OPSWAT.

PRODUCT BROCHURE

Cloud Security for Salesforce

Secure File Uploads for Salesforce

Fortify your Salesforce data with OPSWAT Cloud Security for Salesforce, a cloud-based solution that is designed to complement the native security capabilities of your Salesforce platform. This solution meticulously processes and sanitizes every file before it enters your system, eliminating hidden threats and zero-day malware.

Our application is now listed on

The Salesforce App Exchange Platform

Challenges

Businesses leverage Salesforce to streamline operations and manage vital data. However, file uploads can introduce hidden security risks that threaten the integrity of your information and infrastructure. Here are some challenges that businesses that use Salesforce may face:

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 operates under a shared security model. While they secure the core platform infrastructure, 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

Salesforce data breaches pose a significant challenge due to the sensitive nature of the data stored within the platform. This 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
Integration is easily completed 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 to greatly improve detection rates, reduce outbreak exposure times, and achieve a near-zero exposure rate.

Zero-day Threat Prevention
Disarm potentially malicious and out-of-policy content hidden in files. Our Deep CDR technology regenerates safe, usable files and supports 150+ file types, including PDFs, archives, and most common office documents.

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

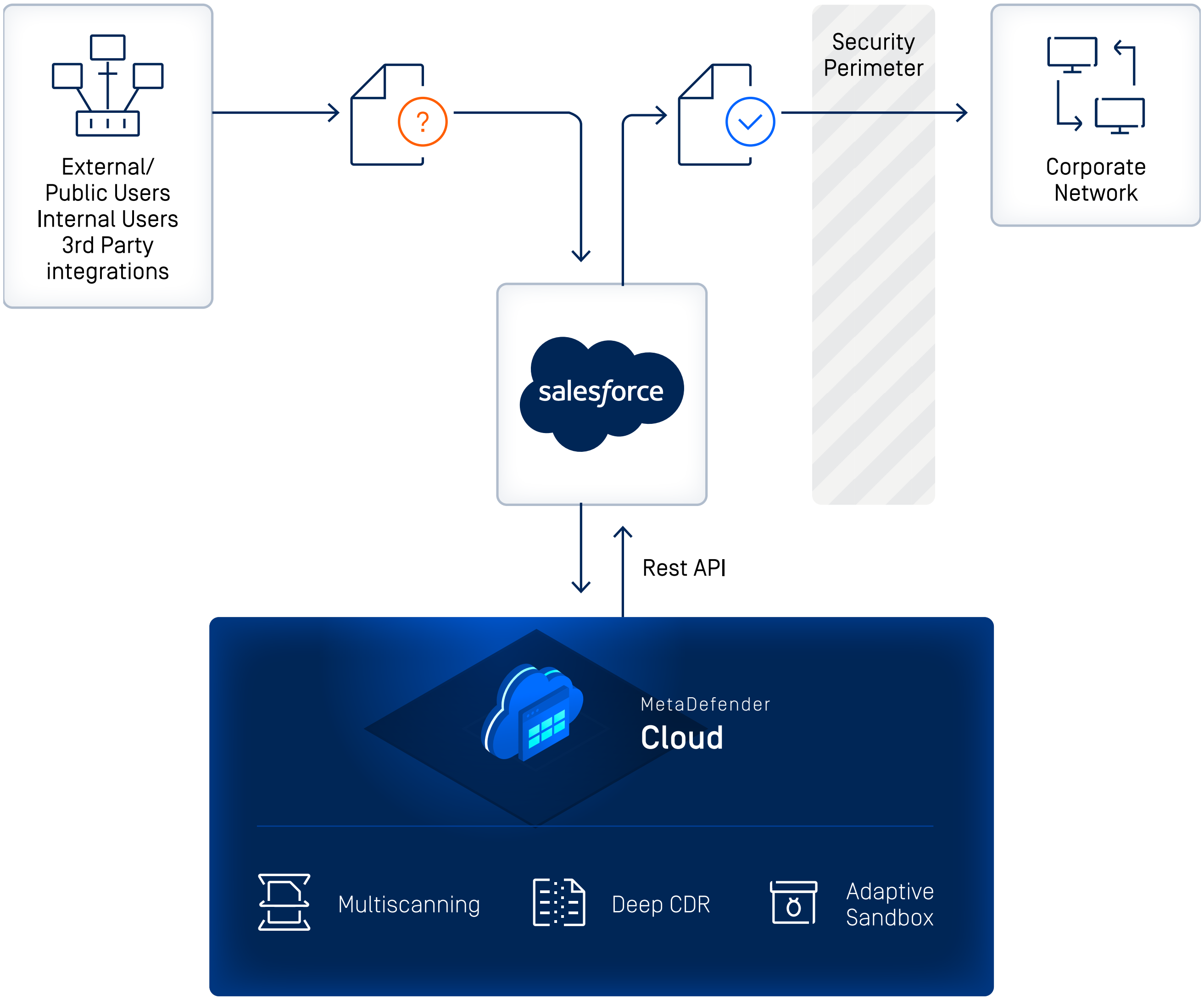
Cloud Scalability
Whether your users are uploading one file or hundreds, our high-performance cloud architecture allows you to scale to any volume of usage as your requirements change.

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 15+ 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 175 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 that 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.
Rescanning on Download	Provides an additional layer of security for users when downloading files.
File Scan Capabilities	Cover file content, email body text, and attachments, further safeguarding 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.



Ready to integrate Cloud Security for Saleforces with 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