OPSWAT.

DATASHEET

OPSWAT Proactive DLP

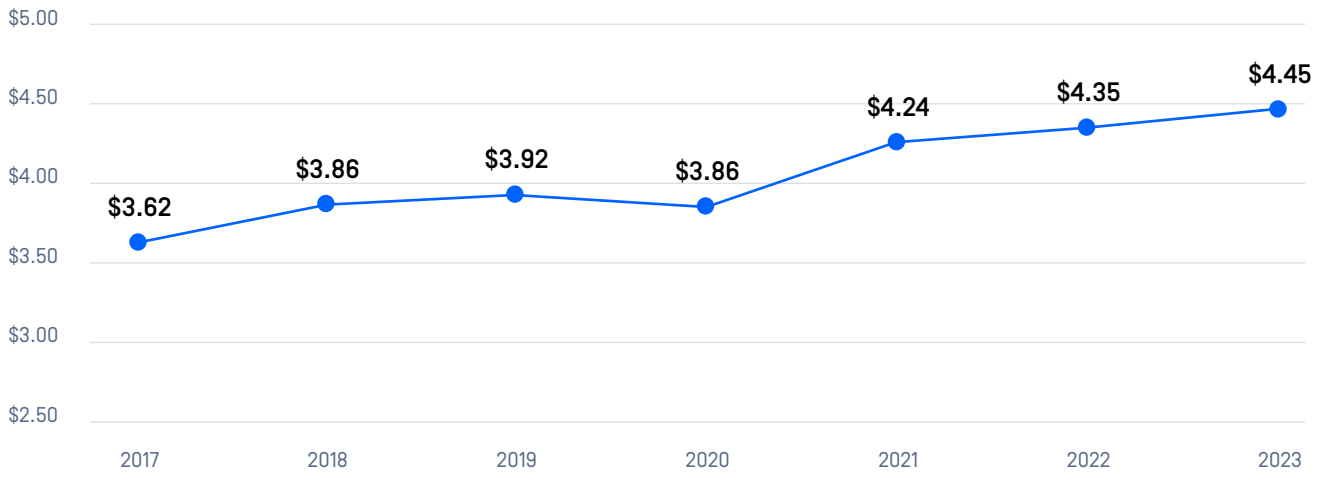
Stop Potential Data Breaches and Regulatory Compliance Violations

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

OPSWAT Proactive DLP (Data Loss Prevention) 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.

Total Cost of a Data Breach

Source: IBM Cost of Data Breach Report 2023



Measured in USD Millions

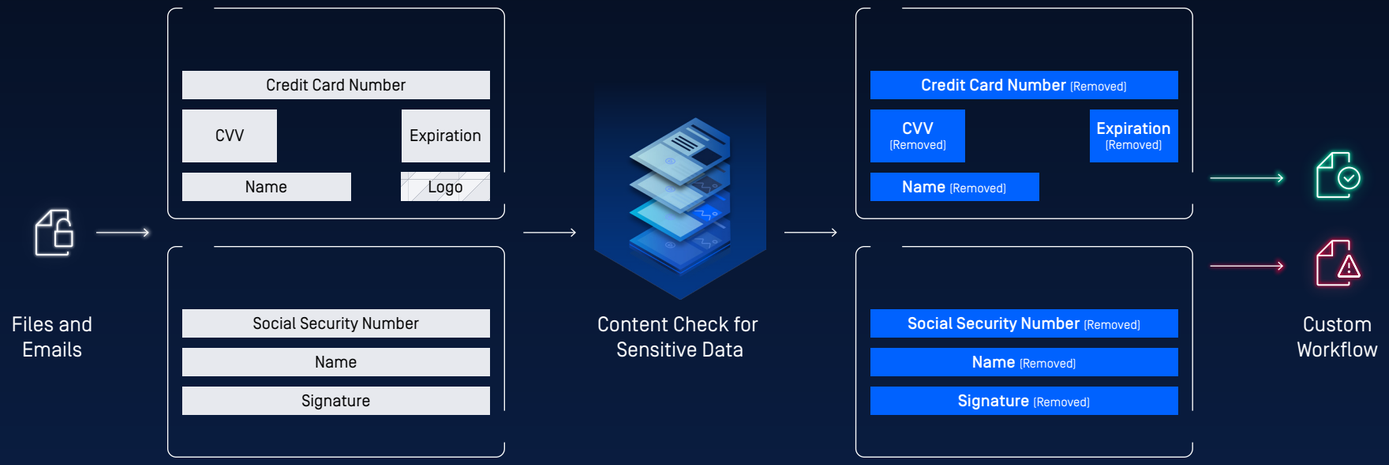
Benefits

- Prevent sensitive and confidential data from entering or leaving an organization without hindering the productivity of users.
- Locate and classify unstructured text into predefined categories with machine-learning powered AI.
- Integrate Proactive DLP with Multiscanning, Deep CDR (Content Disarm and Reconstruction) and File-based Vulnerability Assessment for comprehensive protection.
- Aid compliance with data regulations and industry-standard security requirements such as PCI, HIPAA, Gramm-Leach-Bliley, FINRA and more.
- Prevent secret leaks by automatically identifying various data structures such as API keys, passwords, key IDs, or access keys generated by third parties.
- Establish custom policies to meet your specific policy requirements.

Key Features

- Detect, Block, and Redact Sensitive Data
- 110+ Supported File Types
- Watermark Files
- Remove Metadata

How Proactive DLP Works



Types of Sensitive Data OPSWAT Proactive DLP Detects

- Social Security numbers
- Credit card numbers
- IPv4 addresses and Classless Inter-Domain Routing (CIDR)
- Custom regular expressions (RegEx)
- Secrets in text files (AWS, Microsoft Azure, IBM Cloud, and Google Cloud Platform)
- Protected health information (PHI) and PII in Digital Imaging and Communications in Medicine (DICOM) files

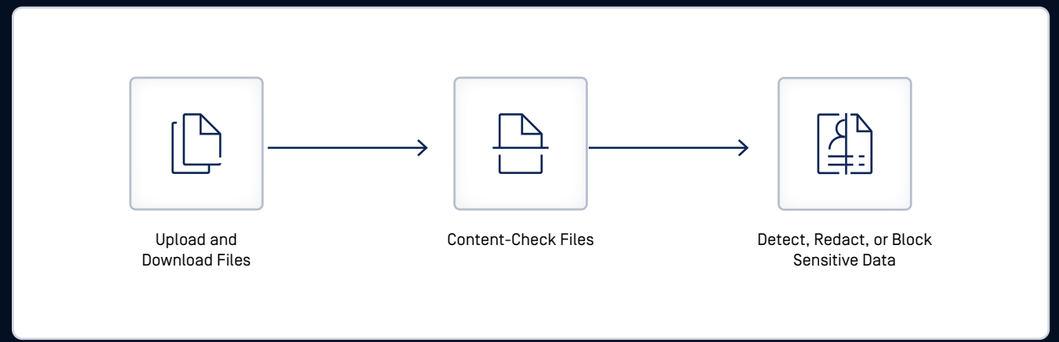
Advanced Sensitive Data Detection

- Proactively detect and block sensitive data in files and emails in 110+ supported file types.
- Automatically redact identified sensitive information in PDFs, Microsoft Word documents and Microsoft 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.
- Utilize our AI-powered named-entity recognition (NER) model to locate and classify unstructured text into predefined categories, such as personally identifiable information (PII).
- Remove metadata containing potentially confidential information like name, company, subject, GPS locations, authors, etc.
- Detect not safe for work (NSFW) content, including adult content in images and offensive language in text, with AI-powered document classification.
- Detect personal identity documents and allow or block them based on company policy.

Use Cases

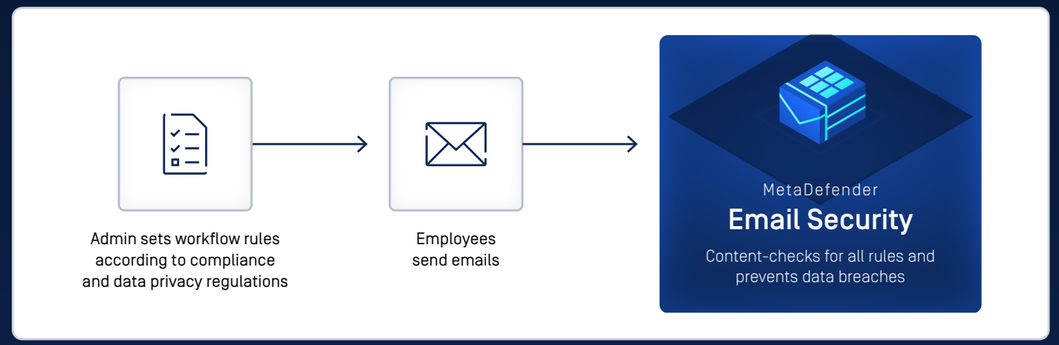
Content-Check File Uploads and Downloads

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.



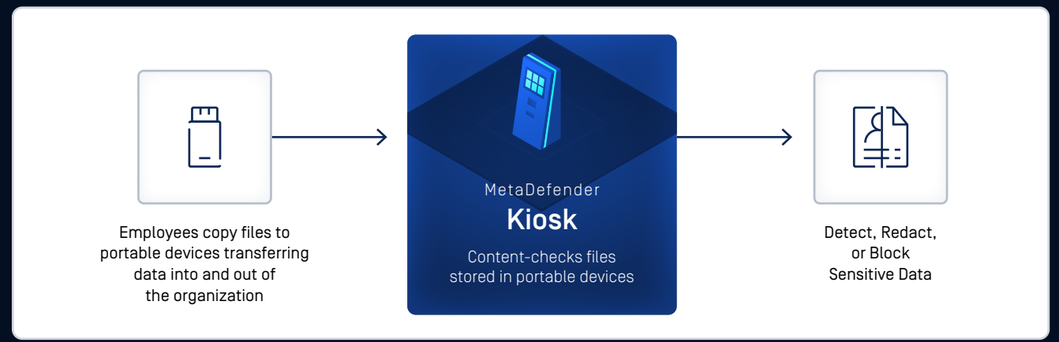
Check Emails for Sensitive Information

To 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.



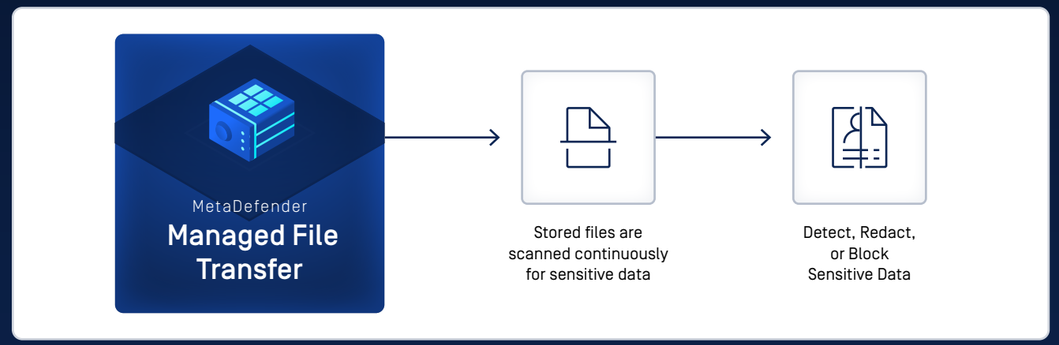
Content-Check Files Transferred Through Air-Gapped Networks

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.



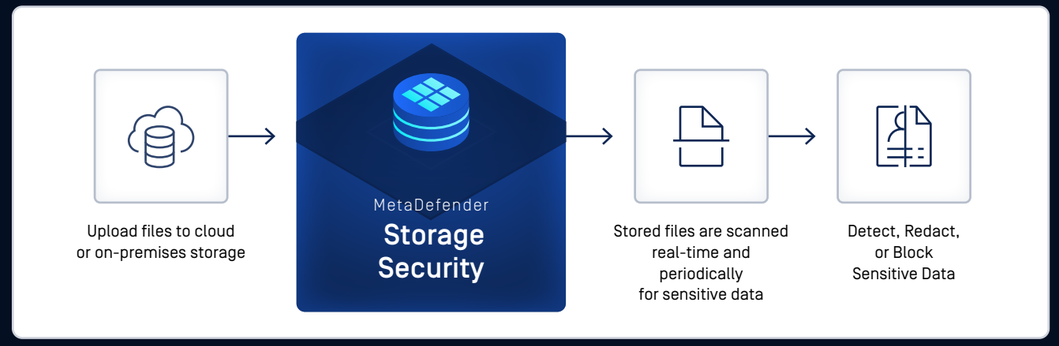
Identify New Custom Sensitive Information in Existing Content

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.



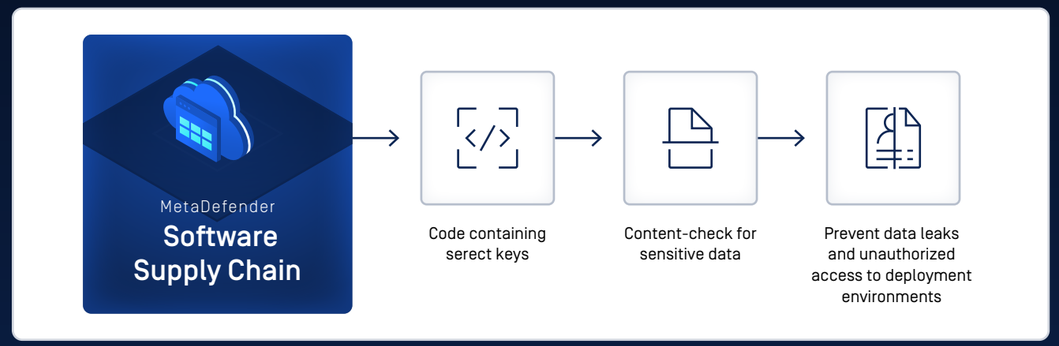
Protect Confidential Information Stored in Data Storage Systems

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).



Test Results

File Type	Average File Size [KB]	Total Files	Sensitive Files	Detection (s/file)		Detection + Redaction (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	314	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

Resource	Windows	Linux
RAM	32GB	32GB
CPU	Intel® Core™ i7-6700 CPU @ 3.40GHz × 8	Intel® Core™ i7-4790 CPU @ 3.60GHz × 8
OS	Windows Server 2019	Ubuntu 20.04.1 LTS
Disk Drive	256GB SSD	256GB SSD
Version	MetaDefender Core v4.19.0 with 8 engines	MetaDefender Core v4.19.0 with 5 engines

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 1,700 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.