SOLUTION BRIEF

Netskope for Salesforce

Organizations worldwide use Salesforce and its AppExchange ecosystem to help their employee teams connect more effectively with customers. Netskope protects Salesforce with deep visibility and granular access controls, combined with advanced threat and data protection to help organizations safely use this solution while keeping it secure and compliant.

KEY USE CASES

- **Content audit.** Assess risk by evaluating standard objects in Salesforce against established compliance policies.
- **Advanced data protection.** Prevent public exposure and possible exfiltration of sensitive content, regardless of user type (e.g., employee, contractor, partner).
- **Malware and threat protection.** Detect malicious content in Salesforce and protect users from downloading it. Stop insider threats such as bulk downloads from Salesforce and bulk uploads to different cloud applications.
- **Conditional access control.** Prevent access to corporate instances of Salesforce from unmanaged/personal devices or select risky geographic regions.

"**20%** of users have **sensitive data** moving between cloud apps and 37% of this data **violates DLP policies**"

Netskope Cloud and Threat Report, February 2020

THE CHALLENGE

Salesforce—the leading customer relationship management (CRM) solution—is a pioneering cloud service used by countless sales, service, and marketing teams worldwide. While it's extremely beneficial to users, Salesforce presents new challenges for IT Security Operations (SecOps) teams in identifying, monitoring, and securing the data shared among employees, partners, and contractors within the application.

SecOps and Compliance teams must ensure that sensitive data is accessible only to authorized individuals and that it is not exfiltrated outside the organization, while adhering to compliance mandates. Additionally, these teams must detect and stop threats from penetrating the organization. While Salesforce provides native security controls such as Shield, Netskope complements and extends these security capabilities.

NETSKOPE FOR SALESFORCE

Netskope helps organizations understand and control risky activities in Salesforce while protecting sensitive data and stopping cloud-enabled threats.

Netskope supplies granular visibility and control of access and activities in Salesforce and its AppExchange ecosystem. Providing rich, contextual details regarding Salesforce usage, including users, devices, activities, and data, Netskope protects customer and business data stored in Salesforce using advanced DLP and encryption of structured and unstructured data. With Netskope, organizations can get the most out of Salesforce while staying safe and compliant within or outside of their ecosystem.

CAPABILITIES

ASSESS RISK VIA DEEP VISIBILITY

Netskope offers deep visibility into Salesforce and AppExchange ecosystem applications that share data with Salesforce. View important contextual details about Salesforce usage, including users, devices, and activities, and assess risk by identifying sensitive data in Salesforce and seeing how it is being used and shared. Find all Salesforce instances running in your environment, whether managed and approved by IT or being used by individuals or business units. Conduct real-time queries regarding Salesforce usage and easily create reports for regular security audits and compliance reporting.

To better assess risk across your cloud environment and for applications you may use in the AppExchange ecosystem, Netskope continuously researches and scans cloud apps for vulnerabilities and actively tracks the impact across more than 33,000 cloud services, as catalogued and ranked in its Cloud Confidence Index™ (CCI). Netskope CCI uses over 50 criteria to assess the risk level of cloud apps, which can then be applied to policies (e.g., block access to all apps with a risk level <75). The User Confidence Index (UCI) is assigned based on monitoring user behavior for anomalies and can also be used for policy enforcement (e.g., enforce step-up authentication for risky users scoring <50).

Additionally, the Netskope for Salesforce Compliance Report, installed from within AppExchange, enables administrators to view and understand Netskope discoveries of the enterprise's use of the CRM application without leaving Salesforce.

ADVANCED DATA PROTECTION IN REAL TIME

Discover and control access and exposure of sensitive data in Salesforce with industry-leading, cloud-native data loss prevention (DLP), which accurately detects sensitive content across 1,400+ file types, using 3,000+ predefined data identifiers, metadata extraction, proximity analysis, fingerprinting, exact match, and more. Uncover and protect content in Salesforce to maintain regulatory compliance using 40+ prebuilt templates, such as personally identifiable information (PII), payment card industry data (PCI), and protected health information (PHI), using DLP policies applied to real-time activities, such as uploads and downloads. The Netskope compliance reporting service runs inside Salesforce and provides an integrated, seamless view of activity and alerts within the app.

With Netskope, you gain deep visibility into Salesforce usage and data movement and can prevent sensitive content from leaving your organization.

Additionally, use API-enabled protection to identify and secure sensitive content already stored in Salesforce. Leverage sophisticated activity-level decoding methods to prevent insider threats like data exfiltration from Salesforce to unmanaged cloud services (e.g., Salesforce transfer of a proprietary file to an online file storage service such as Dropbox). SecOps teams can employ machine learning–enhanced capabilities to expedite document and imaging classification and scanning to protect these sensitive files from exfiltration. Examples of these crucial documents include patents, source code, résumés, and tax forms, while images include desktop screenshots, passports, and driver's license IDs. Incident management and remediation workflows help teams quickly respond to any critical events.

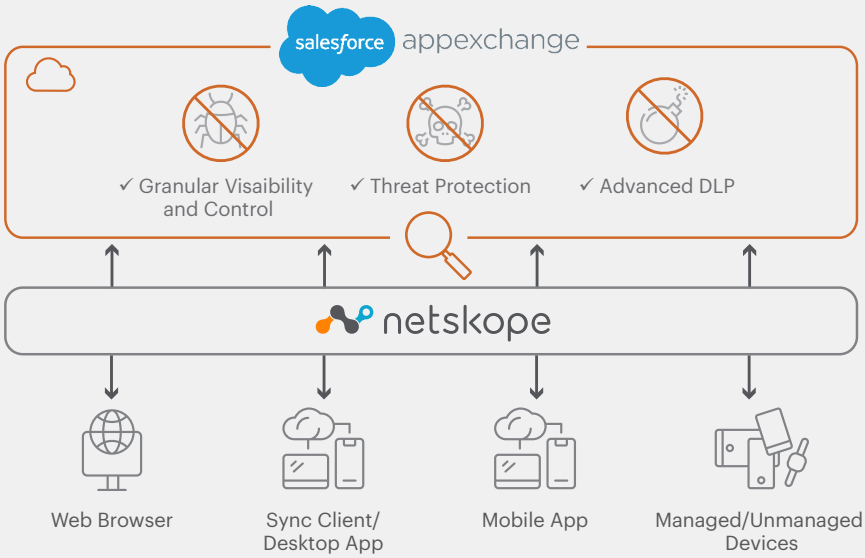

FIGURE 1: Netskope for Salesforce and AppExchange applications

FLEXIBLE OPTIONS FOR ENCRYPTION, TOKENIZATION, AND KEY MANAGEMENT

Encryption and tokenization add another layer of protection for data in Salesforce, and Netskope offers multiple options for this extra protection. To encrypt data at rest in Salesforce while maintaining critical Salesforce functionality—like search and data validation—Netskope can help you "bring your own keys", acting as a key broker and giving you control of your encryption keys for Salesforce Shield native encryption. Netskope also enables the use of function- and format-preserving encryption and tokenization for structured data in Salesforce. For unstructured data in Salesforce, Netskope can automatically and transparently encrypt files with the highest level of AES encryption.

Because Salesforce Shield provides platform encryption and event logging, users can choose which encryption option is best for their environment. Netskope complements and extends the capabilities of Shield with comprehensive visibility and control, as well as consistent data and threat protection across Salesforce, AppExchange, and thousands of other SaaS applications.

COMPREHENSIVE THREAT AND MALWARE PROTECTION

Netskope delivers comprehensive threat defense for Salesforce and the AppExchange ecosystem, with multi-layered threat detection, prevention, and response capabilities. Real-time, inline threat defenses include client traffic exploit protection and advanced malware inspection that quarantines and replaces suspicious files with inert tombstone files Protection against suspicious files is provided via pre-execution analysis and heuristics for 3,500+ file format families, with 3,000+ static binary threat indicators for Windows, Mac OS, Linux, iOS, Android, firmware, Flash, PDF, and other document types. Bare-metal sandboxing for 30+ file types handles executables, scripts, and Microsoft Office documents for Windows OSs further protects your Salesforce environment from elusive threats.

User and entity behavior analytics (UEBA) allow you to baseline your users' normal activities with predefined templates to detect anomalies—even across peer groups—such as bulk uploads, downloads, deletes, failed logins, and rare events. Cloud phishing and cloud-enabled threats are stopped using granular policy controls that enable company instances, while blocking rogue or personal account instances, payloads, and data exfiltration. Machine learning detects anomalies across large sets of metadata, rich with context for cloud services, apps, and web traffic—expediting incident detection and response. Over 40 threat intelligence feeds and the ability to import indicators of compromise (IOCs), including malicious URLs and file hashes, keep your security up to date.

GRANULAR CONTROL OPTIMIZES SECURITY WHILE REDUCING RISK

Netskope applies granular policies to Salesforce, its ecosystem apps, and other cloud applications and services by combining deep cloud context with activity-level control. Beyond simply allowing or blocking unmanaged ecosystem apps that connect to Salesforce, Netskope offers real-time conditional controls that safely enable the applications with specific constraints, while maintaining productivity. For users accessing Salesforce from unmanaged or personal devices or, perhaps, from designated risky geographic regions, you can allow access and viewing of information but block all downloads to prevent sensitive data from leaving your organization. For enterprises maintaining multiple instances of Salesforce, you can define group-level policies to enforce appropriate access for all relevant users. If your employees are using other sales, service, or marketing apps that conflict with Salesforce or are not approved by SecOps, you can let them use these rogue apps, but with limited abilities (e.g., no downloads), and then coach them to use Salesforce through automatic, customizable messages and alerts.

BENEFITS	DESCRIPTION	
DEEP VISIBILITY INTO SALESFORCE USAGE, DATA, AND RISKS	• Follow intuitive audit trails for Salesforce objects for cloud forensic analysis—including user, device, location, app, app instance, activity, and data • Distinguish between different Salesforce instances (i.e., corporate, personal, partner) and optimize usage • Assess risk using ratings for AppExchange and third-party apps (CCI) and users (UCI)	• Enable users to automatically engage with interested customers and prospects via the AppExchange application and view activity and alerts directly in Salesforce, thanks to seamless integration with Netskope
GRANULAR, ACTIVITY-LEVEL CONTROL IN SALESFORCE	• Establish granular policies beyond "allow" and "block" to maintain and enhance business productivity • Create policies based on app and user risk ratings	• Coach end users for security awareness or to enable self-remediation
ADVANCED DATA PROTECTION, INCLUDING OPTIONS FOR ENCRYPTION, TOKENIZATION, AND KEY MANAGEMENT	• Accurately detect sensitive data in Salesforce and the AppExchange ecosystem • Stop data exfiltration from Salesforce to unmanaged cloud services or to unmanaged/personal devices • Respond quickly and effectively with low false positives and closed-loop incident management • Maintain control of encryption keys used for Salesforce Shield native encryption	• Protect structured data in Salesforce with function- and format-preserving encryption and tokenization • Secure unstructured data with AES-256 file encryption • Get machine learning–enhanced protection with optimized document and image scanning and classification
MULTI-LAYERED PROTECTION FOR CLOUD THREATS AND MALWARE	• Gain comprehensive, scalable threat detection and prevention • Use anti-malware engines, client traffic exploit protection, and file type analysis via sandboxing, advanced heuristics, and more methods • Let UEBA detect anomalous activities in Salesforce that could signal a compromised account or insider threats	• Keep security current with 40+ threat intelligence feeds, plus imports of IOCs like malicious URLs and file hashes • Support 350+ families of installers, packers, and compressors with de-obfuscation and recursive file unpacking • Detect unknown threats, anomalies, and behaviors through machine learning deep analysis

CONTACT A NETSKOPE REPRESENTATIVE FOR MORE INFORMATION: https://www.netskope.com/contact-us