

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

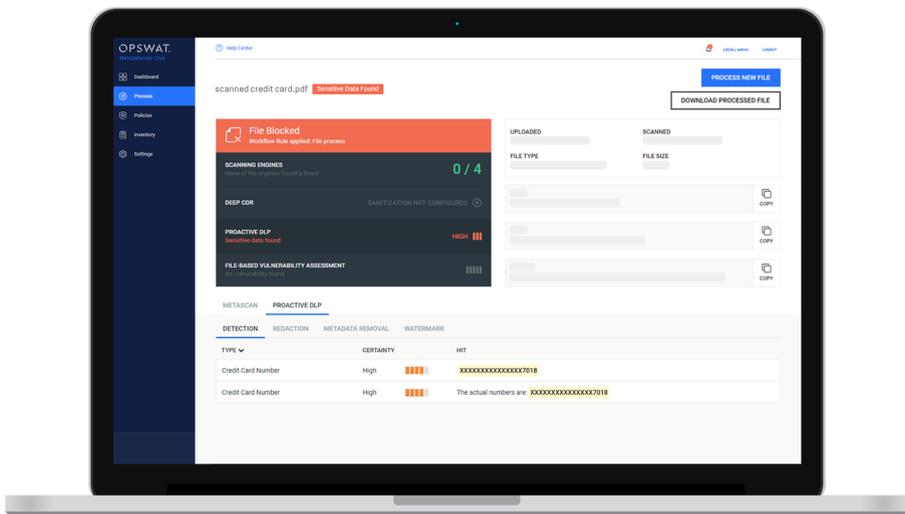
What type of sensitive data can OPSWAT Proactive DLP detect?

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

<p>MetaDefender Core</p> <p>Integrate Proactive Data Loss Prevention via REST API with existing security architectures and file uploads and downloads features on web portals</p> <p>LEARN MORE</p>	<p>MetaDefender ICAP Server</p> <p>Prevent sensitive data from being transferred through your web proxies, secure gateways, web application firewalls, and storage systems</p> <p>LEARN MORE</p>	<p>MetaDefender Email Gateway Security</p> <p>Content-check emails and attachments for PII and sensitive data based on custom regular expressions</p> <p>LEARN MORE</p>	<p>MetaDefender Kiosk</p> <p>Prevent PII or confidential content from being transferred to and from critical air-gapped networks</p> <p>LEARN MORE</p>
<p>MetaDefender Vault</p> <p>Content-check all files transferred and stored in secure networks for sensitive and regulated data.</p> <p>LEARN MORE</p>	<p>MetaDefender Drive</p> <p>Prevent sensitive data leak from files stored in portable devices</p> <p>LEARN MORE</p>	<p>MetaDefender for Secure Storage</p> <p>Prevent PII and sensitive data loss from enterprise data stored in Cloudian, S3, Box, Dropbox, and other storage providers</p> <p>LEARN MORE</p>	

OPSWAT.

Trust no file. Trust no device.

<p>Products</p> <ul style="list-style-type: none"> MetaDefender Core MetaDefender Drive MetaDefender Email Gateway Security MetaDefender ICAP Server MetaDefender Kiosk MetaDefender for Secure Storage MetaDefender Vault MetaAccess Cloud Security for Salesforce SafeConnect NAC Central Management MetaDefender Cloud All Products 	<p>Solutions</p> <ul style="list-style-type: none"> Cross-Domain Solutions Secure Access File Upload Security Malware Analysis Email Security Network Access Control Storage Security For Developers 	<p>Service and Support</p> <ul style="list-style-type: none"> File Upload Assessment Implementation Services Product Training Support Plans 	<p>Technologies</p> <ul style="list-style-type: none"> Deep Content Disarm and Reconstruction (CDR) MetaAccess API OESIS Framework SDK Threat Intelligence Feed Proactive Data Loss Prevention (Proactive DLP) Endpoint Compliance Endpoint Vulnerability Assessment Endpoint Malware Detection Endpoint Application Removal Data Protection 	<p>Developer Tools</p> <ul style="list-style-type: none"> MetaDefender Core MetaAccess API OESIS Framework SDK Threat Intelligence Feed 	<p>Resources</p> <ul style="list-style-type: none"> Academy Blog Case Studies Datasheets Reports Videos White Papers Analyze a File Free Tools Online Store All Resources 	<p>Company</p> <ul style="list-style-type: none"> About Contact Research Center Careers Job Openings at OPSWAT Customers Events Press Releases Compliance and Certifications Channel Partner Directory
--	---	--	---	--	---	---