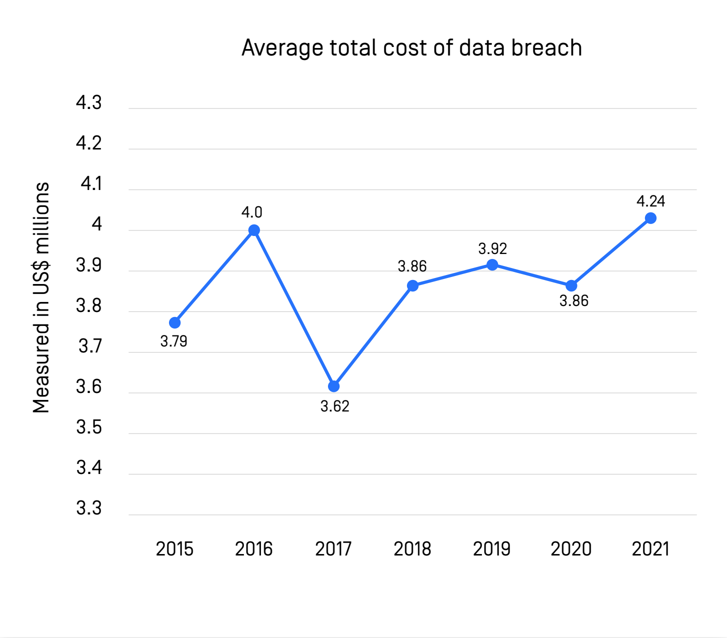
OPSWAT

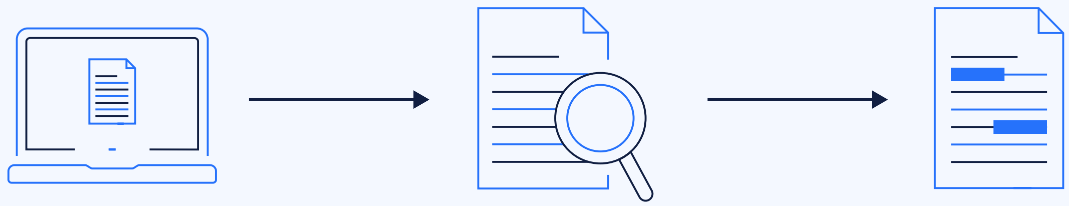
OPSWAT Proactive Data Loss Prevention

Stop Potential Data Breaches and Regulatory Compliance Violations



Changing work styles have led to employees sharing documents over cloud storage and file-sharing services. The more information is delivered electronically, the greater the likelihood that organizations' sensitive and confidential data can be accidentally or deliberately given to unauthorized people. Modern data transfer methods, such as email, web, instant messaging (IM), or FTP, raise huge enterprise security risks.

OPSWAT Data Loss Prevention (DLP) helps prevent potential data breaches and regulatory compliance violations by detecting and blocking sensitive and confidential data in files and emails.



File & Emails

Content-check for sensitive data

Prevent data breaches with custom worflow rules

Benefits

- Prevent sensitive and confidential data from entering or leaving an organization without impacting user productivity
- Secure mobile workforce and enforce security in Bring Your Own Device (BYOD) environments
- Secure data on remote cloud systems
- Aid compliance with data regulations and industry-standard security requirements such as PCI, HIPAA, Gramm-Leach-Bliley, FINRA and more
- Establish custom policies to meet your specific requirements
- 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

Key features

Proactively detect and block sensitive data in 70+ supported file types

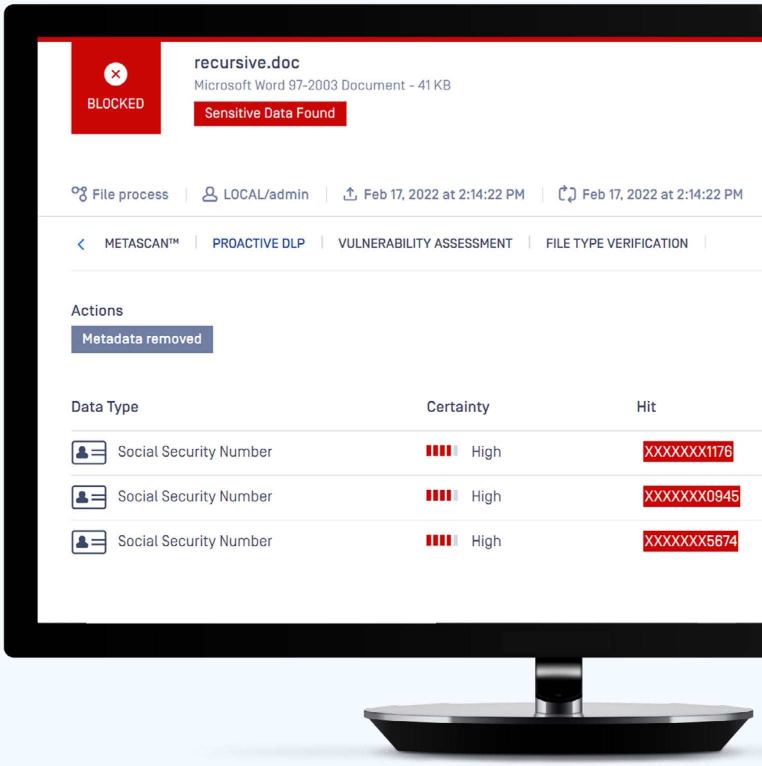
Redact identified sensitive information

Watermark files for better security account ability and traceability

Remove metadata contained within files, which could contain sensitive information like the author, GPS coordinates, etc.

What type of sensitive data can OPSWAT Proactive DLP detect?

- Social Security Numbers
- Credit Card Numbers
- IPv4 addresses and Classless Inter-Domain Routing (CIDR)
- Any specific data pattern using Custom Regular Expressions (RegEx)



BLOCKED

recursive.doc

Microsoft Word 97-2003 Document - 41 KB

Sensitive Data Found

File process | LOCAL/admin | Feb 17, 2022 at 2:14:22 PM | Feb 17, 2022 at 2:14:22 PM

Actions

Metadata removed

Data Type	Certainty	Hit
Social Security Number	High	XXXXXXX1176
Social Security Number	High	XXXXXXX0945
Social Security Number	High	XXXXXXX5674

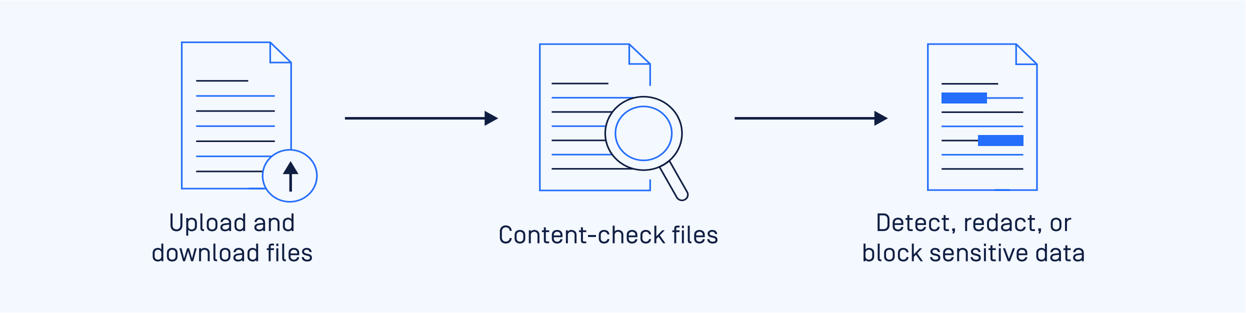
Advanced Sensitive Data Detection

- Detect and redact sensitive information in image-only PDF files or PDF files having embedded images using Optical Character Recognition technology
- Discover confidential data in files embedded or linked to a document (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
- Leverage metadata info added by data classification systems
- 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

Use Cases

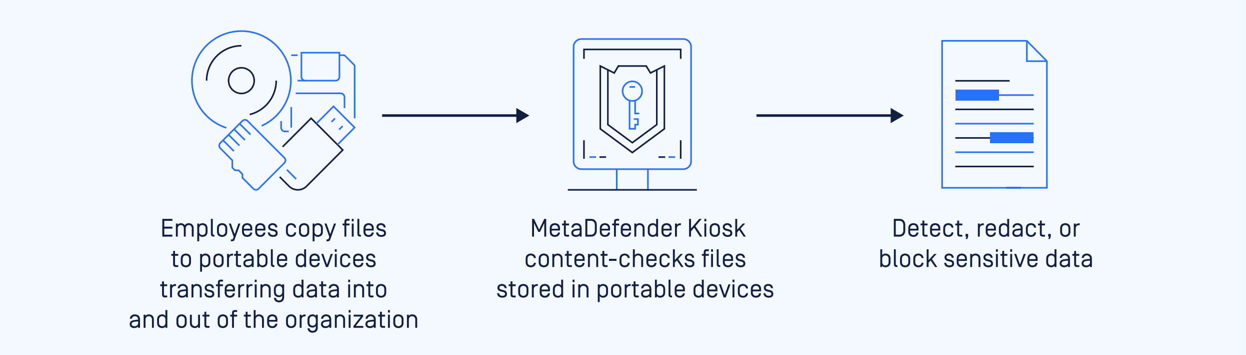
Content-Check File Uploads and Downloads

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


Upload and download files
Content-check files
Detect, redact, or block sensitive data

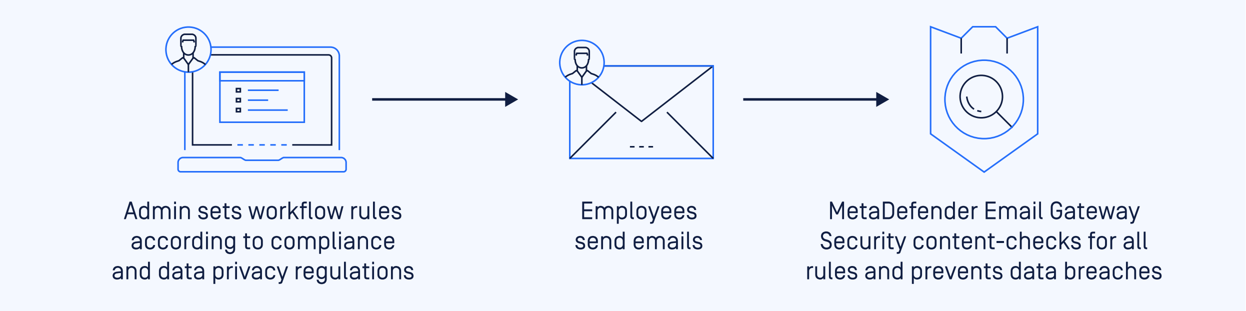
Content-Check Files Transferred Through Air-Gapped Networks

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


Employees copy files to portable devices transferring data into and out of the organization
MetaDefender Kiosk content-checks files stored in portable devices
Detect, redact, or block sensitive data

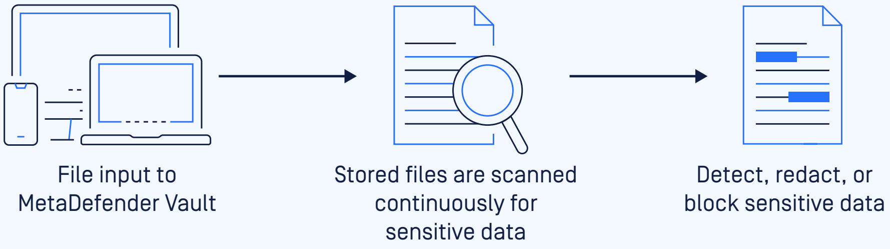
Check Emails for Sensitive Information

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.


Admin sets workflow rules according to compliance and data privacy regulations
Employees send emails
MetaDefender Email Gateway Security content-checks for all rules and prevents data breaches

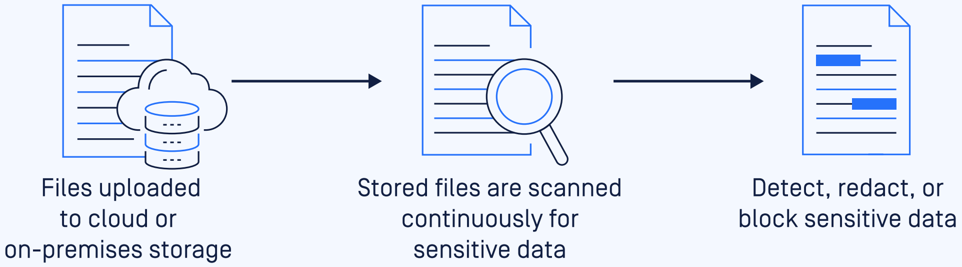
Identify New Custom Sensitive Information in Existing Content

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.


File input to MetaDefender Vault
Stored files are scanned continuously for sensitive data
Detect, redact, or block sensitive data

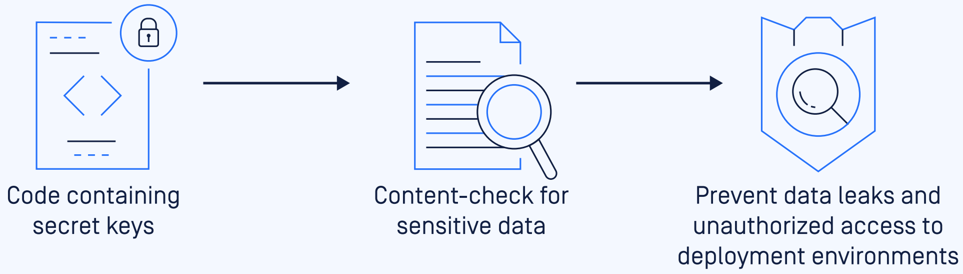
Protect Confidential Information Stored in Data Storage Systems

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.


Files uploaded to cloud or on-premises storage
Stored files are scanned continuously for sensitive data
Detect, redact, or block sensitive data

Detect the secrets in the source code and configuration files

With the power of Proactive DLP in MetaDefender Core, you will be made aware when there is sensitive information in your source code—whether it's secret keys or passwords that someone accidentally revealed in the code. Flexible configuration based on regular expression allows you to capture even unexpected strings such as inappropriate comments or sensitive licenses like the General Public License (GPL).


Code containing secret keys
Content-check for sensitive data
Prevent data leaks and unauthorized access to deployment environments

Performance

File format	File size (KB)	Total files	Detect only (s/file)		Detect and Redact (s/file)	
			Windows	Linux	Windows	Linux
Text (txt, csv, ...)	170	1500	0.04	0.04	0.04	0.04
PDF	400	1500	0.25	0.27	0.43	0.47
MS Word	230	600	0.13	0.15	0.14	0.16
MS Excel	200	3000	0.5	0.44	0,5	0.44

System specs

- Windows Server 2019
- Linux Ubuntu 20.04.1 LTS
- Intel® Core™ i7-6700 CPU @ 3.40GHz × 8
  32GB RAM
  512 SSD

Dataset

- 50% clean files
- 50% files containing sensitive data