vorlon

WHITE PAPER

Rapid Response Breach Playbook - Snowflake

snowflake®

Summary of Breach

In May 2024, Snowflake became aware of unauthorized access to some of its customer accounts, with threat-related activity going back to mid-April 2025. Snowflake states that the unauthorized access likely stemmed from leaked customer credentials not a vulnerability in the platform. However, there are a number of preventive measures their customers can take if they are still concerned.

Investigation Steps

Identify Any Malicious/Unauthorized Access and Sessions

1. Log into Snowflake.
2. Create to a new worksheet and name it accordingly.
3. Run the following query to list any usernames that have attempted a login from one of the suspicious IP addresses.

```
SELECT DISTINCT USER_NAME FROM snowflake.account_usage.login_history
WHERE client_ip IN (
'104.223.91.28',
'198.54.135.99',
'184.147.100.29',
'146.70.117.210',
'198.54.130.153',
'169.150.203.22',
'185.156.46.163',
'146.70.171.99',
'206.217.206.108',
```

‘45.86.221.146’,
‘193.32.126.233’,
‘87.249.134.11’,
‘66.115.189.247’,
‘104.129.24.124’,
‘146.70.171.112’,
‘198.54.135.67’,
‘146.70.124.216’,
‘45.134.142.200’,
‘206.217.205.49’,
‘146.70.117.56’,
‘169.150.201.25’,
‘66.63.167.147’,
‘194.230.144.126’,
‘146.70.165.227’,
‘154.47.30.137’,
‘154.47.30.150’,
‘96.44.191.140’,
‘146.70.166.176’,
‘198.44.136.56’,
‘176.123.6.193’,
‘192.252.212.60’,
‘173.44.63.112’,
‘37.19.210.34’,
‘37.19.210.21’,
‘185.213.155.241’,
‘198.44.136.82’,
‘93.115.0.49’,
‘204.152.216.105’,
‘198.44.129.82’,
‘185.248.85.59’,
‘198.54.131.152’,
‘102.165.16.161’,
‘185.156.46.144’,
‘45.134.140.144’,
‘198.54.135.35’,
‘176.123.3.132’,
‘185.248.85.14’,

‘169.150.223.208’,
‘162.33.177.32’,
‘194.230.145.67’,
‘5.47.87.202’,
‘194.230.160.5’,
‘194.230.147.127’,
‘176.220.186.152’,
‘194.230.160.237’,
‘194.230.158.178’,
‘194.230.145.76’,
‘45.155.91.99’,
‘194.230.158.107’,
‘194.230.148.99’,
‘194.230.144.50’,
‘185.204.1.178’,
‘79.127.217.44’,
‘104.129.24.115’,
‘146.70.119.24’,
‘138.199.34.144’,
‘198.44.136.35’,
‘66.115.189.210’,
‘206.217.206.88’,
‘37.19.210.28’,
‘146.70.225.67’,
‘138.199.43.92’,
‘149.102.246.3’,
‘43.225.189.163’,
‘185.201.188.34’,
‘178.249.209.163’,
‘199.116.118.210’,
‘198.54.130.147’,
‘156.59.50.195’,
‘198.44.136.195’,
‘198.44.129.67’,
‘37.19.221.170’,
‘96.44.189.99’,
‘146.70.134.3’,
‘66.115.189.200’,

‘103.75.11.51’,
‘69.4.234.118’,
‘146.70.173.195’,
‘138.199.60.29’,
‘66.115.189.160’,
‘154.47.30.144’,
‘178.249.211.80’,
‘143.244.47.92’,
‘146.70.132.227’,
‘193.19.207.226’,
‘46.19.136.227’,
‘68.235.44.35’,
‘103.136.147.4’,
‘198.54.133.163’,
‘169.150.203.16’,
‘146.70.224.3’,
‘87.249.134.15’,
‘198.54.134.131’,
‘142.147.89.226’,
‘146.70.117.35’,
‘193.19.207.196’,
‘146.70.144.35’,
‘146.70.173.131’,
‘107.150.22.3’,
‘169.150.201.29’,
‘146.70.117.163’,
‘146.70.138.195’,
‘146.70.184.67’,
‘104.129.57.67’,
‘185.248.85.49’,
‘146.70.168.67’,
‘138.199.43.66’,
‘79.127.217.35’,
‘194.127.167.108’,
‘194.36.25.49’,
‘146.70.171.67’,
‘138.199.60.3’,
‘45.134.212.93’,

‘146.70.187.67’,
‘66.63.167.163’,
‘154.47.29.3’,
‘149.102.246.16’,
‘198.44.129.99’,
‘146.70.128.195’,
‘185.65.134.191’,
‘146.70.119.35’,
‘87.249.134.28’,
‘149.102.240.67’,
‘103.75.11.67’,
‘69.4.234.124’,
‘169.150.196.3’,
‘169.150.201.3’,
‘185.188.61.196’,
‘87.249.134.2’,
‘138.199.15.163’,
‘45.134.213.195’,
‘138.199.6.208’,
‘169.150.227.223’,
‘146.70.200.3’,
‘149.88.22.156’,
‘173.205.85.35’,
‘206.217.206.48’,
‘194.36.25.4’,
‘154.47.16.48’,
‘37.19.200.131’,
‘146.70.166.131’,
‘37.19.221.144’,
‘149.88.20.207’,
‘79.127.222.195’,
‘194.127.167.88’,
‘96.44.191.131’,
‘69.4.234.119’,
‘138.199.6.221’,
‘146.70.128.227’,
‘66.63.167.195’,
‘169.150.196.16’,

‘185.201.188.4’,
‘173.44.63.67’,
‘79.127.222.208’,
‘198.54.134.99’,
‘198.54.135.131’,
‘138.199.43.79’,
‘66.115.189.190’,
‘149.88.20.194’,
‘141.98.252.190’,
‘129.227.46.163’,
‘31.171.154.51’,
‘79.127.217.48’,
‘69.4.234.116’,
‘206.217.206.68’,
‘103.125.233.19’,
‘146.70.188.131’,
‘169.150.227.198’,
‘129.227.46.131’,
‘198.44.136.99’,
‘149.88.22.130’,
‘193.138.7.138’,
‘146.70.168.195’,
‘169.150.203.29’,
‘206.217.205.118’,
‘146.70.185.3’,
‘146.70.124.131’,
‘194.127.199.32’,
‘149.102.240.80’,
‘143.244.47.79’,
‘178.255.149.166’,
‘188.241.176.195’,
‘69.4.234.125’,
‘138.199.21.240’,
‘45.134.79.98’,
‘178.249.209.176’,
‘68.235.44.3’,
‘198.54.133.131’,
‘193.138.7.158’,

‘154.47.30.131’,
‘204.152.216.115’,
‘206.217.205.125’,
‘37.19.200.144’,
‘146.70.171.131’,
‘198.54.130.99’,
‘149.22.81.208’,
‘146.70.197.131’,
‘198.54.131.131’,
‘138.199.15.147’,
‘185.248.85.34’,
‘143.244.47.66’,
‘92.60.40.225’,
‘178.249.214.3’,
‘146.70.133.3’,
‘179.43.189.67’,
‘69.4.234.120’,
‘146.70.199.195’,
‘185.156.46.157’,
‘45.134.142.194’,
‘68.235.44.195’,
‘209.54.101.131’,
‘104.129.41.195’,
‘146.70.225.3’,
‘206.217.205.126’,
‘103.136.147.130’,
‘194.110.115.3’,
‘178.249.211.93’,
‘185.188.61.226’,
‘194.110.115.35’,
‘146.70.198.195’,
‘169.150.198.67’,
‘103.108.229.67’,
‘138.199.60.16’,
‘96.44.191.147’,
‘31.170.22.16’,
‘45.134.140.131’,
‘169.150.196.29’,

‘103.216.220.19’,
‘173.205.93.3’,
‘146.70.199.131’,
‘103.214.20.131’,
‘149.88.22.143’,
‘149.40.50.113’,
‘138.199.21.227’,
‘138.199.6.195’,
‘103.216.220.35’,
‘198.44.136.67’,
‘199.116.118.194’,
‘146.70.129.131’,
‘199.116.118.233’,
‘146.70.184.3’,
‘185.254.75.14’,
‘38.240.225.69’,
‘149.22.81.195’,
‘43.225.189.132’,
‘45.134.142.207’,
‘146.70.196.195’,
‘198.44.140.195’,
‘206.217.205.119’,
‘38.240.225.37’,
‘169.150.227.211’,
‘37.19.200.157’,
‘146.70.132.195’,
‘146.70.211.67’,
‘206.217.206.28’,
‘178.249.214.16’,
‘149.88.22.169’,
‘149.88.104.16’,
‘194.36.25.34’,
‘146.70.197.195’,
‘45.134.212.80’,
‘156.59.50.227’,
‘104.223.91.19’,
‘198.54.130.131’,
‘185.248.85.19’,

```
'45.134.79.68',
'45.134.142.220',
'185.204.1.179',
'146.70.129.99',
'146.70.133.99',
'69.4.234.122',
'178.249.211.67',
'198.54.131.163',
'198.44.129.35',
'103.108.231.51',
'146.70.165.3',
'37.19.221.157',
'92.60.40.210',
'154.47.16.35',
'194.127.199.3',
'37.19.210.2',
'103.108.231.67',
'204.152.216.99',
'176.123.7.143',
'176.123.10.35',
'195.160.223.23' )
```

For any results, assess the username and decide whether to disable the user account.
To disable the user account simply run:

```
set user_name = "SUSPECTED_USER";
ALTER USER IDENTIFIER($user_name) SET DISABLED = TRUE
```

Alternatively, you could automatically disable any users by utilising the above query and passing the results directly into the ALTER USER by:

```
BEGIN
  FOR row IN (
    SELECT DISTINCT USER_NAME FROM snowflake.account_usage.login_history
                WHERE client_ip IN (
                        '104.223.91.28',
                        '198.54.135.99',
                        '184.147.100.29',
                        '146.70.117.210',
                        '198.54.130.153',
                        '169.150.203.22',
                        '185.156.46.163',
                        '146.70.171.99',
                        '206.217.206.108',
                        '45.86.221.146',
                        '193.32.126.233',
                        '87.249.134.11',
                        '66.115.189.247',
                        '104.129.24.124',
                        '146.70.171.112',
                        '198.54.135.67',
                        '146.70.124.216',
                        '45.134.142.200',
                        '206.217.205.49',
                        '146.70.117.56',
                        '169.150.201.25',
                        '66.63.167.147',
                        '194.230.144.126',
                        '146.70.165.227',
                        '154.47.30.137',
                        '154.47.30.150',
                        '96.44.191.140',
                        '146.70.166.176',
                        '198.44.136.56',
                        '176.123.6.193',
                        '192.252.212.60',
```

‘173.44.63.112’,
‘37.19.210.34’,
‘37.19.210.21’,
‘185.213.155.241’,
‘198.44.136.82’,
‘93.115.0.49’,
‘204.152.216.105’,
‘198.44.129.82’,
‘185.248.85.59’,
‘198.54.131.152’,
‘102.165.16.161’,
‘185.156.46.144’,
‘45.134.140.144’,
‘198.54.135.35’,
‘176.123.3.132’,
‘185.248.85.14’,
‘169.150.223.208’,
‘162.33.177.32’,
‘194.230.145.67’,
‘5.47.87.202’,
‘194.230.160.5’,
‘194.230.147.127’,
‘176.220.186.152’,
‘194.230.160.237’,
‘194.230.158.178’,
‘194.230.145.76’,
‘45.155.91.99’,
‘194.230.158.107’,
‘194.230.148.99’,
‘194.230.144.50’,
‘185.204.1.178’,
‘79.127.217.44’,
‘104.129.24.115’,
‘146.70.119.24’,
‘138.199.34.144’,
‘198.44.136.35’,
‘66.115.189.210’,
‘206.217.206.88’,

‘37.19.210.28’,
‘146.70.225.67’,
‘138.199.43.92’,
‘149.102.246.3’,
‘43.225.189.163’,
‘185.201.188.34’,
‘178.249.209.163’,
‘199.116.118.210’,
‘198.54.130.147’,
‘156.59.50.195’,
‘198.44.136.195’,
‘198.44.129.67’,
‘37.19.221.170’,
‘96.44.189.99’,
‘146.70.134.3’,
‘66.115.189.200’,
‘103.75.11.51’,
‘69.4.234.118’,
‘146.70.173.195’,
‘138.199.60.29’,
‘66.115.189.160’,
‘154.47.30.144’,
‘178.249.211.80’,
‘143.244.47.92’,
‘146.70.132.227’,
‘193.19.207.226’,
‘46.19.136.227’,
‘68.235.44.35’,
‘103.136.147.4’,
‘198.54.133.163’,
‘169.150.203.16’,
‘146.70.224.3’,
‘87.249.134.15’,
‘198.54.134.131’,
‘142.147.89.226’,
‘146.70.117.35’,
‘193.19.207.196’,
‘146.70.144.35’,

‘146.70.173.131’,
‘107.150.22.3’,
‘169.150.201.29’,
‘146.70.117.163’,
‘146.70.138.195’,
‘146.70.184.67’,
‘104.129.57.67’,
‘185.248.85.49’,
‘146.70.168.67’,
‘138.199.43.66’,
‘79.127.217.35’,
‘194.127.167.108’,
‘194.36.25.49’,
‘146.70.171.67’,
‘138.199.60.3’,
‘45.134.212.93’,
‘146.70.187.67’,
‘66.63.167.163’,
‘154.47.29.3’,
‘149.102.246.16’,
‘198.44.129.99’,
‘146.70.128.195’,
‘185.65.134.191’,
‘146.70.119.35’,
‘87.249.134.28’,
‘149.102.240.67’,
‘103.75.11.67’,
‘69.4.234.124’,
‘169.150.196.3’,
‘169.150.201.3’,
‘185.188.61.196’,
‘87.249.134.2’,
‘138.199.15.163’,
‘45.134.213.195’,
‘138.199.6.208’,
‘169.150.227.223’,
‘146.70.200.3’,
‘149.88.22.156’,

‘173.205.85.35’,
‘206.217.206.48’,
‘194.36.25.4’,
‘154.47.16.48’,
‘37.19.200.131’,
‘146.70.166.131’,
‘37.19.221.144’,
‘149.88.20.207’,
‘79.127.222.195’,
‘194.127.167.88’,
‘96.44.191.131’,
‘69.4.234.119’,
‘138.199.6.221’,
‘146.70.128.227’,
‘66.63.167.195’,
‘169.150.196.16’,
‘185.201.188.4’,
‘173.44.63.67’,
‘79.127.222.208’,
‘198.54.134.99’,
‘198.54.135.131’,
‘138.199.43.79’,
‘66.115.189.190’,
‘149.88.20.194’,
‘141.98.252.190’,
‘129.227.46.163’,
‘31.171.154.51’,
‘79.127.217.48’,
‘69.4.234.116’,
‘206.217.206.68’,
‘103.125.233.19’,
‘146.70.188.131’,
‘169.150.227.198’,
‘129.227.46.131’,
‘198.44.136.99’,
‘149.88.22.130’,
‘193.138.7.138’,
‘146.70.168.195’,

‘169.150.203.29’,
‘206.217.205.118’,
‘146.70.185.3’,
‘146.70.124.131’,
‘194.127.199.32’,
‘149.102.240.80’,
‘143.244.47.79’,
‘178.255.149.166’,
‘188.241.176.195’,
‘69.4.234.125’,
‘138.199.21.240’,
‘45.134.79.98’,
‘178.249.209.176’,
‘68.235.44.3’,
‘198.54.133.131’,
‘193.138.7.158’,
‘154.47.30.131’,
‘204.152.216.115’,
‘206.217.205.125’,
‘37.19.200.144’,
‘146.70.171.131’,
‘198.54.130.99’,
‘149.22.81.208’,
‘146.70.197.131’,
‘198.54.131.131’,
‘138.199.15.147’,
‘185.248.85.34’,
‘143.244.47.66’,
‘92.60.40.225’,
‘178.249.214.3’,
‘146.70.133.3’,
‘179.43.189.67’,
‘69.4.234.120’,
‘146.70.199.195’,
‘185.156.46.157’,
‘45.134.142.194’,
‘68.235.44.195’,
‘209.54.101.131’,

‘104.129.41.195’,
‘146.70.225.3’,
‘206.217.205.126’,
‘103.136.147.130’,
‘194.110.115.3’,
‘178.249.211.93’,
‘185.188.61.226’,
‘194.110.115.35’,
‘146.70.198.195’,
‘169.150.198.67’,
‘103.108.229.67’,
‘138.199.60.16’,
‘96.44.191.147’,
‘31.170.22.16’,
‘45.134.140.131’,
‘169.150.196.29’,
‘103.216.220.19’,
‘173.205.93.3’,
‘146.70.199.131’,
‘103.214.20.131’,
‘149.88.22.143’,
‘149.40.50.113’,
‘138.199.21.227’,
‘138.199.6.195’,
‘103.216.220.35’,
‘198.44.136.67’,
‘199.116.118.194’,
‘146.70.129.131’,
‘199.116.118.233’,
‘146.70.184.3’,
‘185.254.75.14’,
‘38.240.225.69’,
‘149.22.81.195’,
‘43.225.189.132’,
‘45.134.142.207’,
‘146.70.196.195’,
‘198.44.140.195’,
‘206.217.205.119’,

```
        '38.240.225.37',
        '169.150.227.211',
        '37.19.200.157',
        '146.70.132.195',
        '146.70.211.67',
        '206.217.206.28',
        '178.249.214.16',
        '149.88.22.169',
        '149.88.104.16',
        '194.36.25.34',
        '146.70.197.195',
        '45.134.212.80',
        '156.59.50.227',
        '104.223.91.19',
        '198.54.130.131',
        '185.248.85.19',
        '45.134.79.68',
        '45.134.142.220',
        '185.204.1.179',
        '146.70.129.99',
        '146.70.133.99',
        '69.4.234.122',
        '178.249.211.67',
        '198.54.131.163',
        '198.44.129.35',
        '103.108.231.51',
        '146.70.165.3',
        '37.19.221.157',
        '92.60.40.210',
        '154.47.16.35',
        '194.127.199.3',
        '37.19.210.2',
        '103.108.231.67',
        '204.152.216.99',
        '176.123.7.143',
        '176.123.10.35',
        '195.160.223.23')
)
```

```
    DO
        EXECUTE IMMEDIATE 'ALTER USER ' || row.USER_NAME || ' SET DISABLED =
TRUE';
    END FOR;
END;
```

4. Run the following query to identify access from any of the two suspicious clients provided by Snowflake:

```
SELECT * FROM snowflake.account_usage.sessions
WHERE PARSE_JSON(CLIENT_ENVIRONMENT):APPLICATION = 'rapeflake'
OR (
            PARSE_JSON(CLIENT_ENVIRONMENT):APPLICATION = 'DBeaver_DBeaverUltimate'
    AND
    PARSE_JSON(CLIENT_ENVIRONMENT):OS = 'Windows Server 2022'
    )
```

If any of the queries above return any user accounts that may be suspicious, the following query can be used to disable them:

```
set user_name = "SUSPECTED_USER";
ALTER USER IDENTIFIER($user_name) SET DISABLED = TRUE
```

Alternatively, run the following query to automatically disable any user that had made a call using the suspicious client app names:

```
BEGIN
  FOR row IN (
                SELECT * FROM snowflake.account_usage.sessions
                WHERE PARSE_JSON(CLIENT_ENVIRONMENT):APPLICATION = 'rapeflake'
                OR (
                        PARSE_JSON(CLIENT_ENVIRONMENT):APPLICATION = 'DBeaver_
DBeaverUltimate'
                  AND
                  PARSE_JSON(CLIENT_ENVIRONMENT):OS = 'Windows Server 2022'
                  )
                )
  DO
    EXECUTE IMMEDIATE 'ALTER USER ' || row.USER_NAME || ' SET DISABLED = TRUE';
  END FOR;
END;
```

***Disabling a user will abort all queries and SQL statements currently running or scheduled by the user. All existing sessions for the user are also closed and the user will not be able to log into Snowflake anymore.

Investigate Actions Taken by Suspected Users

1. Log into Snowflake.
2. For each user name in which a login was identified from one of the suspicious IP addresses, run the following replacing the 'SUSPECTED_USER' with the user name found in the results from step 3 and 4 above.

```
set u_name = 'SUSPECTED_USER';
set s_time = '2024-04-01';
set e_time = CURRENT_TIMESTAMP;

SELECT * FROM snowflake.account_usage.query_history
WHERE user_name = $u_name
AND start_time BETWEEN $s_time
AND $e_time
ORDER BY start_time;
```

3. Using the results from step 2 above, replace the QUERY_ID and execute:

```
set q_id = 'QUERY_ID';
set s_time = '2024-04-01';
set e_time = CURRENT_TIMESTAMP;

SELECT
   *
FROM snowflake.account_usage.external_access_history e
   join snowflake.account_usage.query_history q on e.query_id = q.query_id
WHERE q.query_id = $q_id
AND start_time BETWEEN $s_time
AND $e_time
ORDER BY start_time;
```

4. Run the following query and review any sessions for unusual applications:

```
SELECT COUNT(*) AS client_app_count, PARSE_JSON(client_environment) :APPLICATION
:: STRING AS client_application, PARSE_JSON(client_environment) :OS :: STRING AS
client_os, PARSE_JSON(client_environment) :OS_VERSION :: STRING AS client_os_version
FROM snowflake.account_usage.sessions sessions
WHERE 1 = 1
AND sessions.created_on >= '2024-04-01'
GROUP BY ALL
ORDER BY 1 ASC;
```

Best Practices for Security Hygiene in Snowflake

- Restrict user accounts and app integrations in Snowflake to the least privileged access.
- Periodically review user accounts for inactivity; cross-reference user accounts in Snowflake with your IAM platform to ensure terminated users have their access removed.
- Use key pair authentication or OAuth (client credentials grant) instead of static passwords for service accounts.
    - Execute the following to find inactive user accounts:

```
SELECT name AS username, login_name, email, created_on, last_success_login
FROM TABLE(SNOWFLAKE.ACCOUNT_USAGE.USERS)
WHERE login_disabled = TRUE;
```

- Set up account-level and user-level network policies for admin users.
    - Run this query.
- Go through existing accounts and restrict how data can be exported by executing:

```
alter account set PREVENT_UNLOAD_TO_INLINE_URL = true;
alter account set REQUIRE_STORAGE_INTEGRATION_FOR_STAGE_CREATION = true;
alter account set REQUIRE_STORAGE_INTEGRATION_FOR_STAGE_OPERATION = true;
alter account set PREVENT_UNLOAD_TO_INTERNAL_STAGES = true;
```

- Review accounts for unauthorized privilege escalation or configuration changes after running this query:

```
select user_name || ' granted the ' || role_name || ' role on ' || end_time ||' [' || query_text ||']'
as Grants
  from query_history where execution_status = 'SUCCESS'
```

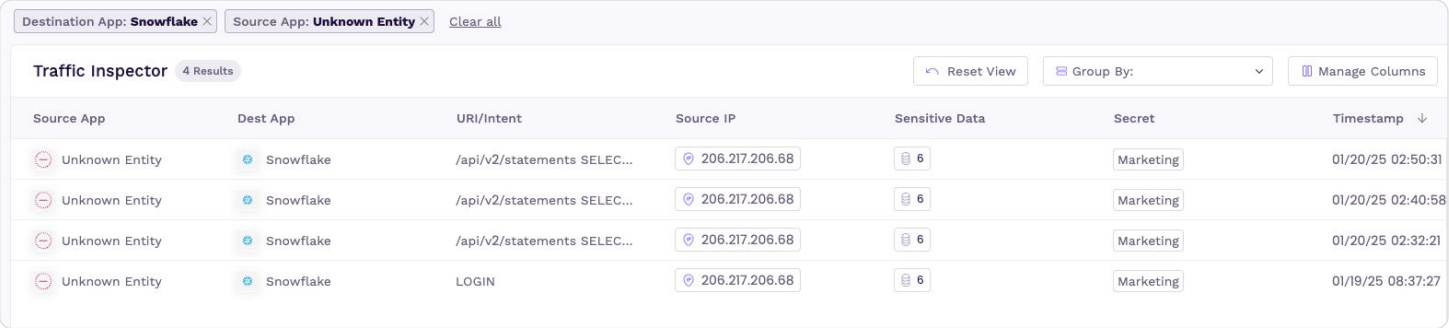
```
  and query_type = 'GRANT' and
  query_text ilike '%grant%accountadmin%to%'
  order by end_time desc;

//Example query to detect unauthorized change management/ security anomalies
SELECT
   query_text,
   user_name,
   role_name,
   start_time,
   end_time
 FROM snowflake.account_usage.query_history
   WHERE execution_status = 'SUCCESS'
     AND query_type NOT in ('SELECT')
     AND (query_text ILIKE '%create role%'
        OR query_text ILIKE '%manage grants%'
        OR query_text ILIKE '%create integration%'
        OR query_text ILIKE '%alter integration%'
        OR query_text ILIKE '%create share%'
        OR query_text ILIKE '%create account%'
        OR query_text ILIKE '%monitor usage%'
        OR query_text ILIKE '%ownership%'
        OR query_text ILIKE '%drop table%'
        OR query_text ILIKE '%drop database%'
        OR query_text ILIKE '%create stage%'
        OR query_text ILIKE '%drop stage%'
        OR query_text ILIKE '%alter stage%'
        OR query_text ILIKE '%create user%'
        OR query_text ILIKE '%alter user%'
        OR query_text ILIKE '%drop user%'
        OR query_text ILIKE '%create_network_policy%'
        OR query_text ILIKE '%alter_network_policy%'
        OR query_text ILIKE '%drop_network_policy%'
        OR query_text ILIKE '%copy%'
        )
 ORDER BY end_time desc;
```

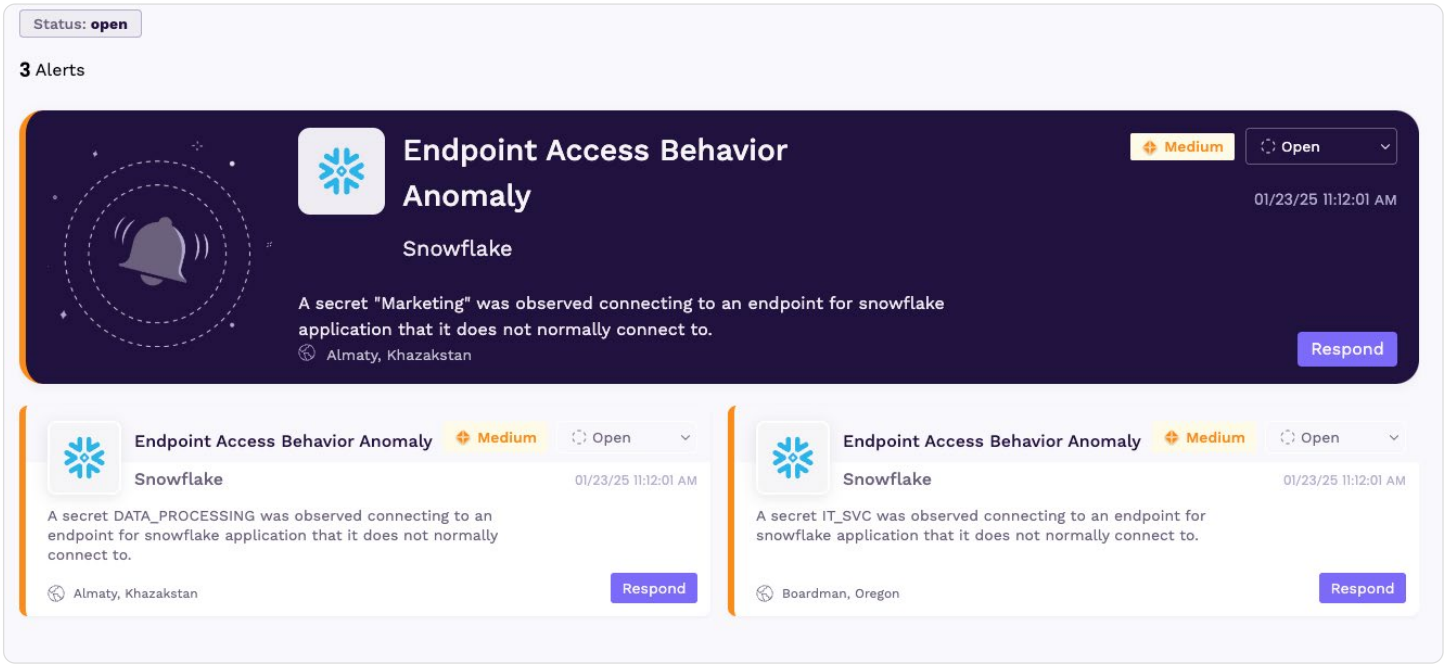
Vorlon Customers

For Vorlon customers already observing Snowflake - we recommend the following steps:

1. **Check for traffic from the listed IP addresses in the Traffic Inspector.**
    - If there is any traffic to your Snowflake instance from those IP addresses, revoke the associated secret or user account.

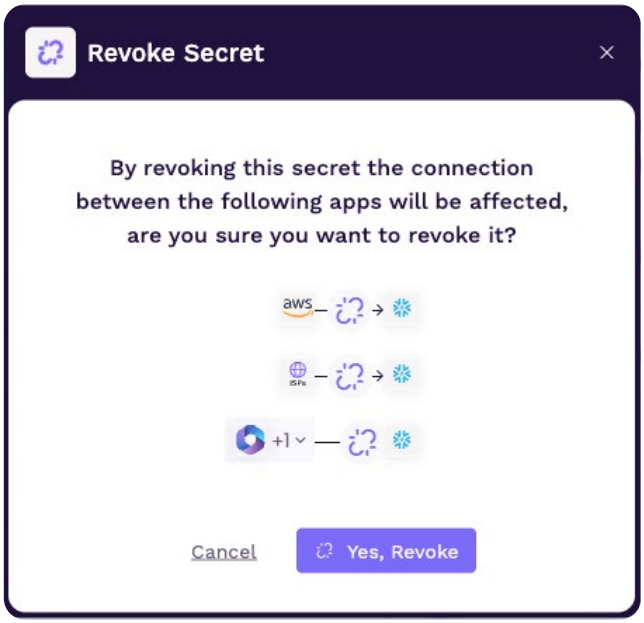


2. **Review all alerts for Snowflake.**



3. **In the Secrets screen, review and consider revoking the following:**

- Snowflake secrets and user accounts that have not been used in over 60 days.
- Admin level Snowflake secrets.



About Vorlon

Vorlon is the first easy way to detect and respond to third-party breaches. With Vorlon Third-Party Application Detection and Response (TADR), your vendor app ecosystem finally gets proactive security coverage like you have for your endpoints and cloud. After an agentless, proxy-free setup, you can monitor sensitive data flows, manage secrets, detect anomalies, and revoke access. Powered by patent-pending DataMatrix® technology, Vorlon creates an algorithmic model of your applications and connected services for faster, AI-driven remediation. Backed by Accel and SOC 2 Type 2 Certified, Vorlon is trusted by Fortune 500 companies and startups.

Learn more at vorlonsecurity.com.