# Forcepoint DLP Architecture Guide

## Core Components
- **Security Manager (FSM)**: Central console
- **DLP Server**: Policy engine
- **Endpoint DLP Agent**: Client-side protection
- **Optional Protectors**: Email, Web, Discovery
- **Fingerprinting/Indexers**
- **Management Infrastructure**

## Supported Endpoints

Endpoint Type	Platform	Protection Scope
Windows Workstations	Win 10/11	Files, print, clipboard, upload
macOS Devices	macOS 11+	Files, removable media
Linux (limited)	RHEL/CentOS/Ubuntu	Audit only via network taps
Email Servers	SMTP	Content inspection
Web Browsers	Chrome/Edge/FF	File uploads, cloud apps
Cloud Services	M365, GDrive	Via CASB (Forcepoint ONE)
Removable Devices	USB, CD/DVD	Audit, block, allow
Printers	Mapped printers	Document print control
Clipboard	All platforms	Copy/paste protection

## Infrastructure Setup

### 1. Prepare Servers
- Windows Server 2019+
- SQL Server 2019+
- 2+ vCPU, 8GB RAM, 100GB storage
- SSL Certificates

### 2. Install FSM
- Install .NET, IIS, SQL client
- Run FSM installer
- Configure DB and HTTPS
- Setup admin login

### 3. Install DLP Server
- Run installer on separate or same VM
- Connect to FSM
- Enable 9443/8443 ports

### 4. Deploy Agents
- Create package in FSM
- Deploy via SCCM, Intune, or GPO
- Manual installer (EXE/MSI)

### 5. Optional Protectors
- **Email**: Configure SMTP relay
- **Web**: Integrate with Web Security
- **Discovery**: Target file shares, schedule scans

### 6. Configure Policies
- FSM > Policies > Templates or Custom
- Fingerprint and content rules
- Alert level + remediation

### 7. Rollout
- Pilot with test OUs
- Tune and expand
- Monitor logs

## Ports

Component	Port	Protocol
FSM Console	9443	HTTPS
Endpoint Comm	8443	HTTPS
SMTP Protectors	25	SMTP
Discovery Server	135, 445	RPC/SMB
LDAP/AD	389, 636	LDAP/LDAPS

## Best Practices
- Use TLS/SSL
- Least-privilege AD access
- Use behavior + fingerprint rules
- Export logs to SIEM
- Bundle with CASB (Forcepoint ONE)

## Integrations
- SIEM: Splunk, QRadar, ArcSight
- CASB: Forcepoint ONE
- UEBA: Insider threat analytics
- Proxy: Forcepoint Web Gateway

## GitHub Bash Commands for Markdown Upload

```bash
git clone https://github.com/YOUR_USERNAME/YOUR_REPO.git
cd YOUR_REPO
cp /path/to/forcepoint_dlp_architecture.md .
git add forcepoint_dlp_architecture.md
git commit -m "Add Forcepoint DLP Architecture Guide"
git push origin main
```

## push_markdown.sh Script

```bash
#!/bin/bash
MD_FILE=$1
REPO_URL=$2
BRANCH=${3:-main}
REPO_NAME=$(basename -s .git $REPO_URL)
if [ ! -d "$REPO_NAME" ]; then
```

```
  git clone $REPO_URL
fi
cd $REPO_NAME || exit 1
cp "$MD_FILE" .
git add $(basename "$MD_FILE")
git commit -m "Add $(basename "$MD_FILE")"
git push origin $BRANCH
```