OPSWAT.

Proactive DLP™

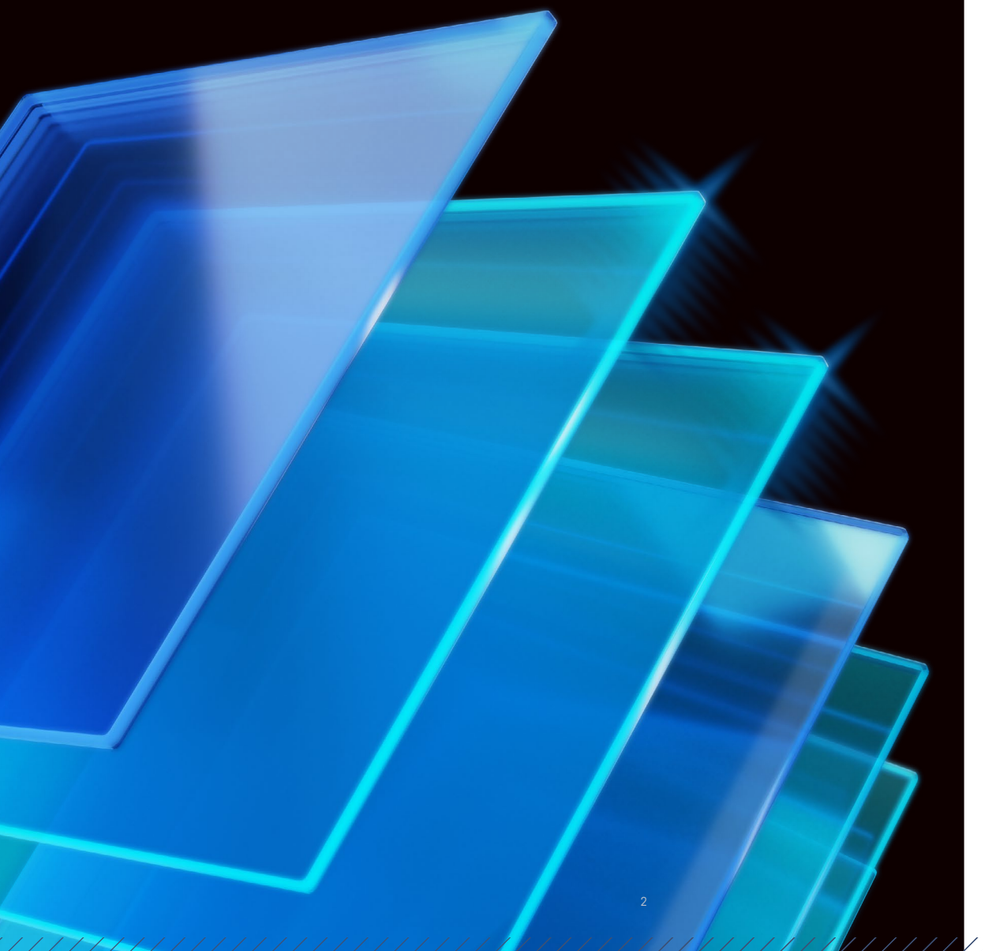
Stop potential data breaches and aid compliance.
Detect & block sensitive data in files & emails.

Protecting the World's Critical Infrastructure

OPSWAT.

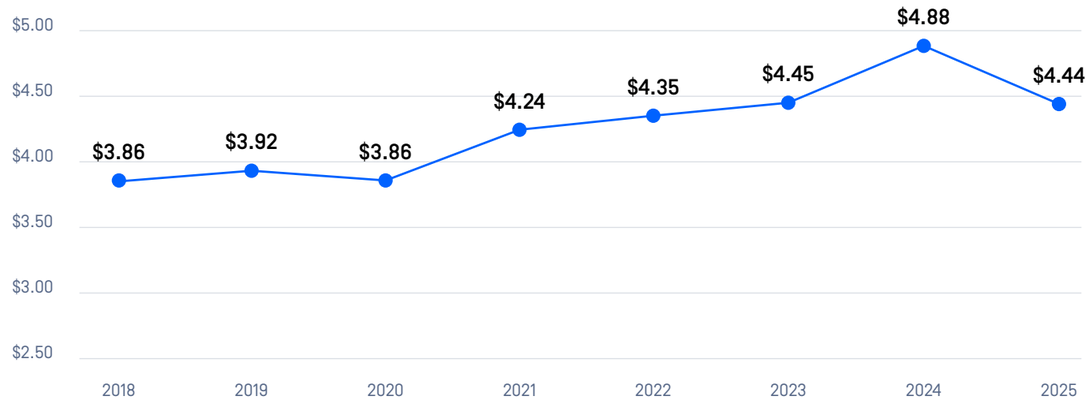
Organizations face increasing risks of data breaches as sensitive information moves constantly across emails, cloud storage, and collaboration platforms.

Proactive DLP™ detects and blocks sensitive information across 125+ file types through AI-powered recursive inspection and content-based policy enforcement, protecting organizations from data breaches and aiding regulatory compliance.



Total Global Average Cost of a Data Breach

Source: IBM Cost of Data Breach Report 2025



Measured in USD Millions

Key Challenges

- **Uncontrolled Data Growth:** Sensitive data spreads across emails, cloud apps, and personal devices, making visibility and control increasingly difficult.
- **Evolving Threats:** Cybercriminals target data through credential theft, exfiltration, and accidental leaks.
- **Fragmented Security Coverage:** Data moves across email, endpoints, web, and cloud, but siloed tools create blind spots that attackers exploit.
- **Rising Compliance Demands:** Regulations like HIPAA, PCI-DSS, and GDPR impose stricter data protection and heavy penalties for violations
- **Limitations of Legacy DLP:** Legacy DLP tools miss hidden or unstructured data and generate high false positives, reducing accuracy and trust.

OPSWAT.

Our Solution

1. Critical Data Protection

Proactive DLP™ gives organizations full visibility and control over their sensitive information through AI-powered content detection and classification. It identifies PII, PHI, financial data, secrets, credentials, and metadata across 125+ file types, even within hidden layers, cropped images, or invisible text, so confidential data is discovered and protected.

2. Comprehensive Data Breach & Insider Threat Prevention

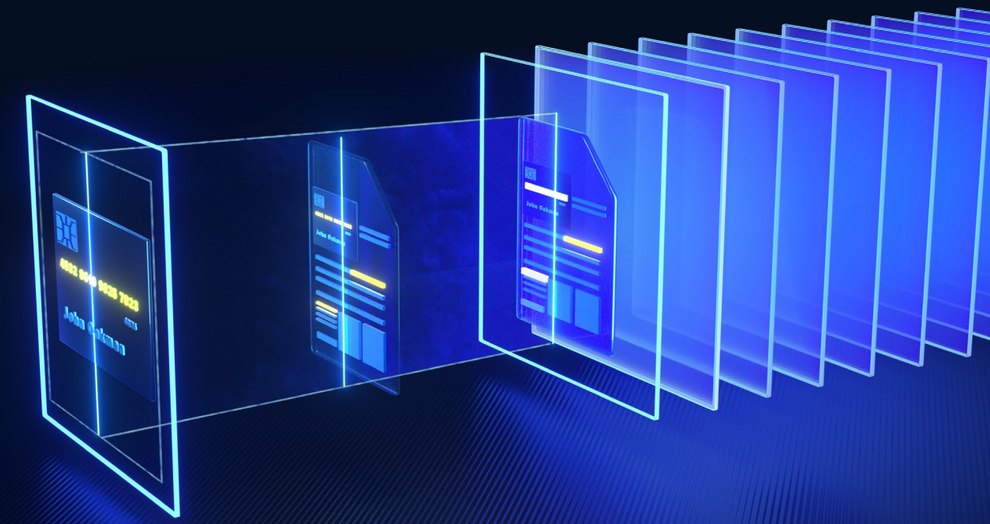
Proactive DLP prevents data leaks before they occur through recursive inspection and automated, content-based policy enforcement. By applying redaction, substitution, metadata removal, and watermarking, it secures data movement across email, endpoints, web, and cloud.

3. Regulatory Compliance Support

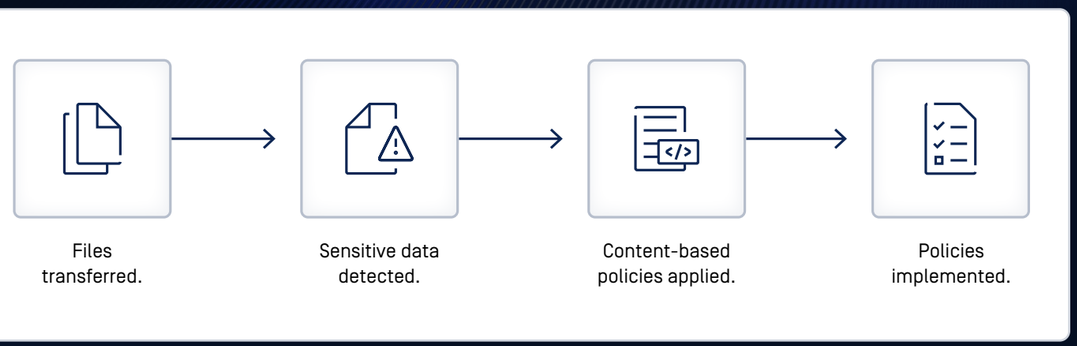
Proactive DLP helps organizations achieve and maintain compliance with key data protection standards such as PCI-DSS, HIPAA, and GDPR. Through consistent, content-based policy enforcement and integration with OPSWAT's security ecosystem, it helps organizations properly classify protect, and handle regulated data in accordance with industry and legal requirements.

Benefits

- Prevent sensitive and confidential data from entering or leaving an organization without hindering the productivity of users.
- Eliminates hidden data risks and insider threats by proactively inspecting nested, embedded, or obscured file layers, ensuring no sensitive content goes undetected.
- Enforces secure data handling automatically with content-based policies that block, redact, remove metadata or watermark files based on sensitivity.
- Simplifies compliance management with built-in support for HIPAA, PCI-DSS, GDPR, and other regulatory frameworks.
- Strengthens data governance and traceability through integrated content classification and tagging for visibility and control.
- Delivers comprehensive, multi-layered protection by integrating seamlessly with OPSWAT's other technologies.



How Proactive DLP works



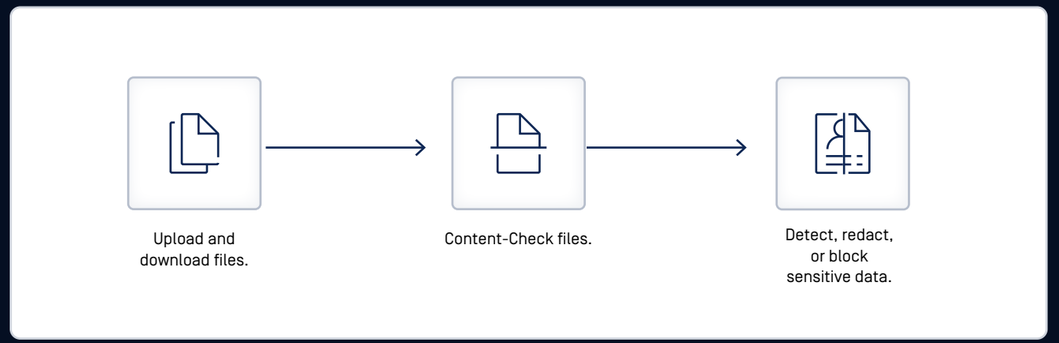
1. **Files Transferred:** Files are transferred across email systems, web uploads or downloads, cloud storage, and file transfer workflows.
2. **Sensitive Data Detected:** Proactive DLP inspects content to detect sensitive and regulated information across over 125 file types, including data hidden in embedded layers, cropped images, or invisible text.
3. **Content-Based Policies Applied:** Based on detected content, predefined policies apply actions such as blocking, redaction, substitution, or metadata removal.
4. **Policies Implemented:** Files are allowed, modified, or blocked according to defined policies.

OPSWAT.

Use Cases

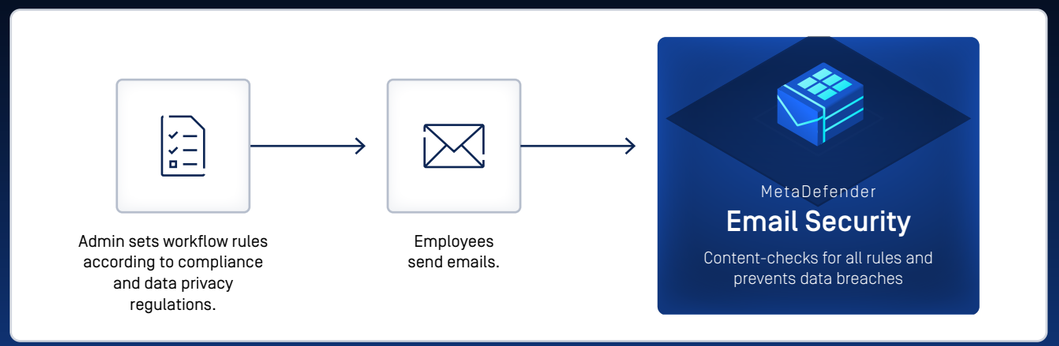
Content-Check File Uploads and Downloads

With **MetaDefender Core™** and **MetaDefender ICAP Server™**, you can content check files for sensitive data when they are uploaded or downloaded from web applications, as well as check files that are transferred through web proxies, secure gateways, web application firewalls, and storage systems.



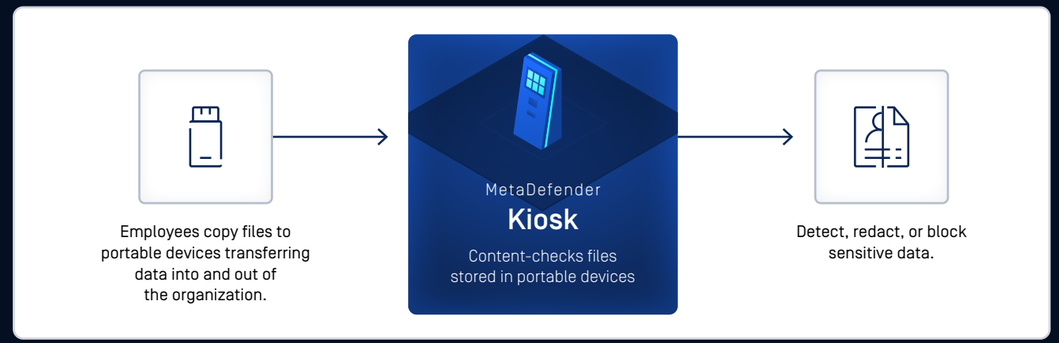
Check Emails for Sensitive Information

To help meet compliance with PCI and other regulations, as well as protect your customers, **MetaDefender Email Security™** can prevent emails with sensitive content from leaving or entering your organization by content-checking the email body and attachments. **MetaDefender Email Security** can identify credit card numbers or social security numbers, as well as alert administrators when emails include content that matches custom regular expressions.



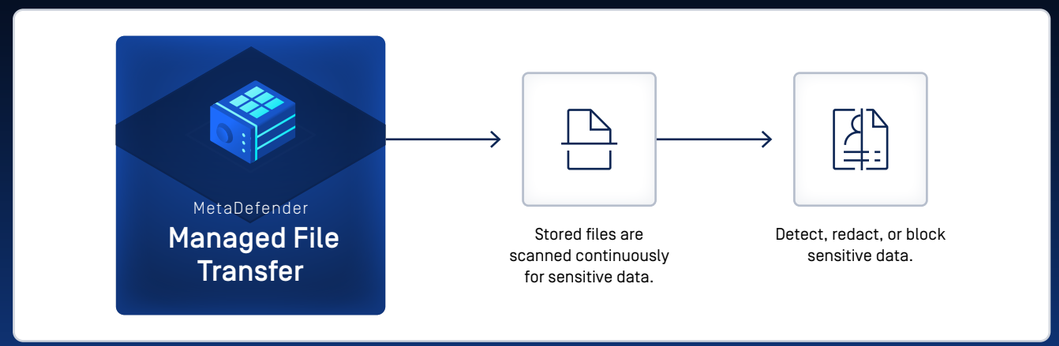
Content-Check Files Transferred Through Air-Gapped Networks

With **MetaDefender Kiosk™**, you can content check files when they are being transferred to and from your air-gapped networks and block PII, business critical data, and top-secret content by using custom regular expressions.



Identify New Custom Sensitive Information in Existing Content

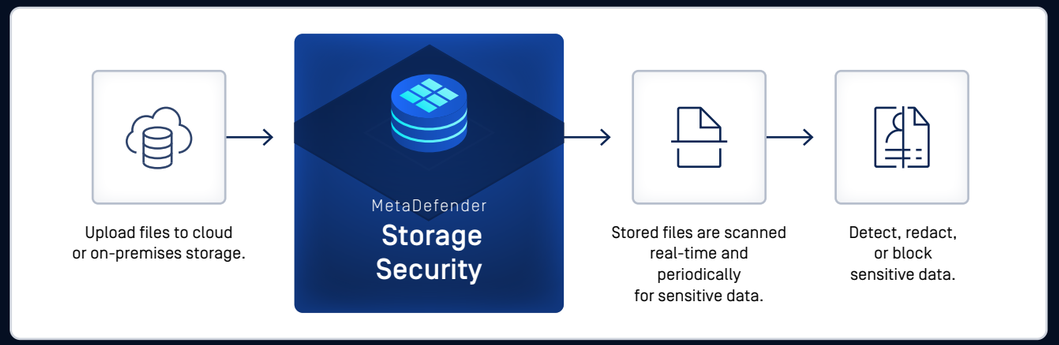
All files stored within **MetaDefender Managed File Transfer™** are continuously checked for sensitive information. Therefore, if you set new custom sensitive information types based on regular expressions, matched information will be automatically detected and redacted once the files are re-scanned. Scans can take place periodically or by request.



OPSWAT.

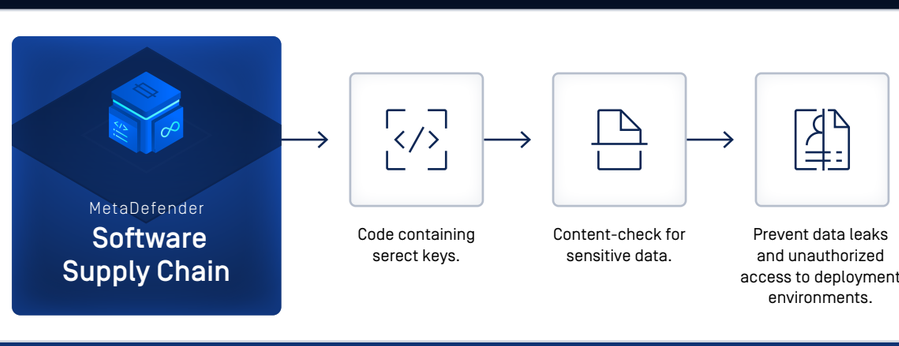
Protect Confidential Information Stored in Data Storage Systems

MetaDefender Storage Security™ prevents the loss of sensitive data from enterprise data stored in various cloud-storage and on-premises storage systems, including AWS, Azure, OneDrive, SharePoint Online, Google Drive, Cloudian, Box, Dropbox and other storage providers.



Detect Secrets in Source Code and Configuration Files

Proactive DLP™ alerts you to sensitive information that may have been inadvertently left in your source code, such as secret keys and passwords. Users can create custom regular expressions to filter out confidential information found in comments or licenses, such as the General Public License (GPL).



Proactive DLP Protects	Primary Function	Data in Motion	Data at Rest	Data in Use
MetaDefender Core & MetaDefender ICAP Server	Content-check files & enforce policies when files are uploaded/downloaded via web apps or transferred through web proxies, secure gateways, WAFs, and storage systems.	✓	✓	
MetaDefender Kiosk	Content-check files & enforce policies when files are transferred to/from air-gapped networks.		✓	
MetaDefender Email Security	Content-check & admin alert for email body and attachments.	✓		✓ (active use)
MetaDefender Managed File Transfer	Content-check & enforce policies when files are stored within MetaDefender Managed File Transfer.		✓	
MetaDefender Storage Security	Content-check & enforce policies when files are stored in cloud or on-prem storage (AWS, Azure, SharePoint, etc.).		✓	
MetaDefender Software Supply Chain	Content-check & alert when sensitive data (e.g., secrets) remain in source code.	✓		✓ (during code development & commit)

GET STARTED

Are you ready to put OPSWAT Proactive DLP™ on the front lines of your cybersecurity strategy?

Talk to one of our experts today.

Scan the QR code or visit us at:
opswat.com/get-started
sales@opswat.com

OPSWAT.
Protecting the World's Critical Infrastructure

For the last 20 years OPSWAT, a global leader in IT, OT, and ICS critical infrastructure cybersecurity, has continuously evolved an end-to-end solutions platform that gives public and private sector organizations and enterprises spanning Financial Services, Defense, Manufacturing, Energy, Aerospace, and Transportation Systems the critical advantage needed to protect their complex networks from cyberthreats.

Built on a "Trust no file. Trust no device.™" philosophy, OPSWAT solves customers' challenges like hardware scanning to secure the transfer of data, files, and device access with zero-trust solutions and patented technologies across every level of their infrastructure. OPSWAT is trusted globally by more than 1,900 organizations, governments, and institutions across critical infrastructure to help secure their devices, files, and networks from known and unknown threats, zero-day attacks, and malware, while ensuring compliance with industry and government-driven policies and regulations.

Discover how OPSWAT is protecting the world's critical infrastructure and securing our way of life; visit www.opswat.com.