

Netskope for Salesforce

Safely cloud-enable your rainmakers

Enterprises of all sizes use Salesforce and its ecosystem to give their teams an edge. With Netskope for Salesforce, you can help your business be more efficient and flexible while you maintain the visibility and security controls you need to protect sensitive data, prevent its loss, and ensure compliance with global regulations.

Understand usage in Salesforce and the AppExchange marketplace

Get visibility into activity and data-level usage details within Salesforce, along with the cloud apps that are part of the Salesforce AppExchange marketplace. This allows you to answer questions like “Who’s sharing sensitive content outside of the company, and with whom?” across any app with a single query. IT can get visibility for security or compliance purposes without disrupting the business.

Features / Benefits

FEATURE	BENEFIT
eDiscover, control, and secure sensitive data stored in Salesforce with industry-leading cloud DLP	Mitigate your security risk by protecting sensitive data
Real-time, granular control of risky activities in Salesforce and AppExchange apps	Allow, don't block. By focusing on identifying specific risky activities and blocking them instead of the app, you can allow safe use of Salesforce and AppExchange apps
Cloud Forensic Analysis	Create an audit trail to help in the investigation of risky activities
Anomaly Detection	Use powerful machine learning to help streamline excessive downloads or shares, logins from multiple locations, or other activities that could signal a security threat
Threat Dashboard	Mitigate your exposure to security risks and potential threats
Data Quarantine	Enable a remediation-centric workflow that helps you mitigate risks, while ensuring impact to users
User Coaching	Make users a part of the solution and not simply a part of the problem

At a glance:

- Prevent loss of sensitive data
- Real-time, granular control of Salesforce and AppExchange marketplace apps
- Understand usage in Salesforce and AppExchange marketplace apps
- Standardize on Salesforce
- Coach users

Standardize on Salesforce

Consolidate redundant instances of Salesforce to save cost, reduce complexity, and encourage collaboration. Discover unsanctioned CRM apps and migrate those users to Salesforce. Use the Netskope Cloud Confidence Index to make data-driven decisions about apps.

Prevent loss of sensitive data using industry-leading Cloud DLP

Netskope inspects real-time activities, such as uploading, downloading, and sharing and can inspect content already resident in Salesforce. IT can find sensitive content using industry-leading DLP with 3,000+ data identifiers, covering 500 file types along with pre-defined profiles, such as PII, PHI, PCI, profanity, and source code.

Cloud forensic analysis

Create a granular cloud activity audit trail following a suspected event such as the theft of sensitive content upon employee departure. IT can reconstruct this activity in the form of a forensic audit trail to understand what that user did with what content in which app, and if they shared the content, with whom they shared it.

Cloud usage anomaly detection

For organizations standardizing on Salesforce, Netskope provides rich detection of activity-level anomalies, such as excessive downloading or sharing from Salesforce, unusually heavy uploads to an unsanctioned app or any app in the Salesforce AppExchange Marketplace, or logins from multiple locations. These usage anomalies can indicate compromised credentials, out-of-compliance behaviors, and even the presence of malware.

Risk Dashboard

Get an at-a-glance view of a variety of factors that contribute to security risks and potential threats. From risky unsanctioned apps that are exchanging data with Salesforce to risky users to risky activities, get a handle on what your potential security risk is when it comes to using Salesforce and AppExchange ecosystem apps. Further evaluate your risk by using the 'Password Breach' visualization to see which users in your environment might be logging into Salesforce or its ecosystem with compromised credentials.

Real-time, granular control of Salesforce and AppExchange apps

Instead of taking a coarse-grained allow vs. block approach, enforce granular policies within Salesforce and AppExchange apps. Apply contextual policies that account for identity, location, activity, and content. For example, "Don't let financial 'insiders' share confidential reports outside of the company." Block risky behavior without blocking apps and protect sensitive content already resident in Salesforce from getting into the wrong hands.

Strong encryption

Netskope for Salesforce provides 256-bit encryption with support for cloud-based, fault-tolerant FIPS 140-2 Level 3 key management with an optional hardware security module or integration with your on-premises, KMIP-compliant key management.

Control access to Salesforce

Netskope provides tight integration with a variety of single sign-on (SSO) vendors in addition to providing built-in device-level access control policies that enable you to restrict access to Salesforce based on whether or not users are using a corporate device. Device-level access control is granular so you can for example restrict certain Salesforce activities to corporate, managed devices.

User coaching

When you enforce policies, it's always a good idea to coach users. That can mean simply letting them know that you've blocked them from an activity because it's against policy. But even more useful is to give them an alternative, such as blocking them from uploading content to an unsanctioned app, and then coaching them with a URL (or simply redirecting them) to sign up for Salesforce.

ANY APP, ANY DEVICE, ANY LOCATION

Allow, Don't Block:

Only Netskope enables you to block the activity, not the app

360° Data Protection:

Only Netskope secures data in sanctioned and unsanctioned apps

Take Action:

Only Netskope enables you to enforce policies in real-time

About Netskope

Netskope is the leader in safe cloud enablement. Only Netskope gives IT the ability to find, understand, and secure sanctioned and unsanctioned cloud apps. With Netskope, organizations can direct usage, protect sensitive data, and ensure compliance in real-time, on any device, including native apps on mobile devices and whether on-premises or remote, and with the broadest range of deployment options in the market. With Netskope, the business can move fast, with confidence. Serving a broad customer base including leading healthcare, financial services, high technology, and retail enterprises, Netskope has been named to CIO Magazine's top 10 cloud security startups and featured in such business media as CBS News, Wall Street Journal, and Forbes.