OPSWAT.

DATASHEET

Cloud Security for Salesforce

Secure Device and File Access for Salesforce

OPSWAT Cloud Security for Salesforce is a cloud-based security solution designed to complement the native security capabilities of the Salesforce platform. This solution inspects every device for endpoint security policy compliance before granting access to Salesforce. Even when you have remote access and work from home, your Salesforce access will be protected. It also scans and sanitizes every file uploaded to Salesforce to prevent any potentially malicious content from hiding inside the file before it is made available in Salesforce.

This capability is particularly important for any organization that needs to provide outside access to their Salesforce instance for customers, partners, or contractors. There are two modules – one for endpoint compliance and the other for file protection.

Benefits

Prevent Data Breaches from Insecure Devices
OPSWAT provides comprehensive device inspection so you can feel confident that only trusted devices access your Salesforce environment while non-compliant, malware-infected, or vulnerable devices can be blocked.

Audit and Secure Access to Uploaded Documents
Threat detection and file sanitizing capabilities ensure that every file uploaded to Salesforce is scanned by 20+ anti-malware engines and infected files are blocked. The files that users download or wish to upload are sanitized by OPSWAT's industry-leading Deep Content Disarm and Reconstruct (CDR) technology to mitigate the risks of undetected malware or zero-day exploits.

Protect Corporate Data
OPSWAT provides enterprise-wide visibility into all managed or BYOD devices, allowing for easy identification of security and compliance issues for any devices that are used for accessing your confidential data from the cloud.

Meet Compliance Requirements
OPSWAT technologies provide detailed visibility and reporting to help meet requirements for PCI DSS, HIPPA, FINRA, HITECH, NIST, ISO, FTC, COBIT, Sarbanes-Oxley, CIS, and SANS, as well as standard audits.

Native Salesforce Integration, Cloud Scalability
This cloud-based security solution Is designed to complement the native security capabilities of the Salesforce platforms. This application was created to help protect the most challenging Salesforce environments. The end user experience is smooth and non-disruptive.

OPSWAT.

MetaDefender Cloud

Features

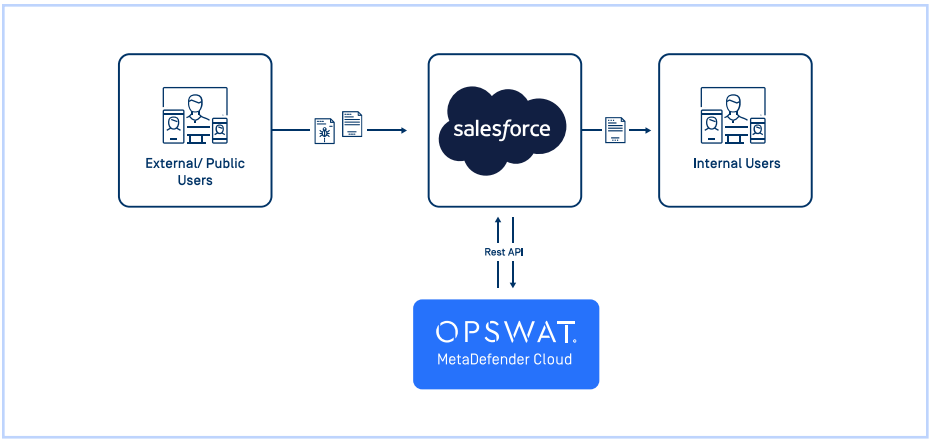
Multiscanning uses 20+ leading anti-malware engines to proactively detect over 99% of file-based threats for the highest and earliest detection of known and unknown threats

Deep Content Disarm and Reconstruction (Deep CDR) technology scans and sanitizes every file uploaded to the Salesforce environment, (supporting over 100 common file types) to ensure maximum protection by securing organizations' Salesforce environment against file-based attacks

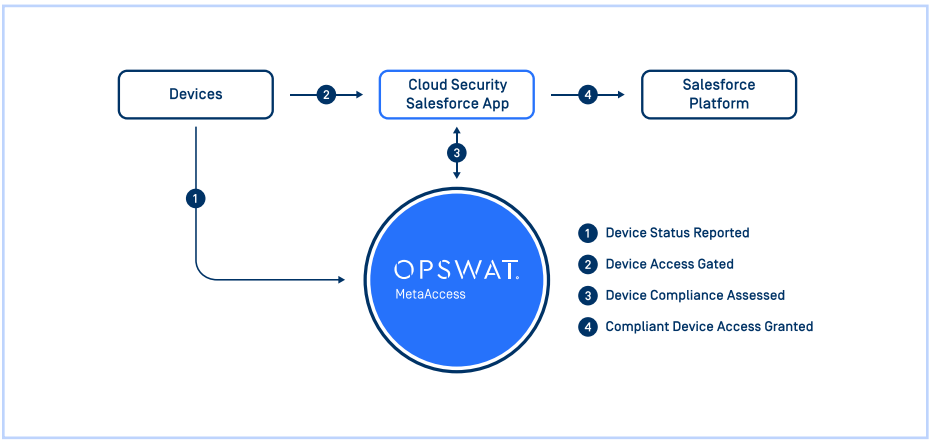
Endpoint Vulnerability Assessment blocks user access to your Salesforce environment until making sure the user's device is compliant, up to date, and malware free

Device Compliance Check operation system and security level including password settings, running firewall, hard drive space availability and custom scripts for unique requirements

Cloud Security for Salesforce – File Scanning



Cloud Security for Salesforce – Endpoint Compliance



Use Cases

File Upload Security
Protect organization's Salesforce environment against malicious file uploads. Salesforce administrators can block or allow file downloads for all users and have control to review and monitor all files uploaded to Salesforce.

Secure Salesforce Access
Protect organizations' Salesforce environment against device access vulnerabilities Salesforce administrators have a holistic dashboard illustrating the activity of devices accessing the Salesforce environment.

Deep CDR
Ensure that even unknown threats are addressed, using technology that removes potentially harmful content.

Automatic & Self-Remediation
Salesforce users get notified on the device compliance remediation steps and can automate and self-remediate to make the device compliant to access the Salesforce environment.

High BYOD Adoption
With remote work and increasing BYOD needs, it's more crucial than ever to protect your organization's Salesforce environment from malware affected devices access and malicious file uploads.

Easy Implementation & Management
Integration with Salesforce greatly eases the implementation, and the SaaS application means minimal maintenance or ongoing efforts.

OPSWAT.

Trust no file. Trust no device.