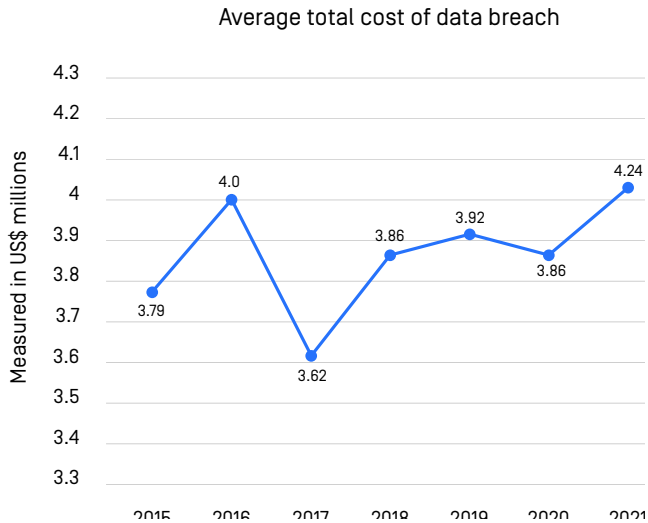
OPSWAT.

OPSWAT Proactive Data Loss Prevention

Stop Potential Data Breaches and Regulatory Compliance Violations



Safeguarding sensitive data is important for all organizations, especially for highly regulated, critical infrastructure like healthcare and financial services.

OPSWAT Data Loss Prevention (DLP) helps reduce the damage of potential data breaches and regulatory compliance violations by detecting and blocking sensitive and confidential data in files and emails, and secrets in source code.

Benefits

- Prevent sensitive and confidential data from entering or leaving an organization
- Enforce your security posture for Bring Your Own Device (BYOD) policies
- No impact on user productivity
- Secure your remote workforce
- Secure data on remote cloud systems
- Automatically detect secrets in source code
- Save time and administrative hassle by easily adapting DLP policies for your entire system
- Experience faster response and investigation time within your security and compliance teams
- Establish custom policies to meet your specific requirements
- Aid compliance with data regulations and industry-standard security requirements such as PCI, HIPAA, Gramm-Leach-Bliley, FINRA and more

OPSWAT.

Key features

Detect, block, and redact sensitive data

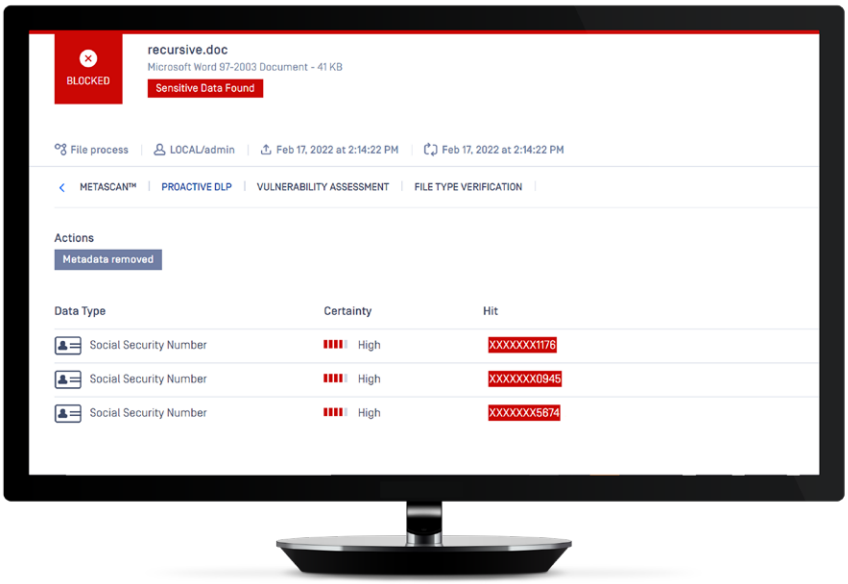
70+ supported file types

Watermark files

Remove metadata

What types of sensitive data does Proactive DLP detect?

- Social Security numbers
- Credit card numbers
- IPv4 addresses and Classless Inter-Domain Routing (CIDR)
- Metadata including author and GPS coordinates
- Custom regular expressions (RegEx)
- Secrets in text files (AWS, Microsoft Azure, Google Cloud Platform, IMB Cloud and private keys)
- Personally identifiable information (PII) and protected health information (PHI) in DICOM files



Advanced Sensitive Data Detection

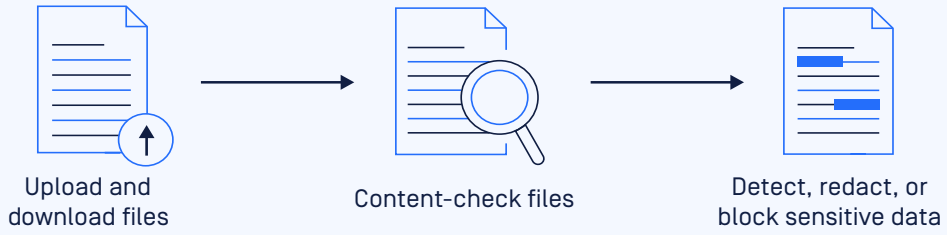
- Leverage Optical Character Recognition (OCR) technology to detect and redact sensitive information in image-only PDF files or embedded images in PDF files.
- Discover confidential data in files embedded in a document with recursive detection.
- Effectively classify blocked or allowed sensitive information types with advanced detection policy configuration.
- Enable administrator to control sensitive data process based on Certainty Level.
- Utilize AI-powered named-entity recognition (NER) model to locate and classify unstructured text into predefined categories, such as personally identifiable information (PII).
- Detect sensitive data within cropped parts of images embedded in MS Word files.
- Remove hidden images in PDF.
- Flexible detection policy with AND and OR logic.
- Leverage metadata info added by data classification systems.

OPSWAT.

Use Cases

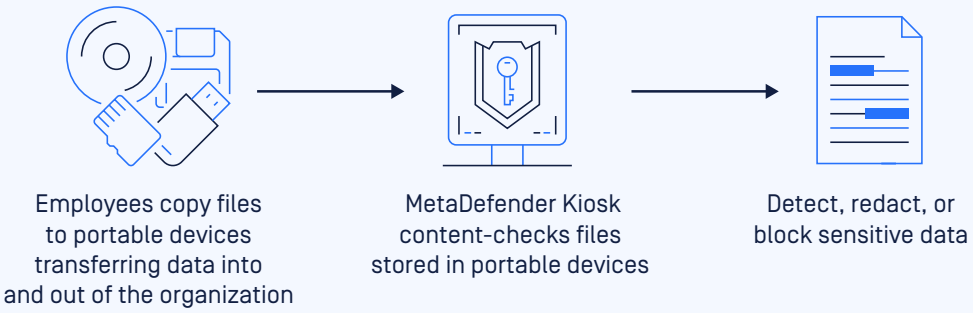
Content-Check File Uploads and Downloads

Check files that are transferred through web proxies, secure gateways, web applications firewalls, and storage systems with MetaDefender Core and MetaDefender ICAP Server for sensitive data when files are uploaded from web applications.



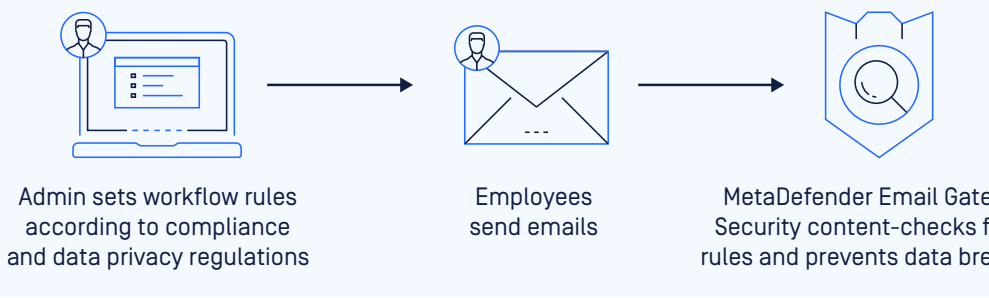
Content-Check Files Transferred Through Air-Gapped Networks

Content-check files transferred to and from your critical air-gapped networks and block personal identifying information (PII) or top-secret content by using custom regular expressions with MetaDefender Kiosk.



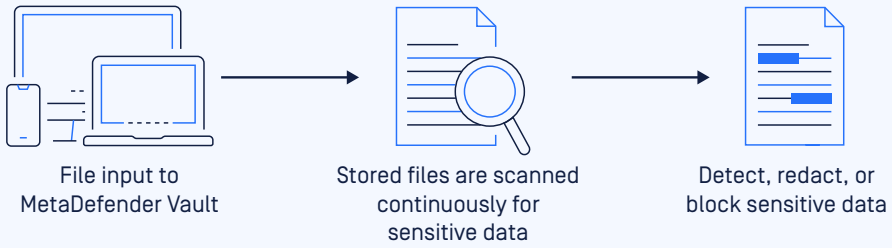
Check Emails for Sensitive Information

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



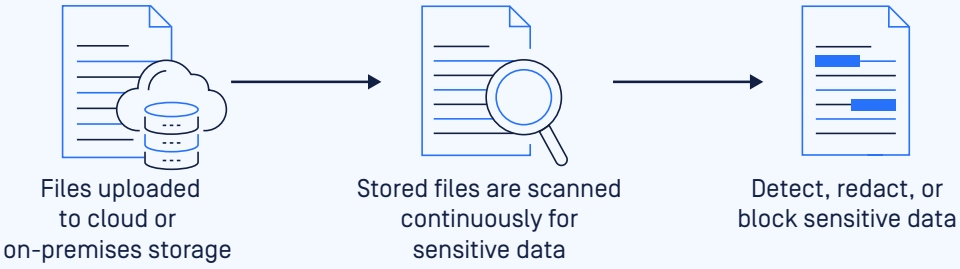
Identify New Custom Sensitive Information in Existing Content

All files stored within MetaDefender Vault are continuously checked for sensitive information. If you define new custom sensitive information types via regular expressions, matched information will be automatically detected and redacted once the files are re-scanned. Scans can take place periodically or on request.



Protect Confidential Information Stored in Data Storage Systems

MetaDefender for Secure Storage prevents sensitive data loss from enterprise data stored in various cloud-storage and on-premises storage systems like 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 accidentally left in your source code, including secret keys and passwords. Custom regular expressions enable users to filterfor confidential information in comments or licenses like the General Public License (GPL).

OPSWAT.

Windows System Info

- RAM: 32GB
- CPU: Intel® Core™ i7-6700 CPU @ 3.40GHz × 8
- OS: Windows Server 2019
- Disk Drive: 256GB SSD

Linux System Info

- RAM: 32GB
- CPU: Intel® Core™ i7-4790 CPU @ 3.60GHz × 8
- OS: Ubuntu 20.04.1 LTS
- Disk Drive: 256GB SSD

Resources

- Windows: MetaDefender Core v4.19.0 with 8 engines
- Linux: MetaDefender Core v4.19.0 with 5 engines

Test Results

File type	Average file size (KB)	Total files	Sensitive files	Detect only (s/file)		Detect and Redact (s/file)	
				Windows	Linux	Windows	Linux
Text	170	1456	728	0.04	0.05	0.04	0.05
Text	3174	864	592	0.25	0.21	0.25	0.22
Pdf	392	1572	785	0.28	0.28	0.44	0.47
Pdf	6553	846	242	2.5	2.72	3.0	4.9
Word	224	629	313	0.14	0.16	0.15	0.16
Word	2969	808	128	0.26	0.26	0.36	0.35
Excel	191	2942	1471	0.51	0.43	0.52	0.46
Excel	1904	840	192	3.3	2.8	3.3	2.7

OPSWAT.
Protecting the World's Critical Infrastructure