PRODUCT DATASHEET

miniOrange Data Loss Prevention

Protect Your Business Data at Every Turn

miniOrange Data Loss Prevention (DLP) is a security solution designed to detect and prevent your business data from being misused, lost, or accessed by unauthorized users. It gives businesses total visibility and control over how their data is stored and shared across devices, emails, cloud apps, and networks, including enforcing secure usage of policies.

DLP solution keeps you compliant with GDPR, HIPAA, ISO, PCI DSS, and RBI regulations, and works across almost all systems and platforms. Designed for businesses of every size, miniOrange DLP is the perfect solution for enterprise-grade data protection and management.

6K+
Integrations

25K+
Customers

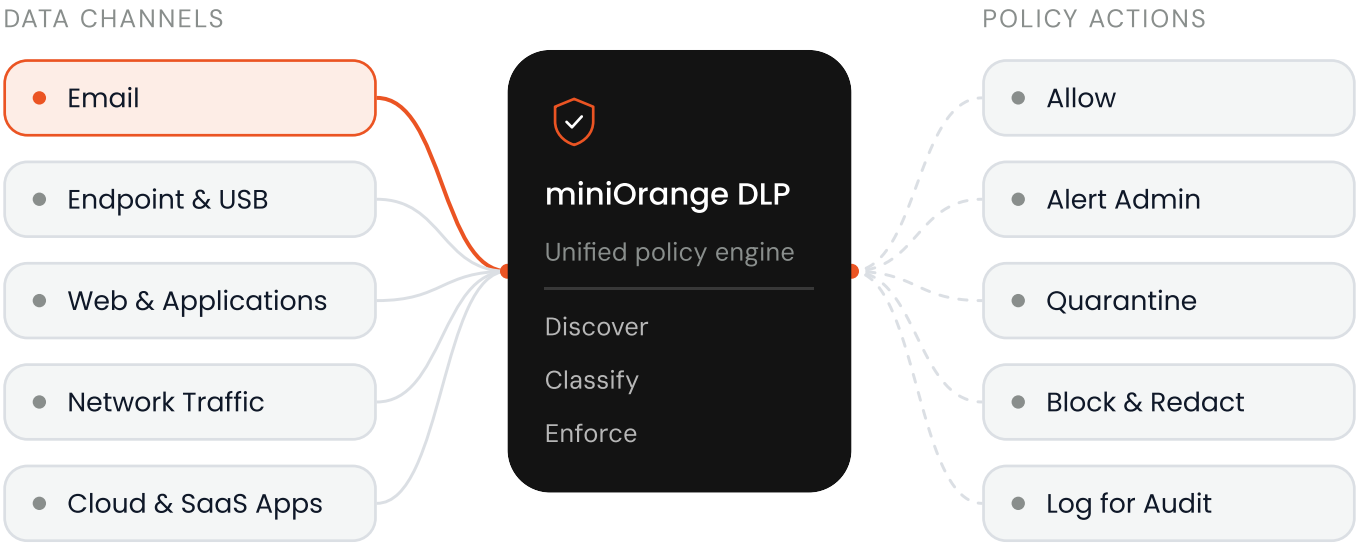
24/7
Active Support

BUILT FOR EVERY BUSINESS

- Trusted Across Industries
- Cloud & On-Prem Ready
- Real-Time Detection & Alerts
- Fast Deployment
- Full Data Lifecycle Protection
- 24/7 Technical Assistance

One control plane across every data channel

Every channel your data can leave through is inspected against the same policy set — a rule written once is enforced everywhere, and every action is logged for audit.



THE DATA PROTECTION LIFECYCLE

01

Discover

Find and label sensitive data stored across endpoint devices.

02

Classify

Apply the right policy based on data sensitivity levels.

03

Monitor

Track device, email, app and network activity in real time.

04

Enforce

Block, quarantine, redact or allow — automatically.

05

Report

Audit trails and alerts for compliance reviews.

Endpoint & Removable Media

Prevent Data Loss via Removable Devices

PREVENTS

Business data walking out on a USB stick, external disk or print job — unseen and unlogged.

- Control and monitor how users interact with removable storage like USB drives, external HDDs, printers and network devices.
- Use blocklisting to find and label devices that should be disabled.
- Add temporary relaxation of defined policies across multiple data channels, auto-revoked after a set period.
- Monitor, audit and log every data transfer from removable storage for compliance and end-to-end visibility.

Device Management

PREVENTS

A lost or stolen laptop becoming an open door into corporate data.

- Remote Lock — instantly lock devices to stop unauthorized access and protect business data.
- Remote Wipe — erase work data from lost or stolen devices to protect confidential information.
- Password Policy Enforcement — push strong password rules across the fleet.
- Login Monitoring — track login activity to detect suspicious behavior before a breach.
- Registry Management — centralize registry configuration for consistent system settings.

Device Remote Access

PREVENTS

Downtime and unpatched endpoints caused by needing physical access to a machine.

- Remotely access user devices to diagnose and fix technical issues quickly, reducing downtime.
- Configure, update and maintain systems or software without physical access to devices or servers.
- Manage accounts, install software and enforce security policies to maintain compliance.
- Continuously monitor performance, detect breaches and run remote diagnostics.

Email, Web & Applications



Email Security

PREVENTS

Confidential data leaving the organization in an email body or attachment before anyone reviews it.

- Define email DLP policies to classify, whitelist or quarantine emails based on attachments, content and recipient domains.
- Scan outbound email (Gmail, Outlook, Slack, Mithi) for confidential business data and quarantine suspicious messages before delivery.
- Classify device actions, alert admins, and block access or redact data to prevent security risks.
- Protect data transmitted through corporate and cloud-based email services such as Gmail or Outlook.



Application & Network Control

PREVENTS

Risky sites and unapproved apps becoming an unmonitored exit route for company data.

- Block risky websites and categories while allowing safe ones, using content filtering to minimize data leaks.
- The DLP agent monitors all HTTP traffic and enforces policies that block sites by default except those explicitly allowed.
- Set time-based policies for site or app access, letting users request entry while admins approve or deny permissions.



File Upload Restrictions

PREVENTS

Employees uploading documents, archives or executables to platforms IT never approved.

- Prevent uploads of unauthorized files — documents (PDF, DOCX, XLSX), archives (ZIP, RAR) and executables (EXE, MSI) — to unapproved platforms.
- Stay compliant by controlling what content employees can share, supporting data governance and regulatory standards.
- Scan files against set rules to detect policy violations and keep sensitive information protected.

Monitoring, Governance & Device Control

Reporting & Monitoring

PREVENTS

Policy breaches going unnoticed because no one has a single view of device, email and app activity.

- Detailed insight into device, peripheral, email and app activity across the organization.
- Track unusual network or peripheral behavior to spot early signs of threats.
- Monitor user activity for compliance, with audit trails for regulatory checks.
- Analyze device and network usage to find inefficiencies and improve allocation.
- Instant alerts on unusual activity for faster detection and resolution.

Employee Monitoring Policies

PREVENTS

Cameras, screenshots and unattended sessions being used to move data off the record.

- Improve accountability and strengthen organizational oversight.
- Impose camera and screenshot policies to prevent misuse of business information.
- Monitor AD user sessions for real-time activity tracking.
- Capture anomalies or unusual session behavior for security auditing.

Roles & Permissions

PREVENTS

Over-privileged admins reaching dashboards and reports they should never see.

- Role-Based Access — define roles with permissions controlling dashboard and report access.
- Simplified User Management — assign privileges to roles, not individuals.
- Custom Roles — tailor what each role can edit, delete or access.

Geo-Location & Tracking

PREVENTS

A missing device staying missing, with no way to locate or contain it.

- Locate, track and manage devices from the admin console.
- View real-time device location to aid recovery or compliance.
- Combine with remote lock and wipe for improved physical security.

Latest additions to miniOrange DLP

New capabilities shipped since the previous release, framed the same way as the rest of this datasheet: what it does, what it prevents, and what changes for your team.

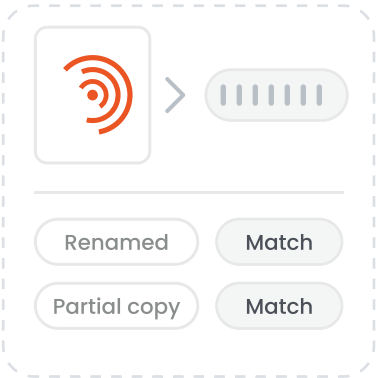
Google Drive Data Discovery and Classification

- Automatically scan Google Drive (including Shared Drives) to locate and categorize sensitive data such as PII, financial records, or confidential business content that is stored across files, folders, and attachments.
- Analyzes actual file content and metadata, not just file names, and aligns the results with enterprise policies and regulatory requirements like GDPR, PCI DSS, HIPAA, etc.
- Google Workspace itself supports AI-powered classification labels that appear directly in Drive views, allowing users to instantly see a file's sensitivity level.



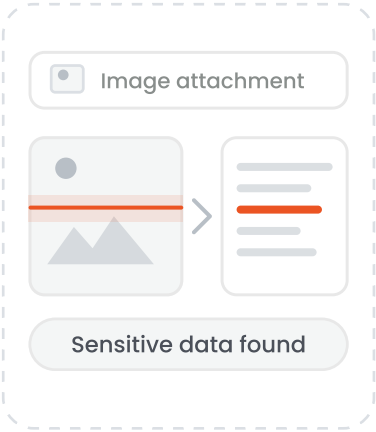
File Fingerprinting

- File fingerprinting (also called document or data fingerprinting) creates a unique digital "signature" of a document or set of documents.
- The DLP solution then uses this fingerprint to detect copies, partial copies, or derivatives of that document moving across the network, even if the file is renamed or reformatted.
- Set a confidence score (e.g., 70%) so the system flags files that match 70% or more of the fingerprinted content, giving you control over sensitivity.



Advanced Email Content Inspection

- This is an OCR (Optical Character Recognition) and occurrence-based process. The occurrence count is based on regex matches.
- OCR handling means the system can extract and inspect text embedded inside images attached to emails, detecting sensitive data even in scanned documents or screenshots.
- Get email redaction to automatically redact sensitive messages before sending.

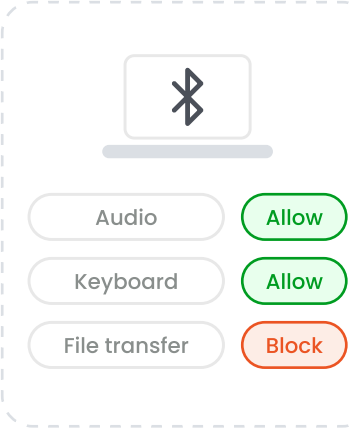


New features in DLP

Continued: new capabilities added to miniOrange DLP in this release.

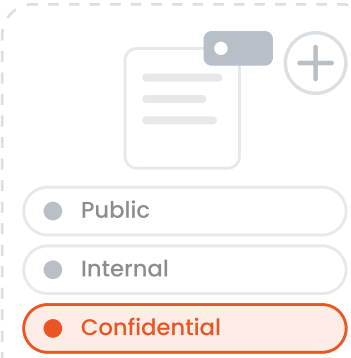
Bluetooth Device Control

- This is an endpoint security feature that governs which Bluetooth devices (headsets, keyboards, file-transfer devices) can connect to corporate endpoints.
- Admins can create policies to block Bluetooth peripherals based on device type or pairing status, preventing data exfiltration via unauthorized Bluetooth file transfers.
- This is commonly managed through endpoint DLP or UEM (Unified Endpoint Management) agents.



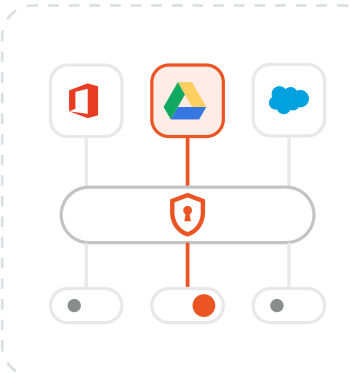
Custom Data Classification and Tagging

- This allows organizations to define their own data sensitivity labels beyond pre-built templates (like “Confidential,” “Internal,” “Public”).
- Tags can be applied manually by users or automatically by policy rules, and they then drive downstream enforcement.
- Tags determine what DLP rules, sharing restrictions, or lifecycle policies apply to a file.



Cloud Application Access Control

- This feature enforces access to cloud apps (e.g., Google Drive, Salesforce, Office 365) based on contextual conditions.
- The contextual conditions mainly include location, IP address, and device restrictions.
- It acts like a CASB-style control that ensures access is denied if the context is untrusted, even when credentials are valid.

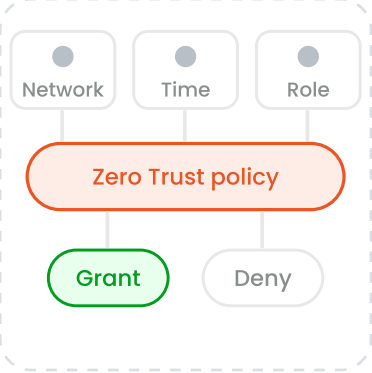


New features in DLP

Continued: new capabilities added to miniOrange DLP in this release.

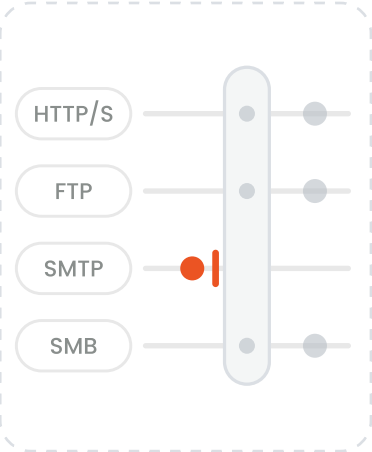
Context-Aware Access Policies

- These policies evaluate multiple runtime signals to grant or deny access.
- Policies are based on network, time frame, and user role.
- This can fall under a Zero Trust-aligned approach, where trust is never implicit, always verified against real-time context.



Network DLP

- Network DLP monitors and controls data moving across common transmission protocols.
- These protocols are HTTP/HTTPS, FTP, SMTP, and SMB.
- Policies can block, quarantine, or alert when sensitive information is detected traversing any of these channels, preventing exfiltration.



SIEM Integration

- SIEM integration connects your DLP or security tool to a central platform that aggregates logs and security events from across the organization.
- It enables threat detection, compliance reporting, and automated incident response.
- Get real-time alerts the moment a DLP policy violation or anomalous data access event occurs.



What changes once DLP is in place

01

Prevention of Personal Email Login

Prevent data leaks at the source by restricting access to personal email accounts across all devices and networks.

02

Agentless Email Data Protection

Block data from leaving the organization without installing agents on user devices. Outbound email is scanned in real time and risky messages are quarantined automatically.

03

Protection of Business Data

Monitor activity, control access and spot security issues in real time, so only authorized users can reach important information.

04

Regulatory Compliance

Stay compliant with GDPR, HIPAA, ISO, PCI DSS and RBI by enforcing security policies on all devices, reducing the risk of breaches and violations.

05

Secure Authentication

Verify users before any transmission and limit email access to approved domains for added security.

06

Detect & Block Suspicious Activity

Monitor endpoint actions for risky behavior. Block unauthorized access and suspicious transfers instantly across channels like USB and printers.

07

Enhanced Data Visibility & Control

Track how users and devices handle data across networks and clouds, with real-time alerts to spot and stop issues quickly.

08

Data Discovery & Classification

Find and label sensitive data stored across endpoint devices, then apply the right policy based on sensitivity level.

09

Remote Lock

Change the passwords of all device users and lock the device from the admin console.

10

Remote Wipe

Securely erase data from lost or unused devices, with a full device format available.

Fits the estate you already run

Deploy on your own infrastructure and connect DLP to the identity, device and cloud-access tooling already in place — so policy follows the user, not the product boundary.

FLEXIBLE DEPLOYMENT OPTIONS

Cloud DLP

Secures cloud apps and remote work with no on-site infrastructure to maintain.

On-Premise DLP

Runs inside your own network for maximum control over sensitive data.

Hybrid DLP

One policy set across cloud and on-premise, with unified visibility.

COMPLIANCE COVERAGE

GDPR
EU personal data

HIPAA
Patient health data

ISO
Information security

SEBI
Indian securities market

PCI DSS
Cardholder data

RBI
Indian financial data

INTEGRATIONS

AD
Active Directory

MDM
Mobile Device Management

CASB
Cloud Access Security Broker

IAM
Identity and Access Management

WHY TRUST miniORANGE DLP

- Enterprise-Focused DLP Data Security
- Customizable DLP Policies for Every Business Model
- Unified Platform: DLP + IAM + CASB + MDM Integration
- Simple, Intuitive Interface for IT Teams
- Flexible, Scalable Pricing Options
- 24×7 Global Support & Dedicated Team
- Fast Deployment with Guided Onboarding
- Continuous Updates, Patches, Training & Enhancements

Where teams put miniOrange DLP to work

The same policy engine, tuned to the data each industry is accountable for.

Healthcare

Protect patient data and meet HIPAA rules. Keep full control over data held in hospital systems, EHRs and mobile endpoints.

Finance

Keep financial data safe and meet PCI DSS standards. Protect cardholder details, banking records and payment information across apps like Microsoft 365, Salesforce and ERP systems.

Education

Secure student and staff data from accidental or insider leaks, so educators and administrators can focus on learning rather than on data risk.

Manufacturing

Lock down trade secrets, blueprints and R&D data. Enforce strong data-sharing limits, track file transfers and isolate risky systems.

Remote Workforce

Shield files on personal or corporate devices, apply adaptive data policies and track user sessions in real time — then lock or wipe remotely if a device is lost.

IT & Technology

Block uploads to personal repositories, detect code fragments in outbound email, and restrict unauthorized cloning or copying in real time.