Building identity for an open perimeter

Tejas Dharamshi
Senior Security Software Engineer
@tejasdharamshi

NETFLIX

06 January 2016

Netflix Is Now Available Around the World

World's Leading Internet TV Service Now Live in More than 190 Countries

Las Vegas, January 6, 2016 -- Netflix launched its service globally, simultaneously bringing its Internet TV network to more than 130 new countries around the world. The company made the announcement -- and the service went live -- during a keynote by Co-founder and Chief Executive Reed Hastings at CES 2016.

#netflixeverywhere

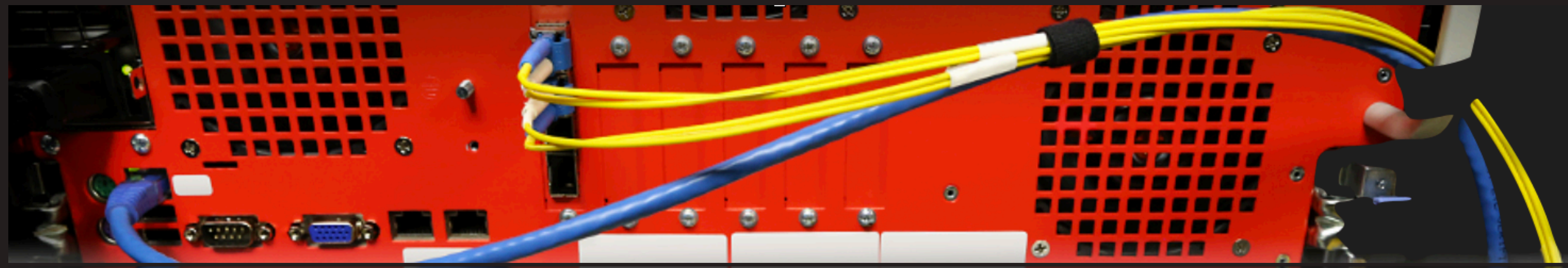
NETFLIX
THE CROWN
NETFLIX
STRANGER THINGS
A NETFLIX ORIGINAL SERIES
ALL EPISO
July
NETFLIX
SACRED GAMES
NETFLIX
OZARK
NETFLIX
ORANGE is the new BLACK
A NETFLIX ORIGINAL SERIES
HOUSE of CARDS
THE FINAL SEASON
NOV 2 | NETFLIX
NETFLIX
NARCOS
NETFLIX
BODYGUARD

B2B

Content & Studio

Over
700
apps

Device Partner



Open Connect

360

NETFLIX
Employee Landing Page

workday.

zendesk

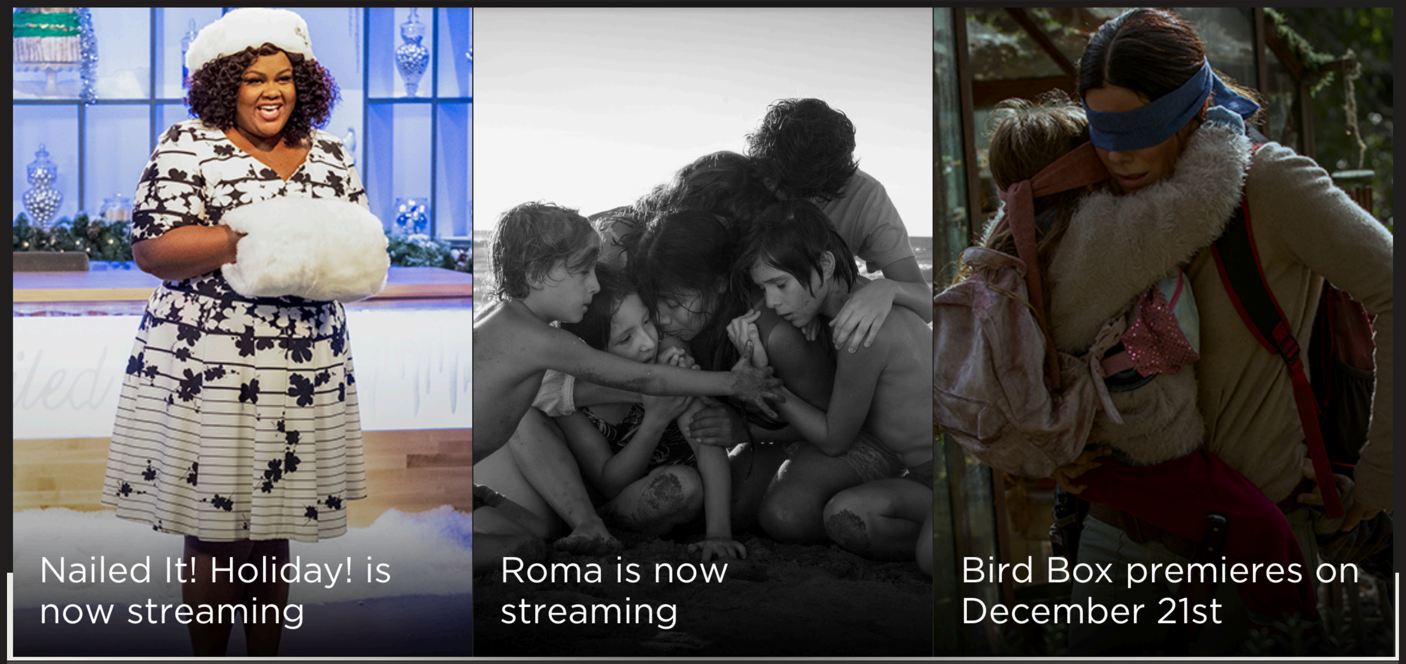
Corporate

NETFLIX
Big Data Portal

NETFLIX
Lemur

spinnaker

Engineering



Nailed It! Holiday! is now streaming

Roma is now streaming

Bird Box premieres on December 21st

Media Partners

NETFLIX

Location Independent Security Approach (LISA)

NETFLIX

BeyondCorp

Google

Beyond the Edge

intel

Zero Trust

FORRESTER

NETFLIX

Zero Trust
Principle 1

Zero Trust Principle 1

Netflix Identity Platform (aka Meechum)

Federation

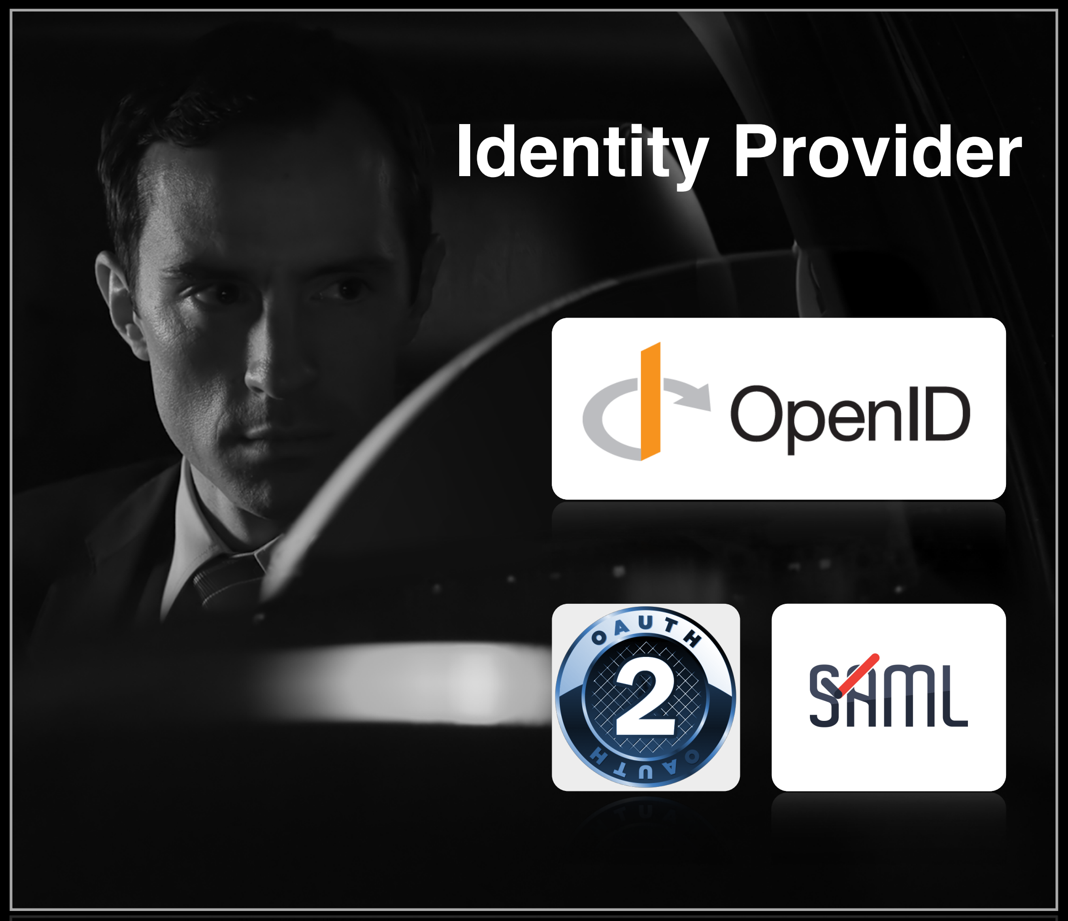
SSO

Delegate

Signed and Verifiable Identity Information

Self-service

Pluggable



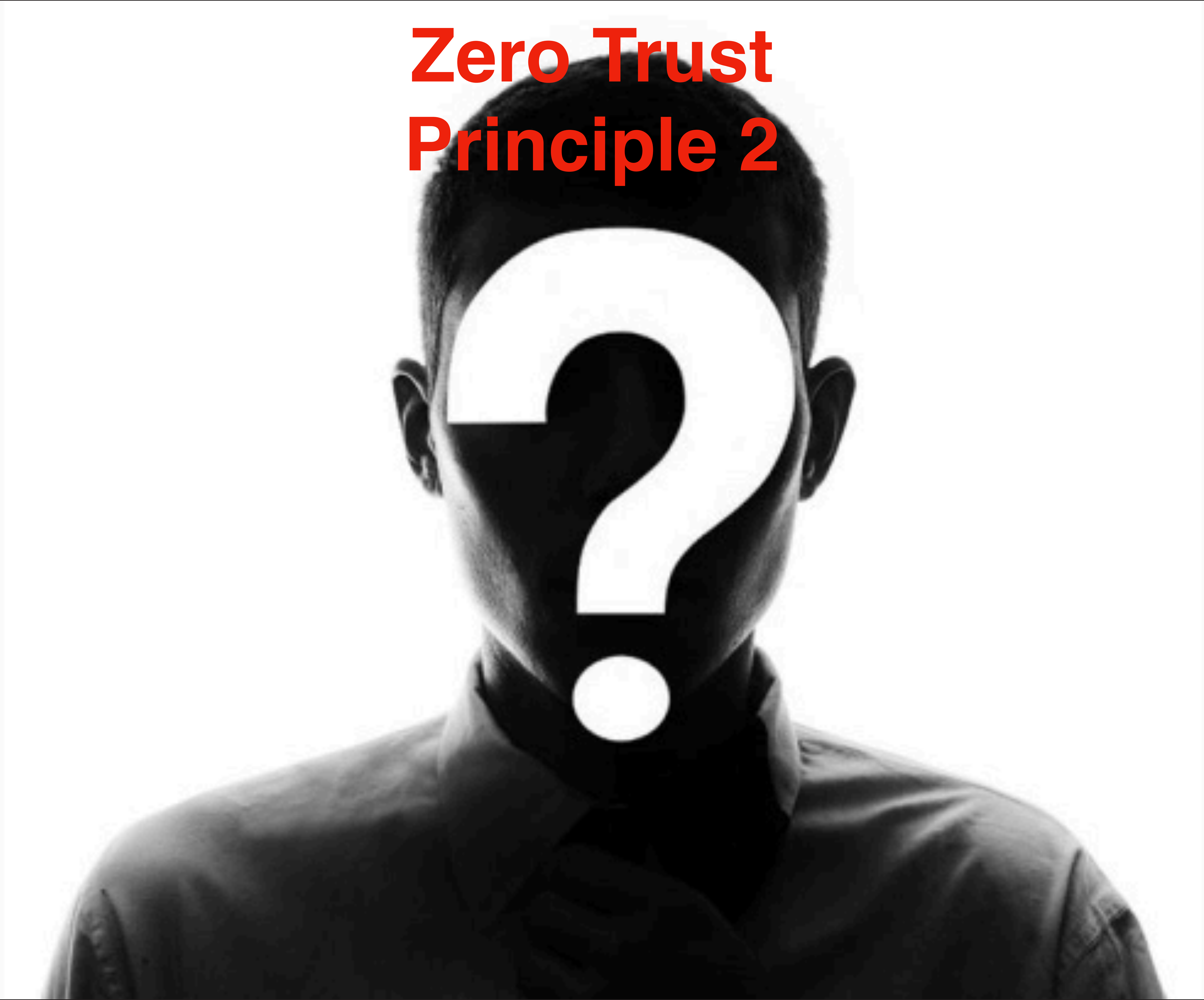
Standards (OpenId Connect, OAuth 2.0, SAML)

Layered Security

Signed and Verifiable Identity Information

User Experience

Zero Trust Principle 2



OpenLDAP™
http://www.OpenLDAP.org

Microsoft
Active Directory

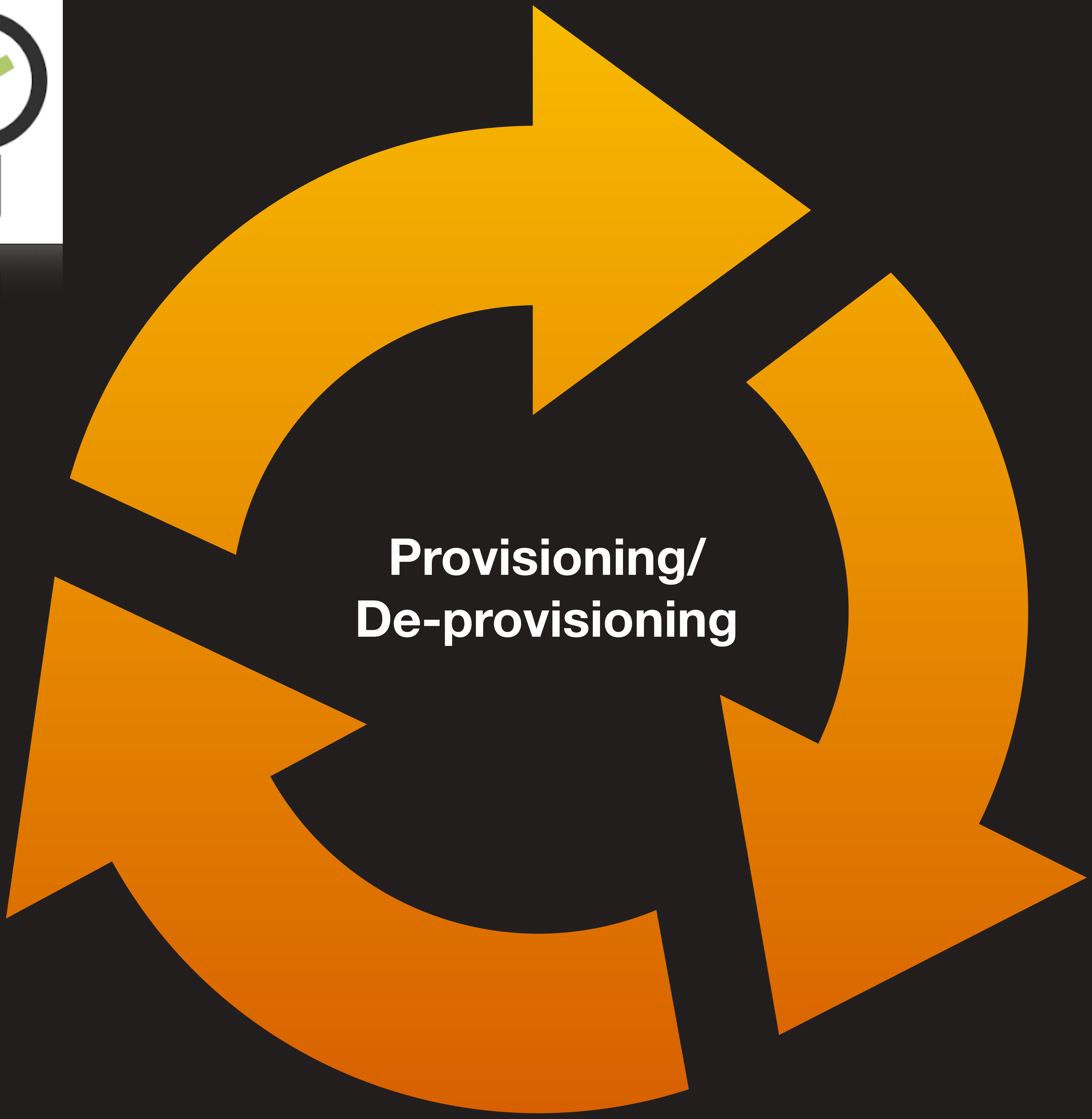
MySQL®

cassandra

Crowd

workday

STUDIO NETWORK

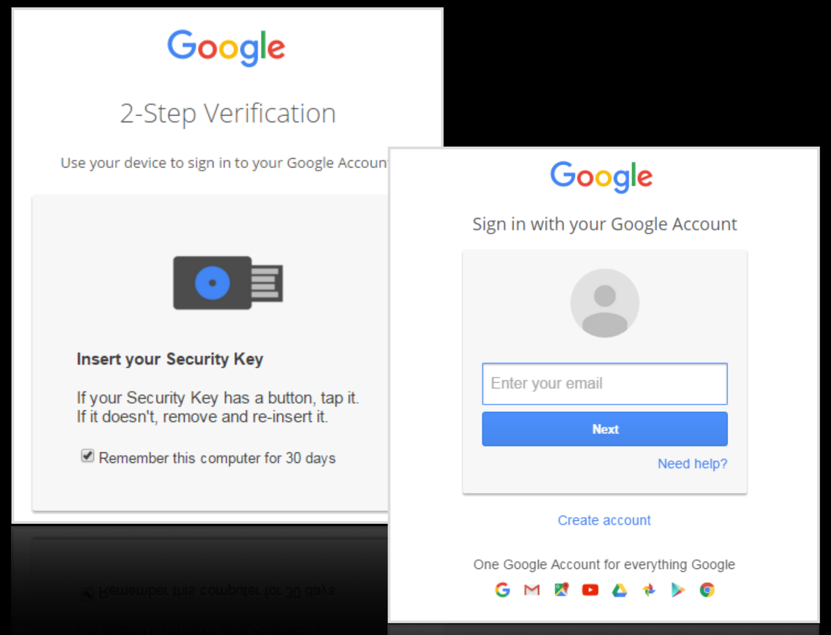

Provisioning/
De-provisioning

Google

NETFLIX

Zero Trust
Principle 3

Federation Hub (Layered Security)



Google

2-Step Verification

Use your device to sign in to your Google Accoun

Insert your Security Key

If your Security Key has a button, tap it.
If it doesn't, remove and re-insert it.

☑ Remember this computer for 30 days

Google

Sign in with your Google Account

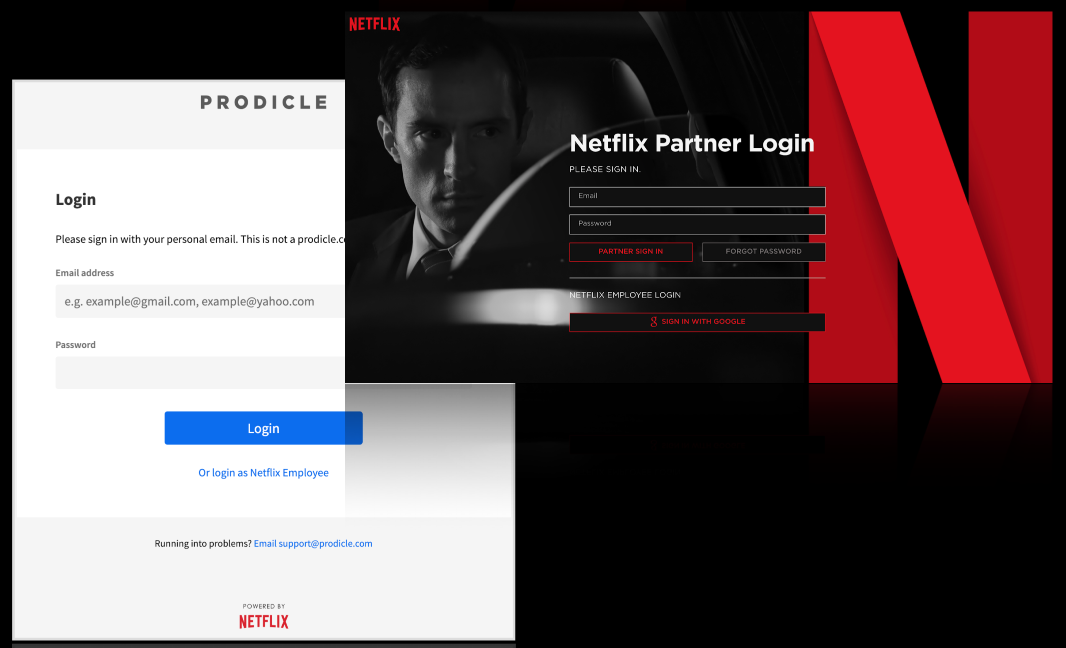
Enter your email

Next

Need help?

Create account

One Google Account for everything Google



PRODICLE

Login

Please sign in with your personal email. This is not a prodicle.c

Email address

e.g. example@gmail.com, example@yahoo.com

Password

Login

Or login as Netflix Employee

Running into problems? Email support@prodicle.com

POWERED BY NETFLIX

NETFLIX

Netflix Partner Login

PLEASE SIGN IN.

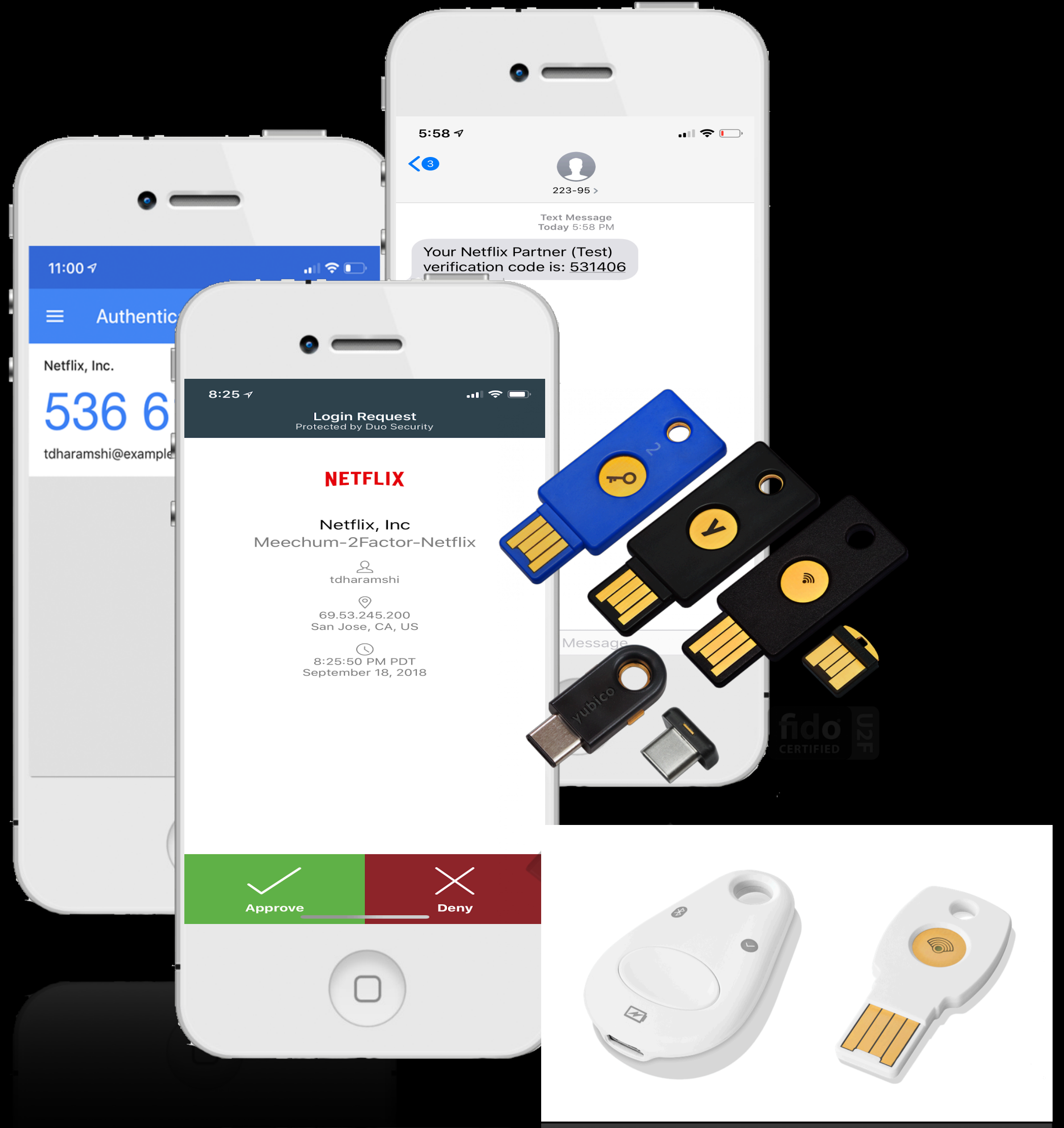
Email

Password

PARTNER SIGN IN | FORGOT PASSWORD

NETFLIX EMPLOYEE LOGIN

SIGN IN WITH GOOGLE



11:00

Authentic

Netflix, Inc.

536 6

tdharamshi@example

5:58

223-95 >

Text Message
Today 5:58 PM

Your Netflix Partner (Test) verification code is: 531406

8:25

Login Request
Protected by Duo Security

NETFLIX

Netflix, Inc
Meechum-2Factor-Netflix

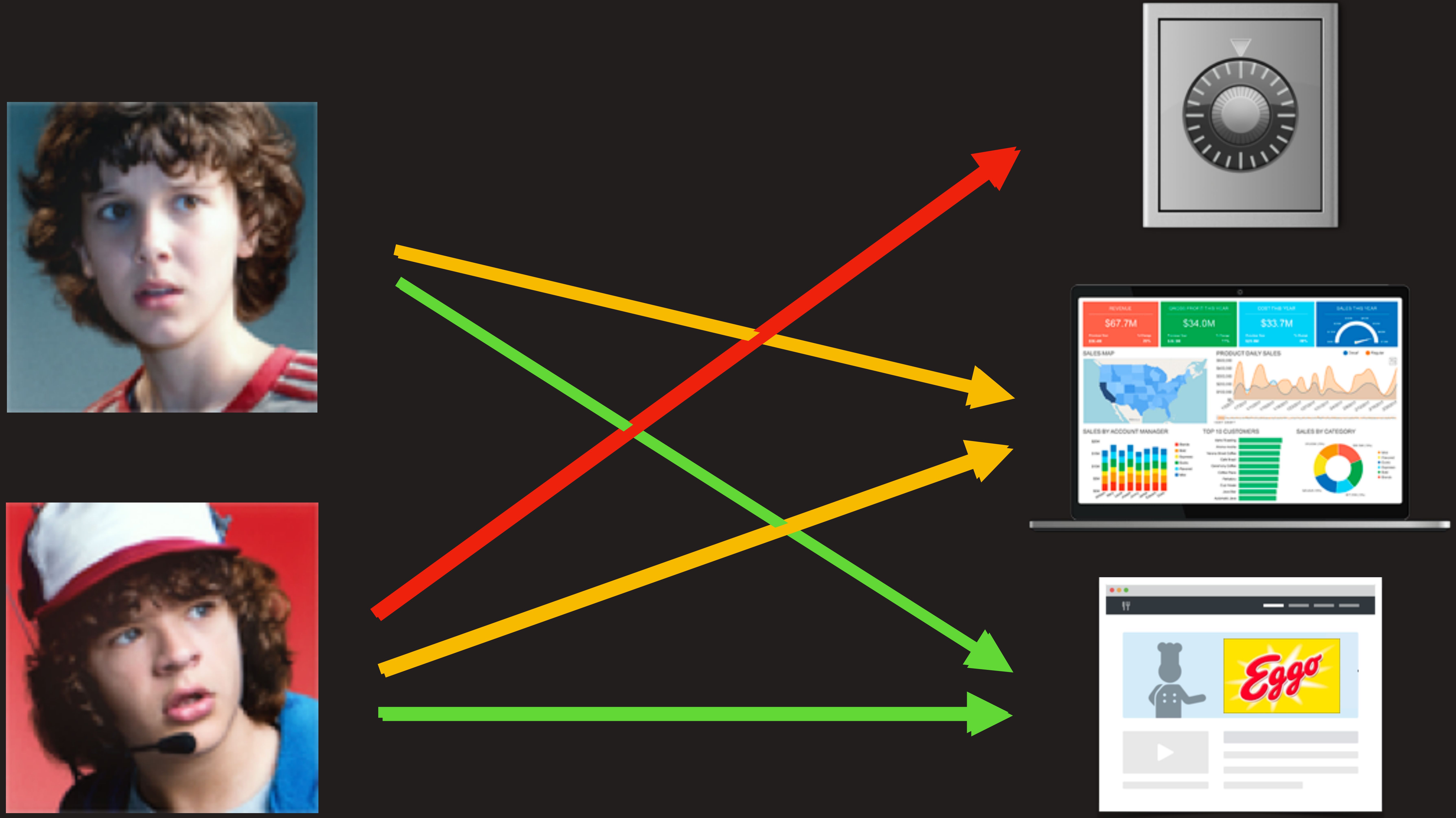
tdharamshi

69.53.245.200
San Jose, CA, US

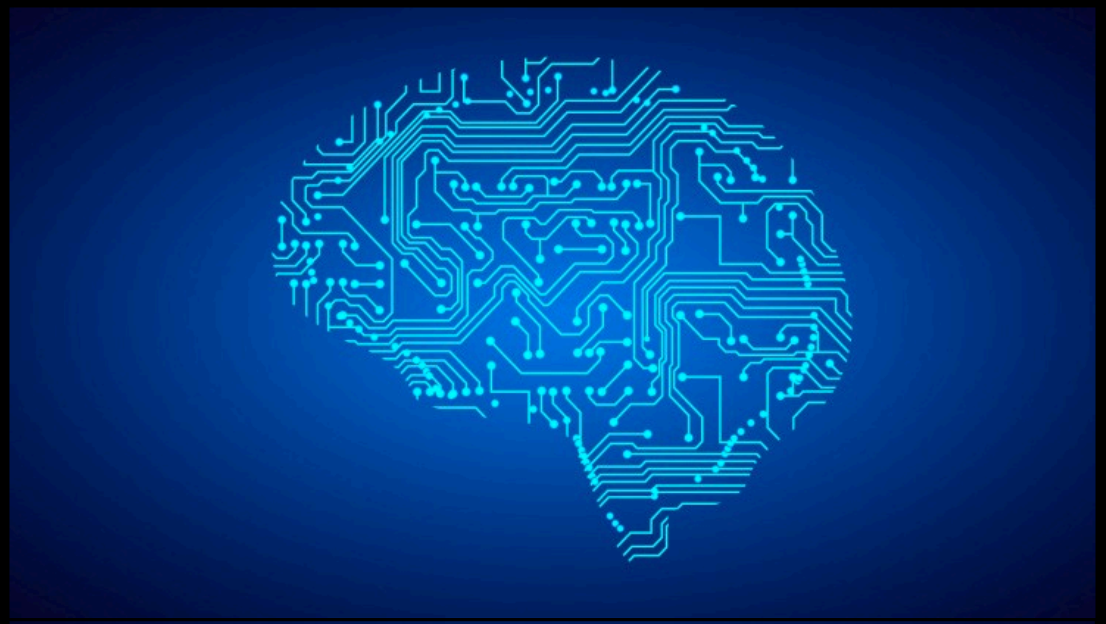
8:25:50 PM PDT
September 18, 2018

Approve | Deny

Are all access patterns the same?

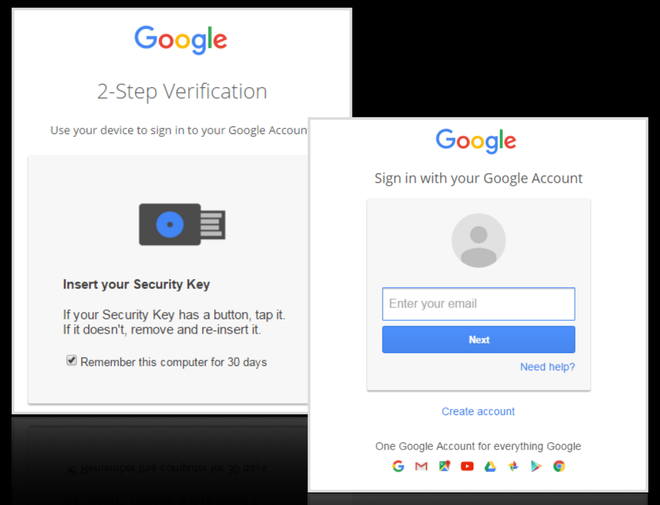


NETFLIX



Adaptive Authentication

Federation Hub (Layered Security)



Google

2-Step Verification

Use your device to sign in to your Google Accoun

Insert your Security Key

If your Security Key has a button, tap it.
If it doesn't, remove and re-insert it.

☑ Remember this computer for 30 days

Google

Sign in with your Google Account

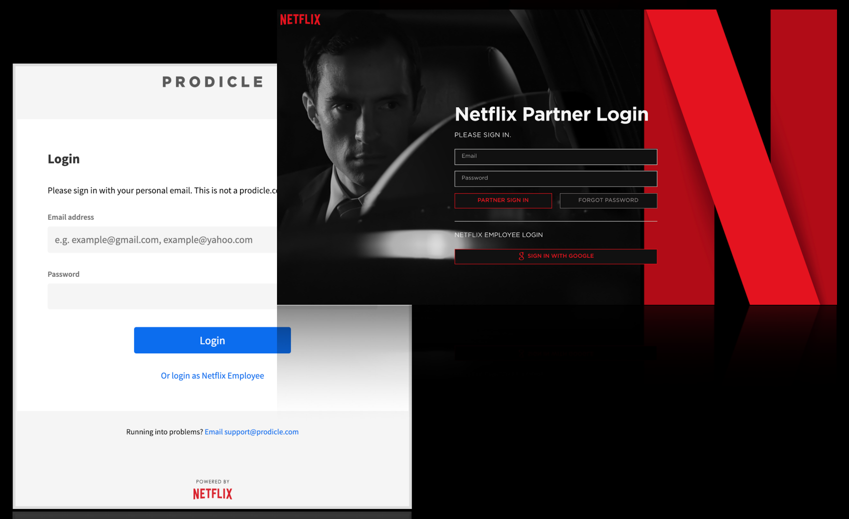
Enter your email

Next

Need help?

Create account

One Google Account for everything Google



PRODICLE

Login

Please sign in with your personal email. This is not a prodicle.c

Email address

e.g. example@gmail.com, example@yahoo.com

Password

Login

Or login as Netflix Employee

Running into problems? Email support@prodicle.com

POWERED BY
NETFLIX

NETFLIX

Netflix Partner Login

PLEASE SIGN IN.

Email

Password

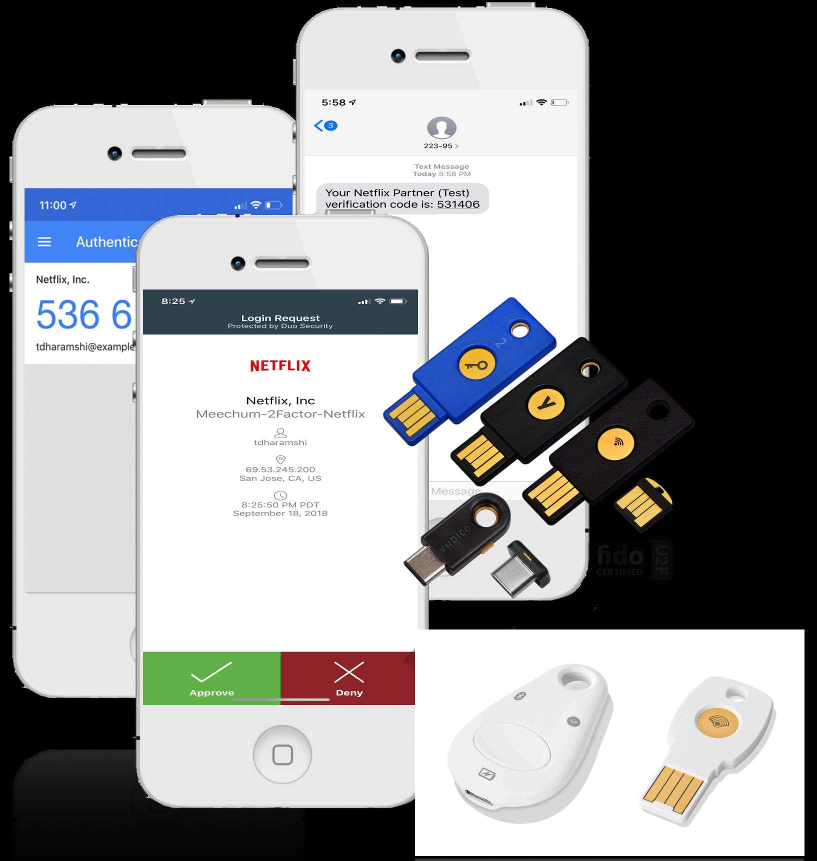
PARTNER SIGN IN

FORGOT PASSWORD

NETFLIX EMPLOYEE LOGIN

SIGN IN WITH GOOGLE

VERY LOW
LOW
MODERATE
HIGH
VERY HIGH



11:00

Authentic

Netflix, Inc.

536 6

tdharamshi@example

5:58

223-95

Text Message
Today 5:58 PM

Your Netflix Partner (Test) verification code is: 531406

8:25

Login Request
Protected by Duo Security

NETFLIX

Netflix, Inc
Meechum-2Factor-Netflix

tdharamshi

69.53.245.200
San Jose, CA, US

8:25:50 PM PDT
September 18, 2018

Approve

Deny

Zero Trust Principle 4

Bitdefender®

eset®

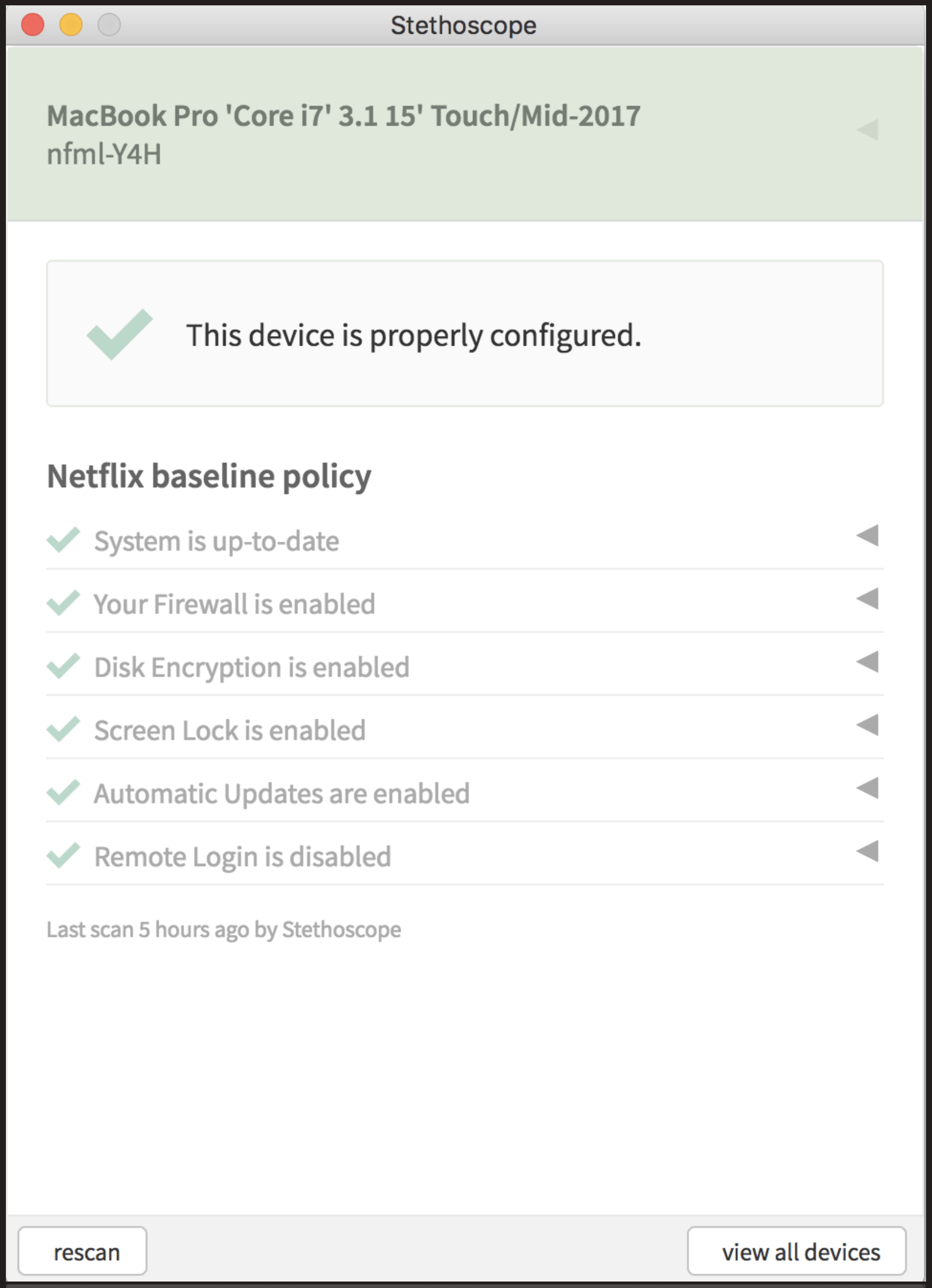
ENJOY SAFER TECHNOLOGY™

Symantec.

F-Secure®

ivanti

EXIT



Stethoscope

MacBook Pro 'Core i7' 3.1 15' Touch/Mid-2017
nfml-Y4H

✓ This device is properly configured.

Netflix baseline policy

- ✓ System is up-to-date
- ✓ Your Firewall is enabled
- ✓ Disk Encryption is enabled
- ✓ Screen Lock is enabled
- ✓ Automatic Updates are enabled
- ✓ Remote Login is disabled

Last scan 5 hours ago by Stethoscope

NETFLIX

NETFLIX

Authenticate

CHECKING DEVICE SECURITY

The OS X device you are using is unidentified.

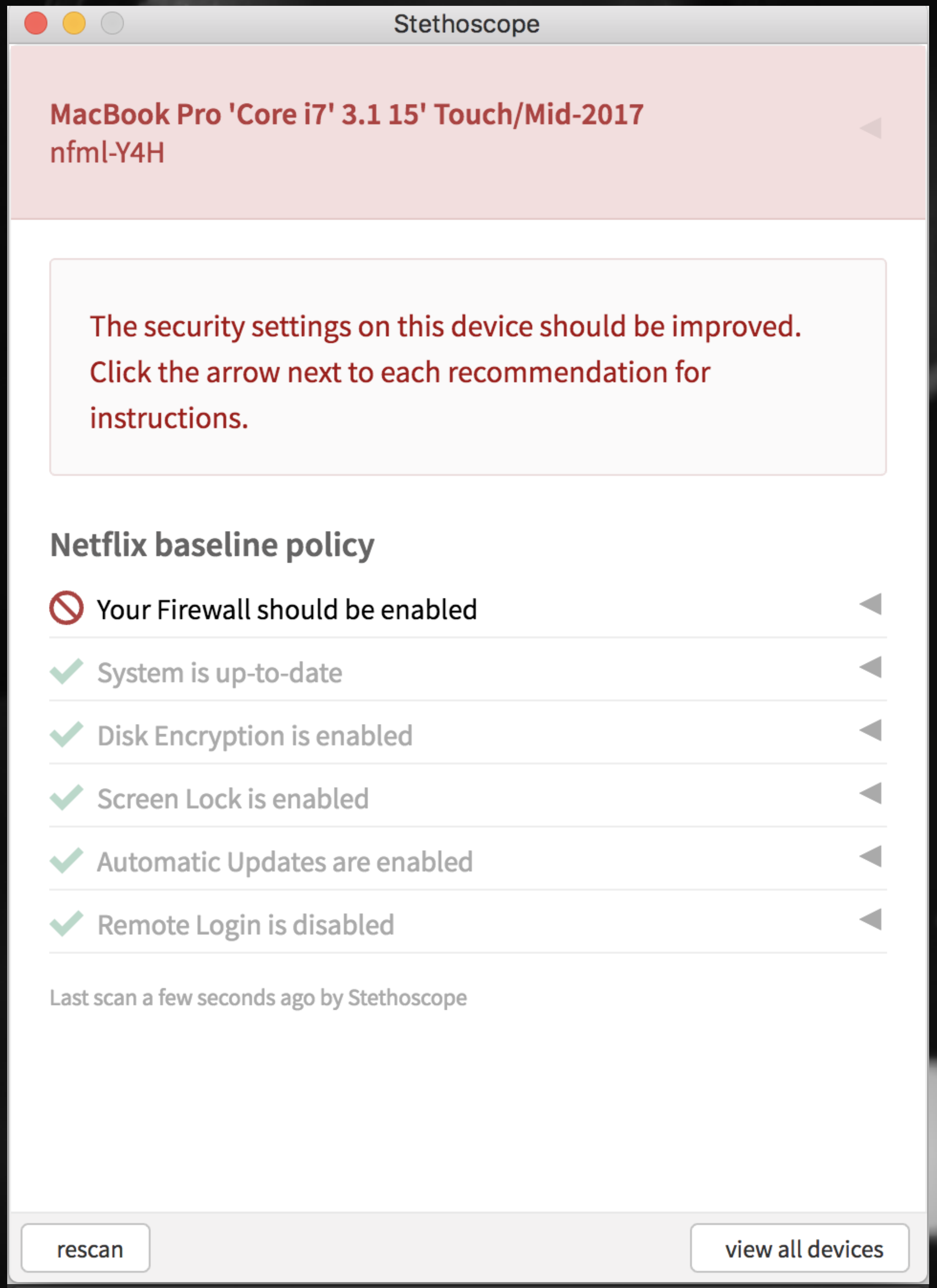
Run the Stethoscope app

□ Automatically launch next time

The Stethoscope app is a way to check your computer's security settings when accessing Netflix systems.

Learn more
SKIP ▸

NETFLIX



MacBook Pro 'Core i7' 3.1 15' Touch/Mid-2017
nfml-Y4H

The security settings on this device should be improved. Click the arrow next to each recommendation for instructions.

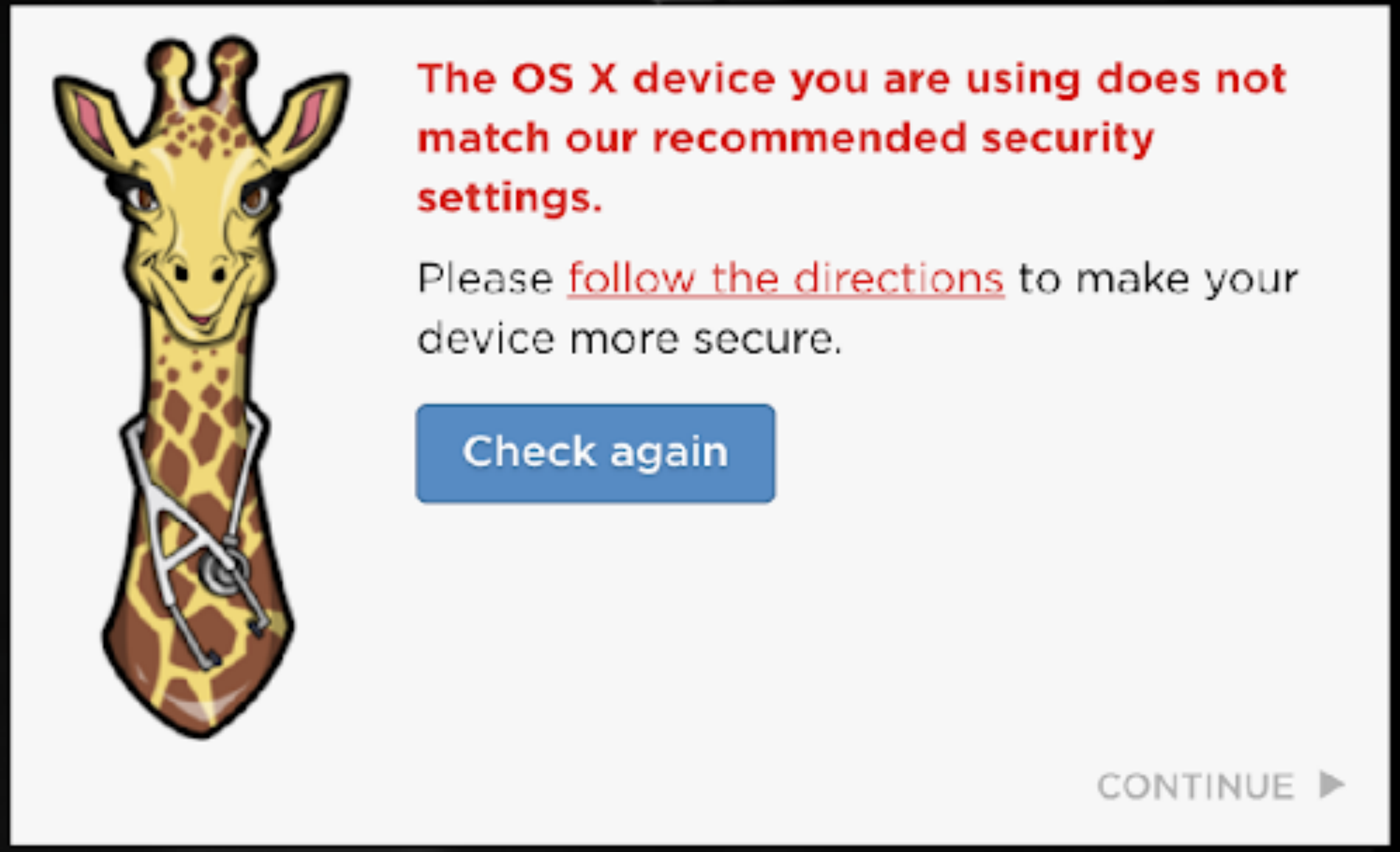
Netflix baseline policy

- ⊘ Your Firewall should be enabled
- ✓ System is up-to-date
- ✓ Disk Encryption is enabled
- ✓ Screen Lock is enabled
- ✓ Automatic Updates are enabled
- ✓ Remote Login is disabled

Last scan a few seconds ago by Stethoscope

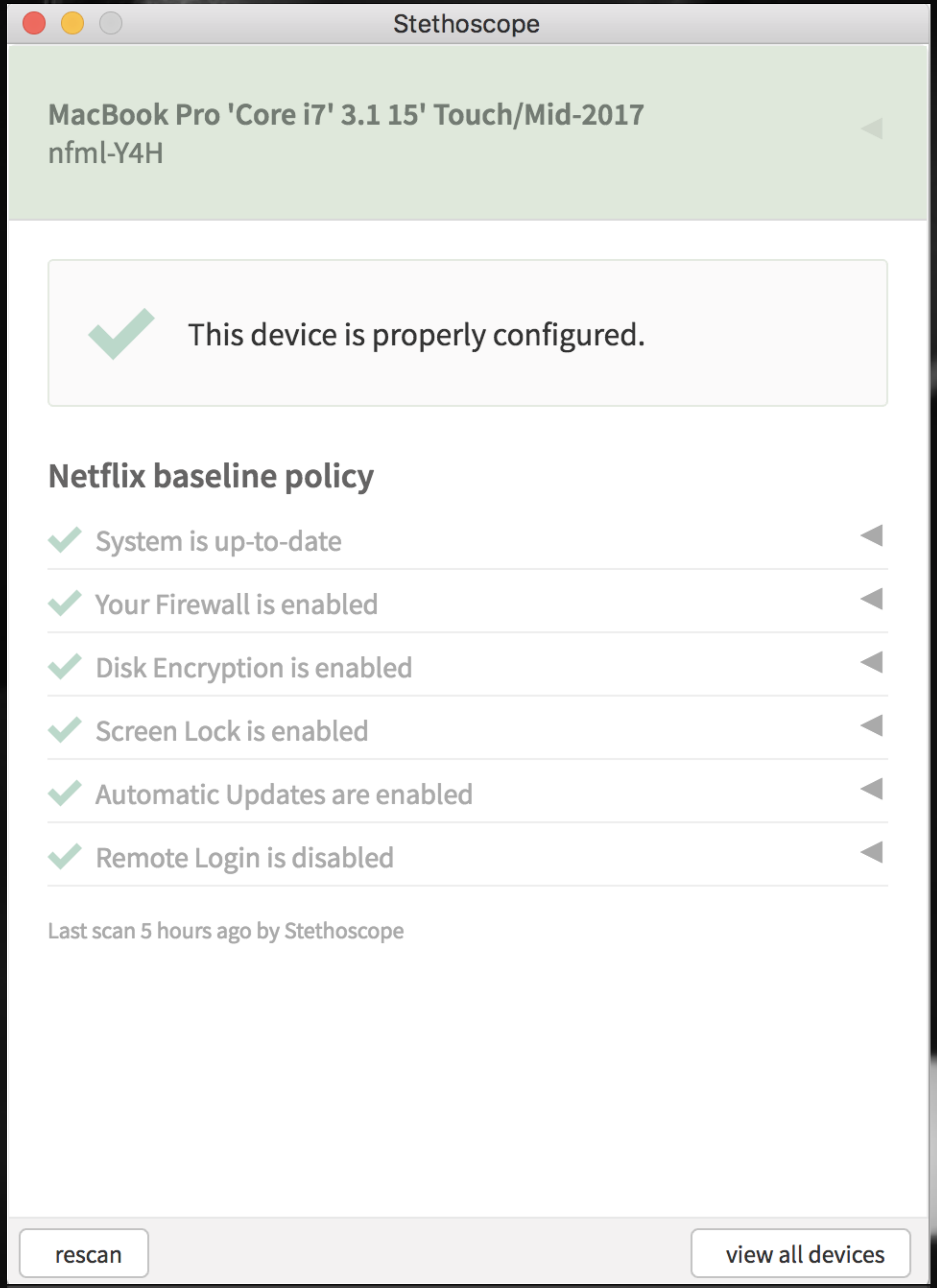
Authenticate

CHECKING DEVICE SECURITY



The OS X device you are using does not match our recommended security settings.

Please follow the directions to make your device more secure.



Stethoscope

MacBook Pro 'Core i7' 3.1 15' Touch/Mid-2017
nfml-Y4H

✓ This device is properly configured.

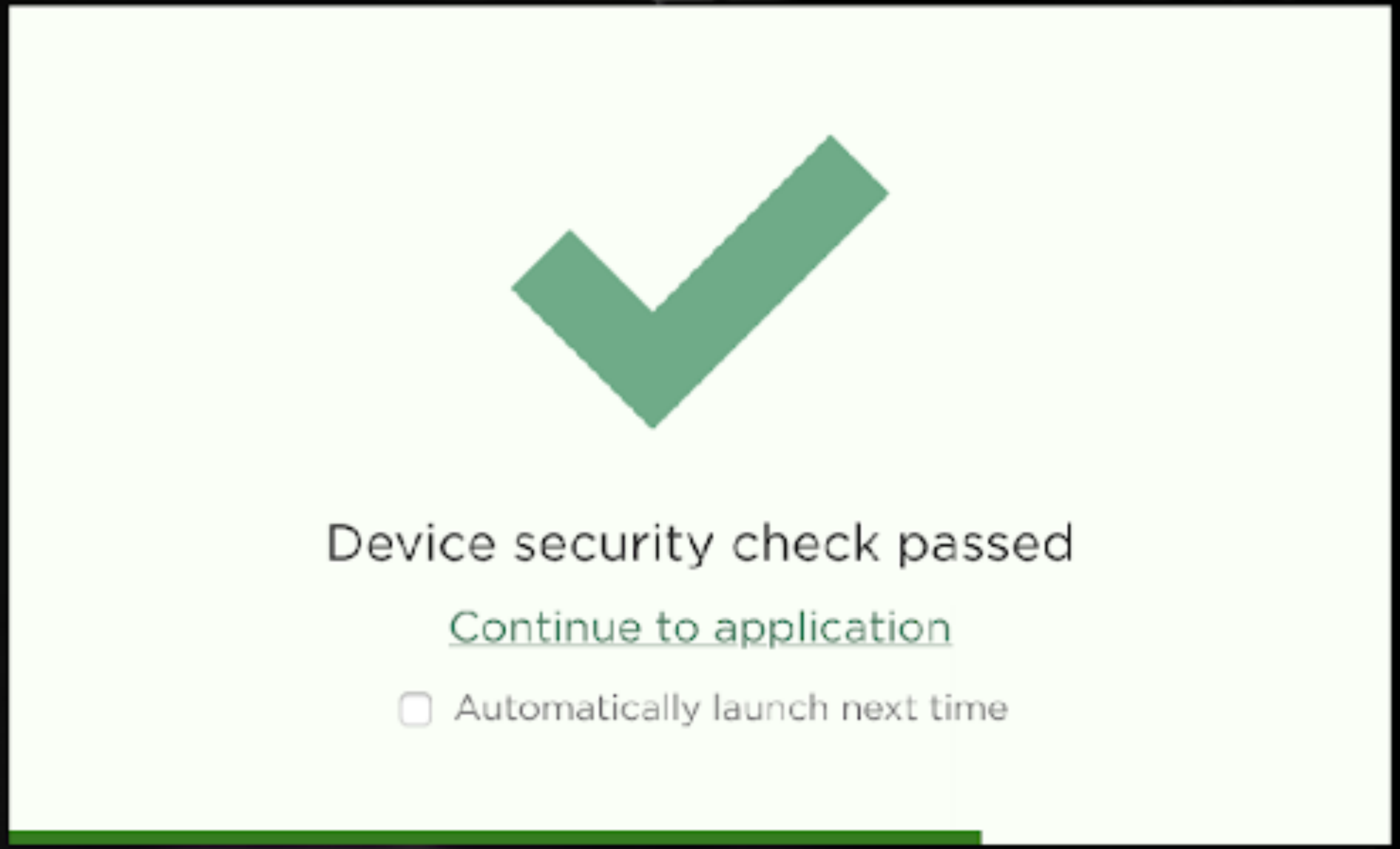
Netflix baseline policy

- ✓ System is up-to-date
- ✓ Your Firewall is enabled
- ✓ Disk Encryption is enabled
- ✓ Screen Lock is enabled
- ✓ Automatic Updates are enabled
- ✓ Remote Login is disabled

Last scan 5 hours ago by Stethoscope

Authenticate

CHECKING DEVICE SECURITY



Device security check passed

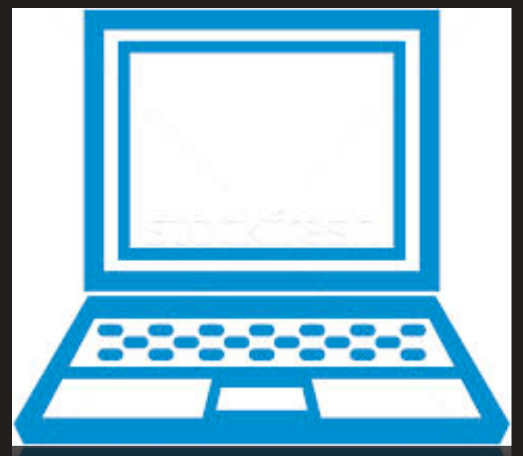
Continue to application

□ Automatically launch next time

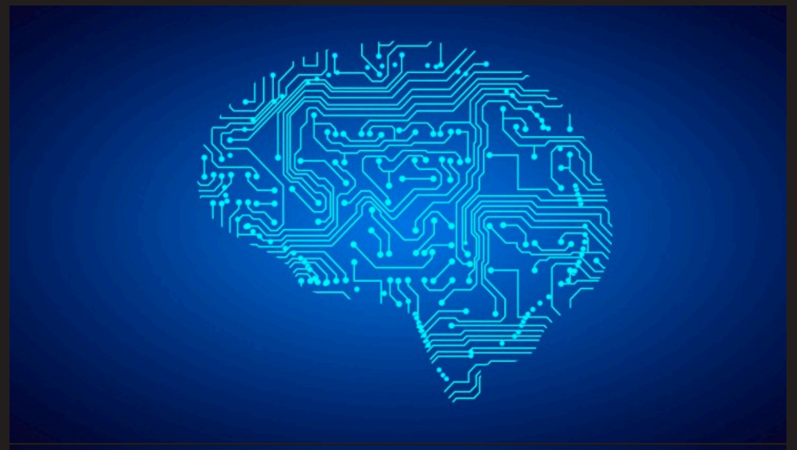
$67.7M
$34.0M
$33.7M

NETFLIX
Big Data Portal
STRANGER THINGS
HOUSE of CARDS
THE CROWN
NARCOS
Lemur
360
Employee Landing Page
workday.
zendesk

R
I
S
K

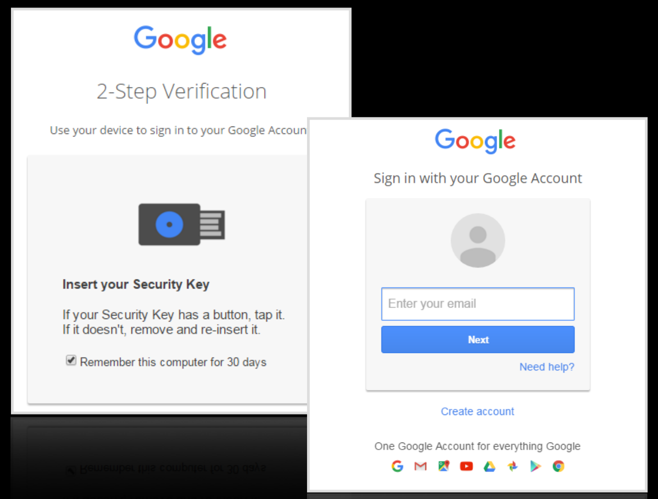


VERY LOW
LOW
MODERATE
HIGH
VERY HIGH



NETFLIX

Federation Hub (Layered Security)



Google

2-Step Verification

Use your device to sign in to your Google Accoun

Insert your Security Key

If your Security Key has a button, tap it.
If it doesn't, remove and re-insert it.

☑ Remember this computer for 30 days

Google

Sign in with your Google Account

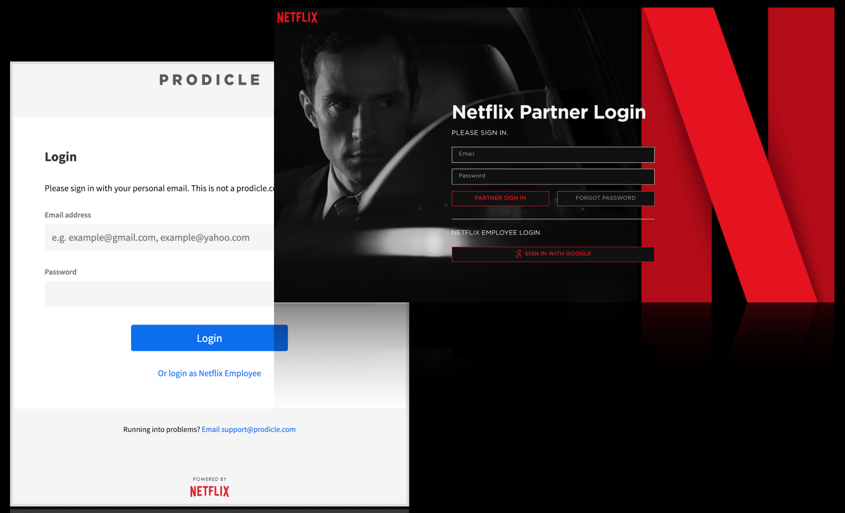
Enter your email

Next

Need help?

Create account

One Google Account for everything Google



PRODICLE

Login

Please sign in with your personal email. This is not a prodicle.c

Email address

e.g. example@gmail.com, example@yahoo.com

Password

Login

Or login as Netflix Employee

Running into problems? Email support@prodicle.com

POWERED BY NETFLIX

NETFLIX

Netflix Partner Login

PLEASE SIGN IN.

Email

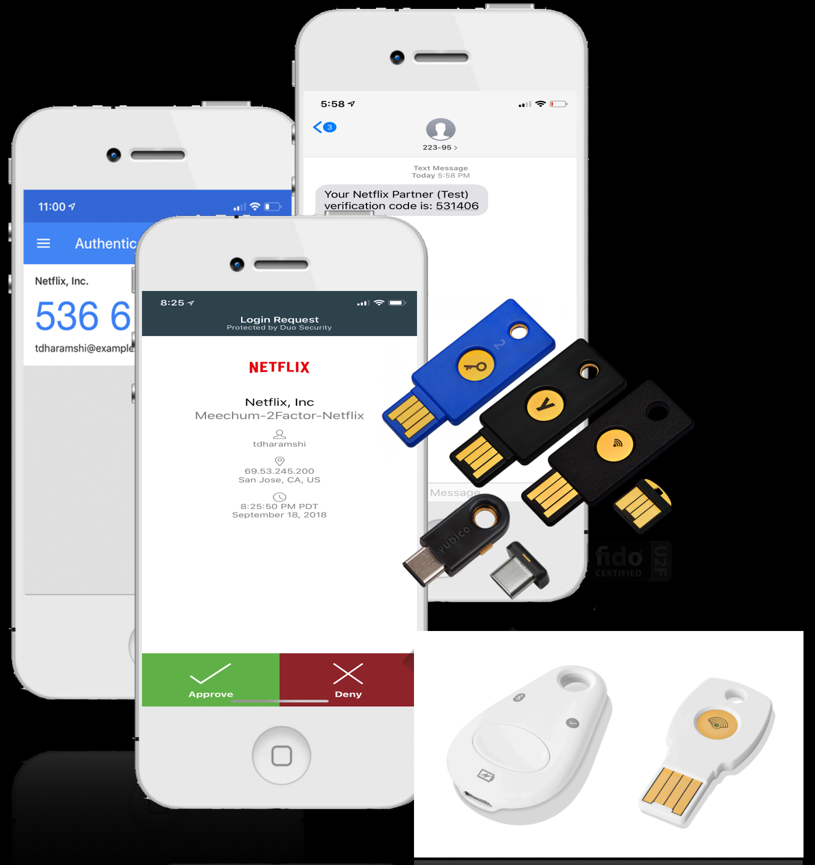
Password

PARTNER SIGN IN

FORGOT PASSWORD

NETFLIX EMPLOYEE LOGIN

SIGN IN WITH GOOGLE



11:00

Authentic

Netflix, Inc.

536 6

tdharamshi@example

5:58

223-95 >

Text Message
Today 5:58 PM

Your Netflix Partner (Test) verification code is: 531406

8:25

Login Request
Protected by Duo Security

NETFLIX

Netflix, Inc
Meechum-2Factor-Netflix

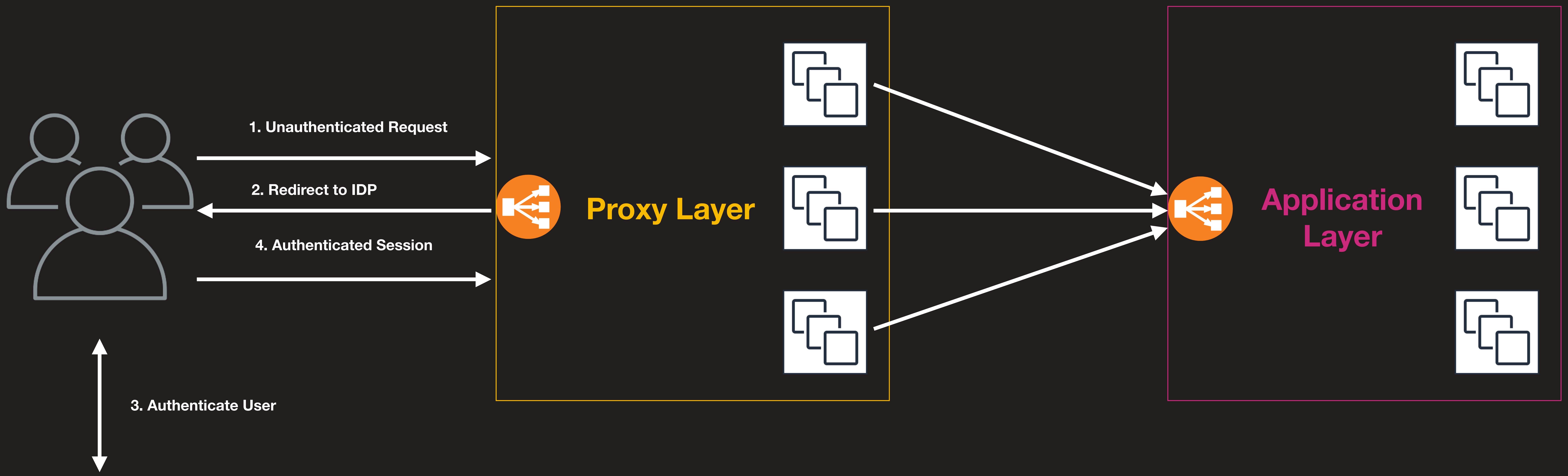
tdharamshi

69.53.245.200
San Jose, CA, US

8:25:50 PM PDT
September 18, 2018

Approve

Deny



1. Unauthenticated Request

2. Redirect to IDP

4. Authenticated Session

3. Authenticate User

Proxy Layer

Application Layer

Identity Provider

EDWARD
Search for: applications, scopes
Tejas Dharamshi
General
Grants
Redirect Uri's
Scopes
Access Control
Attributes
Summary
Actions
Update Token Manager
Configuration
Regenerate Secret
Delete
Help
Help
security-help
PROGRESS
FINISHED
Cancel
Back
Save Changes

iaetester-java (Client ID: iaetester-java)

Allowed Grant Types

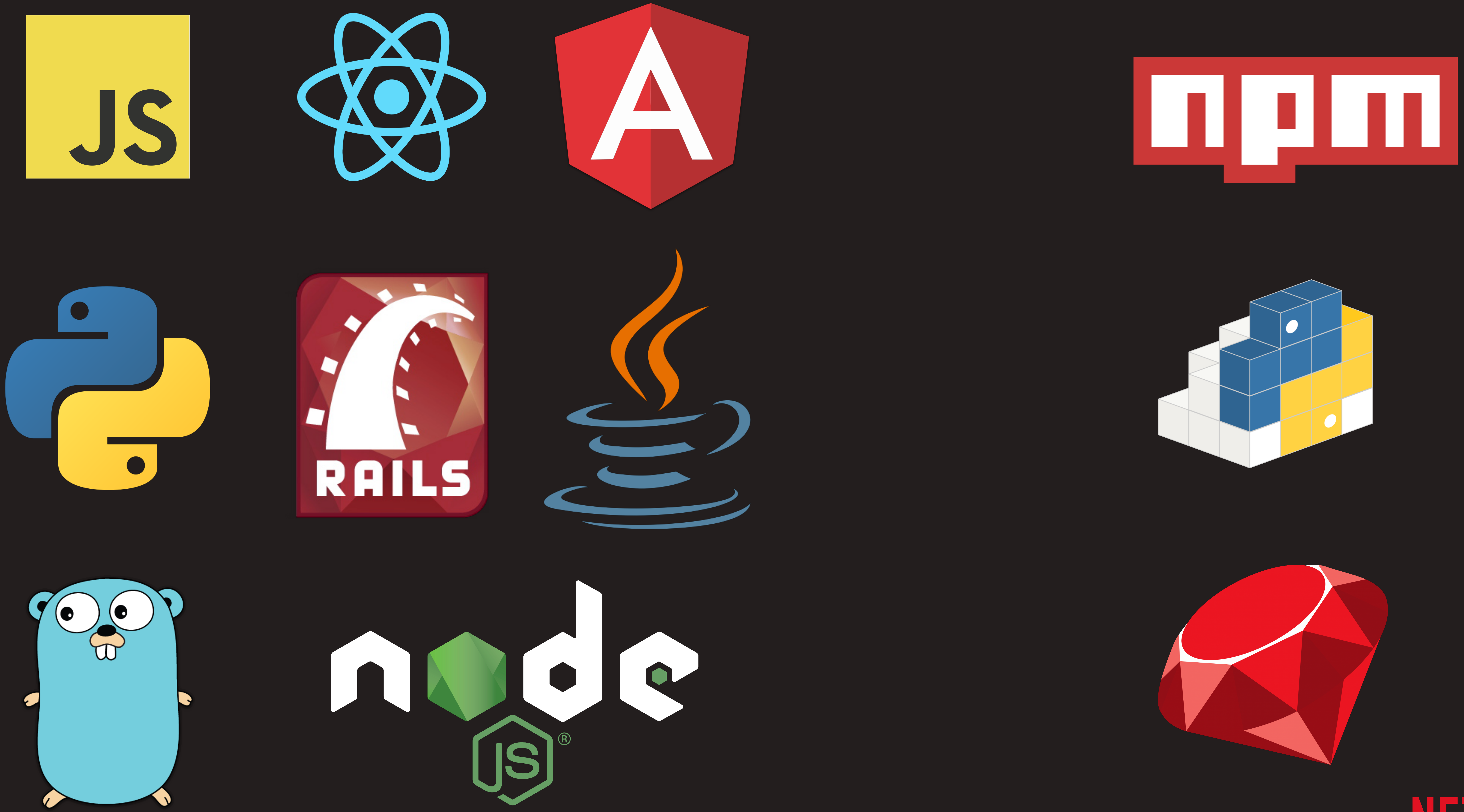
☑ **Authorization Code (Recommended - Default option for ezconfig)**
Intended for traditional web apps as well as native and mobile apps. This flow offers optimal security, as tokens are not revealed to the browser and the client app can also be authenticated.

☐ **Implicit**
Intended for browser (JavaScript single-page-applications) based apps that don't have a backend. The ID token is received directly with the redirection response from Meechum. Client_secret is not required and thus refresh tokens are not allowed with this flow.

☐ **Refresh Token**
This grant type enables refresh tokens to be included with access tokens. Once the original access token expires, the corresponding refresh token can be sent to Meechum to obtain a fresh access token without requiring the resource owner to re-authenticate.

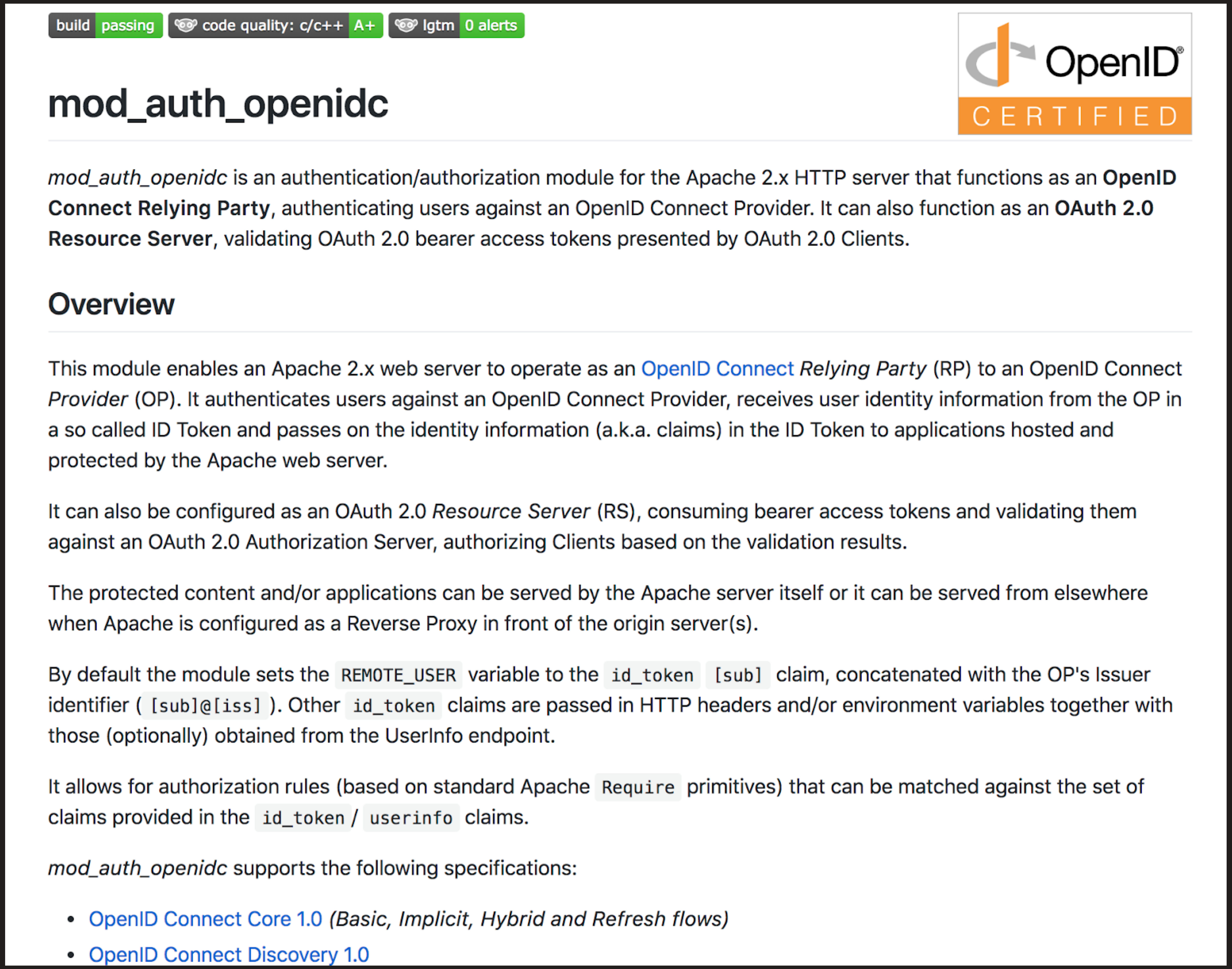
☐ **Remote Access Token Validation**
This grant type enables an application to remotely validate Meechum access tokens with the introspection endpoint.

{ api }


JS
RAILS
npm
node
JS

Paved Road

THE APACHE SOFTWARE FOUNDATION



mod_auth_openidc

mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an **OpenID Connect Relying Party**, authenticating users against an OpenID Connect Provider. It can also function as an **OAuth 2.0 Resource Server**, validating OAuth 2.0 bearer access tokens presented by OAuth 2.0 Clients.

Overview

This module enables an Apache 2.x web server to operate as an OpenID Connect *Relying Party* (RP) to an OpenID Connect *Provider* (OP). It authenticates users against an OpenID Connect Provider, receives user identity information from the OP in a so called ID Token and passes on the identity information (a.k.a. claims) in the ID Token to applications hosted and protected by the Apache web server.

It can also be configured as an OAuth 2.0 *Resource Server* (RS), consuming bearer access tokens and validating them against an OAuth 2.0 Authorization Server, authorizing Clients based on the validation results.

The protected content and/or applications can be served by the Apache server itself or it can be served from elsewhere when Apache is configured as a Reverse Proxy in front of the origin server(s).

By default the module sets the `REMOTE_USER` variable to the `id_token` `[sub]` claim, concatenated with the OP's Issuer identifier (`[sub]@[iss]`). Other `id_token` claims are passed in HTTP headers and/or environment variables together with those (optionally) obtained from the UserInfo endpoint.

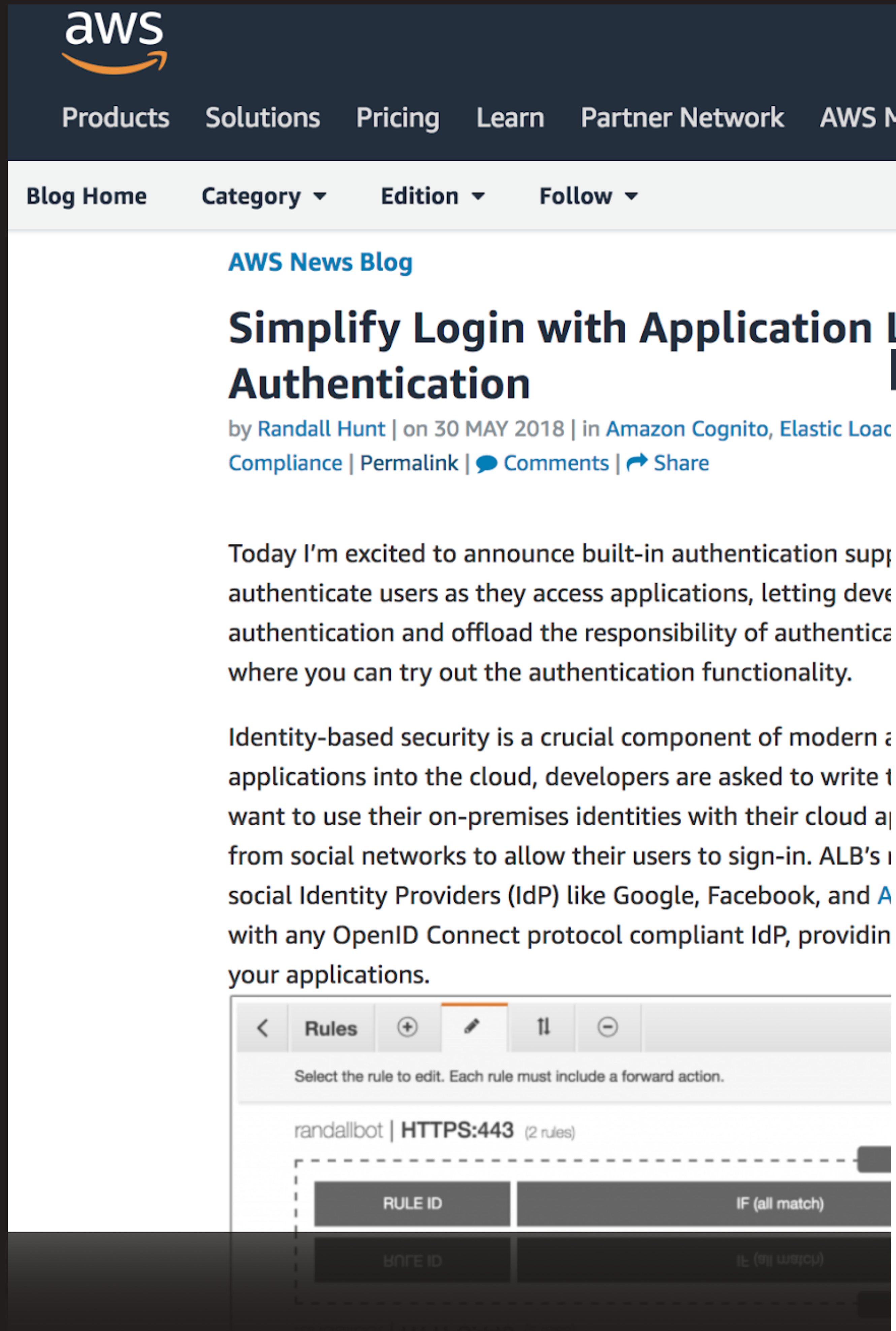
It allows for authorization rules (based on standard Apache `Require` primitives) that can be matched against the set of claims provided in the `id_token` / `userinfo` claims.

mod_auth_openidc supports the following specifications:

- OpenID Connect Core 1.0 *(Basic, Implicit, Hybrid and Refresh flows)*
- OpenID Connect Discovery 1.0

https://github.com/zmartzone/mod_auth_openidc

Application Load Balancers



AWS News Blog

Simplify Login with Application Load Balancer Built-in Authentication

by Randall Hunt | on 30 MAY 2018 | in Amazon Cognito, Elastic Loac
Compliance | Permalink | Comments | Share

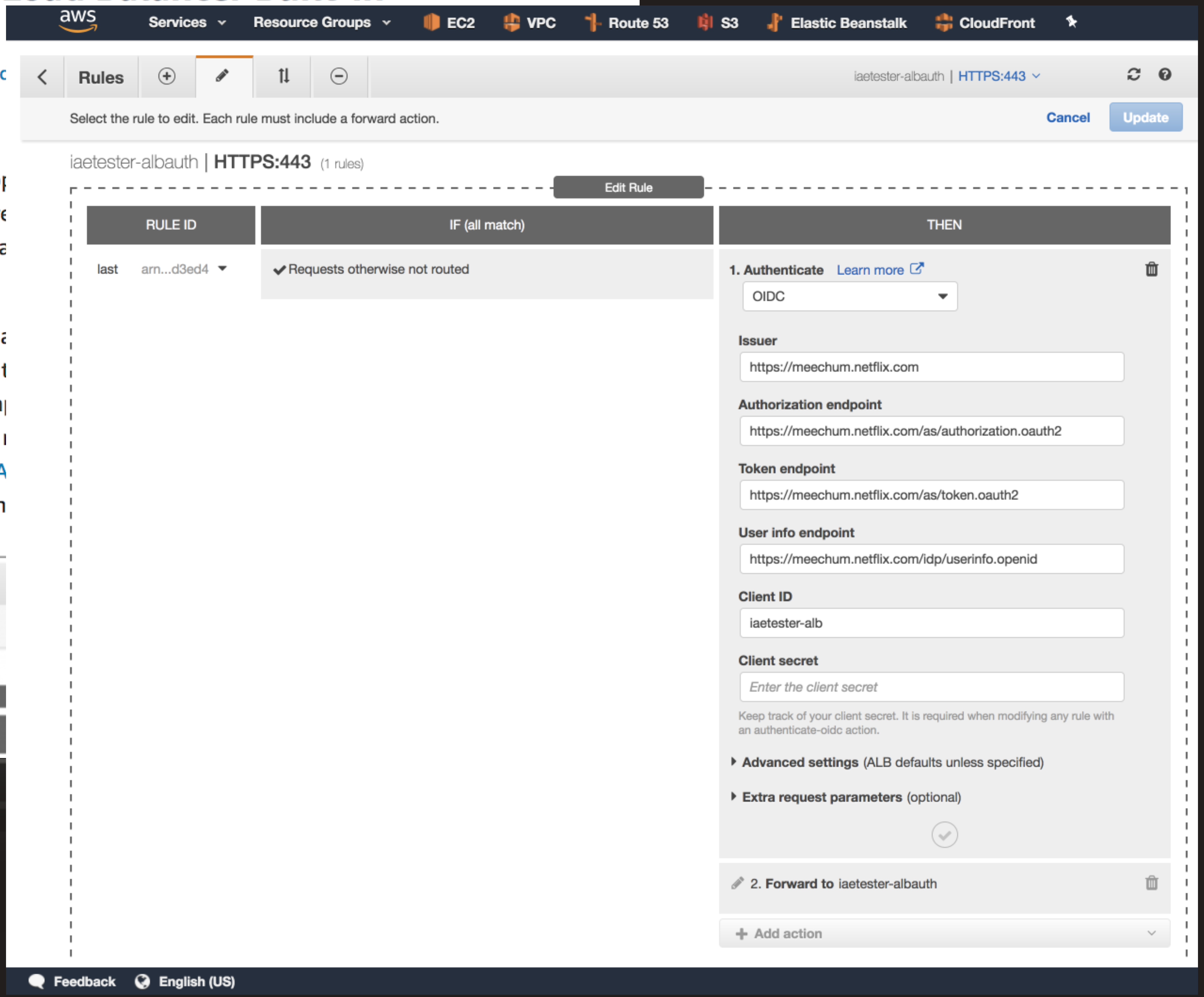
Today I'm excited to announce built-in authentication supp
authenticate users as they access applications, letting deve
authentication and offload the responsibility of authentica
where you can try out the authentication functionality.

Identity-based security is a crucial component of modern a
applications into the cloud, developers are asked to write t
want to use their on-premises identities with their cloud a
from social networks to allow their users to sign-in. ALB's i
social Identity Providers (IdP) like Google, Facebook, and A
with any OpenID Connect protocol compliant IdP, providin
your applications.

Select the rule to edit. Each rule must include a forward action.

randallbot | HTTPS:443 (2 rules)

RULE ID	IF (all match)



Select the rule to edit. Each rule must include a forward action.

iaetester-albauth | HTTPS:443 (1 rules)

RULE ID	IF (all match)	THEN
last arn...d3ed4	✓ Requests otherwise not routed	1. Authenticate Learn more OIDC

Issuer: https://meechum.netflix.com

Authorization endpoint: https://meechum.netflix.com/as/authorization.oauth2

Token endpoint: https://meechum.netflix.com/as/token.oauth2

User info endpoint: https://meechum.netflix.com/idp/userinfo.openid

Client ID: iaetester-alb

Client secret: Enter the client secret

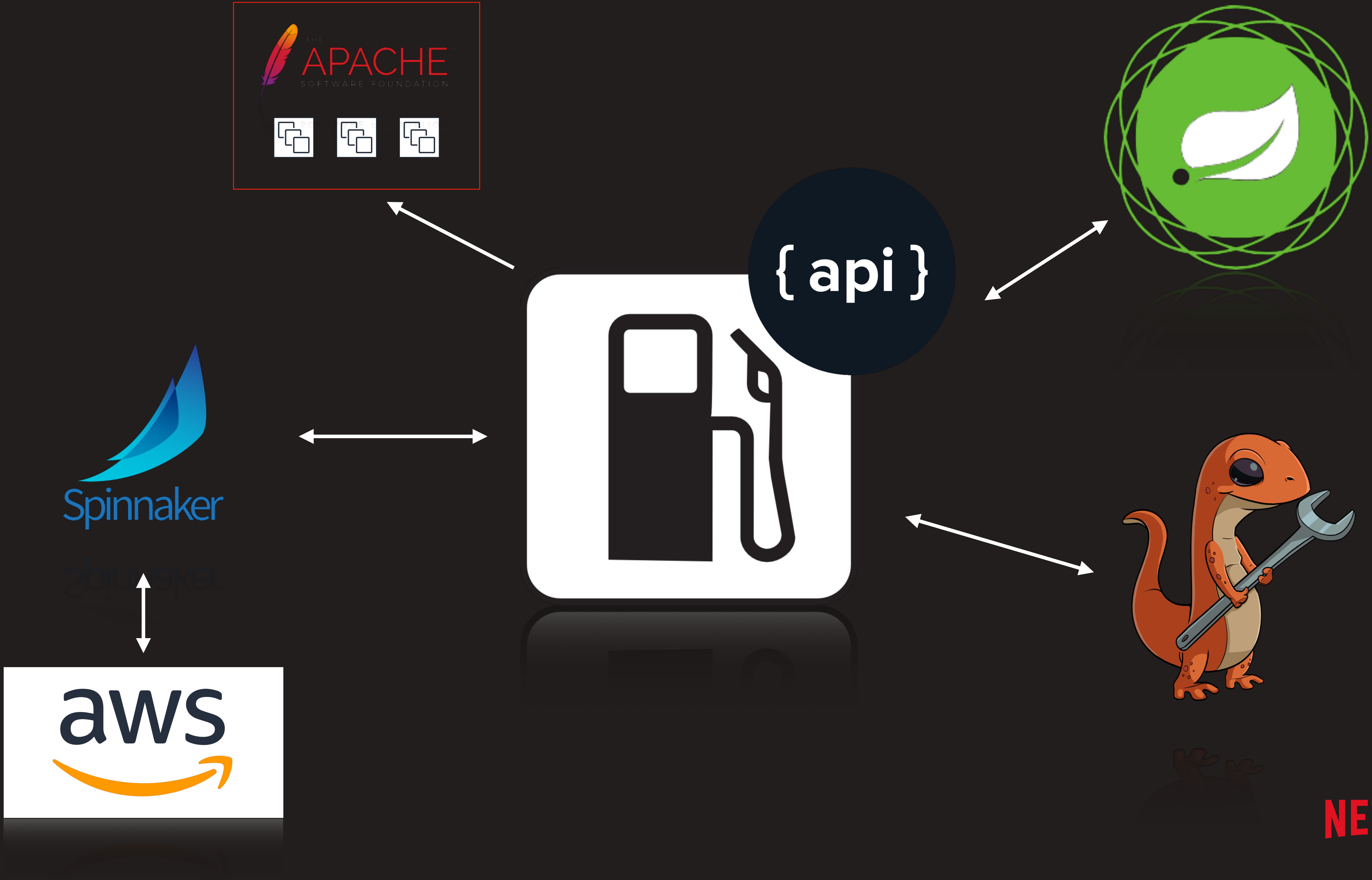
Keep track of your client secret. It is required when modifying any rule with an authenticate-oidc action.

▸ Advanced settings (ALB defaults unless specified)

▸ Extra request parameters (optional)

2. Forward to iaetester-albauth

+ Add action


THE APACHE SOFTWARE FOUNDATION
{ api }
Spinnaker
aws

Zero Trust Principle 5

EDWARD
Search for: applications, scopes
Tejas Dharamshi
General
Grants
Redirect Uri's
Scopes
Access Control
Attributes
Summary
Actions
Update Token Manager
Configuration
Regenerate Secret
Delete
Help
Help
security-help
PROGRESS
FINISHED

iaetester-java (Client ID: iaetester-java)

Access Control

Access Control, provides a mechanism to constrain **"User"** to **"App"** access.

You can constrain access to your app to specific **domains**. Further, you can constrain access to **groups** and **users** in the selected domains.

Please select the domains you want to constrain access to:

☑ Netflix.com (employee's only)

□ NetflixContractors.com (contractors and vendors only)

□ NetflixCS.com (customer service only)

□ Svc.netflix.net (service accounts only)

☑ Pandora Prod (Partner Directories)

□ Pandora Test (Partner Directories)

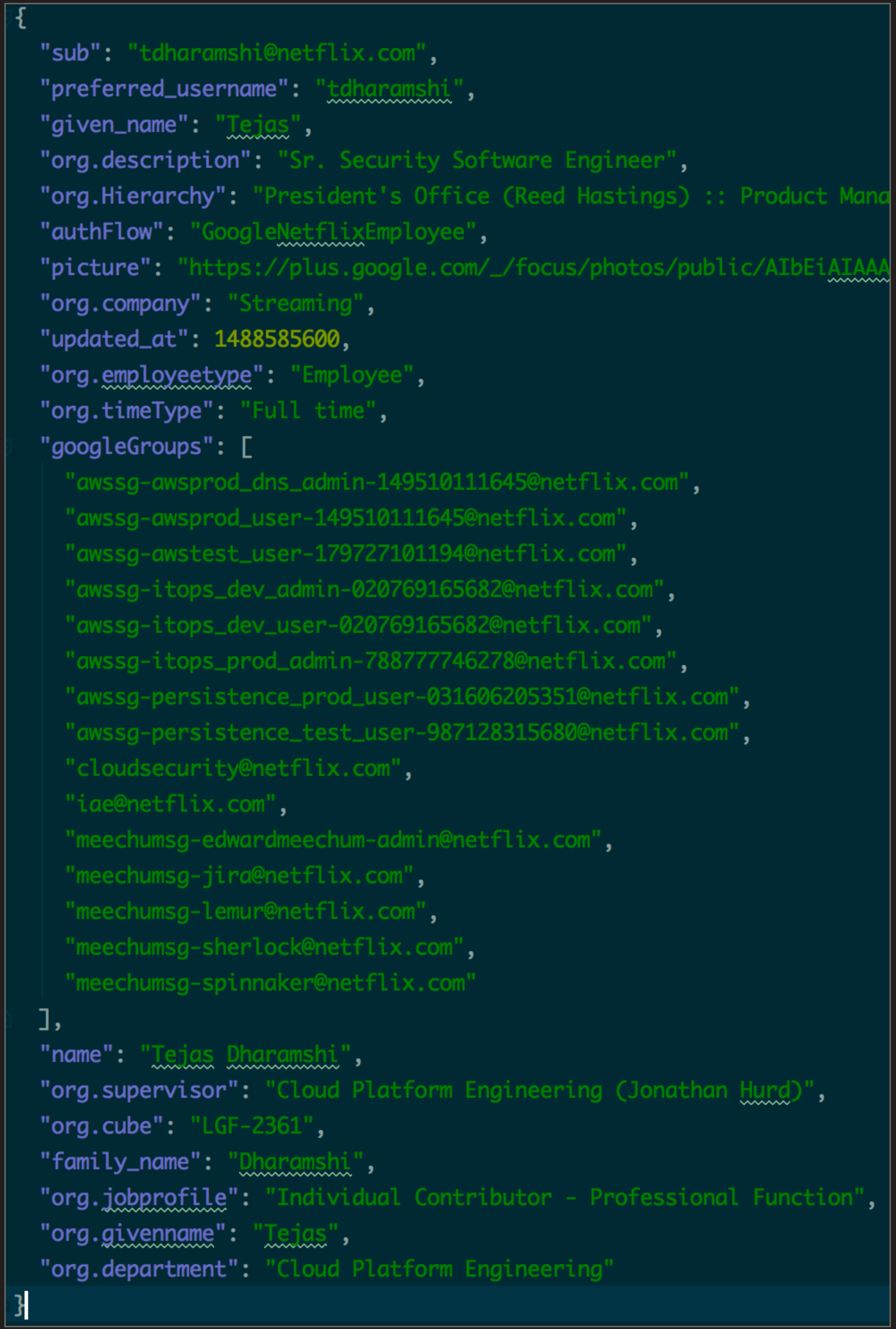
□ Moon.film (Prodicle production)

N

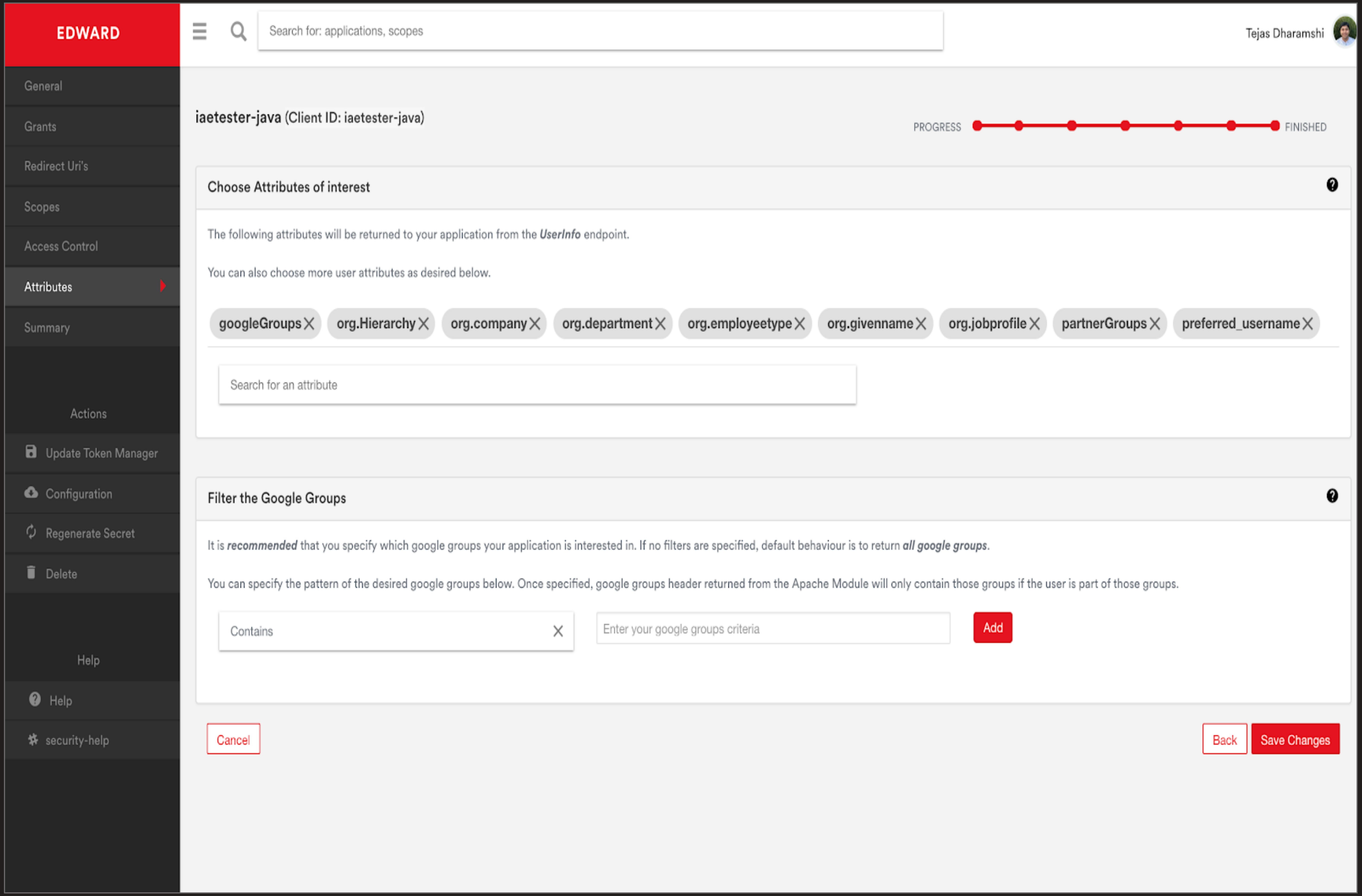
Op

Groups	**Identity and Access Engineering** iae@netflix.com
Users	**Antonia Ellis** antoniae@netflix.com

iae@



```
{
  "sub": "tdharamshi@netflix.com",
  "preferred_username": "tdharamshi",
  "given_name": "Tejas",
  "org.description": "Sr. Security Software Engineer",
  "org.Hierarchy": "President's Office (Reed Hastings) :: Product Mana
  "authFlow": "GoogleNetflixEmployee",
  "picture": "https://plus.google.com/_/focus/photos/public/AIbEiAIAAA
  "org.company": "Streaming",
  "updated_at": 1488585600,
  "org.employeetype": "Employee",
  "org.timeType": "Full time",
  "googleGroups": [
    "awssg-awsprod_dns_admin-149510111645@netflix.com",
    "awssg-awsprod_user-149510111645@netflix.com",
    "awssg-awstest_user-179727101194@netflix.com",
    "awssg-itops_dev_admin-020769165682@netflix.com",
    "awssg-itops_dev_user-020769165682@netflix.com",
    "awssg-itops_prod_admin-788777746278@netflix.com",
    "awssg-persistence_prod_user-031606205351@netflix.com",
    "awssg-persistence_test_user-987128315680@netflix.com",
    "cloudsecurity@netflix.com",
    "iae@netflix.com",
    "meechumsg-edwardmeechum-admin@netflix.com",
    "meechumsg-jira@netflix.com",
    "meechumsg-lemur@netflix.com",
    "meechumsg-sherlock@netflix.com",
    "meechumsg-spinnaker@netflix.com"
  ],
  "name": "Tejas Dharamshi",
  "org.supervisor": "Cloud Platform Engineering (Jonathan Hurd)",
  "org.cube": "LGF-2361",
  "family_name": "Dharamshi",
  "org.jobprofile": "Individual Contributor - Professional Function",
  "org.givenname": "Tejas",
  "org.department": "Cloud Platform Engineering"
}
```



iaetester-java (Client ID: iaetester-java)

Choose Attributes of interest

The following attributes will be returned to your application from the ***UserInfo*** endpoint.

You can also choose more user attributes as desired below.

googleGroups ✕ org.Hierarchy ✕ org.company ✕ org.department ✕ org.employeetype ✕ org.givenname ✕ org.jobprofile ✕ partnerGroups ✕ preferred_username ✕

Filter the Google Groups

It is ***recommended*** that you specify which google groups your application is interested in. If no filters are specified, default behaviour is to return ***all google groups***.

You can specify the pattern of the desired google groups below. Once specified, google groups header returned from the Apache Module will only contain those groups if the user is part of those groups.

Contains ✕

Recap

Cleanup

Identity Silos

Password Policy

Employee Landing Page

Lemur

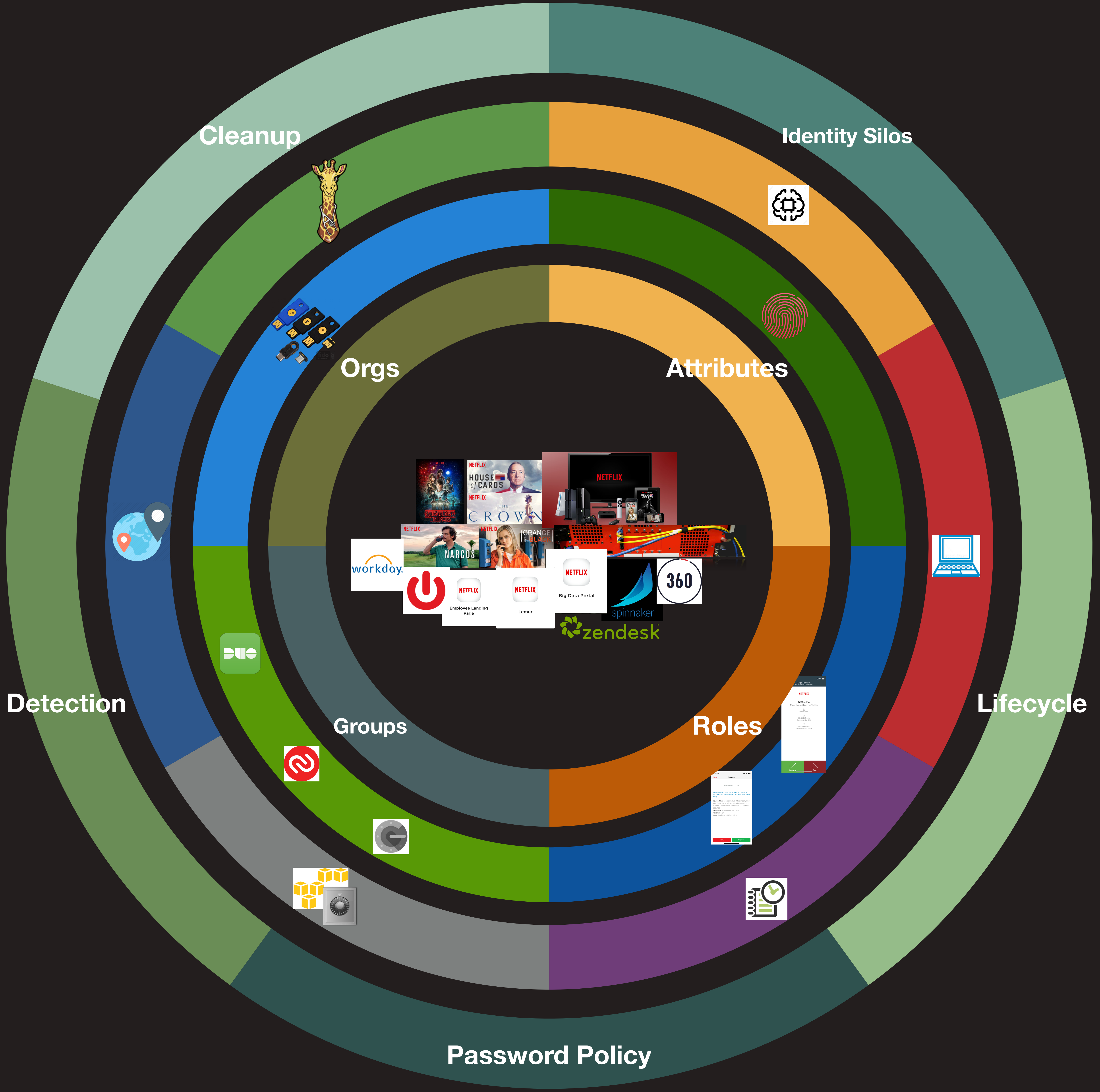
Big Data Portal

Identity as the Security Perimeter

OpenID

OAUTH 2

SAML



THE APACHE SOFTWARE FOUNDATION

Spinnaker

NETFLIX

Thank you.
Questions?

Tejas Dharamshi
Senior Security Software Engineer
@tejasdharamshi

NETFLIX