, use, and modify connections. Implement least-privilege access principles and regular permission audits.

Monitoring and Maintenance

Track connection usage, identify unused connections, and maintain credential freshness to ensure optimal security and performance.

Connection Security Best Practices

Authentication Strategy

Implement OAuth 2.0 where available, use service principals for automated processes, and avoid embedded credentials in applications. Regular rotation of service account passwords is essential.

- Multi-factor authentication enforcement
- Service principal management
- Regular credential audits

Access Control

Establish clear policies for connection sharing and permissions. Use Azure AD groups for scalable permission management and implement approval workflows for sensitive connections.

- Role-based access controls
- Connection sharing policies
- Approval workflow implementation

Power Platform Admin Center: Your Governance Hub

The Power Platform Admin Center provides comprehensive tools for implementing and maintaining governance across your organization. It serves as the central command center for all administrative activities.

Environment Management

Create, configure, and manage environments with appropriate security boundaries. Control data residency and implement environment-specific policies that align with business requirements.

Policy Enforcement

Deploy and monitor DLP policies, tenant settings, and compliance requirements. Track policy violations and generate reports for audit purposes.

Usage Analytics

Monitor platform adoption, identify usage patterns, and optimize resource allocation. Generate insights for capacity planning and license optimization.

Resource Governance

Manage applications, flows, and chatbots across the organization. Implement approval processes and lifecycle management for business-critical resources.

Comprehensive Governance Strategy Framework

A successful Power Platform governance strategy requires careful planning, clear policies, and ongoing management. This framework provides a structured approach to implementing governance at scale.

Assessment and Planning

Evaluate current state, identify requirements, and define governance objectives. Engage stakeholders across business and IT to ensure alignment with organizational goals.

Policy Development

Create comprehensive policies covering data classification, security standards, and operational procedures. Document approval workflows and exception processes.

Implementation

Deploy governance controls, configure monitoring systems, and establish support processes. Train administrators and end users on new policies and procedures.

Monitoring and Optimization

Continuously monitor compliance, gather feedback, and refine governance approaches. Regular reviews ensure policies remain effective and aligned with business needs.

Key Takeaways and Next Steps

Master the Fundamentals

Understanding data connectors, gateway architecture, and DLP policies forms the foundation of effective Power Platform governance. These elements work together to create a secure, scalable platform.

Implement Proactively

Don't wait for security incidents to drive governance decisions. Establish policies and monitoring early in your Power Platform journey to prevent issues and ensure smooth scaling.

Continuous Improvement

Governance is not a one-time activity. Regularly review policies, monitor compliance, and adapt to changing business requirements and security landscapes.