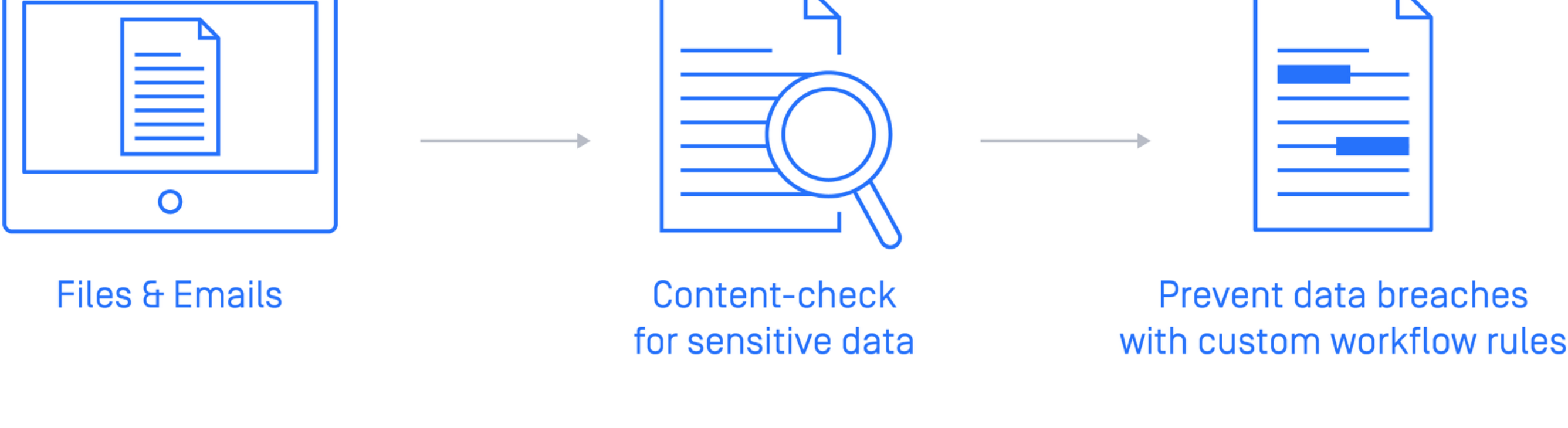


# Proactive Data Loss Prevention [Proactive DLP]

Detect and Block Sensitive Data in Files and Emails

OPSWAT Proactive Data Loss Prevention (Proactive DLP) can help prevent potential data breaches and regulatory compliance violations by detecting and blocking sensitive and confidential data in files and emails, including credit card numbers and social security numbers. OPSWAT Proactive DLP supports a wide range of file types, including Microsoft Office and PDF.



## Aid Compliance with OPSWAT Proactive DLP

To comply with industry regulations, such as Payment Card Industry Data Security Standard (PCI), Health Information Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), General Data Protection Regulation (GDPR) and Financial Industry Regulatory Authority (FINRA), organizations have the obligation to keep personally identifiable information (PII) private.

Also, in today's increasingly litigious and highly competitive business environment, the privacy of confidential business information is an essential lifeline for every enterprise. Confidential information, such as trade secrets, intellectual assets, financial statements, can be disclosed or sent to unauthorized individuals via a multitude of channels, including email, the internet, portable storage devices, and cloud services. Data breaches can be costly, damage a company's brand and reputation, and diminish the trust of customers and partners.

OPSWAT Proactive DLP can help organizations prevent sensitive and regulated data from leaving or entering the organization's systems by content-checking files and emails before they are transferred. MetaDefender can search over 30 file types for sensitive content, including Microsoft Office, PDF, CSV, HTML and image files.

53%

of companies found over 1,000 sensitive files exposed to all employees

\$3,9M

is the average cost of a data breach

24%

of data breaches are caused by human error

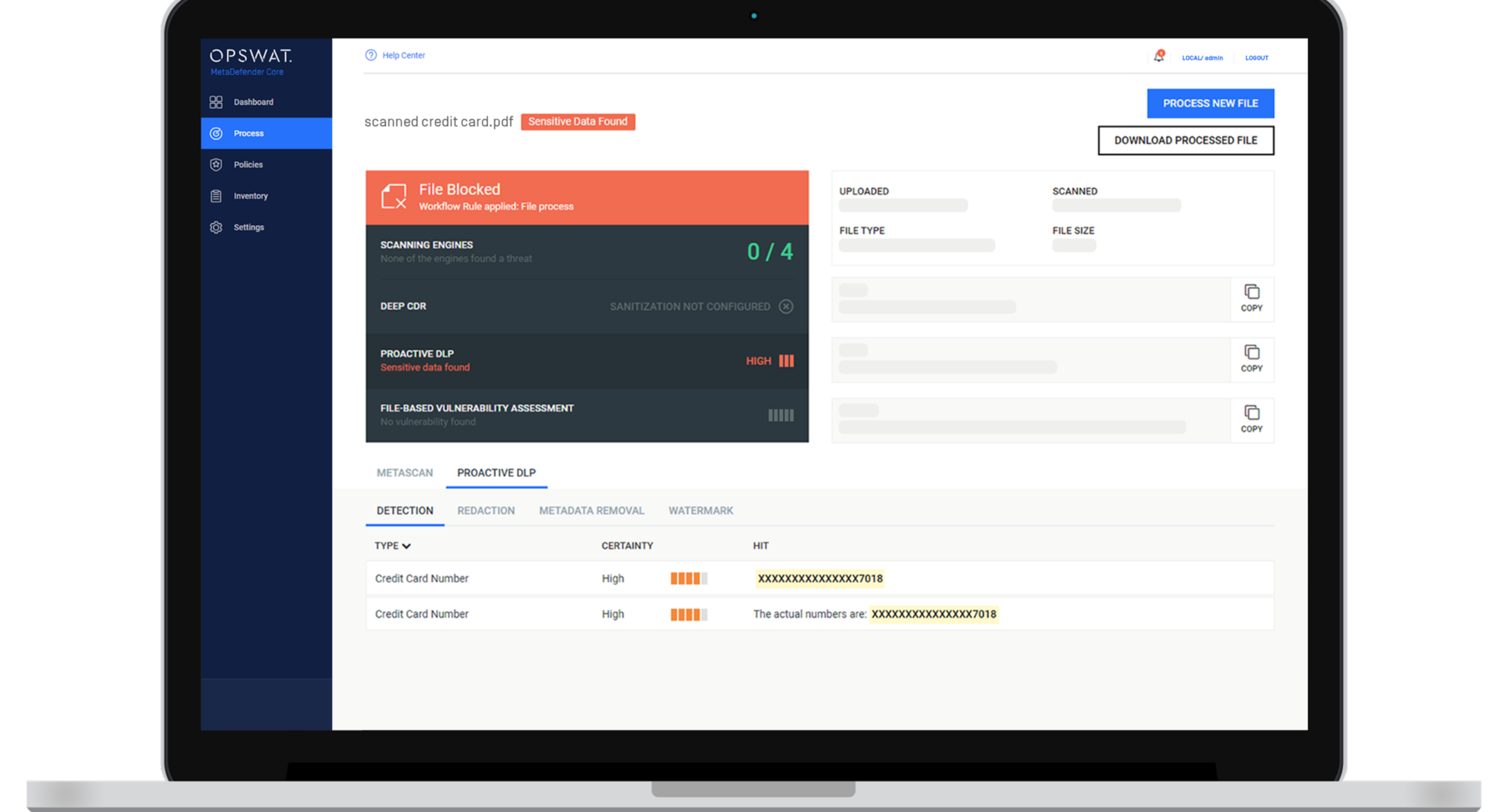
## What type of sensitive data can OPSWAT Proactive DLP detect?

MetaDefender can detect the following PII and sensitive data in files:

- Social Security Numbers
- Credit Card Numbers
- IPv4 addresses
- Classless Inter-Domain Routing (CIDR)
- Custom Regular Expressions (RegEx)

## Benefits of OPSWAT Proactive DLP

- ✓ Prevent sensitive and confidential data from entering or leaving an organization without hindering the productivity of users
- ✓ 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 policy requirements
- ✓ Integrate Proactive DLP with [Multiscanning](#), [Deep Content Disarm and Reconstruction](#) and [File-based Vulnerability Assessment](#) for comprehensive protection



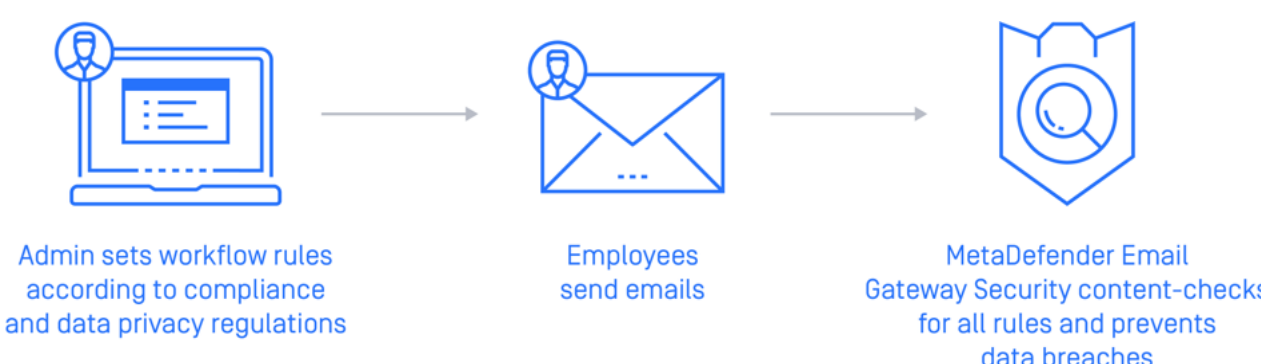
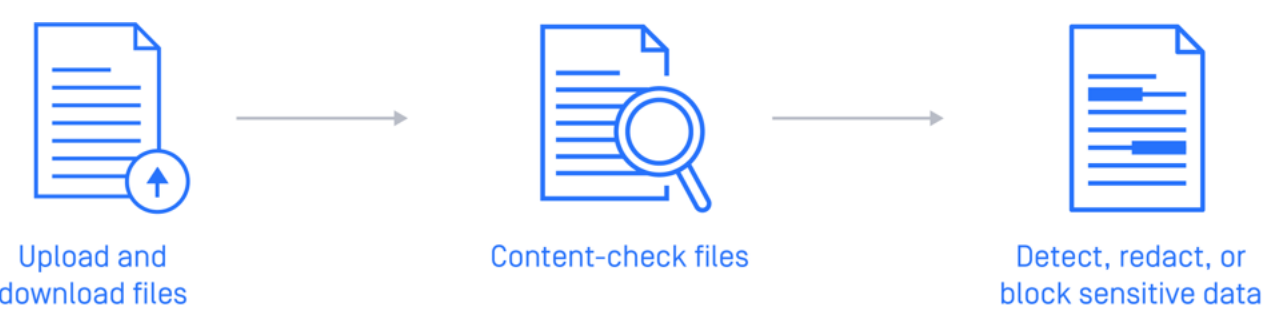
## How it works

- Proactively detect and block sensitive data in files and emails in 30+ supported file types
- Automatically redact identified sensitive information in PDFs, MS Word documents and MS Excel spreadsheets
- Leverage Optical Character Recognition (OCR) technology to detect and redact sensitive information in image-only PDF files or PDF files having embedded images
- Remove metadata containing potentially confidential information like name, company, subject, GPS locations, authors, etc.
- Watermark files for better security accountability and traceability

## OPSWAT Proactive DLP 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 being transferred through web proxies, secure gateways, web application firewalls, and storage systems.

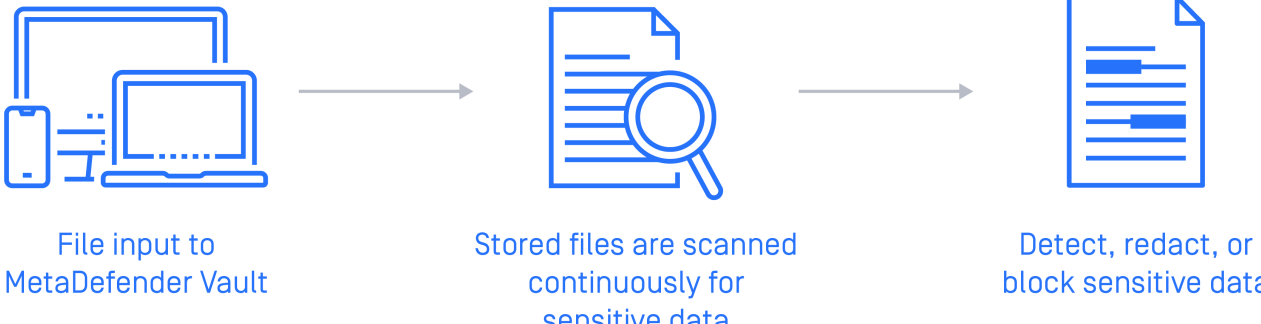
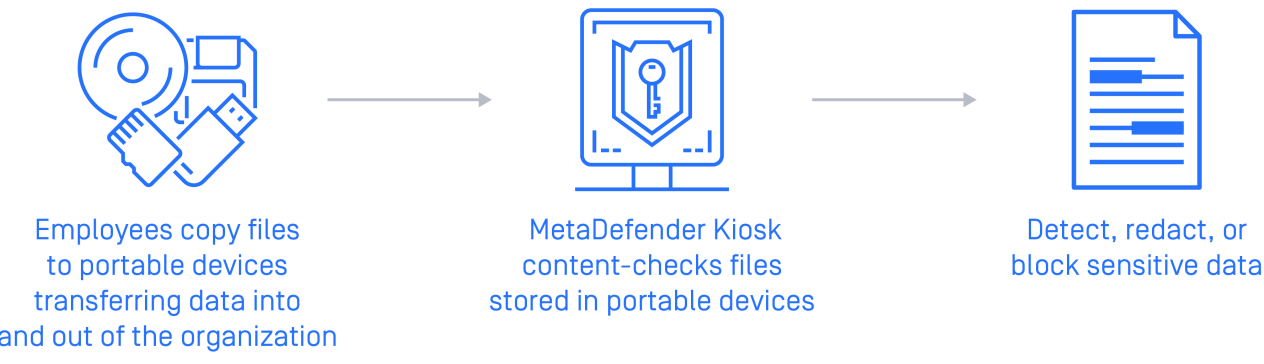


### Check Emails for Sensitive Information

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.

### 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.



### Identify New Custom Sensitive Information in Existing Content

All files stored within [MetaDefender Vault](#) 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.

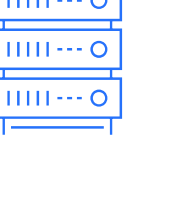
## OPSWAT Products That Offer Proactive Data Loss Prevention



MetaDefender Core

Integrate Proactive Data Loss Prevention via REST API with existing security architectures and file uploads and downloads features on web portals


LEARN MORE



MetaDefender ICAP Server

Prevent sensitive data from being transferred through your web proxies, secure gateways, web application firewalls, and storage systems


LEARN MORE



MetaDefender Email Gateway Security

Content-check emails and attachments for PII and sensitive data based on custom regular expressions

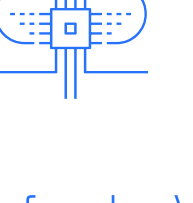
LEARN MORE



MetaDefender Kiosk

Prevent PII or confidential content from being transferred to and from critical air-gapped networks

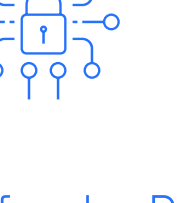
LEARN MORE



MetaDefender Vault

Content-check all files transferred and stored in secure networks for sensitive and regulated data.


LEARN MORE



MetaDefender Drive

Prevent sensitive data leak from files stored in portable devices

LEARN MORE



MetaDefender for Secure Storage

Prevent PII and sensitive data loss from enterprise data stored in Cloudian, S3, Box, Dropbox, and other storage providers

LEARN MORE

OPSWAT.  
Trust no file.  
Trust no device.

Products	Solutions	Service and Support	Technologies	Developer Tools	Resources	Company
<a href="#">MetaDefender Core</a>	<a href="#">Cross-Domain Solutions</a>	<a href="#">File Upload Assessment</a>	<a href="#">Deep Content Disarm and Reconstruction (CDRI)</a>	<a href="#">MetaDefender Core</a>	<a href="#">Academy</a>	<a href="#">About</a>
<a href="#">MetaDefender Email Gateway Security</a>	<a href="#">Secure Access</a>	<a href="#">Implementation Services</a>	<a href="#">MetaAccess API</a>	<a href="#">MetaAccess API</a>	<a href="#">Blog</a>	<a href="#">Contact</a>
<a href="#">MetaDefender ICAP Server</a>	<a href="#">File Upload Security</a>	<a href="#">Product Training</a>	<a href="#">Multiscanning</a>	<a href="#">OESIS Framework SDK</a>	<a href="#">Case Studies</a>	<a href="#">Research Center</a>
<a href="#">MetaDefender Kiosk</a>	<a href="#">Malware Analysis</a>	<a href="#">Support Plans</a>	<a href="#">File-Based Vulnerability Assessment</a>	<a href="#">Threat Intelligence Feed</a>	<a href="#">Datashheets</a>	<a href="#">Careers</a>
<a href="#">MetaDefender for Secure Storage</a>	<a href="#">Email Security</a>		<a href="#">Proactive Data Loss Prevention (Proactive DLP)</a>		<a href="#">Reports</a>	<a href="#">Job Openings at OPSWAT</a>
<a href="#">MetaDefender Vault</a>	<a href="#">Network Access Control</a>		<a href="#">Endpoint Compliance</a>		<a href="#">Videos</a>	<a href="#">Customers</a>
<a href="#">MetaAccess</a>	<a href="#">Storage Security</a>		<a href="#">Endpoint Vulnerability Assessment</a>		<a href="#">White Papers</a>	<a href="#">Compliance and Certifications</a>
<a href="#">Cloud Security for Salesforce</a>	<a href="#">For Developers</a>		<a href="#">Endpoint Malware Detection</a>		<a href="#">Analyze a File</a>	<a href="#">Press Releases</a>
<a href="#">SafeConnect NAC</a>			<a href="#">Endpoint Application Removal</a>		<a href="#">Free Tools</a>	<a href="#">Channel Partner Directory</a>
<a href="#">Central Management</a>			<a href="#">Data Protection</a>		<a href="#">All Resources</a>	
<a href="#">MetaDefender Cloud</a>						
<a href="#">All Products</a>						