DATA SHEET

Last Updated: 12 February 2021

Duo

Duo is a centralized authentication provider for cloud applications that supports two-factor authentication and device management. Obsidian provides an additional layer of monitoring to detect suspicious user logins, account settings, and provisioning practices.

CONNECT

Supported Duo subscription levels

- Duo MFA
- Duo Access
- Duo Beyond

* Within the Admin API the Endpoints data is available for Duo Beyond subscriptions only.

Privileges requested for Duo

Data type	Privilege level
Grant administrators	read, write, delete
Grant read log	read only
Grant read resource	read only
Grant settings	read & write

API

Frequency of Duo API calls

Activity Data every 10 minutes

State Data every 24 hours

Duo APIs connected

- Events API
- Audit Logs API
- SCIM API
- Web API
- Admin API

Duo API rate limit

Duo's rate limit

Duo doesn't have generic rate limit rules

Obsidian's rate limit etiquette

Obsidian does not generate traffic that triggers Duo's rate limits.

DATA SHEET

DATA

Data Collection - Activity data

- authentication log events
- administrator log events
- telephony log events

Data Collection - State data

- users
- admins
- groups
- settings
- integrations
- tokens

How quickly will data become available?

ingestion takes from 5 mins - 4 hours

Days of historical data available on day 1

Activity data: 30 days

State data: 30 days

Data availability for active customers

Accessible via our UI: 90 days of cleansed state and activity data; alert data from the date you last onboarded

Archival data, inaccessible via UI or API: Raw state and activity data from the date you last onboarded; subject to truncation at any time

Obsidian standard data retention

90 days, subject to contract terms

DETECTION

Anomaly detection

Time to detection - Obsidian custom alerts

- 2 - 8 weeks depending on alert type

Obsidian custom alerts target

- Account compromise
- Anomaly detection
- Brute force attacks
- Security hygiene

Security alerts

- **Disallowed logins** - Duo prevents authentications from anonymous IP addresses, devices without disk encryption, tampered devices, login attempts flagged as fraudulent by end-users, and unapproved operating systems which are pulled forward into Obsidian's UI and our data science environment
- **Anomalous behavior** - logins using Tor, bad IPs, untrustworthy locations and out-of-band behavior trigger alerts
- **Configurations and compliance** - Duo configurations and usage inform Obsidian's compliance dashboards (coming soon).

TRUST

Why does Obsidian need these privileges?

In order to pull back the data required to enumerate configurations, gain access to repository activity, and read user information including user privileges, Obsidian requires the specific privileges outlined here. These privileges may give us access to more data than we use or store.