RSAConference™2023

San Francisco | April 24 – 27 | Moscone Center

Stronger Together

SESSION ID: IDY-T01

The Dark Underbelly of 3rd-Party Application Access to Corporate Data

#RSAC

Jenko Hwong

Principal Threat Researcher
Netskope

Twitter: @jenkohwong
Mastodon: @jenko@infosec.exchange

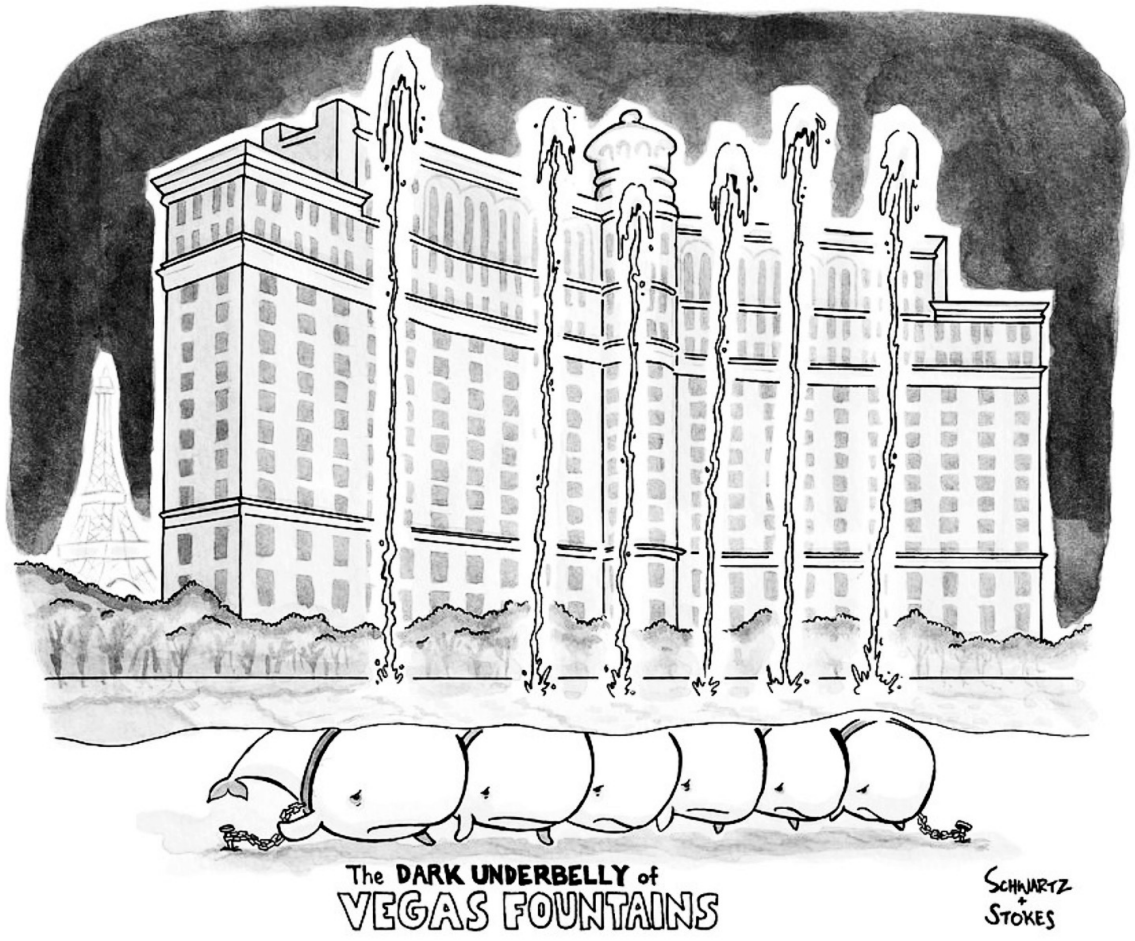
Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference™ or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2023 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

Dark Underbelly...



The side of something that is not normally seen. Figuratively, it means a vulnerable or weak part, similar to the term Achilles' heel, or alternatively, a hidden, illicit side of society.

The Plot

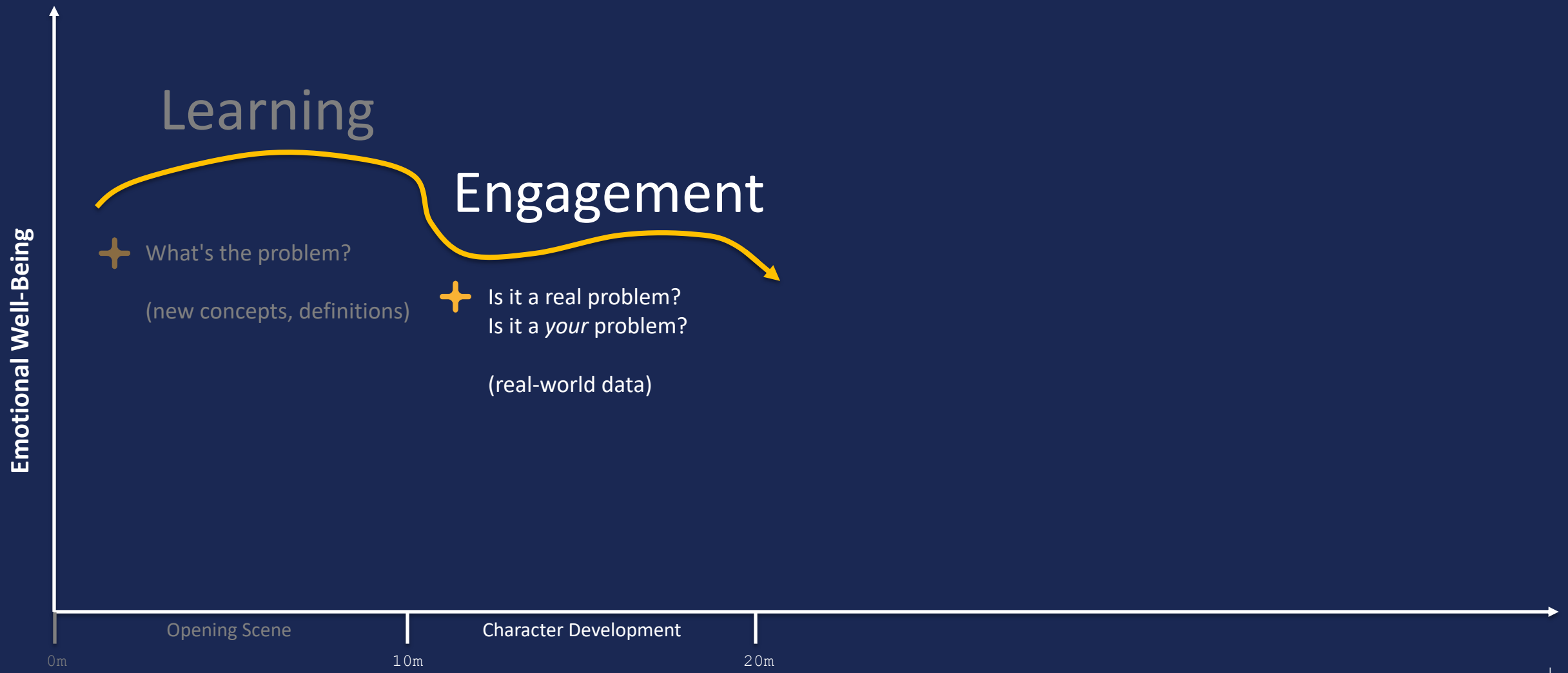
The Dark Underbelly of 3rd-Party Application Access to Corporate Data Using OAuth 2.0

The Plot

The Dark Underbelly of 3rd-Party Application Access to Corporate Data Using OAuth 2.0

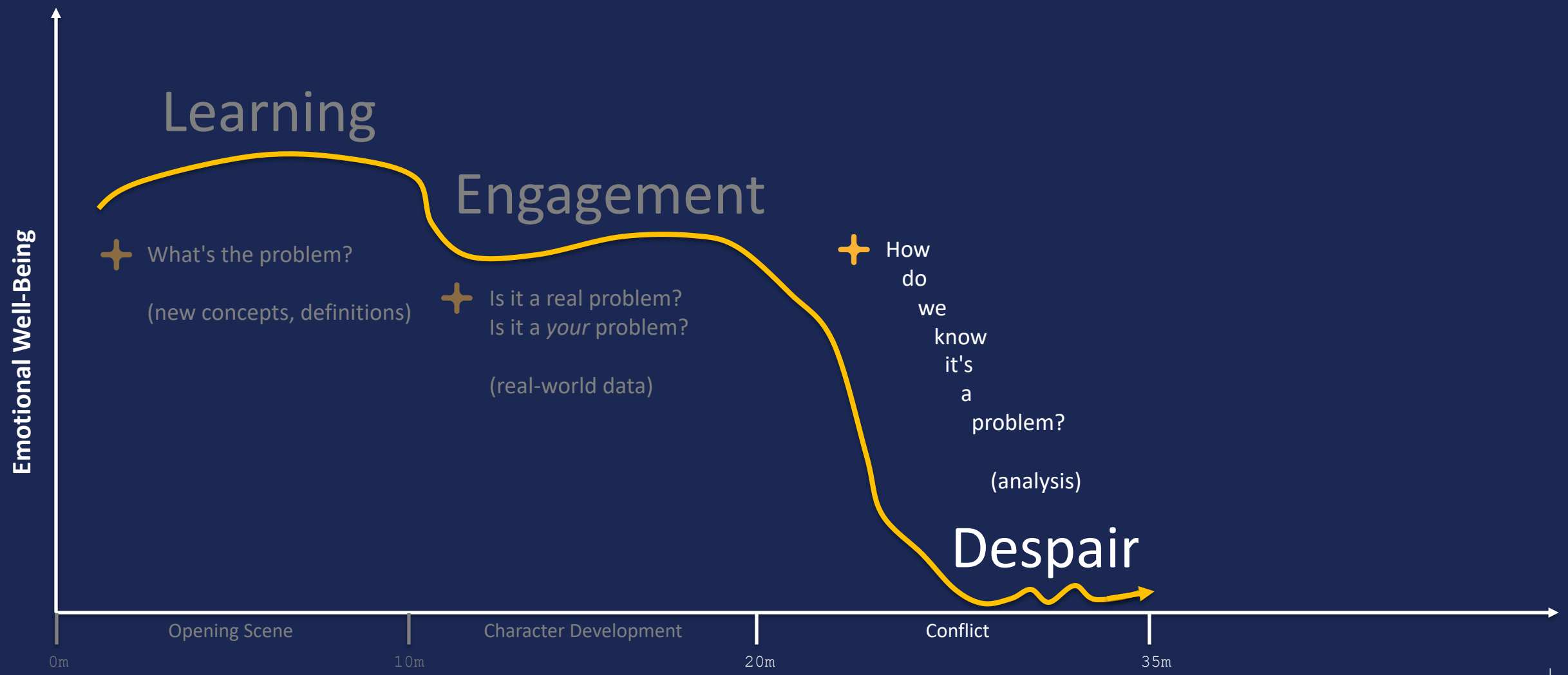
The Plot

The Dark Underbelly of 3rd-Party Application Access to Corporate Data Using OAuth 2.0



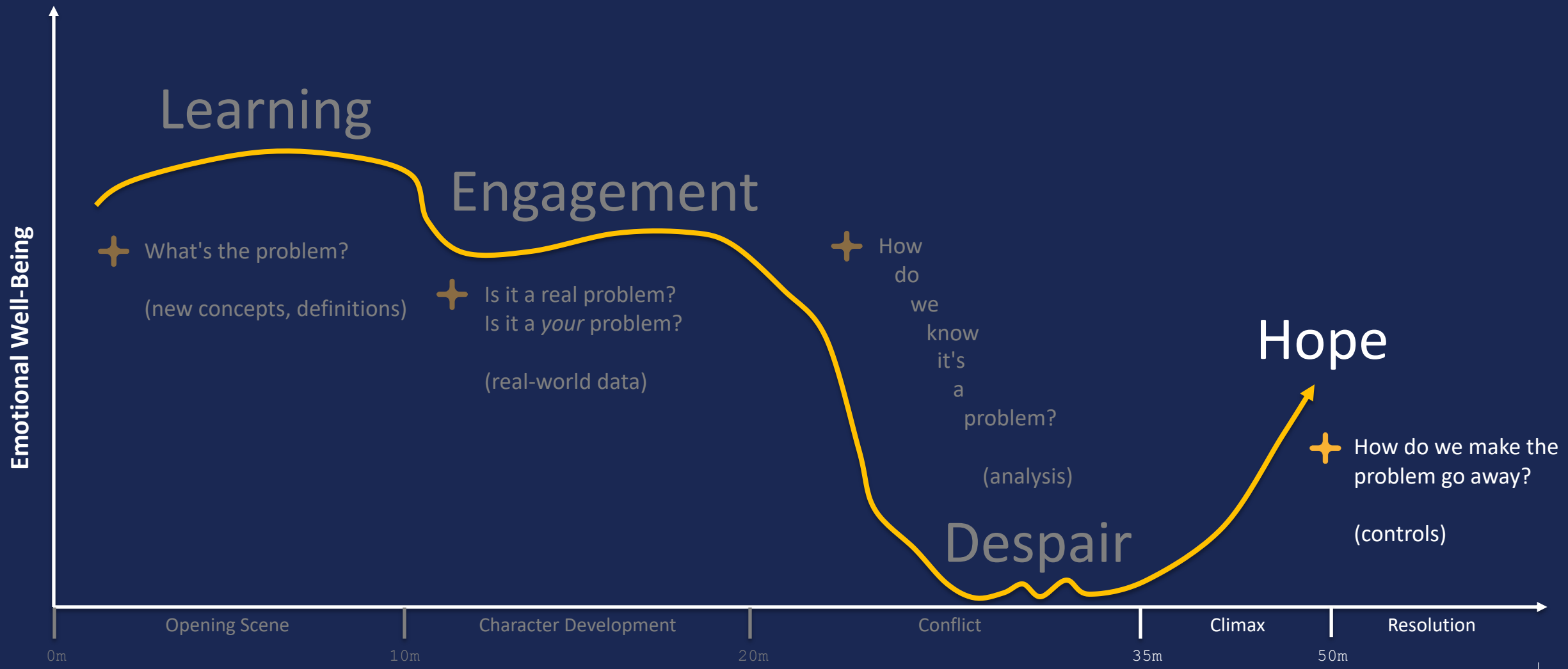
The Plot

The Dark Underbelly of 3rd-Party Application Access to Corporate Data Using OAuth 2.0



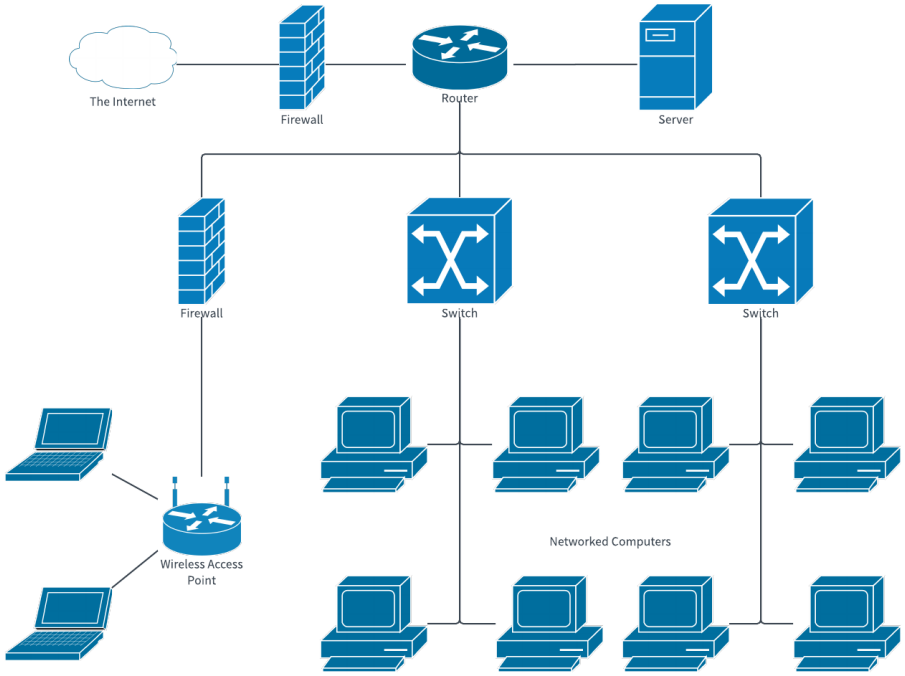
The Plot

The Dark Underbelly of 3rd-Party Application Access to Corporate Data Using OAuth 2.0



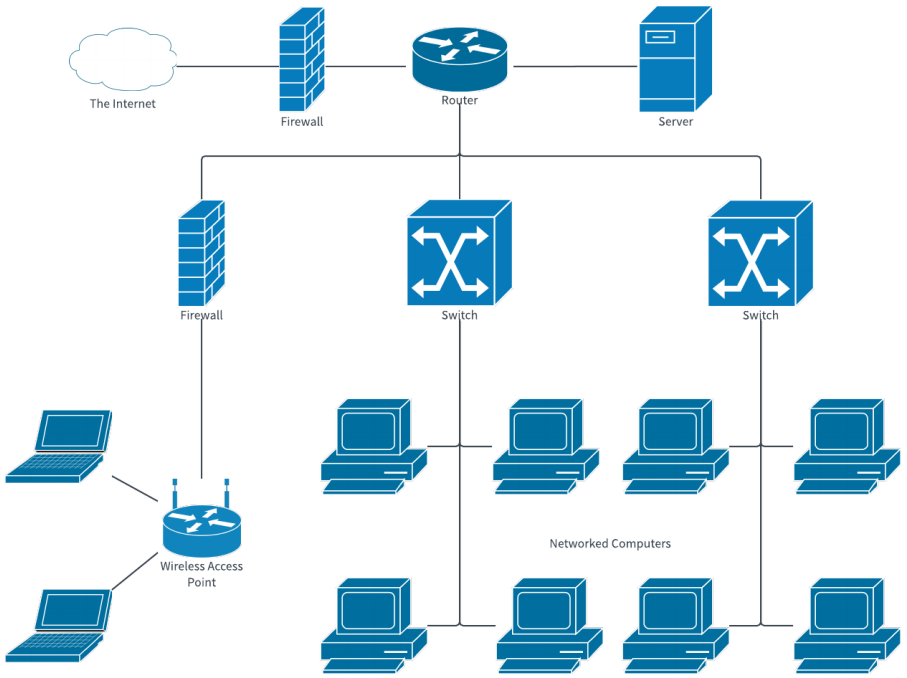
The world used to be simple...

with on-premise networks, apps, and data...

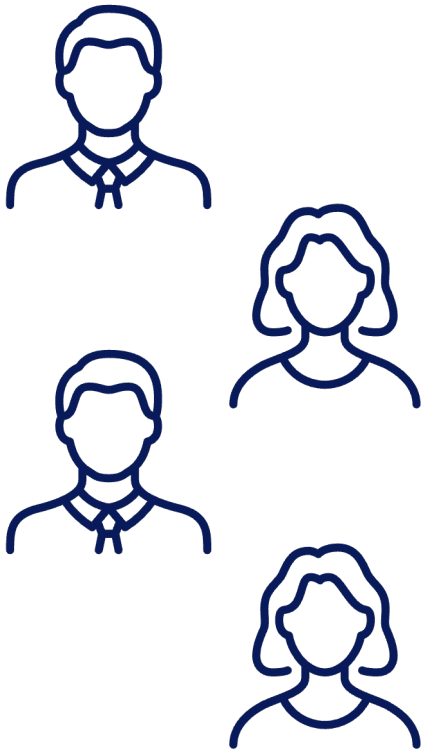


The world used to be simple...

with on-premise networks, apps, and data...with explicit IT access controls.



- wifi access
- install software
- app credentials
- website credentials
- database logins
- SSO

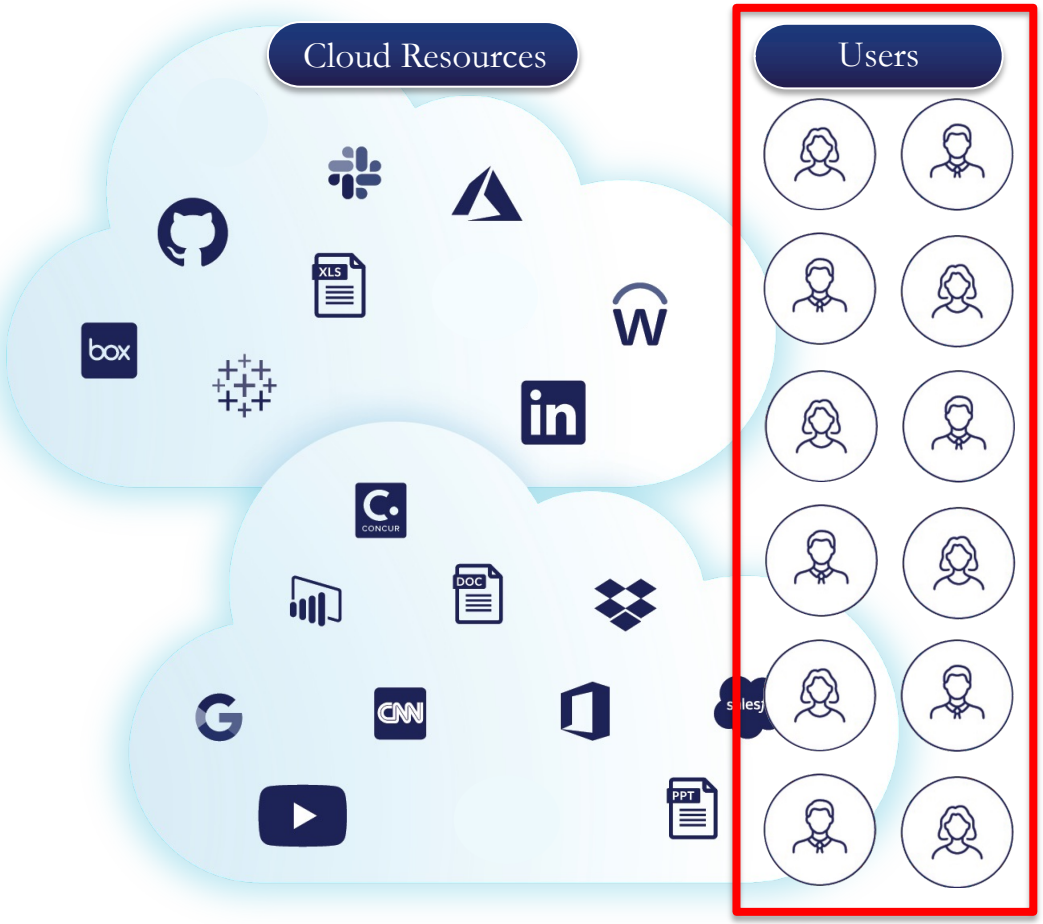


Then came the cloud...

with cloud apps and data...

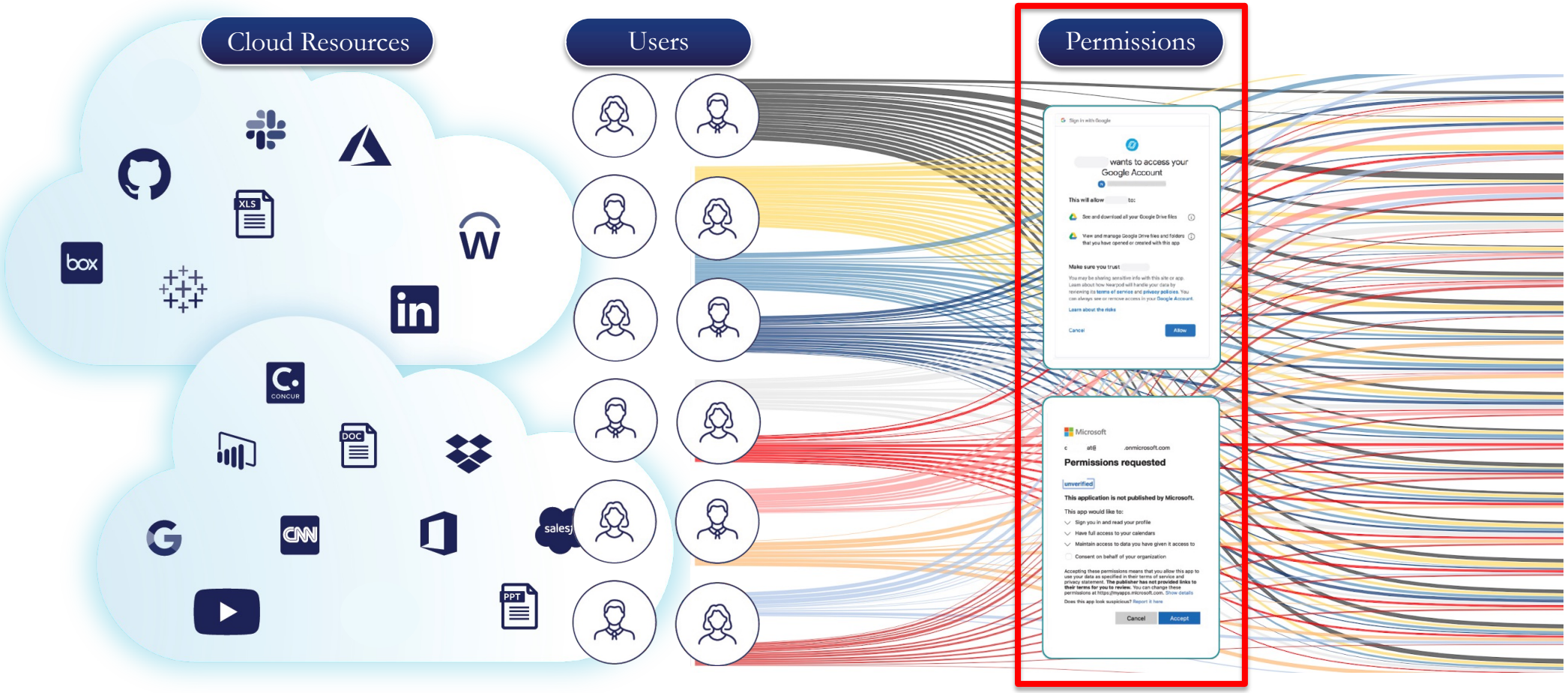
Then came the cloud...

with cloud apps and data...and a user model



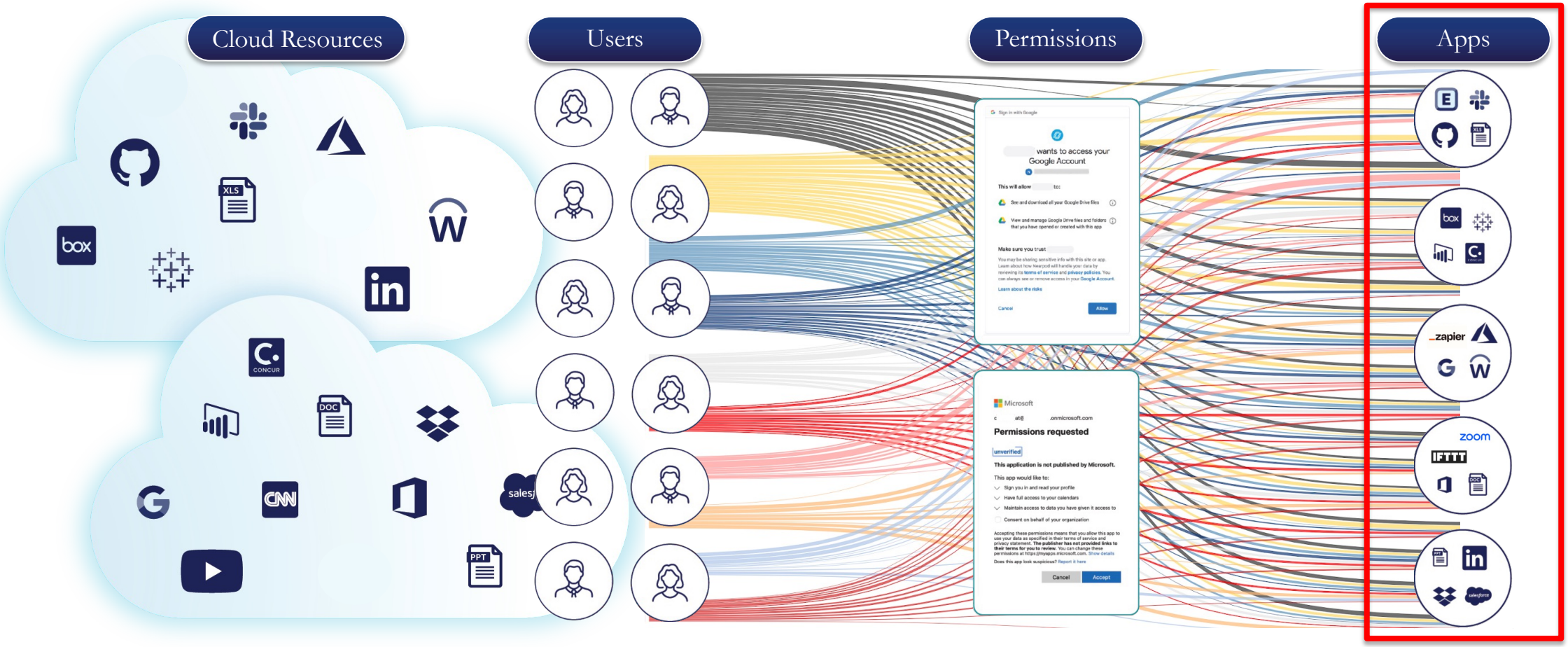
Then came the cloud...

with cloud apps and data...and a user model for granting



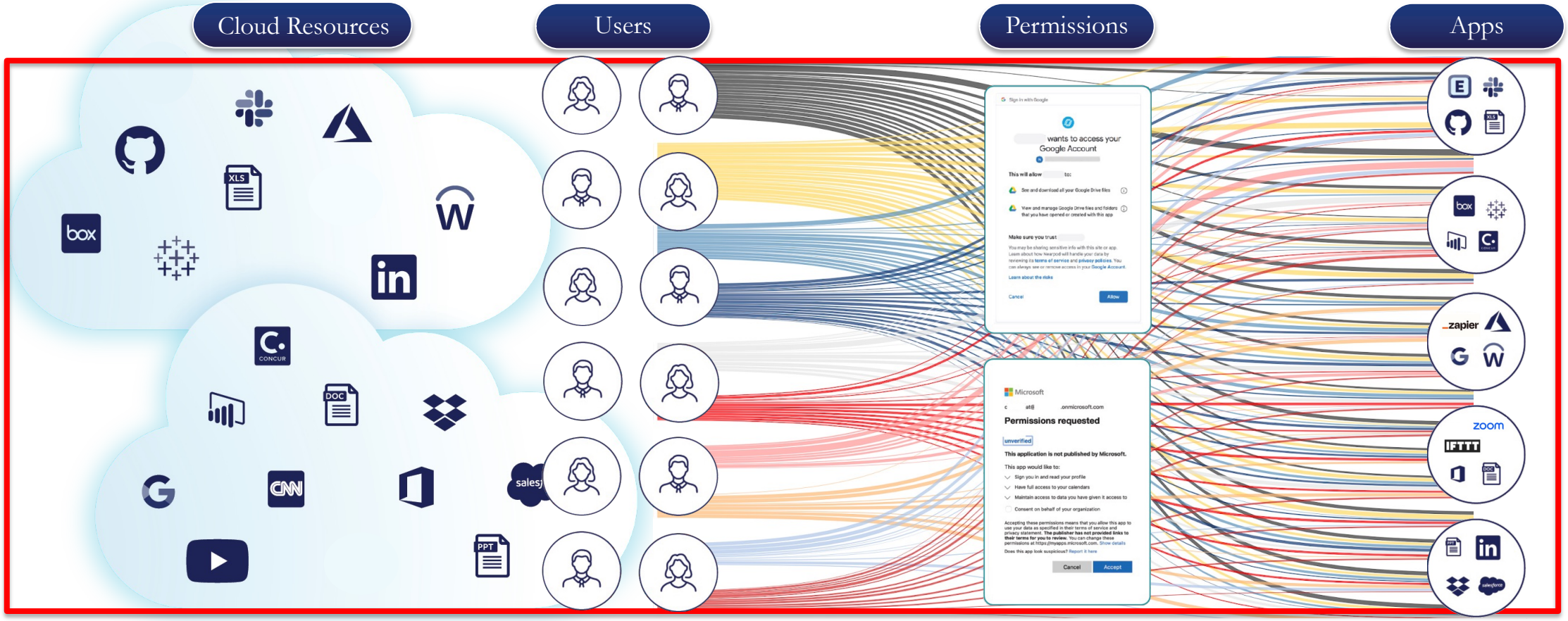
Then came the cloud...

with cloud apps and data...and a user model for granting 3rd-party app access.



Then came the cloud...

with cloud apps and data...and a user model for granting 3rd-party app access.



Is this Relevant?

Real-World Data

About the Data

Stronger Together

Type

- OAuth app approvals
- Google Resources
  - GDrive
  - GMail
  - Google Cloud
- Microsoft similar
- Other big SaaS ecosystems (fileshare, CRM, cloud service environments)

About the Data: OAuth Approvals

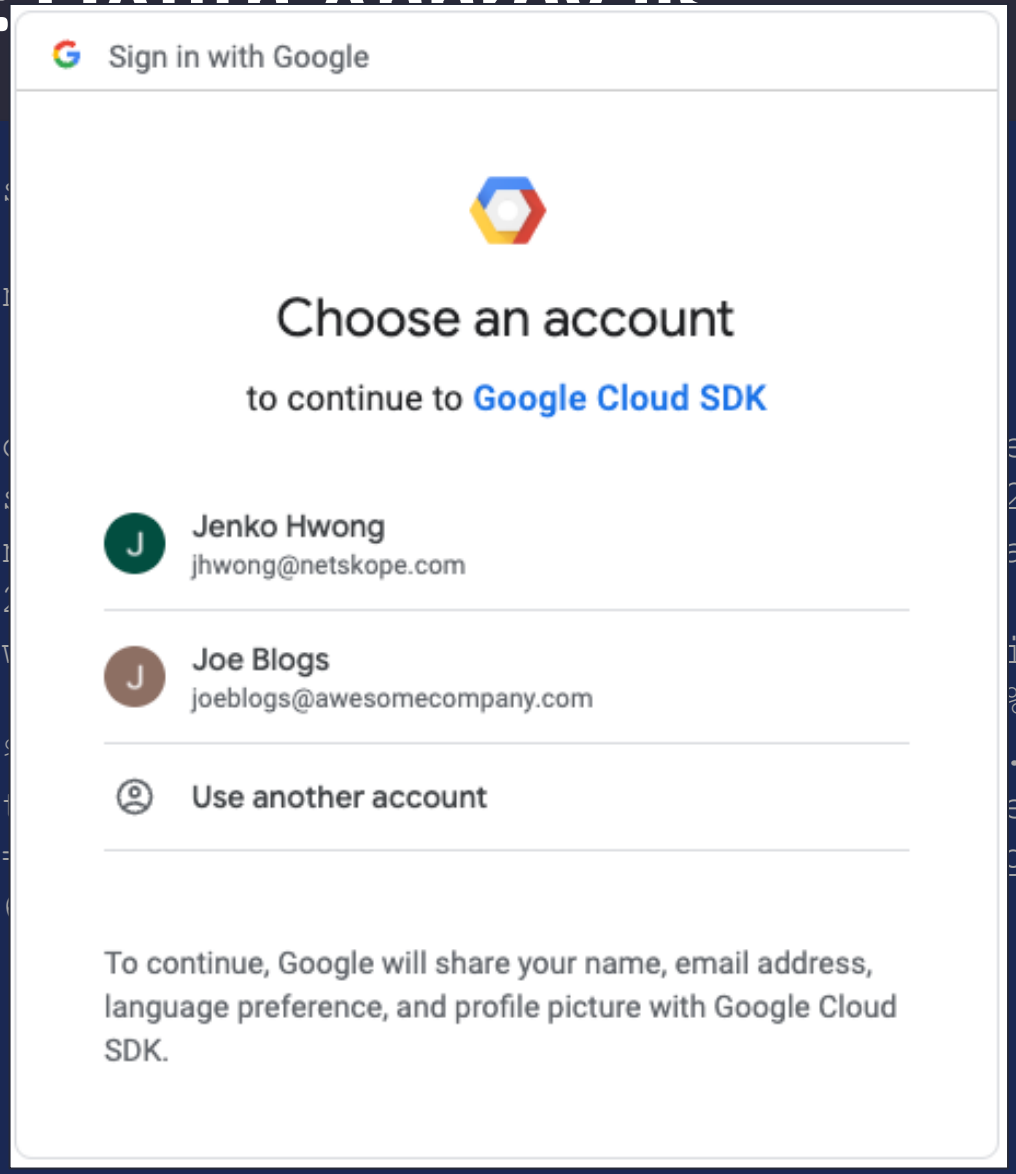
```
gcloud auth login joeblogs@awesomecompany.com --force
```

About the Data: OAuth Approvals

```
gcloud auth login joeblogs@awesomecompany.com --force

Your browser has been opened to visit:


https://accounts.google.com/o/oauth2/auth?response_type=code&client_id
=32555940559.apps.googleusercontent.com&redirect_uri=http%3A%2F%2Floca
lhost%3A8085%2F&scope=openid+https%3A%2F%2Fwww.googleapis.com%2Fauth%2
Fuserinfo.email+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcloud-
platform+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fappengine.admin+htt
ps%3A%2F%2Fwww.googleapis.com%2Fauth%2Fsqlservice.login+https%3A%2F%2F
www.googleapis.com%2Fauth%2Fcompute+https%3A%2F%2Fwww.googleapis.com%2
Fauth%2Faccounts.reauth&state=CQExSNj9shBhTv2d4CZ6KgQILOwGi4&access_ty
pe=offline&code_challenge=jEgY3JaBuV4KJujldiEId49TLE4ghPATL9mPcUg6dTY&
code_challenge_method=S256
```

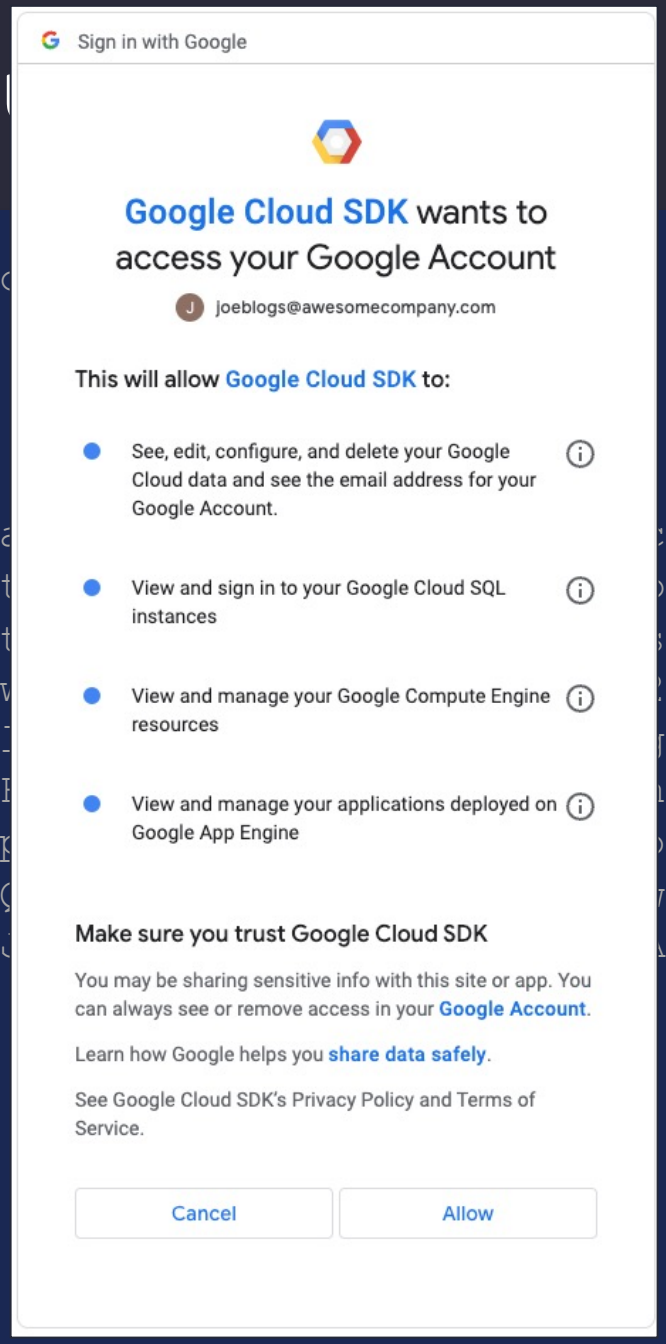
About the Data: OAuth Approvals

```
gcloud auth login joeblogs

Your browser has been open


https://accounts.google.co                                  ent_id
=32555940559.apps.googleus                                  2Floca
lhost%3A8085%2F&scope=open                                  auth%2
Fuserinfo.email+https%3A%2
platform+https%3A%2F%2Fwww                                  in+htt
ps%3A%2F%2Fwww.googleapis                                   %2F%2F
www.googleapis.com%2Fauth                                   .com%2
Fauth%2Faccounts.reauth&st                                  ess_ty
pe=offline&code_challenge=                                  g6dTY&
code_challenge_method=S256
```



About the Data: OA

```
gcloud auth login joeblogs@awesc

Your browser has been opened to


https://accounts.google.com/o/oa                                  code&client_id
=32555940559.apps.googleusercont                                  %3A%2F%2Floca
lhost%3A8085%2F&scope=openid+htt                                  s.com%2Fauth%2
Fuserinfo.email+https%3A%2F%2Fw                                   Fcloud-
platform+https%3A%2F%2Fwww.goog                                   gine.admin+htt
ps%3A%2F%2Fwww.googleapis.com%2                                   ttps%3A%2F%2F
www.googleapis.com%2Fauth%2Fcom                                   gleapis.com%2
Fauth%2Faccounts.reauth&state=C                                   Gi4&access_ty
pe=offline&code_challenge=jEgY3                                  TL9mPcUg6dTY&
code_challenge_method=S256
```



About the Data: OAuth Approvals

```
gcloud auth login joeblog

Your browser has been ope


https://accounts.google.c                                   ient_id
=32555940559.apps.googleu                                   %2Floca
lhost%3A8085%2F&scope=ope                                   Fauth%2
Fuserinfo.email+https%3A%                                   -
platform+https%3A%2F%2Fww                                   min+htt
ps%3A%2F%2Fwww.googleapis                                   A%2F%2F
www.googleapis.com%2Fauth                                   s.com%2
Fauth%2Faccounts.reauth&s                                   cess_ty
pe=offline&code_challenge                                   Jg6dTY&
code_challenge_method=S25
```

Resources

esources

Cloud SDK > Documentation > Guides

You are now authenticated with the gcloud CLI!

The authentication flow has completed successfully. You may close this window, or chec

Information about command-line tools and client libraries

To learn more about Google Cloud CLI commands, see the gcloud CLI guide.

To learn more about the command-line tools for App Engine, Compute Engine, Cloud Stor
Cloud DNS (which are all bundled with the gcloud CLI), see Accessing services with the g

If you're a client application developer and want to find out more about accessing Google
programming language or framework, see Client Libraries Explained.

About the Data: OAuth Approvals

```
gcloud auth login joeblogs@awesomecompany.com --force

Your browser has been opened to visit:


https://accounts.google.com/o/oauth2/auth?response_type=code&client_id
=32555940559.apps.googleusercontent.com&redirect_uri=http%3A%2F%2Floca
lhost%3A8085%2F&scope=openid+https%3A%2F%2Fwww.googleapis.com%2Fauth%2
Fuserinfo.email+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcloud-
platform+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fappengine.admin+htt
ps%3A%2F%2Fwww.googleapis.com%2Fauth%2Fsqlservice.login+https%3A%2F%2F
www.googleapis.com%2Fauth%2Fcompute+https%3A%2F%2Fwww.googleapis.com%2
Fauth%2Faccounts.reauth&state=CQExSNj9shBhTv2d4CZ6KgQILOwGi4&access_ty
pe=offline&code_challenge=jEgY3JaBuV4KJujldiEId49TLE4ghPATL9mPcUg6dTY&
code_challenge_method=S256


You are now logged in as [joeblogs@awesomecompany.com].
```

About the Data

Type

- OAuth app approvals
- Google Resources
  - GDrive
  - GMail
  - Google Cloud
- Microsoft similar
- Other big SaaS ecosystems (fileshare, CRM, cloud)

Scope

- Production data
- Users: millions
- Orgs: thousands
- Size: SMB to enterprise
- Verticals: all
- Geo: worldwide
- Timeframe: ~3 months 2022

About the Data

Stronger Together

Type

- OAuth app approvals
- Google Resources
  - GDrive
  - GMail
  - Google Cloud
- Microsoft similar
- Other big SaaS ecosystems (fileshare, CRM, cloud)

Scope

- Production data
- Users: millions
- Orgs: thousands
- Size: SMB to enterprise
- Verticals: all
- Geo: worldwide
- Timeframe: ~3 months 2022

Source

- Everytime a user approves an app, an entry is logged
- Audit logs gathered via Console or API

About the Data: Audit Log Console

admin.google.com/u/1/ac/sc/investigation?ref=reporting

Admin

Search for users, groups or settings

Home
Dashboard
Directory
Devices
Apps
Security
Reporting
Billing
Account
Rules
Storage
Send feedback

Reporting > Audit and investigation

OAuth log events | Filter | Condition builder

+ Add a filter

SEARCH

Showing 1–14 of 14 results | Export all

Date	Application ID	Application name	Event	Description
2023-04-23T02:19:56-07:00	77185...tent.com	Google Chrome	Grant	Joe Blogs authorized access to G
2023-04-23T02:05:01-07:00	80454...tent.com	Google Hyper-Search Engine	Grant	Joe Blogs authorized access to G
2023-04-23T01:26:28-07:00	32555...tent.com	Google Cloud SDK	Grant	Joe Blogs authorized access to G
2023-04-23T01:15:03-07:00	32555...tent.com	Google Cloud SDK	Grant	Joe Blogs authorized access to G
2023-04-23T00:44:24-07:00	77185...tent.com	Google Chrome	Grant	Joe Blogs authorized access to Google Chrome for
2023-04-23T00:39:57-07:00	32555...tent.com	Google Cloud SDK	Grant	Joe Blogs authorized access to Google Cloud SDK f
2023-04-23T00:35:20-07:00	32555...tent.com	Google Cloud SDK	Grant	Joe Blogs authorized access to Google Cloud SDK f
2023-03-12T00:13:43-08:00	77185...tent.com	Google Chrome	Revoke	Joe Blogs revoked access to Google Chrome for htt
2023-02-24T16:40:48-08:00	77185...tent.com	Google Chrome	Grant	Joe Blogs authorized access to Google Chrome for
2023-02-20T02:47:22-08:00	32555...tent.com	Google Cloud SDK	Revoke	Joe Blogs revoked access to Google Cloud SDK for
2023-02-18T22:16:21-08:00	32555...tent.com	Google Cloud SDK	Revoke	Joe Blogs revoked access to Google Cloud SDK for
2023-02-15T20:17:05-08:00	32555...tent.com	Google Cloud SDK	Revoke	Joe Blogs revoked access to Google Cloud SDK for
2023-02-12T00:41:13-08:00	32555...tent.com	Google Cloud SDK	Revoke	Joe Blogs revoked access to Google Cloud SDK for
2022-12-07T22:02:17-08:00	32555...tent.com	Google Cloud SDK	Revoke	Joe Blogs revoked access to Google Cloud SDK for

Log Details

Date	2023-04-23T01:26:28-07:00
Application ID	32555940559.apps.googleusercontent.com
Application name	Google Cloud SDK
Event	Grant
Description	Joe Blogs authorized access to **Google Cloud SDK** for **https://www.googleapis.com/auth/cloud-platform** scopes
User	joeblogs@awesomecompany.com
Scope	https://www.googleapis.com/auth/cloud-platform
API name	
API method	
Number of response bytes	0
IP address	123.XX.XX.23
Product	Other
Client type	Native Desktop

About the Data: Audit Log Console

admin.google.com/u/1/ac/sc/investigation?ref=reporting

Admin

Search for users, groups or settings

Home
Dashboard
Directory
Devices
Apps
Security
Reporting
Billing
Account
Rules
Storage
Send feedback

Reporting > Audit and investigation

OAuth log events

Filter

Add a filter

SEARCH

Showing 1–14 of 14 results

Export all

Date	Application ID	Application name	Event	Description
2023-04-23T02:19:56-07:00	77185...tent.com	Google Chrome	Grant	Joe Blogs authorized access to G
2023-04-23T02:05:01-07:00	80454...tent.com	Google Hyper-Search Engine	Grant	Joe Blogs authorized access to G
2023-04-23T01:26:28-07:00	32555...tent.com	Google Cloud SDK	Grant	Joe Blogs authorized access to G
2023-04-23T01:15:03-07:00	32555...tent.com	Google Cloud SDK	Grant	Joe Blogs authorized access to G
2023-04-23T00:44:24-07:00	77185...tent.com	Google Chrome	Grant	Joe Blogs authorized access to Google Chrome for
2023-04-23T00:39:57-07:00	32555...tent.com	Google Cloud SDK	Grant	Joe Blogs authorized access to Google Cloud SDK f
2023-04-23T00:35:20-07:00	32555...tent.com	Google Cloud SDK	Grant	Joe Blogs authorized access to Google Cloud SDK f
2023-03-12T00:13:43-08:00	77185...tent.com	Google Chrome	Revoke	Joe Blogs revoked access to Google Chrome for htt
2023-02-24T16:40:48-08:00	77185...tent.com	Google Chrome	Grant	Joe Blogs authorized access to Google Chrome for
2023-02-20T02:47:22-08:00	32555...tent.com	Google Cloud SDK	Revoke	Joe Blogs revoked access to Google Cloud SDK for
2023-02-18T22:16:21-08:00	32555...tent.com	Google Cloud SDK	Revoke	Joe Blogs revoked access to Google Cloud SDK for
2023-02-15T20:17:05-08:00	32555...tent.com	Google Cloud SDK	Revoke	Joe Blogs revoked access to Google Cloud SDK for
2023-02-12T00:41:13-08:00	32555...tent.com	Google Cloud SDK	Revoke	Joe Blogs revoked access to Google Cloud SDK for
2022-12-07T22:02:17-08:00	32555...tent.com	Google Cloud SDK	Revoke	Joe Blogs revoked access to Google Cloud SDK for

Export results from Search 1

Export name

0 / 80

Select format

- (•) Google Sheets
- ( ) Comma-separated values (.csv)

The maximum number of exported results depends on the data source and export format.
Learn more about export limits

CANCEL EXPORT

Log Details

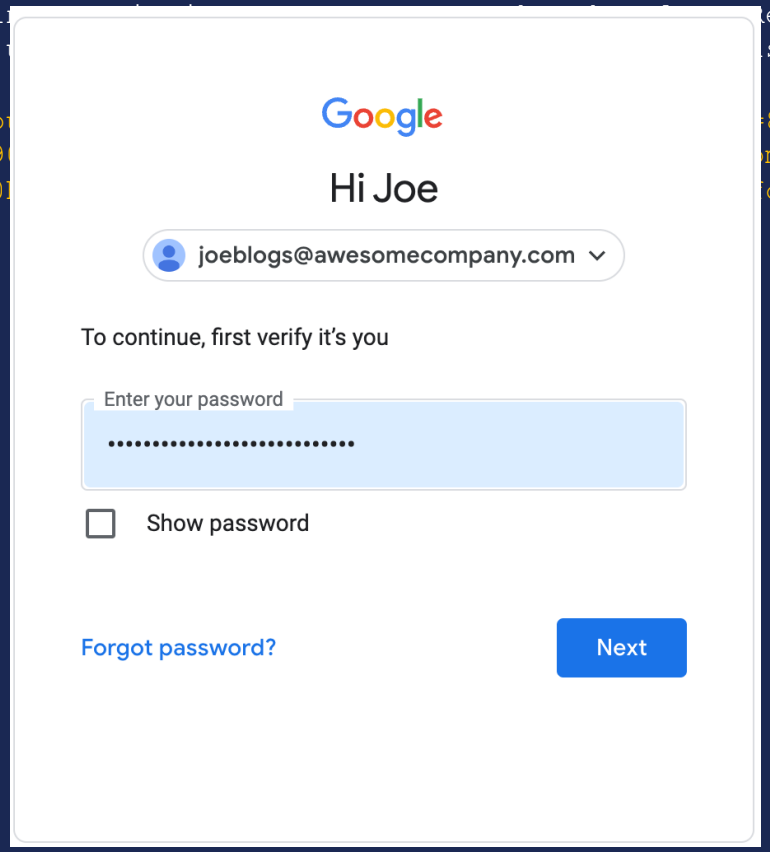
Date	2023-04-23T01:26:28-07:00
Application ID	32555940559.apps.googleusercontent.com
Application name	Google Cloud SDK
Event	Grant
Description	Joe Blogs authorized access to **Google Cloud SDK** for **https://www.googleapis.com/auth/cloud-platform** scopes
User	joeblogs@awesomecompany.com
Scope	https://www.googleapis.com/auth/cloud-platform
API name	
API method	
Number of response bytes	0
IP address	123.XX.XX.23
Product	Other
Client type	Native Desktop

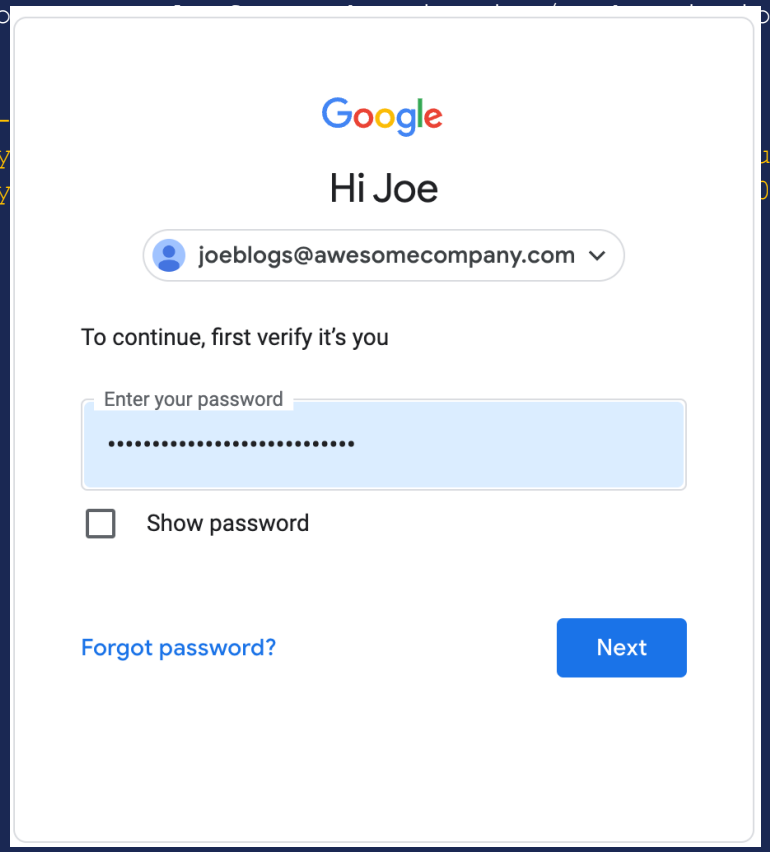
About the Data: Audit Log API

```
$ /bin/sh oauth_audit_report.sh

1) App requesting permissions to access OAuth token log. Redirecting you to Google for authentication/authroziation
   by starting up webserver on your local machine with this URL:

   https://accounts.google.com/o/oauth2/v2/auth?client_id=804540243761-
puvq6928tmj1dh9002q93h2bjv9dki6v.apps.googleusercontent.com&response_type=code&scope=https://www.googleapis.com/auth/admin.reports.au
dit.readonly%20https://www.googleapis.com/auth/cloud-platform&access_type=offline&redirect_uri=http://localhost:9000
```

About the Data: Audit Log API

```
$ /bin/sh oauth_audit_report.sh

1) App requesti                                  edirecting yo                                                  on
   by starting                                   s URL:

   https://acco                                  804540243761-                                                  uth/admin.reports.au
puvq6928tmj1dh9                                  m&response_ty
dit.readonly%20                                  orm&access_ty                                                  000
```





About the Data: Audit Log API

```
$ /bin/sh

1) App re                    en log. Redirecting you to Google for authentication/authroziation
   by sta                     with this URL:

   https:                    lient_id=804540243761-
puvq6928t                    ont                                                    s.au
dit.reado                    ouc
```

Sign in with Google

Google Hyper-Search Engine wants to access your Google Account

joeblogs@awesomecompany.com

This will allow Google Hyper-Search Engine to:

- See, edit, configure, and delete your Google Cloud data and see the email address for your Google Account.

Make sure you trust Google Hyper-Search Engine

You may be sharing sensitive info with this site or app. You can always see or remove access in your Google Account.

Learn how Google helps you share data safely.

See Google Hyper-Search Engine's Privacy Policy and Terms of Service.

Cancel | Allow

Sigr | Goo | loca | Loa | App | Sec

localhost:9000/?code=4/0AVHEtk6qCgsQbBJWVQ49BHHwTLBRlVFXRe

Thanks for successfully logging in. You can now close this tab and return to the application.

About the Data: Audit Log API

```
$ /bin/sh oauth_audit_report.sh

1) App requesting permissions to access OAuth token log. Redirecting you to Google for authentication/authroziation
   by starting up webserver on your local machine with this URL:

   https://accounts.google.com/o/oauth2/v2/auth?client_id=804540243761-
puvq6928tmj1dh9002q93h2bjv9dki6v.apps.googleusercontent.com&response_type=code&scope=https://www.googleapis.com/auth/admin.reports.au
dit.readonly%20https://www.googleapis.com/auth/cloud-platform&access_type=offline&redirect_uri=http://localhost:9000

2) Login in and approve scopes

   This app will listen on port 9000 for an OAuth grant code from Google, which will be sent to the redirect URI in the original
URL...

3) Received OAuth code from Google Identity: 4/0AVHEtk7jdDUuNOX6WkSRLdb9coP9BtEFKzpn1J2GX51MNaoDs_VumNaA7GBhGGsatcagUg

4) Using the OAuth code to retrieve the OAuth tokens:

curl -s --data client_id=804540243761-puvq6928tmj1dh9002q93h2bjv9dki6v.apps.googleusercontent.com --data
client_secret=_Tjam0jax1aYlLcpqrZj1b47 --data code=4/0AVHEtk7jdDUuNOX6WkSRLdb9coP9BtEFKzpn1J2GX51MNaoDs_VumNaA7GBhGGsatcagUg --data
redirect_uri=http://localhost:9000 --data grant_type=authorization_code https://www.googleapis.com/oauth2/v4/token
```

About the Data: Audit Log API

5) Retrieved OAuth tokens


```
{
  "access_token":
"ya29.a0Ael9sCPyjjVW4G0KngGDC7C4erWrvNIgnmuptaES7cP-dR9U0aooM5-
CGG0l1LFvH3LS5foRPTQJ3zxJAWnn4DWK4_nMG_BzuvfE3a_YhelCllY1wB49sBupXQfh
S-xYWuB9ivtpLy9n-
DzfPEJH9siLbxuxaCgYKATgSARESFQF4udJhf67qCxyvkeEdxRWX6TGAPA0163",
  "expires_in": 3581,
  "scope":
"https://www.googleapis.com/auth/admin.reports.audit.readonly
https://www.googleapis.com/auth/cloud-platform",
  "token_type": "Bearer"
}
```


6) Fetching admin report:

```
curl -s -H "Authorization: Bearer
ya29.a0Ael9sCPyjjVW4G0KngGDC7C4erWrvNIgnmuptaES7cP-dR9U0aooM5-
CGG0l1LFvH3LS5foRPTQJ3zxJAWnn4DWK4_nMG_BzuvfE3a_YhelCllY1wB49sBupXQfh
S-xYWuB9ivtpLy9n-
DzfPEJH9siLbxuxaCgYKATgSARESFQF4udJhf67qCxyvkeEdxRWX6TGAPA0163"
https://admin.googleapis.com/admin/reports/v1/activity/users/all/appl
ications/token?maxResults=25
```


```
{
  "kind": "admin#reports#activities",
  "etag": "\"P4UZt3E47YE1EedEgRGeNMKVdI4cxfy8A0aTCl4A_NM/RFrt6Zz39_-
vvHTeIkk-S0BNqtc\"",
  "items": [
    {
      "kind": "admin#reports#activity",
      "id": {
        "time": "2023-04-24T21:47:28.605Z",
        "uniqueQualifier": "-7690708801800961903",
        "applicationName": "token",
        "customerId": "C011xktk6"
      },
      "etag":
"\"P4UZt3E47YE1EedEgRGeNMKVdI4cxfy8A0aTCl4A_NM/1QpOzCwQYYr2jo2HxWYK9nP9lEs\"
",
      "actor": {
        "email": "joeblogs@awsomecompany.com",
        "profileId": "117226486721886598480"
      },
      "ipAddress": "192.77.111.2",
 "events": [
        {
          "name": "authorize",
          "parameters": [
            {
              "name": "client_id",
              "value": "804540243761-
puvq6928tmj1dh9002q93h2bjv9dki6v.apps.googleusercontent.com"
            },
            {
              "name": "app_name",
              "value": "Google Hyper-Search Engine"
```

Is this a Problem?

How many 3rd-party apps?

Start with app counts

Stronger Together

Organizations on average granted more than 440 third-party applications access to their Google data and applications.

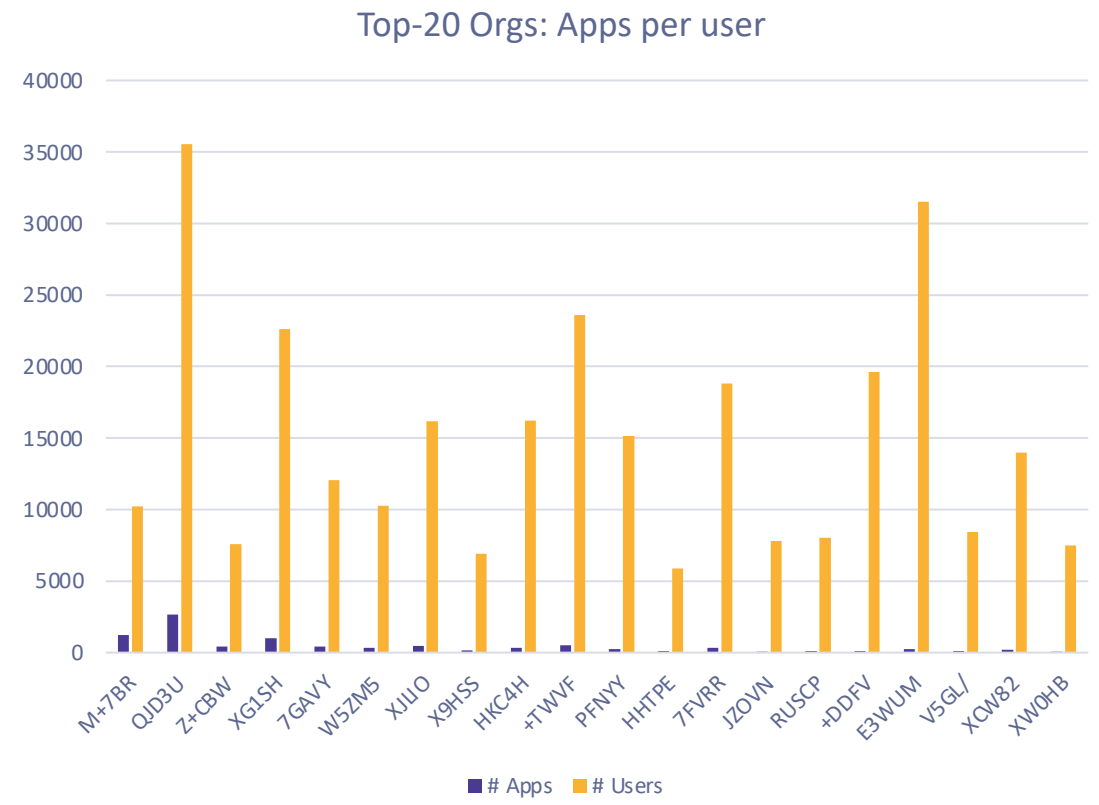
82% of organizations with at least 500 users, granted access to at least 250 different cloud applications.

12,330 different applications were authorized by users in one organization.

Application Risk

- Users: >5000
- Google Drive Apps
- Any permissions

# Apps	# Users	Apps / user
1218	10243	0.12
2666	35551	0.07
422	7597	0.06
1011	22599	0.04
430	12068	0.04
339	10271	0.03
451	16186	0.03
166	6905	0.02
353	16200	0.02
520	23600	0.02
243	15133	0.02
98	5860	0.02
331	18804	0.02
59	7822	0.01
88	8043	0.01
129	19621	0.01
253	31529	0.01
105	8428	0.01
202	13990	0.01
53	7481	0.01



What kind of apps?

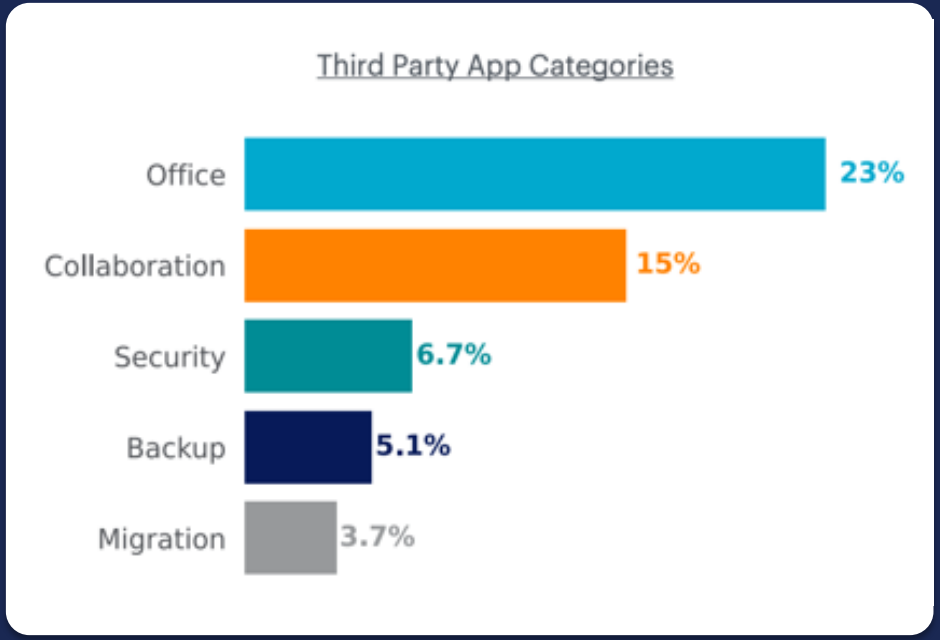
Top 3rd-Party Application Access	Category	%
Google Chrome	Browser	16.1%
iOS Account Manager	Mobile	6.6%
Zoom	Video Conferencin	5.9%
Slack	Messaging	5.1%
Android device	Mobile	3.9%
Virtru	Encryption	3.0%
Google Drive for desktop	Storage	2.9%
iOS	Mobile	2.5%
Atlassian	Workflow/Collabo	2.5%
macOS	Desktop	1.3%
LinkedIn	Jobs	1.1%
Adobe	Design	0.9%
Zoom for G Suite	Video Conferencin	0.8%
diagrams.net (draw.io)	Graphics	0.8%
Figma	Graphics	0.7%
Miro	Workflow/Collabo	0.7%
LucidChart	Graphics	0.6%
Google Data Studio	Analytics	0.6%
Canva	Graphics	0.5%
Grammarly	Office	0.5%
Confluence	Workflow	0.5%
Trello	Task	0.5%
Dropbox	Storage	0.5%
Postman	Developer	0.4%
Microsoft apps & services	Workflow/Collabo	0.4%
Pinterest	Social Media	0.4%
Medium	Social Media	0.4%
Windows	Desktop	0.3%
Glassdoor	Jobs	0.3%
Google Drive LTI by Canvas	Storage	0.3%
Zendesk	Service Desk	0.3%
Twitter	Social Media	0.3%

Expected

Google Chrome
iOS Account Manager
Zoom
Android device
Slack
Virtru
iOS
Atlassian
Google Drive for desktop
macOS
Adobe

Unexpected

Pinterest
The New York Times
Glassdoor
Postman



What permissions are granted to these apps?

Google Identity | Authentication | Authorization | Credential management | Credential verification | Search | English

Using OAuth 2.0 | Authorizing for Web | Google Account Linking

Filter

- Overview
- Cross-client Identity
- OAuth 2.0 Scopes
- OAuth 2.0 Policies

Access to Google APIs
- for Server-side Web Apps
- for JavaScript Web Apps
- for Mobile & Desktop Apps
- for TV & Device Apps
- for Service Accounts

Prepare your app for production
- Comply with OAuth 2.0 policies
- Submit for brand verification
- Sensitive scope verification
- Restricted scope verification
- Additional considerations for Google Workspace

Resources
- Best practices
- Out-of-band (OOB) Migration
- Loopback IP Address Migration for Mobile and Chrome Apps

Related topics
- Cross-Account Protection (RISC)
- WebAuthn

Admin SDK API, v1

Scopes	
https://www.googleapis.com/auth/admin.reports.audit.readonly	View audit reports for your G Suite domain
https://www.googleapis.com/auth/admin.reports.usage.readonly	View usage reports for your G Suite domain

Admin SDK API, v1

Scopes	
https://www.googleapis.com/auth/admin.datatransfer	View and manage data transfers between users in your organization
https://www.googleapis.com/auth/admin.datatransfer.readonly	View data transfers between users in your organization

Admin SDK API, v1

Scopes	
https://www.googleapis.com/auth/admin.chrome.printers	See, add, edit, and permanently delete the printers that your organization can use with Chrome
https://www.googleapis.com/auth/admin.chrome.printers.readonly	See the printers that your organization can use with Chrome
https://www.googleapis.com/auth/admin.directory.customer	View and manage customer related information
https://www.googleapis.com/auth/admin.directory.customer.readonly	View customer related information
https://www.googleapis.com/auth/admin.directory.device.chromeos	View and manage your Chrome OS devices' metadata
https://www.googleapis.com/auth/admin.directory.device.chromeos.readonly	View your Chrome OS devices' metadata

On this page
- AI Platform Training & Prediction API, v1
- Access Approval API, v1
- Access Context Manager API, v1
- Ad Exchange Buyer API II, v2beta1
- AdMob API, v1
- AdSense Host API, v4.1
- Admin SDK API, v1
- Admin SDK API, v1
- Admin SDK API, v1
- Analytics Reporting API, v4
- Android Management API, v1
- Apigee API, v1
- App Engine Admin API, v1
- Apps Script API, v1
- BigQuery API, v2
- BigQuery Connection API, v1beta1
- BigQuery Data Transfer API, v1
- BigQuery Reservation API, v1
- Binary Authorization API, v1
- Blogger API, v3
- Books API, v1
- Calendar API, v3
- Campaign Manager 360 API, v4
- Cloud Asset API, v1
- Cloud Bigtable Admin API, v2
- Cloud Billing API, v1

Recommended for you
- Using OAuth 2.0 for Web Server Applications
  Updated Mar 30, 2023
- Using OAuth 2.0 for Server to Server Applications
  Updated Mar 6, 2023
- OAuth 2.0 for Client-side Web Applications
  Updated Mar 30, 2023

https://developers.google.com/identity/protocols/oauth2/scopes

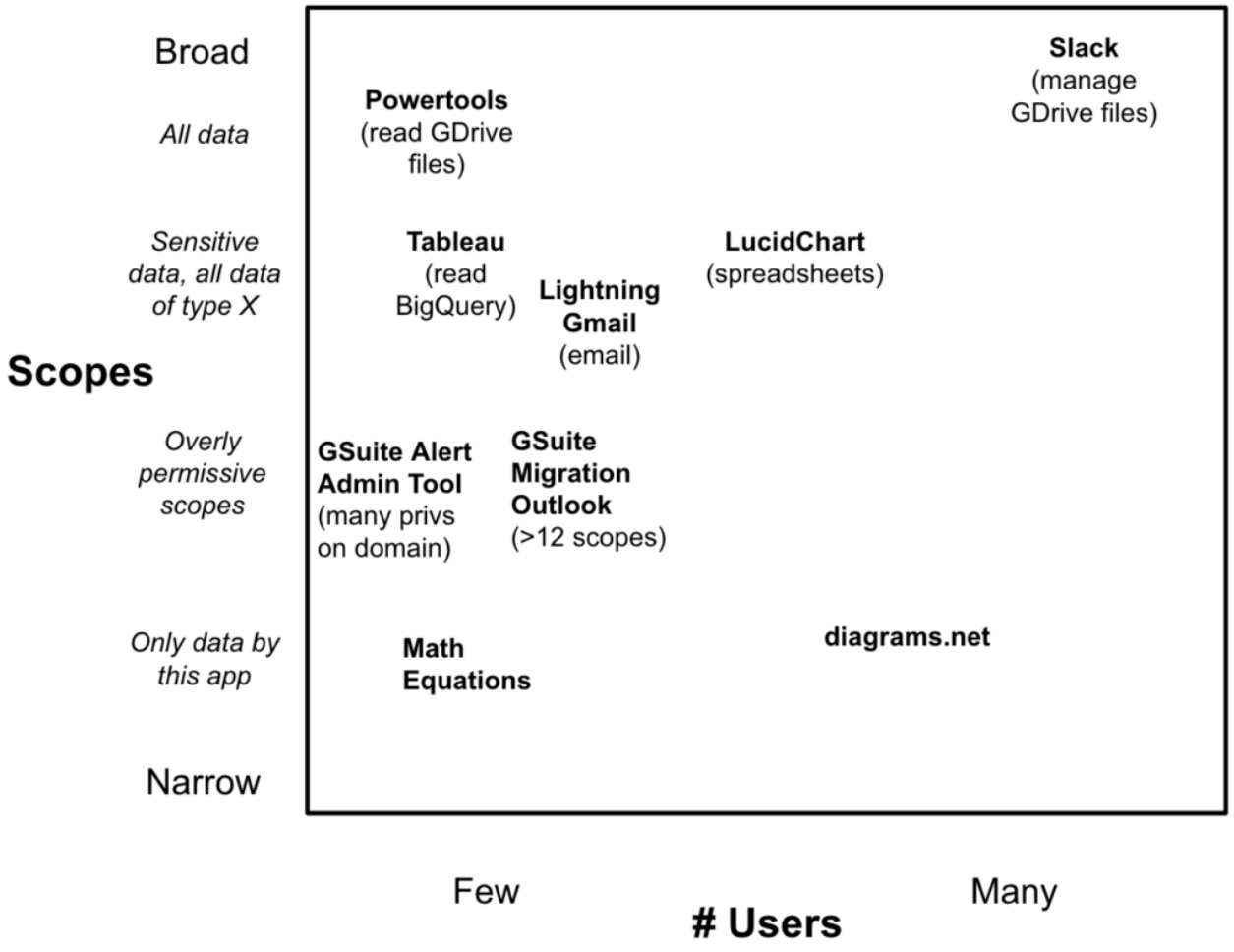
What permissions are granted to these apps?

Stronger Together

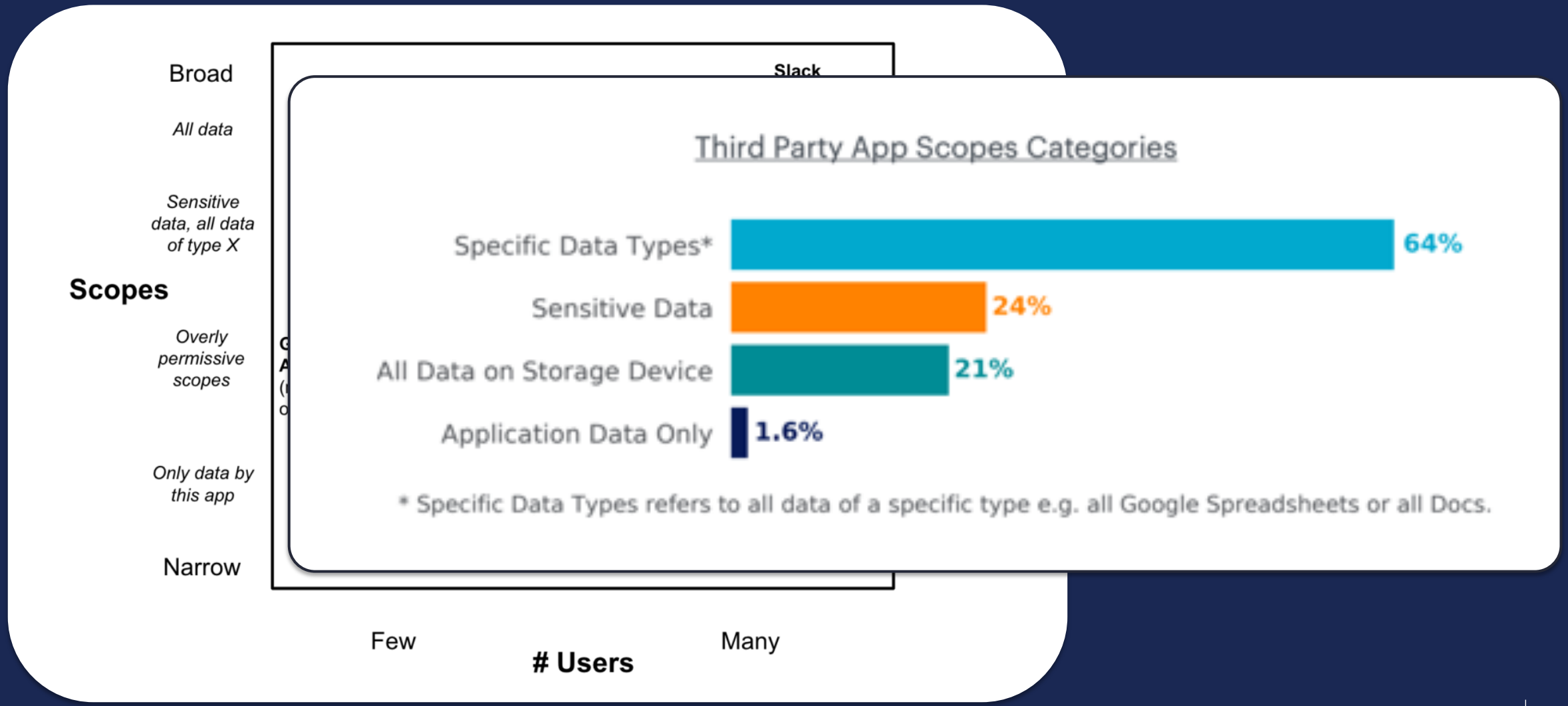
Top permissions granted by users

Scopes	# Users	# Apps
View and manage the files in your Google Drive	168,369	3,605
Manage your calendars	113,798	1,152
View and manage your mail	107,402	3,145
View and manage Google Drive files and folders that you have opened or created with this app	84,529	755
View and manage your spreadsheets in Google Drive	34,591	11,124
View and manage its own configuration data in your Google Drive	26,949	458
Manage your contacts	14,665	220
Manage mailbox labels	14,300	55
View and manage the provisioning of users on your domain	12,341	146
Manage your tasks	11,996	78

What permissions are granted to these apps?



What permissions are granted to these apps?



What permissions are granted to these apps?

Stronger Together

- More than 44% of third-party applications accessing Google Drive have access to either sensitive data or all data on the user's Google Drive.

of applications request write permission on all data on a user's Google Drive.

What permissions are granted to these apps?

All files of type 'spreadsheet'

Scopes	# Users	# Apps	Application
View and manage your spreadsheets in Google Drive	34591	11124	Slack
View and manage your spreadsheets in Google Drive	34591	11124	draw.io
View and manage your spreadsheets in Google Drive	34591	11124	LucidChart
View and manage your spreadsheets in Google Drive	34591	11124	Zendesk
View and manage your spreadsheets in Google Drive	34591	11124	Asana
View and manage your spreadsheets in Google Drive	34591	11124	Doordash
View and manage your spreadsheets in Google Drive	34591	11124	Untitled project
View and manage your spreadsheets in Google Drive	34591	11124	Zapier
View and manage your spreadsheets in Google Drive	34591	11124	Project Default Service Account
View and manage your spreadsheets in Google Drive	34591	11124	Titus
View and manage your spreadsheets in Google Drive	34591	11124	JIRA
View and manage your spreadsheets in Google Drive	34591	11124	Awesome Table
View and manage your spreadsheets in Google Drive	34591	11124	SurveyMonkey
View and manage your spreadsheets in Google Drive	34591	11124	MITRA
View and manage your spreadsheets in Google Drive	34591	11124	Yet Another Mail Merge
View and manage your spreadsheets in Google Drive	34591	11124	Google APIs Explorer
View and manage your spreadsheets in Google Drive	34591	11124	Google Marketing Platform
View and manage your spreadsheets in Google Drive	34591	11124	Quickstart
View and manage your spreadsheets in Google Drive	34591	11124	Remove Duplicates
View and manage your spreadsheets in Google Drive	34591	11124	HubSpot

What permissions are granted to these apps?

Overly permissive scopes

Scopes	# Users	# Apps	Application	# Users
View and manage your mail	107402	3145	Virtru	63217
View and manage your mail	107402	3145	iOS	53334
View and manage your mail	107402	3145	macOS	31860
View and manage your mail	107402	3145	Lever	12991
View and manage your mail	107402	3145	Microsoft apps & services	11055
View and manage your mail	107402	3145	G Suite Sync for Microsoft Outlook¬Æ	8866
View and manage your mail	107402	3145	TemplateEmailService	7759
View and manage your mail	107402	3145	Gmail to PDF	6543
View and manage your mail	107402	3145	Untitled project	4189
View and manage your mail	107402	3145	Adobe Acrobat	3155
View and manage your mail	107402	3145	Boomerang for Gmail	3059
View and manage your mail	107402	3145	Outreach	2991
View and manage your mail	107402	3145	Project Default Service Account	2681
View and manage your mail	107402	3145	Highspot	2081
View and manage your mail	107402	3145	Salesforce.com	2005
View and manage your mail	107402	3145	Yet Another Mail Merge	1774
View and manage your mail	107402	3145	Samsung Email	1748
View and manage your mail	107402	3145	Google APIs Explorer	1723
View and manage your mail	107402	3145	cloudHQ	1567
View and manage your mail	107402	3145	Mailtrack	1504

Sensitive permissions

Permissions Category	# Users	# Apps
fitness	235	87
classroom	578	139

What permissions are granted to these apps?

One application found only in one organization with domain-wide privileges

```
Manage data access permissions for users on your domain
Manage delegated admin roles for your domain
Manage messages in groups on your domain
Manage the list of sites and domains you control
Manage your Google Classroom class rosters
Manage your Google Classroom classes
Manage your calendars
Manage your contacts
View and manage Google Apps licenses for your domain
View and manage customer related information
View and manage data transfers between users in your organization
View and manage organization units on your domain
View and manage the provisioning of calendar resources on your domain
View and manage the provisioning of domains for your customers
View and manage the provisioning of groups on your domain
View and manage the provisioning of user schemas on your domain
View and manage the provisioning of users on your domain
View and manage the settings of a Google Apps Group
View and manage your Chrome OS devices' metadata
View and manage your mobile devices' metadata
View audit reports of Google Apps for your domain
View the email addresses of people in your classes
View the profile photos of people in your classes
View usage reports of Google Apps for your domain
View your basic profile info
View your data in Google Cloud Storage
View your email address
```

"How bad could this be?" asked the smoker in the saw mill.

What permissions are granted to these apps?

Stronger Together

CamScanner application approved by 219 users (.04% of 509,079)

Requests “View and manage all files in your Google Drive”

CamScanner was found by Kaspersky in August 2019 to contain malware [1]

Banned by the Indian government over security concerns in June 2020 [2]

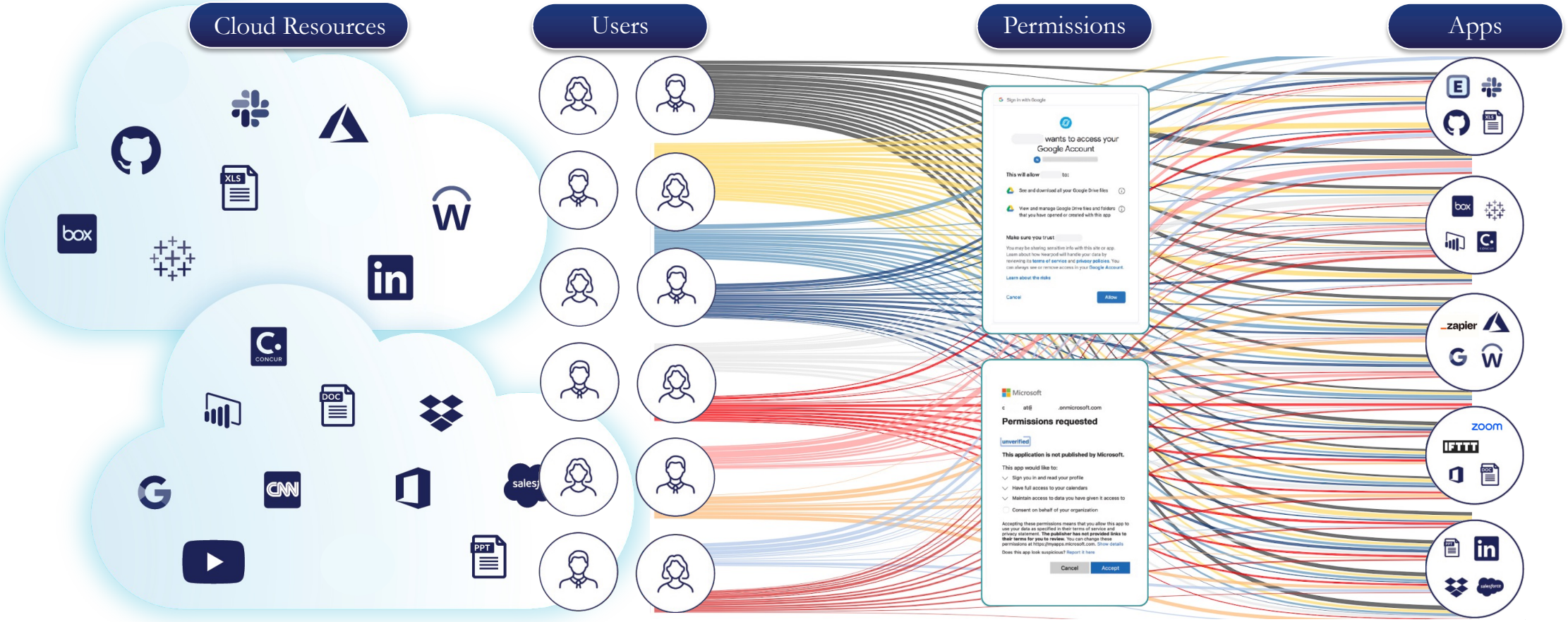
[1] https://usa.kaspersky.com/blog/camscanner-malicious-android-app/18535/
[2] https://theprint.in/india/delhi-police-admits-it-used-banned-chinese-app-camscanner-apologises-on-twitter/582767/

Risk Analysis Framework

Impact

Vulnerability
Attack Surface Area

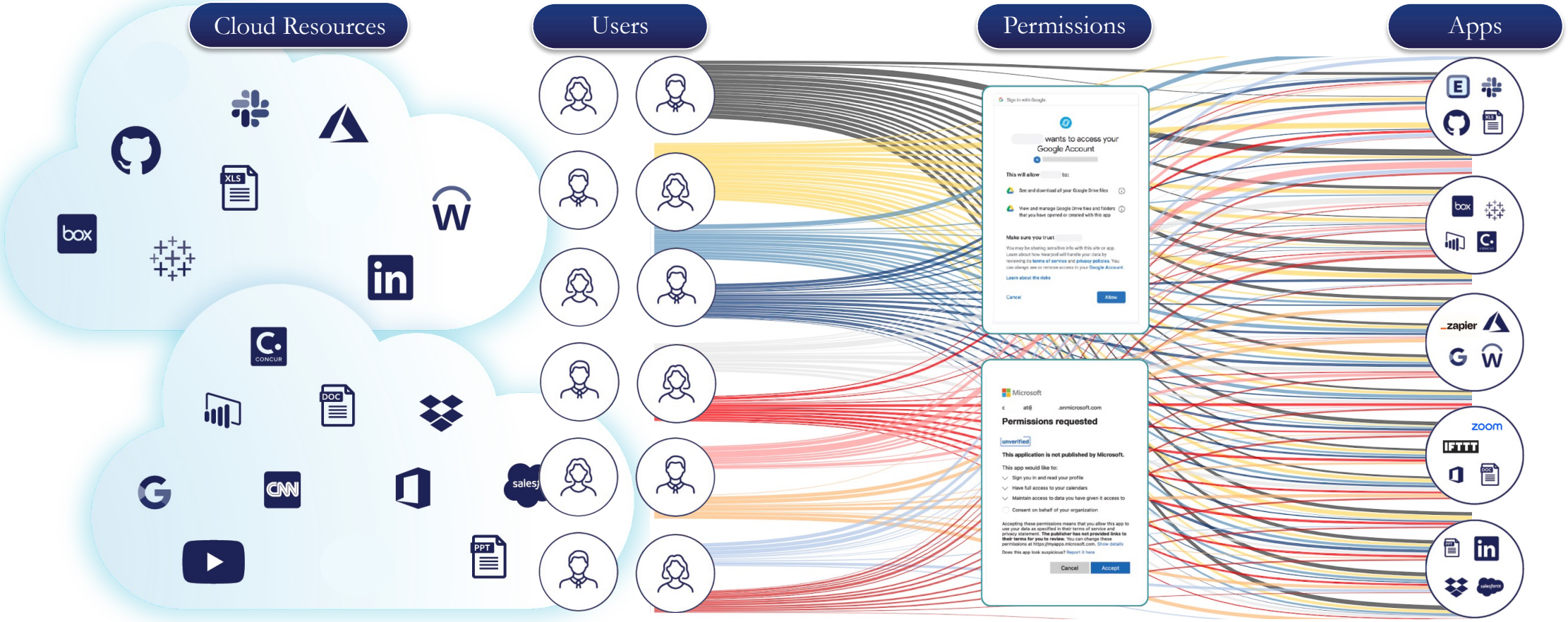
Threat



Risk Analysis Framework

- Risk Concepts: Threat, Vulnerability/Attack Surface, Impact
- Data: OAuth approval logs + user groups/roles

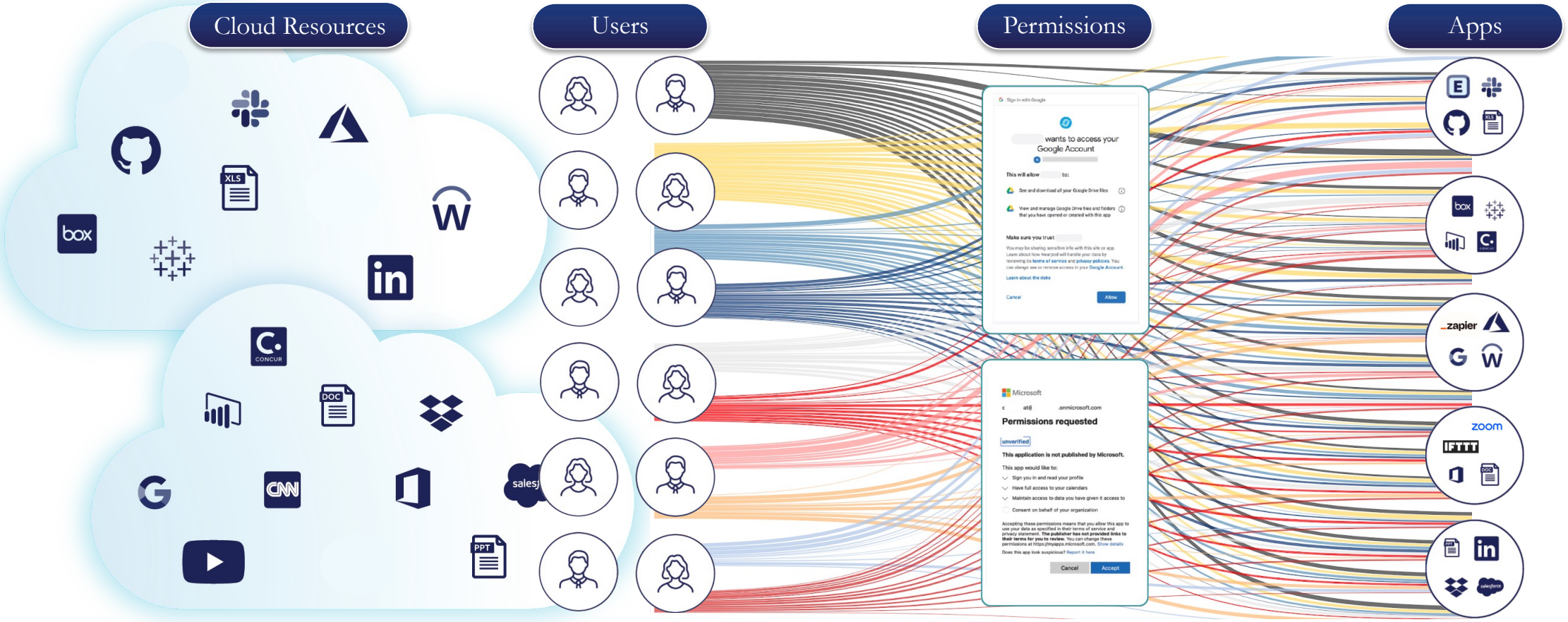
Impact | Vulnerability Attack Surface Area | Threat



Risk Analysis Framework

- Risk Concepts: Threat, Vulnerability/Attack Surface, Impact
- Data: OAuth approval logs + user groups/roles
- Approach
  - App risk -> scope risk -> user risk
  - Assess -> filter/refine -> prioritize/remediate

Impact | Vulnerability Attack Surface Area | Threat

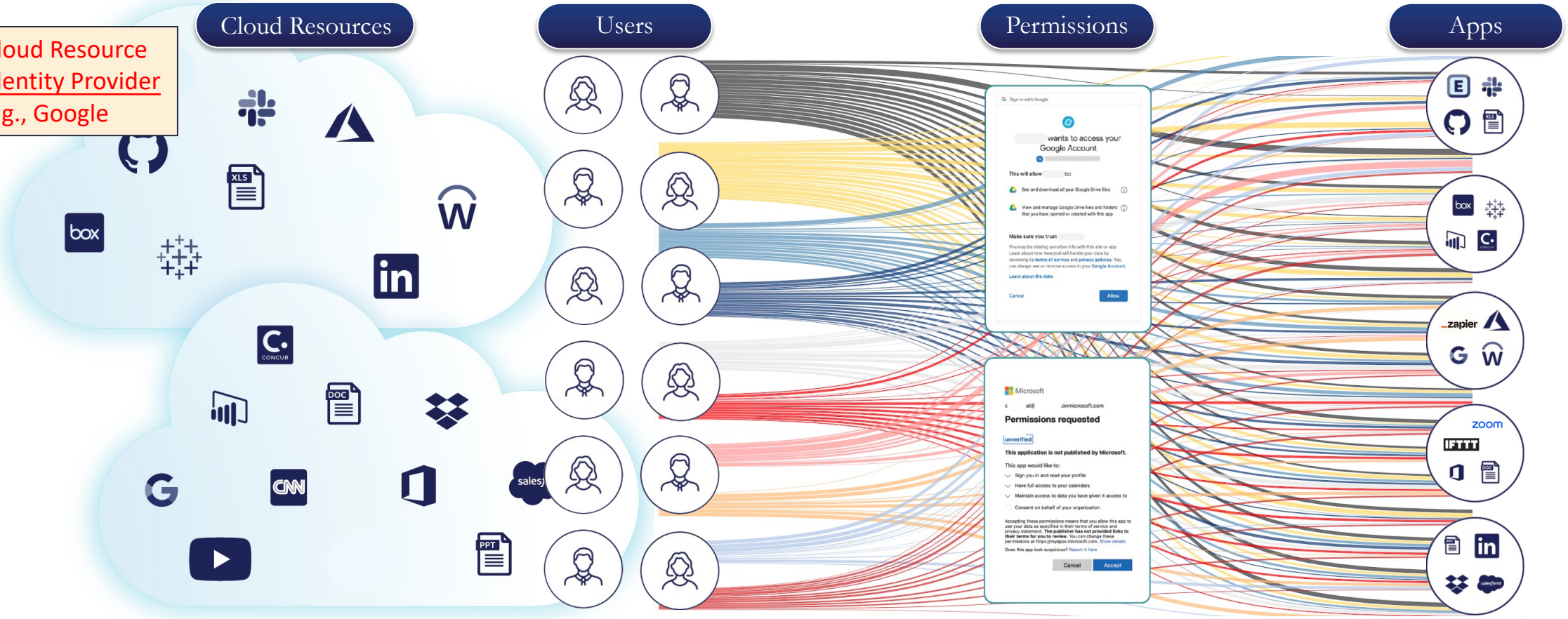


Risk Analysis Framework

- Risk Concepts: Threat, Vulnerability/Attack Surface, Impact
- Data: OAuth approval logs + user groups/roles
- Approach
  - App risk -> scope risk -> user risk
  - Assess -> filter/refine -> prioritize/remediate

Impact | Vulnerability Attack Surface Area | Threat

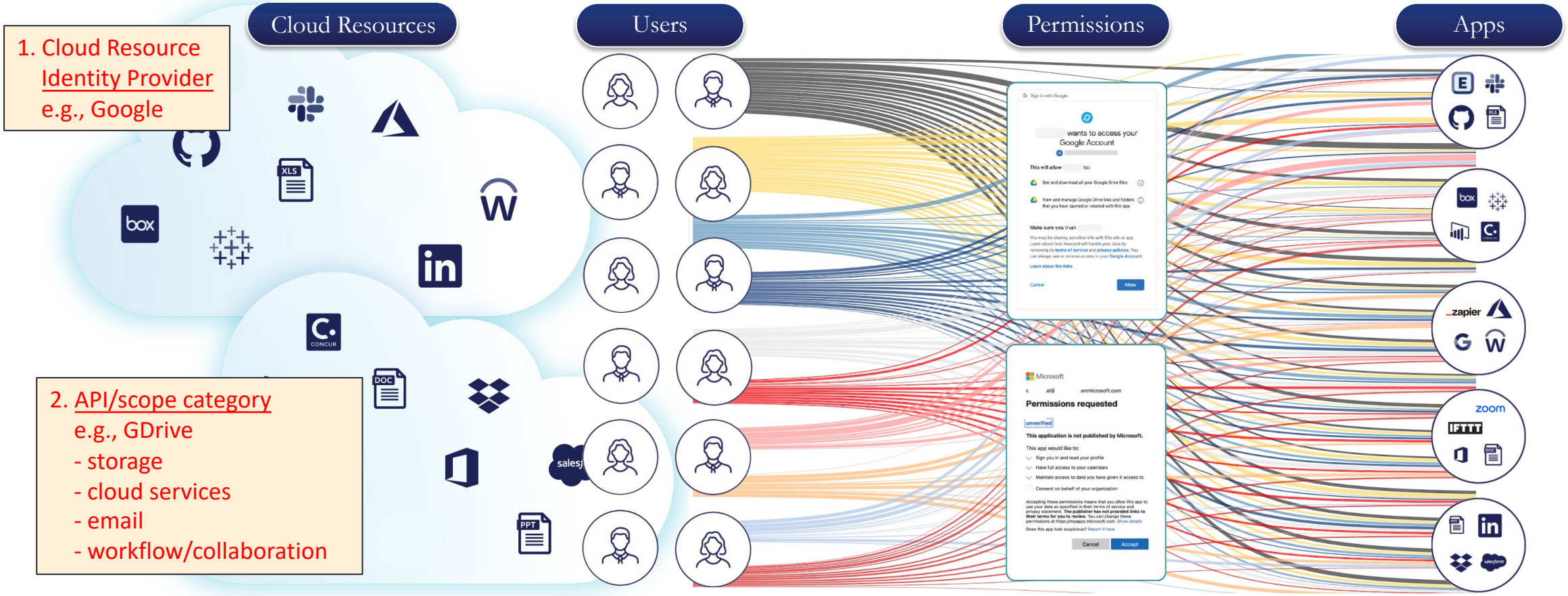
1. Cloud Resource Identity Provider e.g., Google



Risk Analysis Framework

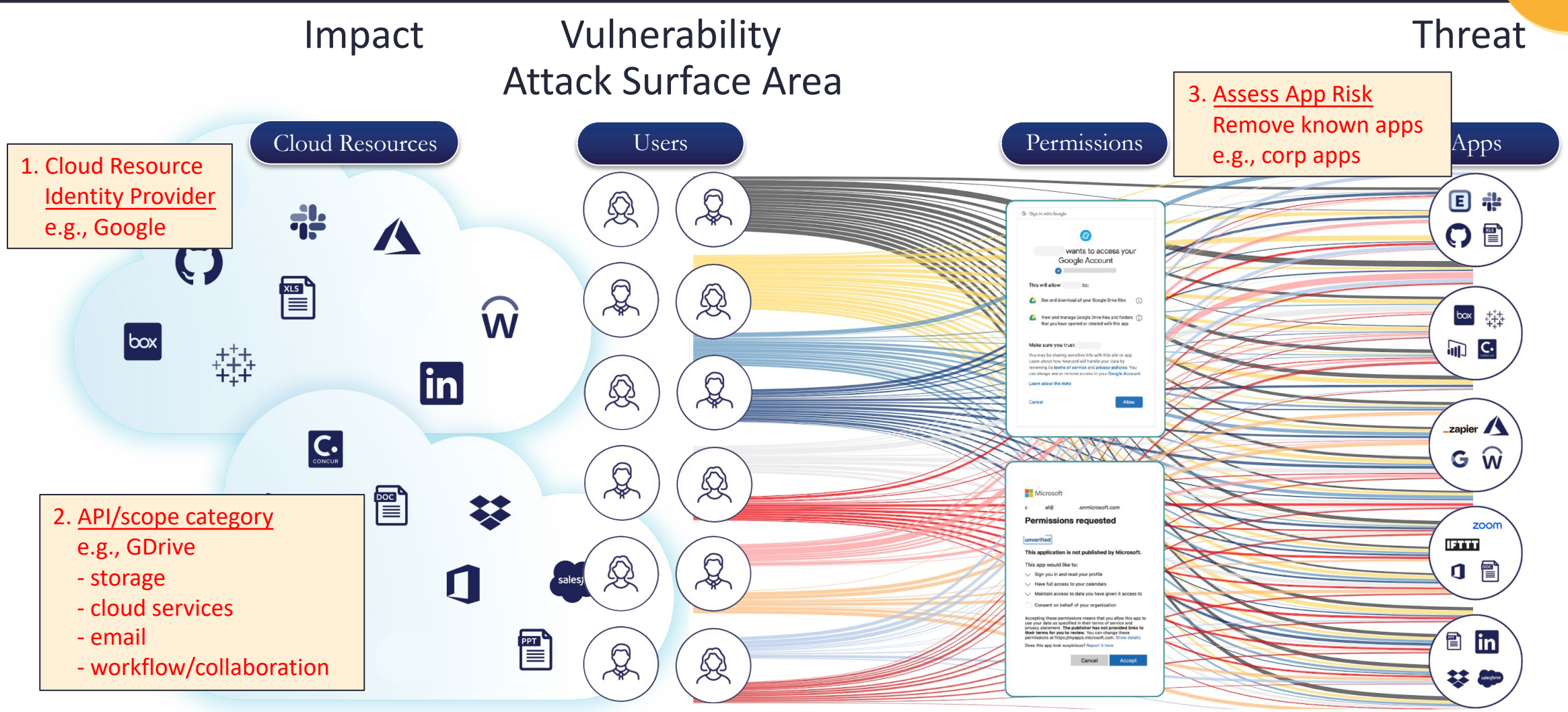
- Risk Concepts: Threat, Vulnerability/Attack Surface, Impact
- Data: OAuth approval logs + user groups/roles
- Approach
  - App risk -> scope risk -> user risk
  - Assess -> filter/refine -> prioritize/remediate

Impact | Vulnerability Attack Surface Area | Threat



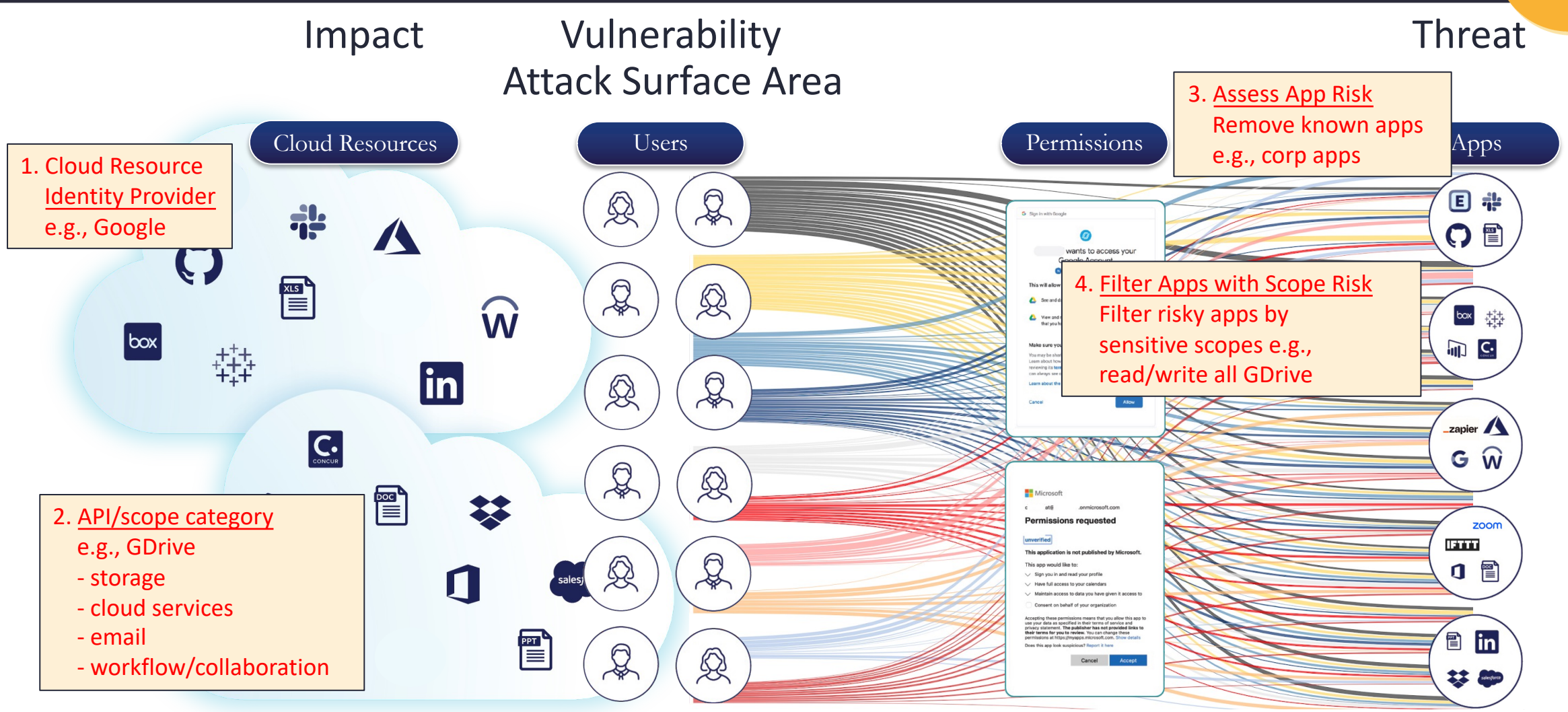
Risk Analysis Framework

- Risk Concepts: Threat, Vulnerability/Attack Surface, Impact
- Data: OAuth approval logs + user groups/roles
- Approach
  - App risk -> scope risk -> user risk
  - Assess -> filter/refine -> prioritize/remediate



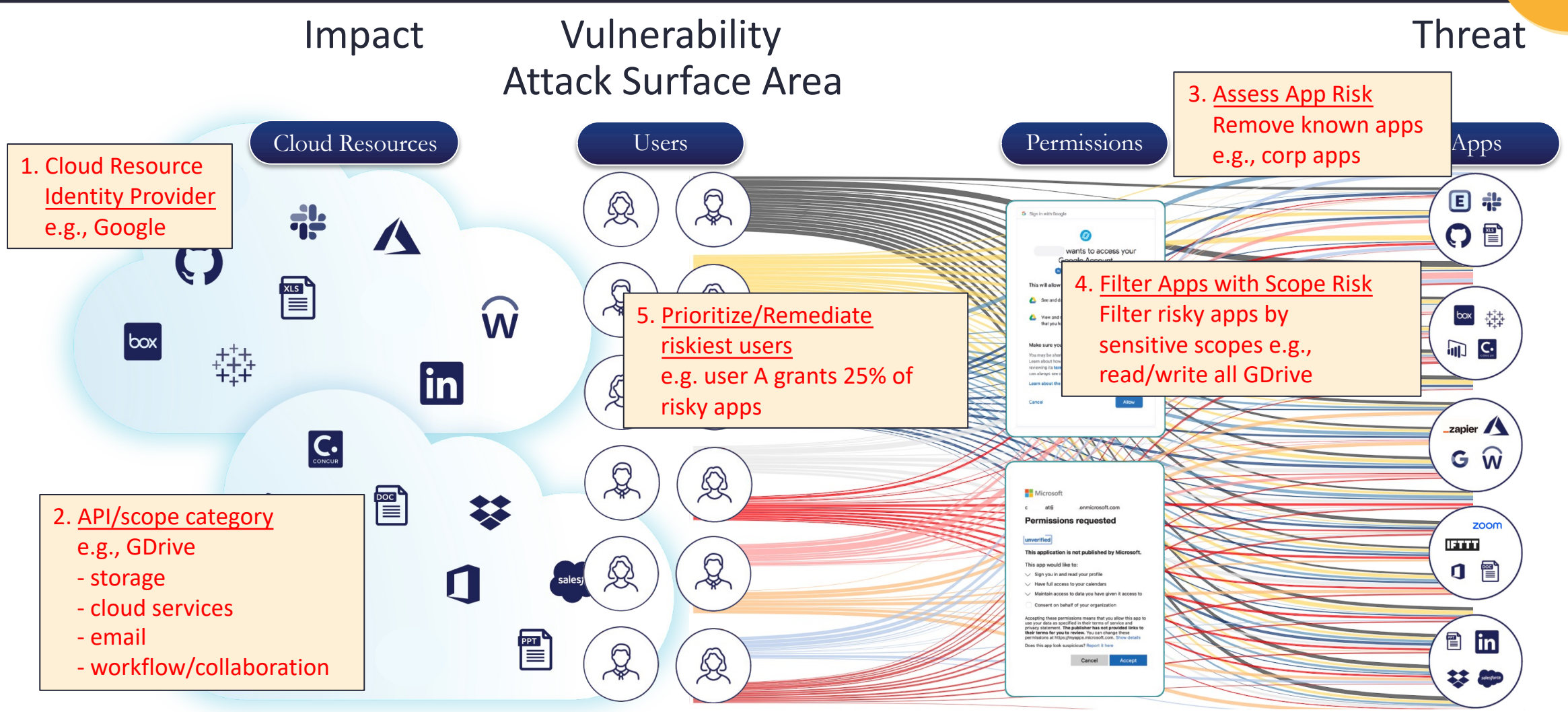
Risk Analysis Framework

- Risk Concepts: Threat, Vulnerability/Attack Surface, Impact
- Data: OAuth approval logs + user groups/roles
- Approach
  - App risk -> scope risk -> user risk
  - Assess -> filter/refine -> prioritize/remediate



Risk Analysis Framework

- Risk Concepts: Threat, Vulnerability/Attack Surface, Impact
- Data: OAuth approval logs + user groups/roles
- Approach
  - App risk -> scope risk -> user risk
  - Assess -> filter/refine -> prioritize/remediate



Why, why, why?

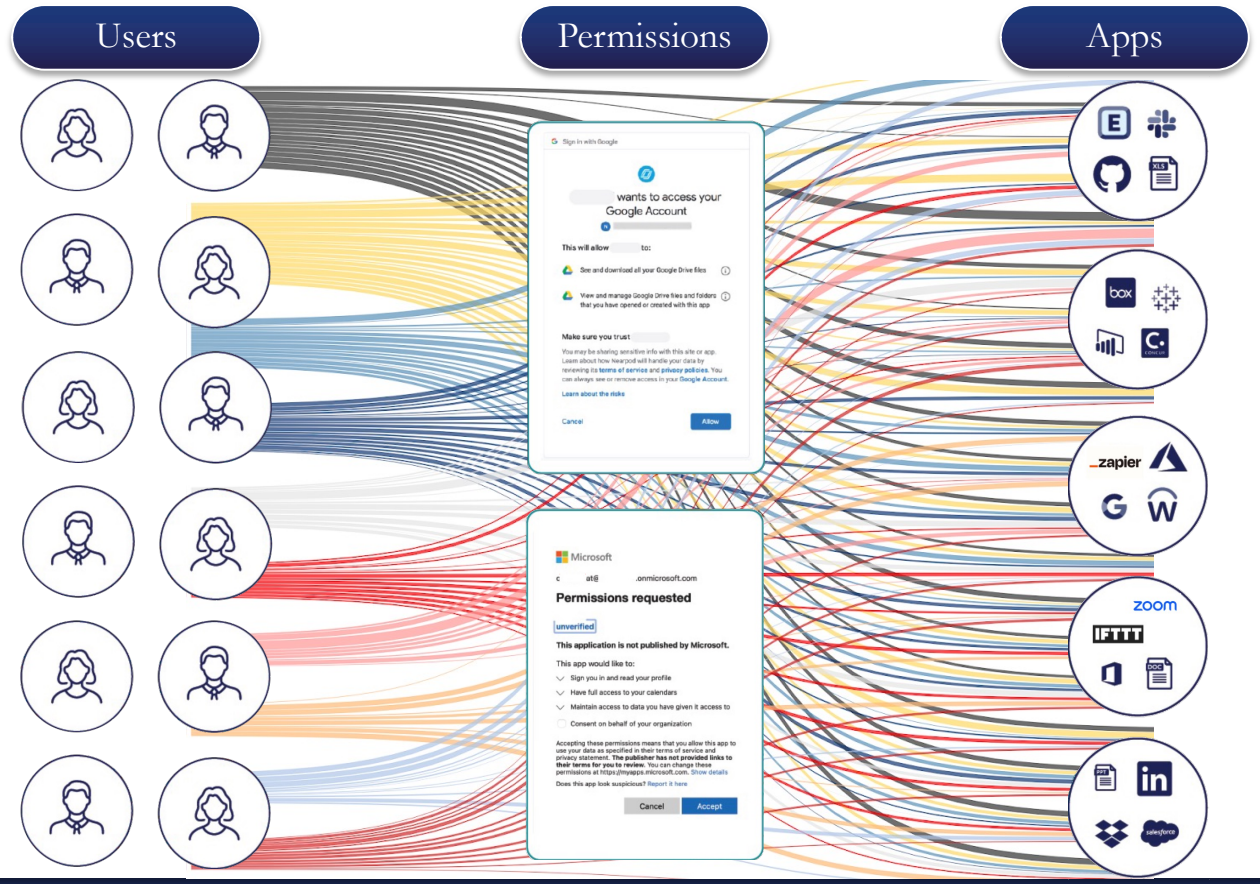
"The man who can smile when things go wrong has thought of someone else he can blame it on." – Robert Bloch

Why did this happen?

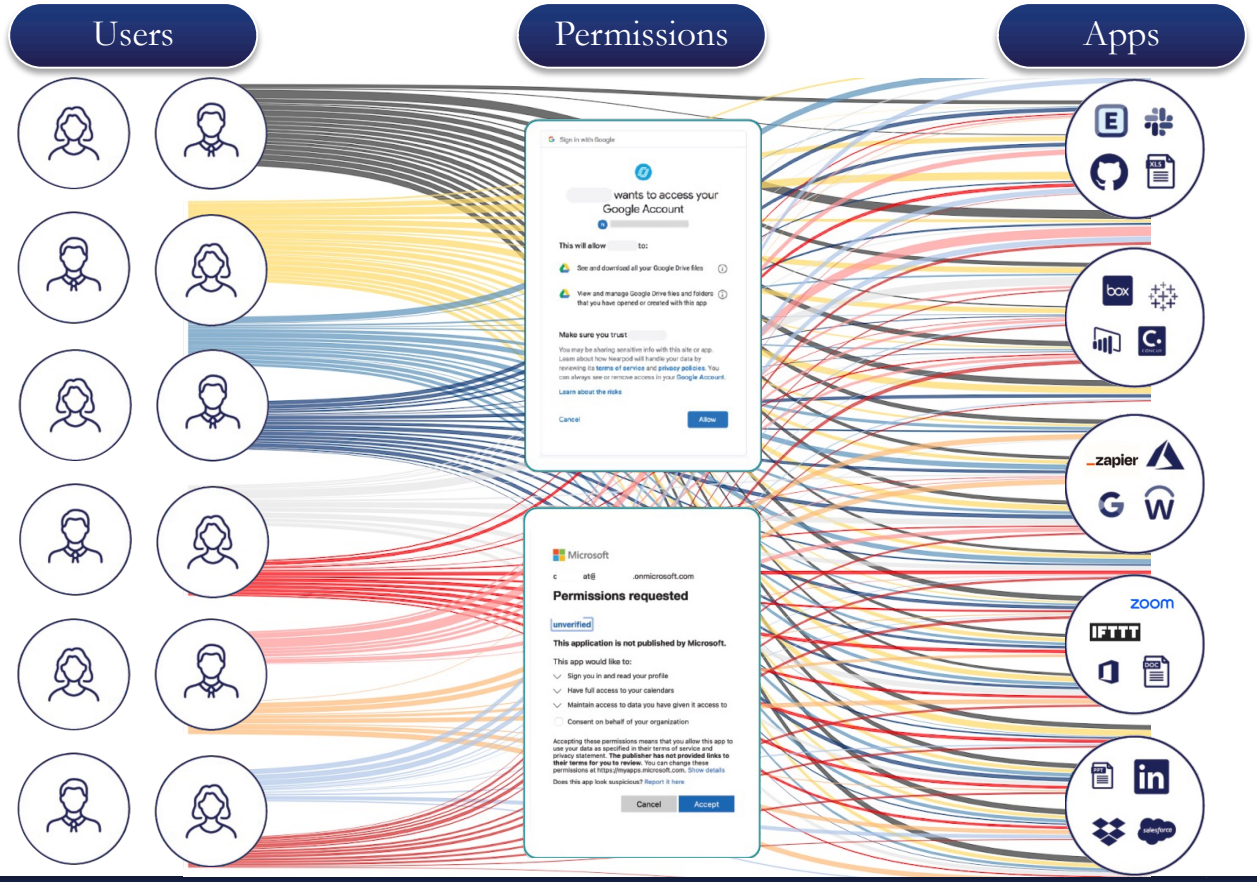
"It's human to make mistakes and some of us are more human than others."

— Ashleigh Brilliant

A decade of consumer-driven Internet (OAuth 2.0)



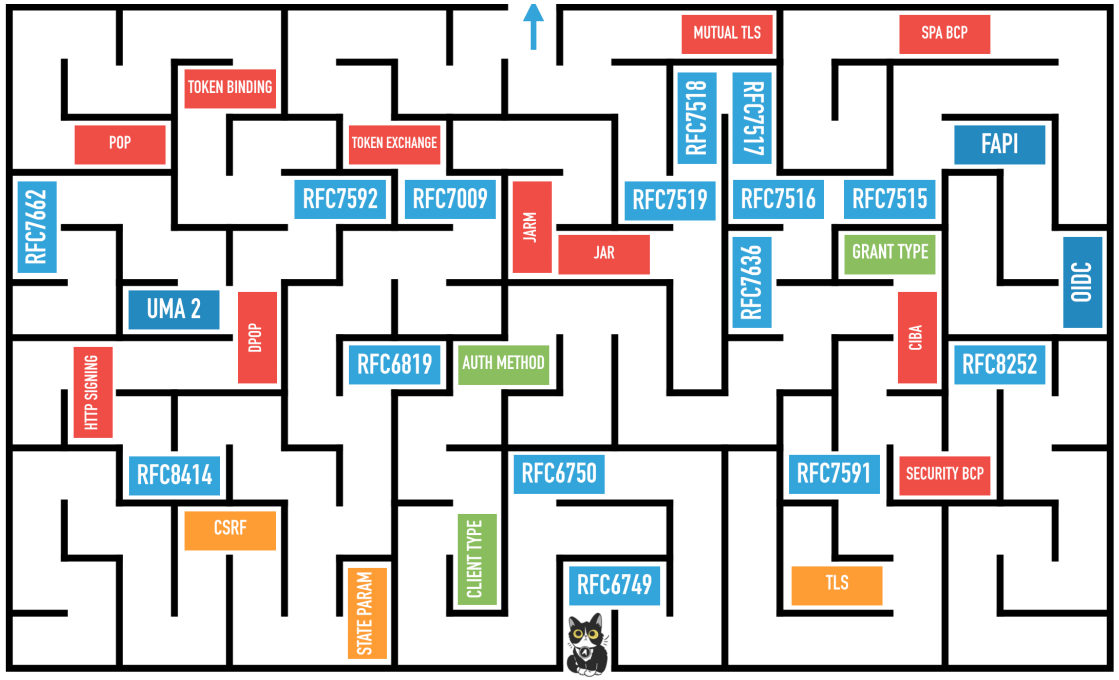
A decade of consumer-driven Internet (OAuth 2.0)



Protocol Confusion

- **OAuth 2.0 (2012)**
  Users dynamically granting approval of 3rd-party applications to corporate data.
- **OIDC (2014): SSO using OAuth**
  Let's use an authorization framework for authentication
- **OAuth 2.0 Device Authorization Grant (2019)**
  I need a consumer enterprise authorization protocol to log into Netflix on my ~~Smart~~ Dumb TV.
- **SSO on top of Custom OAuth Flows (ongoing)**
  - *Microsoft SSO allows device code flow with dynamic changing of scopes during token refresh*
  - *AWS SSO called OIDC but is device code flow for SSO for browser+CLI that involves API keys.*

Securing Cloud Resource Access



OAuth 2.0 RFCs [1]

[1] OAuth 2.1: How Many RFCs Does it Take to Change a Lightbulb?
https://developer.okta.com/blog/2019/12/13/oauth-2-1-how-many-rfcs

Every use~~less~~ case and the kitchen sink

What can I do?

"Once I wanted total happiness – now I will settle for a little less pain.

— Ashleigh Brilliant

What can I do?

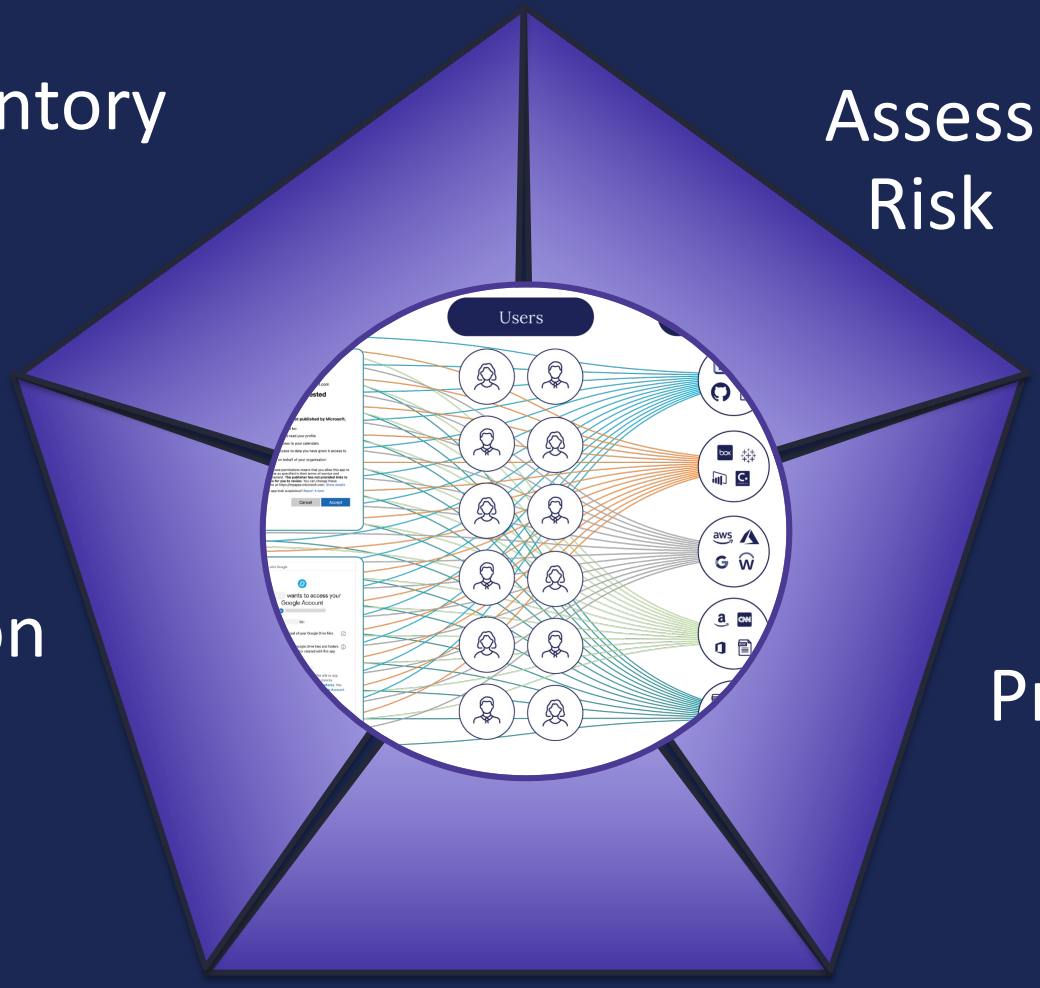
ON THE ROAD TO SUCCESS,
THERE ARE NO SHORTCUTS.
JOIN OUR TEAM
800-669-0322
shaffertrucking.com
SHAFFER
TRUCKING
OUR MOST
VALUABLE
RESOURCE SITS
63 FEET AHEAD.

What ~~can~~ should I do?

Stronger Together

Inventory

Assess Risk



Remediation

Prevention

Detection

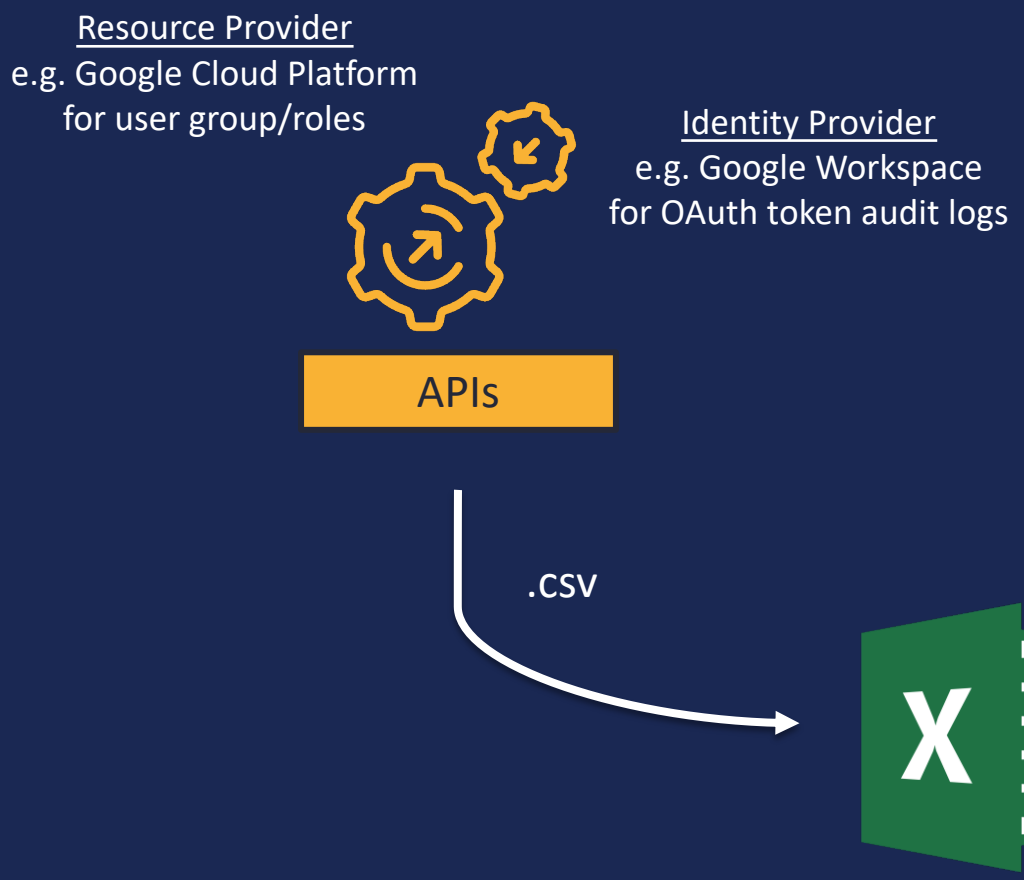
Inventory

Data

- Identity provider audit logs
- User groups/roles from identity or resource provider
- Approvals, revocations

Tools

- Vendor console / APIs
- Vendor APIs (example scripts to read audit logs or dump directory info)



Assess Risk

Risk Analysis Framework

- Risk Concepts: Threat, Vulnerability/Attack Surface, Impact
- Data: OAuth approval logs + user groups/roles
- Approach
  - App risk -> scope risk -> user risk
  - Assess -> filter/refine -> prioritize/remediate

Stronger Together

Unexpected

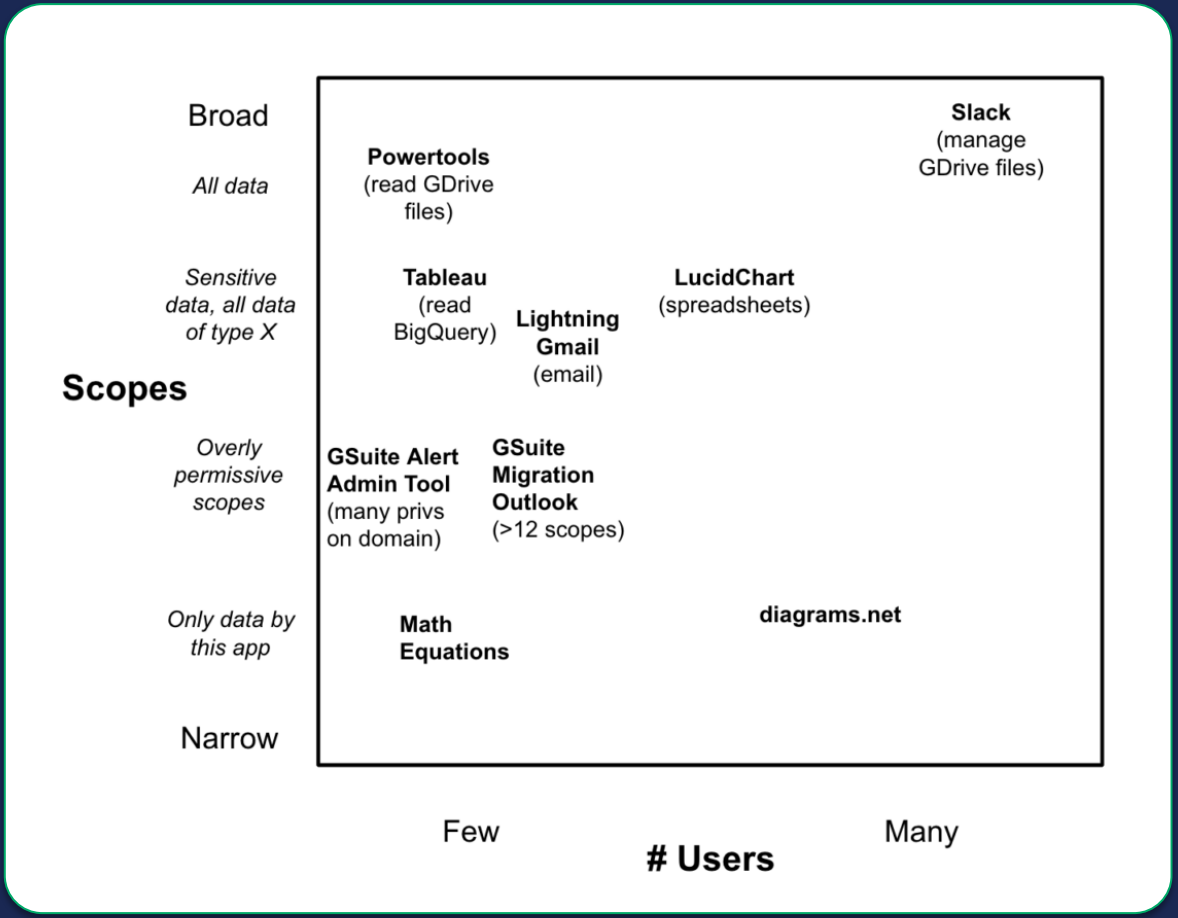
- Unrecognized or unauthorized applications
- Confusing or wide-ranging scopes
- Demo, Untitled, dev, one-off applications

Outliers

- Large # apps granted per user
- Large # repeated requests by users

Sensitivity

- Sensitive scopes granted by user
- Sensitive scopes requested by applications

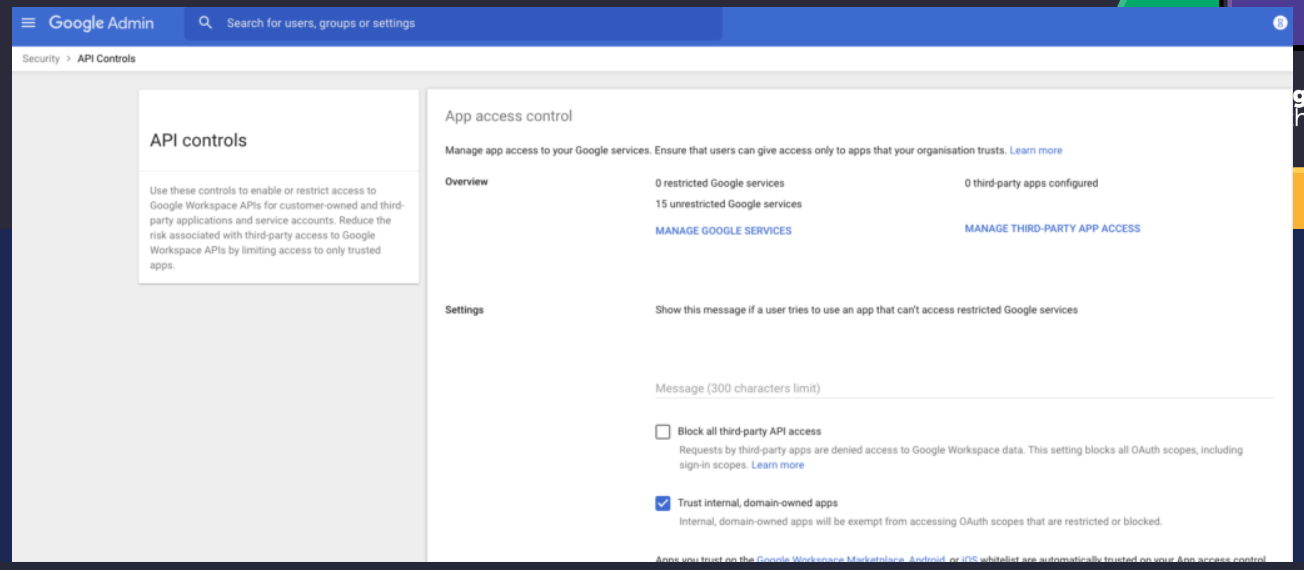


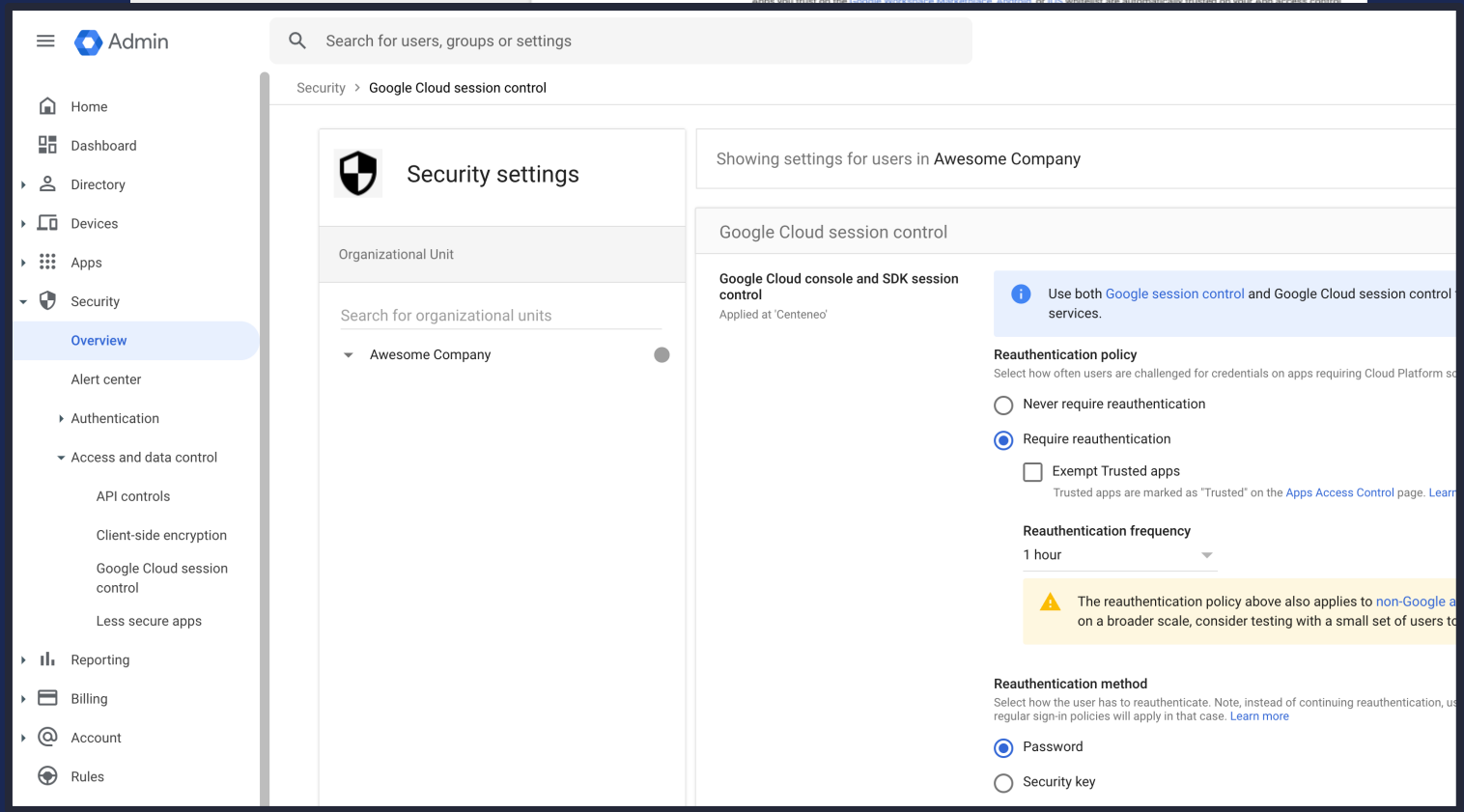
Prevention Controls

Approval Process

- Move to domain-wide / admin-created approved app list (pare to minimum)
- Remove user-only approval processes -> shift to admin-only approvals

Session timeouts





netskope

Detection Measures

Stronger Together

App Lists

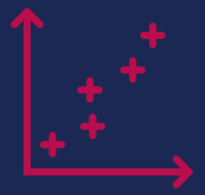
- Allowed apps are whitelisted
- Unrecognized apps generate alerts

Utilize vendor-supplied behavioral detection (M/L)

- Allowed apps are whitelisted
- Unrecognized apps generate alerts

Audit app authorizations/approvals (OAuth) with user activity

- Track credential usage
- Revoke unused applications



Remediation Procedures

- Revoking access when credentials are compromised

- Both OAuth access and refresh tokens
- Revoke access across multiple, synchronized identity systems (e.g. SSO)

- Test and retest

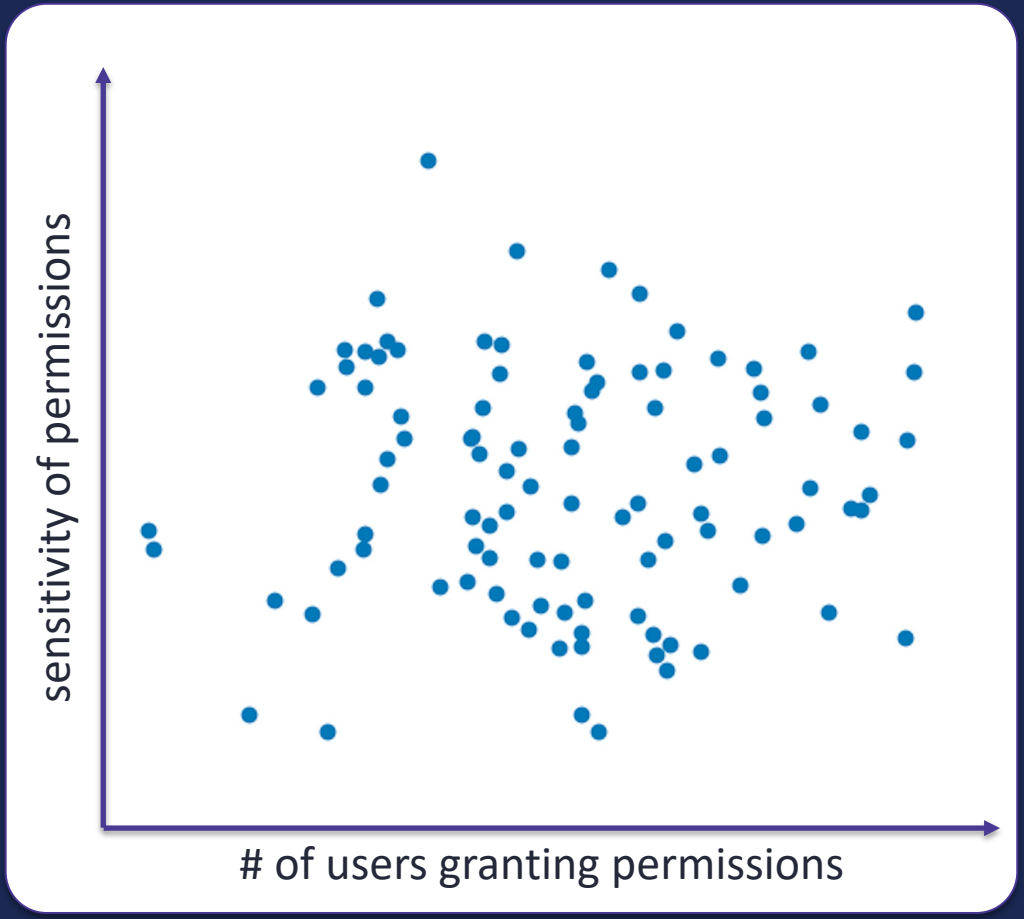
Apply What You Have Learned

Next week, create a baseline

- Assign a resource to review OAuth application data risk
- Review the information in this presentation; Ask questions or clarifications.
- Audit the current applications granted access by all users and the permissions, using your identity provider Console, APIs, or example scripts.
- Create a baseline of applications, permissions, and user data in a reporting tool or database (Excel at a minimum), using the audited data.

Apply What You Have Learned

- Next month, assess risk
  - Unexpected
    - Unrecognized or unauthorized applications
    - Confusing or wide-ranging scopes
    - Demo, Untitled, dev, one-off applications
  - Outliers
    - Large # apps granted per user
    - Large # repeated requests by users
  - Sensitivity
    - Sensitive scopes granted by user
    - Sensitive scopes requested by applications



Apply What You Have Learned

- Within three months, address high-risk areas
  - Implement better preventative controls
    - Enforce session timeouts
    - Move to domain-wide/admin-created approved app list (pare to minimum)
    - Remove user-only approval processes -> shift to admin-only approvals
  - Improve detection measures
    - Allowed apps are whitelisted, unrecognized apps generate alerts
    - Utilize vendor-supplied behavioral detection (M/L)
    - Correlate app authorizations/approvals (OAuth) with user activity with those apps to track credential usage and to revoke unused applications

Apply What You Have Learned

- Within three months, address high-risk areas
  - Review and correct remediation procedures
    - Revoking access when credentials are compromised
    - Revoke both OAuth access and refresh tokens
    - Revoke access across multiple, synchronized identity systems (e.g. SSO)
    - Test and retest
  - Implement a testing process
    - When evaluating new apps, identify OAuth dependencies early on, record OAuth client ids and use in prevention, detection, and remediation procedures
  - Operationalize audit and testing stages into your processes
  - Create relative improvement goals, measure (report)

RSAConference™2023

Stronger Together

Thank you

Jenko Hwong

Principal Threat Researcher
Netskope
Twitter: @jenkohwong
Mastodon: @jenko@infosec.exchange