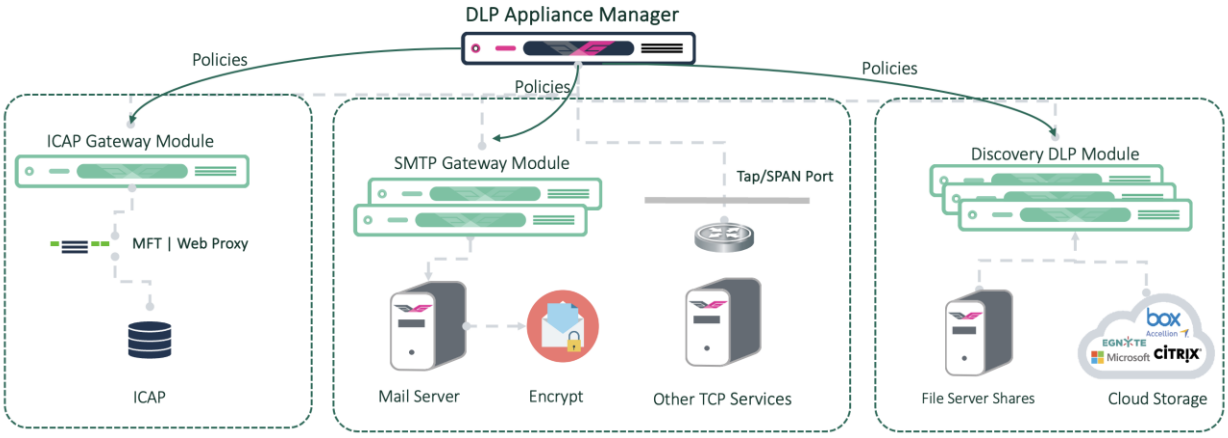
Fortra DLP Secure ICAP Gateway

Fortra's DLP Secure ICAP Gateway is a purpose-built, network-based Data Loss Prevention (DLP) solution engineered to protect sensitive data **in motion**, **at rest**, and **in use** across enterprise environments. The Fortra DLP Secure ICAP Gateway is one of the three modules of the Fortra (DG) DLP appliance solution.

The DLP appliance solution delivers **deep content inspection** through full packet inspection, **advanced policy enforcement**, fingerprinting and **exact data matching** to prevent data leakage and ensure compliance. It consists of three modules, that can be deployed and managed separately to meet diverse operational needs:

- **ICAP Gateway module** – Integrates with Managed File Transfer (MFT) systems and web proxies to inspect and control file-based data flows.
- **SMTP Gateway module** – Intercepts email traffic via MTA routing for real-time inspection and policy-based enforcement on outbound communications.
- **Discovery DLP module** – Scans data at rest across on-premises and cloud storage environments to identify and secure sensitive information.

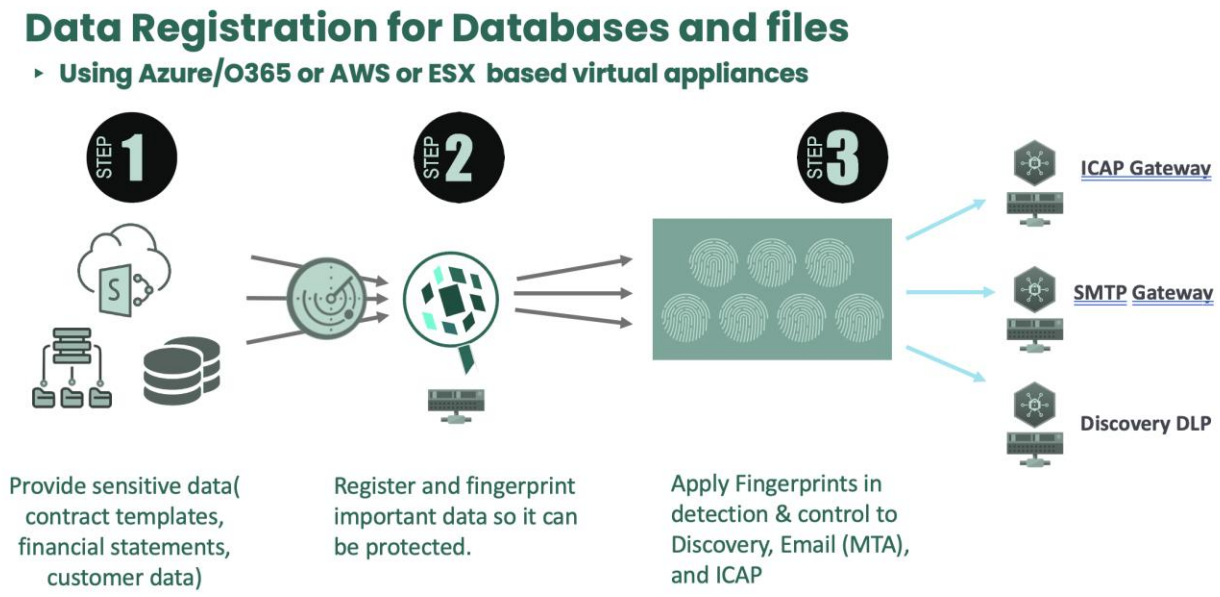
These modules can also be purchased separately.



Appliance DLP modules

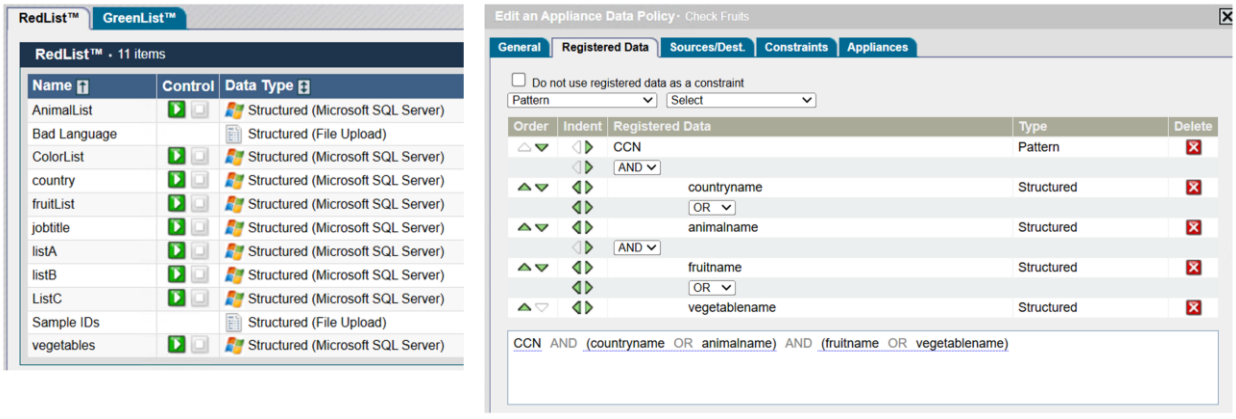
Exact Data Match

Sensitive data samples—such as confidential intellectual property documents, contract templates, financial statements, and customer records—are placed in a secure share and scanned using the Fortra (DG) DLP appliance to generate digital fingerprints. These fingerprints are then applied to data-at-rest discovery and remediation rules, as well as to detection and control rules for data-in-motion, including ICAP-based workflows, enabling accurate identification and protection of critical information across the environment.



Data registration and fingerprinting use cases

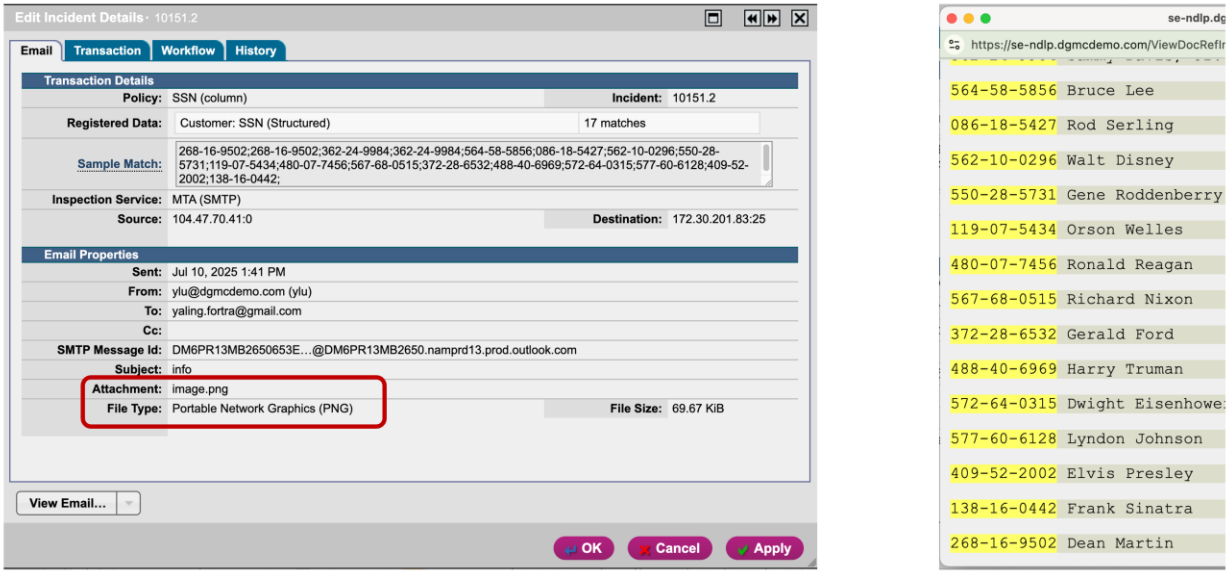
Those fingerprints can be used to create a complex detection rule.



An example of complex detection rule

Optical Character Recognition (OCR)

In addition to fingerprinting, Optical Character Recognition (OCR) can also be used to identify sensitive information embedded within images, scanned documents, and PDFs. By extracting and analyzing text from visual content, OCR enhances data discovery and protection capabilities, ensuring that non-textual or image-based data containing confidential information is accurately detected and governed across both data-at-rest and data-in-motion scenarios.



OCR detection results

Key features:

Feature	Description
ICAP Support	Enables integration with Managed File Transfer (MFT) platforms (e.g., GoAnywhere) and web proxies to secure file-based traffic.
Policy Engine	Supports flexible rule logic, including keywords, regular expressions, file fingerprinting, and data classification.
MPIP Integration	Integrates with Microsoft Purview Information Protection (MPIP) to detect and enforce policies on MIP-classified documents.
File and DB Cell Fingerprinting (structured data)	Leverages Exact Data Matching (EDM) to detect sensitive information by comparing content against pre-registered reference datasets.
Deep Content Fingerprinting (unstructured)	Proprietary form of Index Data Matching enables the registration of unstructured data from virtually any file type and in any language. Although the fingerprint is only a fraction of the original source's size, it allows for the detection of registered content even if it appears as derivatives or small snippets of the original document.

Optical Character Recognition (OCR)	OCR is a powerful technology that scans and converts text within images into readable, actionable data. This extends data protection to image-based content, allowing organizations to detect and secure sensitive information that might otherwise go unnoticed.
Data-at-Rest Scanning	Scans data stored in file shares, SharePoint, databases, and supported cloud storage platforms such as Microsoft OneDrive, Google Drive, Box, and Amazon S3 to identify and protect sensitive information.
Full Network Packet Inspection	Performs deep packet inspection across protocols such as SMTP, HTTP, and FTP.
Multi-Platform Support	Deployable on VMware, Microsoft Azure, or Amazon Web Services (AWS).
Part of the Fortra DLP Portfolio	A core component of Fortra's broader data protection suite, designed for seamless integration with other Fortra security solutions.

Centralized ICAP Management and Enterprise Integration

The Fortra DLP Secure ICAP Gateway can be deployed in a manager-inspector architecture to centralize policy management, enabling unified policies across multiple ICAP inspectors. It seamlessly integrates with existing enterprise infrastructure—such as SIEM systems and domain controllers—to streamline policy enforcement, event correlation, and user identity mapping. This integration provides organizations with unified visibility, simplified administration, and more effective coordination of data protection efforts across all inspection points.

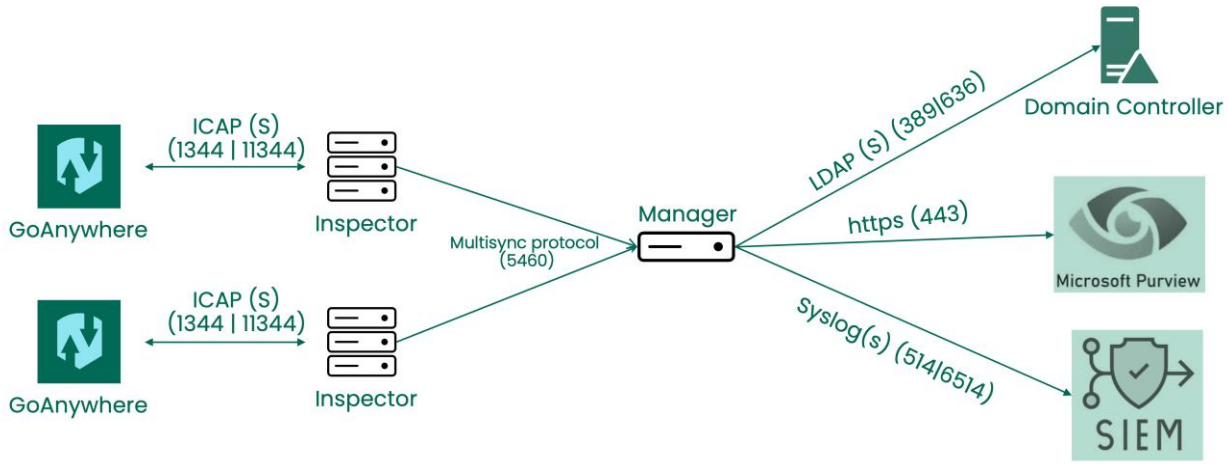


Diagram of ports requirements for enterprise integration

About Fortra Data Protection

Fortra Data Protection is a unified solution designed to give your organization comprehensive visibility and control over critical data—whether on-premises, across endpoints, in transit, or throughout cloud environments.

It empowers organizations to discover, classify, monitor, and protect sensitive information wherever it lives, with intelligent automation and actionable insights that reduce risk and simplify compliance.

Analytics & Reporting – Deep visibility into DLP actions for faster threat response.
Network Appliance – Secure data in transit with precise monitoring and control.
Management Console – Simplify security with centralized policy management and actionable insights.
Endpoint Agent – Monitor, Audit and Mitigate data threats across Windows, OSX, Linux workstations, servers and VDI images.
Secure Service Edge – Extend data protection to cloud and hybrid environments with secure access enforcement.
Fortra DSPM (Data Security Posture Management) – Continuously discover, classify, and assess sensitive data across SaaS, IaaS, and multi-cloud environments to reduce data exposure risk.
Fortra Data Classification – Empower users and automate the labeling of sensitive files and emails to enhance data awareness and enforce policy consistently across endpoints and cloud services.
Fortra Secure Collaboration – Apply encryption, dynamic access controls, and usage tracking to files—wherever they travel—ensuring persistent data protection even outside the corporate perimeter.