Netskope + IBM Security QRadar

Seamlessly integrate cloud app usage details and risk metrics into IBM Security QRadar

At a glance:

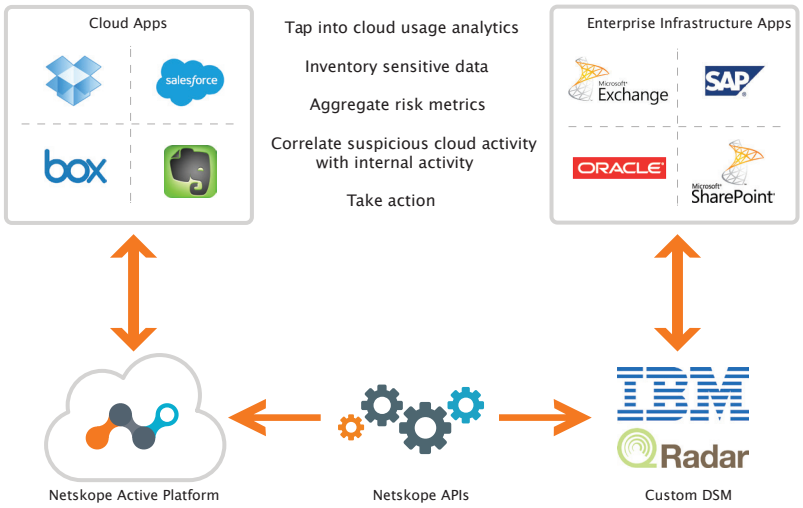
- Understand cloud app usage
- Correlate suspicious cloud activity with internal activity
- Tight integration via QRadar custom DSM and Netskope APIs

IBM Security QRadar SIEM consolidates log source event data from thousands of devices, endpoints and applications distributed throughout a network. The QRadar SIEM solution provides a custom built DSM that seamlessly integrates events generated by the Netskope Active Platform to get a deeper understanding of cloud app usage, sensitive data leakage and key risk metrics. This tight integration between QRadar and Netskope helps customers ensure their move to the cloud is a safe one.

Tap into cloud usage analytics

Bring in details about what cloud apps are discovered, who the users are and what devices they are using to access the cloud apps.

Netskope and QRadar Integration



Aggregate risk metrics

Import risk metrics and get details about specific users, apps and data. From anomalies, to compromised credentials, to apps that have a low enterprise-readiness score to what content has triggered a DLP policy violation, bring this data into QRadar and aggregate into a single view to help assess your risk associated with cloud usage.

Correlate suspicious cloud activity with internal activity

For example, a user bulk uploads documents to an unsanctioned cloud storage application minutes after downloading them from the corporate finance database.

Take action

Understanding cloud usage is the first step to enabling a safe cloud environment. The next step is to take action, and the Netskope Active Platform enables you to perform real-time policy control leveraging what was gleaned from the findings presented in your QRadar dashboards. The final step is to track the effectiveness of your Netskope cloud usage policies by creating a dashboard in QRadar containing what policies have been triggered and what action was taken.

Inventory sensitive data

Find sensitive data stored in sanctioned cloud apps such as Office 365 OneDrive, Box, Google Apps, Dropbox for Business, Salesforce and Egnyte and present an inventory of that data in QRadar.

Summary of IBM QRadar and Netskope Integration

INTEGRATION

- Netskope REST API
- IBM QRadar custom DSM for Netskope

DATA SOURCES

- 10,000+ cloud apps
- Cloud app traffic from users on premises, remote, and mobile
- Data stored (sanctioned apps) and transmitted (all cloud apps)

DATA COLLECTED

- Number of cloud apps, users, and sessions
- Granular cloud usage detail in context of identity, device, app, activity, and data
- Risk data covering users, apps, and data. Includes anomalies, compromised credentials, enterprise-readiness score of discovered apps, and DLP policy violations for data stored and transmitted

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.