OPSWAT.

PRODUCT BROCHURE

MetaDefender for Salesforce

Secure File Uploads for Salesforce

Protect your Salesforce data with automatic file-scans at upload, without slowing down your workflows. OPSWAT's MetaDefender for Salesforce catches known and unknown threats, removes malicious content, and prevents infected files from reaching user or being shared across the system.

No extra steps. No user action required. Just automatic protection where it counts.

MetaDefender for Salesforce is now listed on:

The Salesforce App Exchange Platform

Salesforce Challenges

More than 150,000 businesses use Salesforce, due to undeniable advantages in terms of flexibility, ease-of-use, and accessibility. However, the lack of built-in malware scanning leaves organizations vulnerable to cyberattacks, introduced via file uploads. Here are some of the challenges faced by businesses using Salesforce:

Malware

Salesforce itself doesn't scan uploaded files for malware, which creates an opening for threat actors to embed malware within documents before they are uploaded.

Shared Security Responsibility

Salesforce is responsible for securing the core platform infrastructure, but the responsibility for configuring security settings, managing user access controls, and implementing data protection measures falls squarely on your organization.

Third-Party Application File Upload Vulnerabilities

Security protocols within third-party applications designed for file upload functionality may vary significantly. Unlike Salesforce, some third-party applications might possess weaker defenses against malware or malicious content embedded within uploaded files.

Data Breaches

Data stored in Salesforce usually includes customer information, financial data, and proprietary business processes. A breach can lead to severe consequences, such as financial loss, reputational damage, and regulatory fines.

Benefits

Native Salesforce Integration
Purpose-built for Salesforce, MetaDefender for Salesforce integrates with your system in a few minutes.

Advanced Threat Detection
All files are scanned with up to 15 commercial anti-malware engines, which employ a combination of heuristics, machine learning, and signature-based detection methods. Multiscanning improves detection rates, reduces outbreak exposure times, and achieves a near-zero exposure rate.

Zero-day Threat Prevention
Using our Deep CDR technology, each file is disarmed and regenerated, ensuring only safe, clean and usable content reaches your systems. Deep CDR supports 130+ file types, including PDFs, archives, and most common office documents.

Data Loss Prevention
Prevent potential data leaks and regulatory compliance violations by detecting and blocking sensitive, out-of-policy, and confidential data in files and emails.

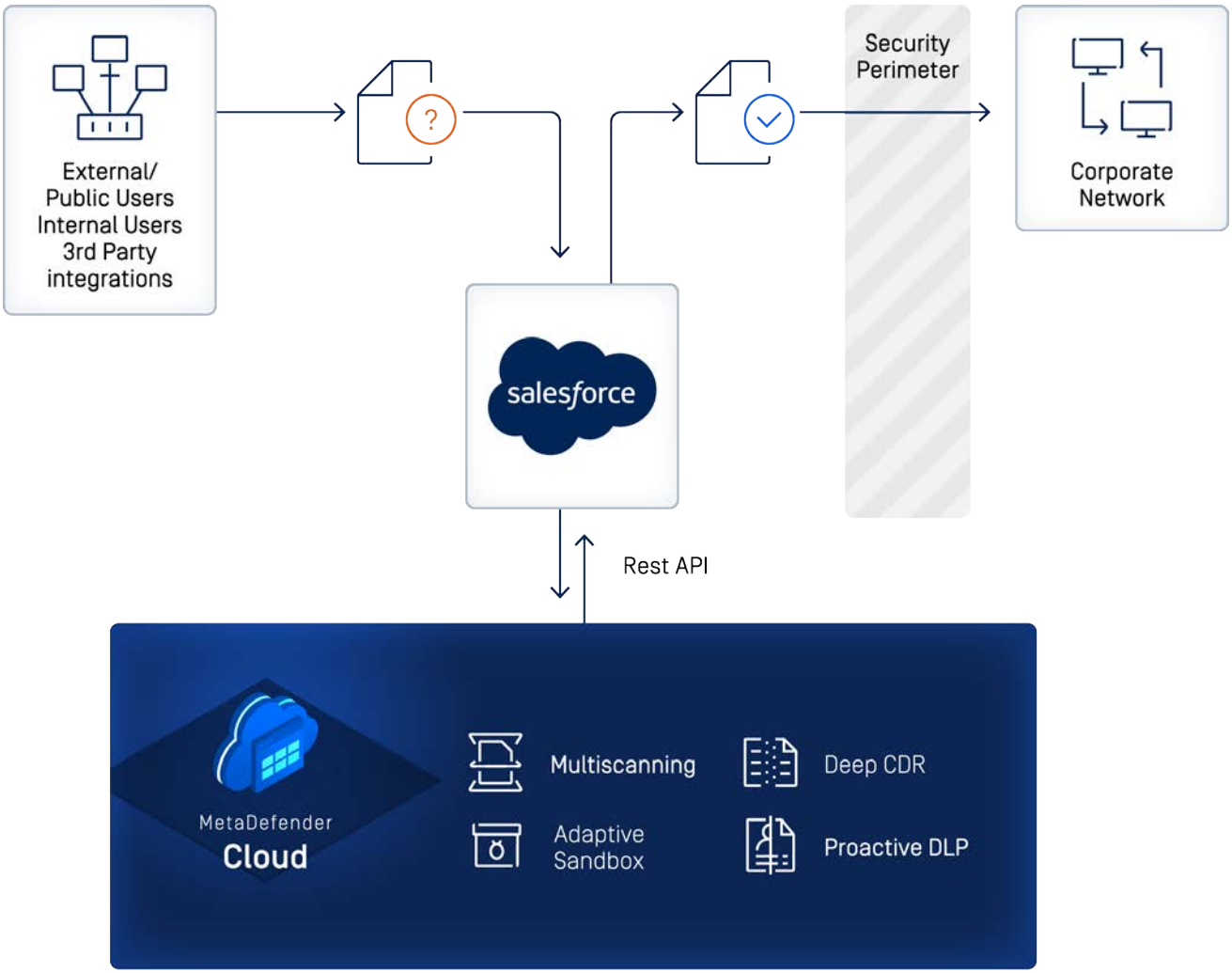
Cloud Scalability
Whether your users upload one file or hundreds, our high-performance cloud architecture allows you to scale to any volume of usage as your requirements change.

Regulatory Compliance
A dynamic dashboard provides complete visibility, real-time reports, and management tools from one interface, which helps meet requirements for PCI DSS, HIPAA, NIST as well as standard audits.

Features

MetaScan®	Uses 30+ leading anti-malware engines to proactively detect over 95% of file-based threats for the highest and earliest detection of malware.
Deep CDR™	Scans, sanitizes, and regenerates over 200 common file types uploaded to the Salesforce environment, ensuring maximum protection against file-based attacks.
Adaptive Sandbox	Detects and analyzes malware by exposing and recording malicious behavior in an emulated environment. The Adaptive Sandbox runs 10x faster and 100x more efficiently than a conventional sandbox.
Proactive DLP™	Detects and blocks sensitive, out-of-policy, and confidential data within files and emails. Supporting over 110+ file types, including Microsoft Office, PDF, CSV, HTML and image files.
Private Scanning	Analyzes user-submitted files without exposing their content. After the analysis, files are deleted from OPSWAT servers.
Large File Scanning	Scans and processes files larger than 10MB.
Rescan on Download	Provides an additional layer of security for users when downloading files.
Rescan on Demand	The option to rescan uploaded files on demand, based on a selected response, providing more control over flagged files or re-checks.
Skip Scanning	A configuration to define what file extensions (based on the file name) can be skipped. Available for certain file types.
Email Body Scanning	Ability to scan the incoming emails within Salesforce.
Advanced File Scan Capabilities	Cover file content, email body text, and attachments, further protecting against malicious content.
Profile-based Security Assessment	Allows administrators to classify profiles and designate files from untrusted profiles for security processing.
Flexible Administration Permissions	Ensure role-based access for additional security.
Infected File Notifications	Sent in-app and via email to ensure administrators are immediately informed of any infected files.
Centralized Control and Visualization Report	Provides a dynamic dashboard with complete visibility, real-time reports, and management tools in one interface.

OPSWAT.



Protect Your Salesforce Data Against File-Borne Threats with MetaDefender for Salesforce

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