



# Cloud Security Engineer

## About Netskope:

Netskope is a fast-growing cloud security company in the Cloud Access Security Broker (CASB) market that provides discovery, visibility, monitoring, granular control and security for both sanctioned AND unsanctioned cloud apps. Many enterprises believe they have a low rate of cloud app adoption or take a "block all cloud app posture." The most recent Netskope Cloud Report indicates an average of 1031 actively used cloud apps per enterprise. Netskope enables IT organizations to discover apps, direct usage, protect sensitive data, defend against threats, and ensure compliance in real-time, on any device, including native apps on mobile devices and whether on-premises "in the enterprise network" or remote "out of network."

Netskope has been featured in The Wall Street Journal, Forbes, and TechCrunch and was recently named a SINET 16 2015 Innovator. The company's technology has been recognized by leading publications including SC Magazine, Security Products Magazine, and CIO. Netskope is headquartered in Los Altos, California. Visit us at [www.netskope.com](http://www.netskope.com) and follow us on Twitter [@Netskope](https://twitter.com/Netskope) and [Facebook](https://www.facebook.com/Netskope).

## Job Duties

Netskope's customers include some of the largest Fortune 500 companies that demand best in class customer support. You will be the primary point of contact for dealing with top class IT administrators.

### In this job you will:

- Be the primary point of contact for all escalations
- Work with customers, Sales Engineers, Customer Success Managers to report issues to engineering
- Regularly communicate status update to customers
- Receive functional, performance and security issues from customers and promptly follow-up with engineering and DevOPS
- Follow published SLA for turning requests around in a timely manner
- Manage customer support portal contents

## Qualifications/Requirements

- 2+ years of experience in supporting enterprise customers
- Prefer to have prior experience in supporting technologies including but not limited to: Proxies, NG Firewalls, SSL/IPSec, VPN's, SSO, DLP and Encryption gateways.





- Demonstrable experience with systems installation, configuration and administration UNIX/Linux and Windows- based systems (prior Active Directory/LDAP experience desirable)
- Knowledge and/or experience in Linux, SSL, HTTP, Layer 4-7
- Familiarity with cloud apps and services
- Excellent communication – strong spoken and written English skills is a must-have

