Data Sheet

Securing Salesforce and Slack Deployments with Zscaler

The adoption of cloud apps has transformed modern organizations. Applications such as Salesforce and Slack have tremendous potential to improve productivity and agility while driving down cost and complexity. That said, the challenge is that your sensitive data has already been transmitted to the Salesforce and Slack cloud and is no longer behind your data center security, which leaves your organization at risk.

With cloud and mobility, your data is exposed and easily accessible over the internet. Additionally, users accessing Salesforce or Slack often expose data through collaboration, with IT lacking the ability to find and control it. Lastly, partner and third-party Party vendors often require access to Salesforce and Slack data from BYOD devices, which exposes your data to additional risk from unmanaged devices.

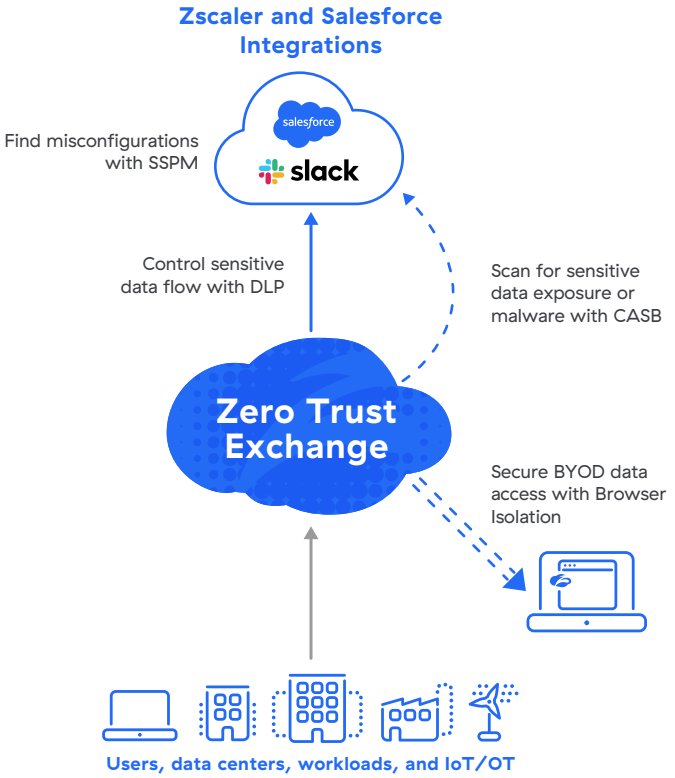
Zscaler with Salesforce and Slack Integration Benefits

- Scan and discover sensitive data and malicious content across your multiple Salesforce and Slack tenants
- Block direct access into Salesforce and Slack by BYOD and securely enable B2B access to data
- Enable secure collaboration of data between disparate teams
- Find and close dangerous misconfigurations across Saleforce deployments
- Intuitive remediation workflows to block malicious and threat activities thereby keeping the Salesforce and Slack tenants safe
- Enforce tenant restrictions to prevent exchange of data between unauthorized tenants

Zscaler + Salesforce and Slack: Securing collaboration to deliver the ultimate customer experience

Protect data with Zscaler CASB and DLP

With Zscaler Data Protection, organizations can secure sensitive data within Salesforce and Slack as well as during upload and download. Zscaler ensures that every content is treated with the same organizational security and compliance policies across all Salesforce and Slack tenants and other SaaS platforms, thus providing detailed and consistent visibility of violations. Security and compliance teams can use standard policies for PCI and PII data to enforce granular control over sensitive data, or leverage custom DLP dictionaries to enforce organizational specific data. Zscaler also helps organizations enforce tenant restriction requirements so data doesn't flow between authorized and unauthorized tenants. Zscaler Data Protection also provides remediation workflows to block the upload of sensitive data files through proactive enforcement.



Stop malware in its tracks with Zscaler Data Protection

Malicious actors are targeting public SaaS applications like Salesforce and Slack to host or upload malware, thus providing a launch pad for malware proliferation. With Zscaler Data Protection, you can scan existing content on the platform as well as content that is being uploaded to Salesforce and Slack tenants currently for malware infection. Zscaler Data Protection also protects organizations from zero-day malware attacks by detonating the payload in Zscaler Sandbox and blocking the malicious spread from infecting your tenants.

Reduce the attack surface by preventing misconfigurations

Misconfigurations within Salesforce and the lenient use of app-native security controls can often create dangerous gaps that can be exploited by internal and external threats. Zscaler SaaS Security Posture Management can provide a gap analysis between the desired and real state of security and platform compliance and provide impact analysis and remediation workflows to address anomalies such as password hygiene, encryption usage, and audit trail management.

Control access across BYOD and unmanaged devices

Unmanaged and BYOD devices are another challenge for today's organizations. Employees, partners, and vendors often have legitimate access to sensitive data in Salesforce and Slack, but downloading this data to unmanaged devices increases risk as control over that data is lost after download. With Zscaler Cloud Browser Isolation, organizations can enable safe access to data by BYOD via an isolated browser. Data is delivered down to the BYOD device only in the form of pixels, so copying, downloading, and printing can be prevented.

zscaler™ | Experience your world, secured.™

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com