RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: IDY-T06

Building Identity for an Open Perimeter

Tejas Dharamshi
Senior Security Software Engineer
Netflix, Inc.
@tejasdharamshi

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

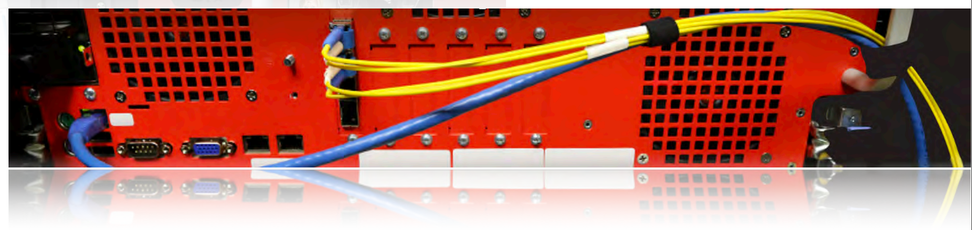

B2B


EXIT

Application Landscape

Content & Studio

Device Partner



Open Connect

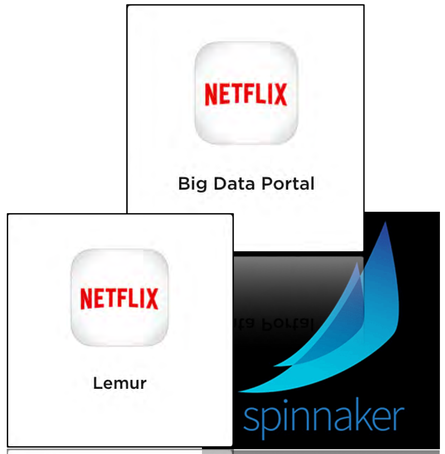
Over **700** apps

360 Employee Landing Page

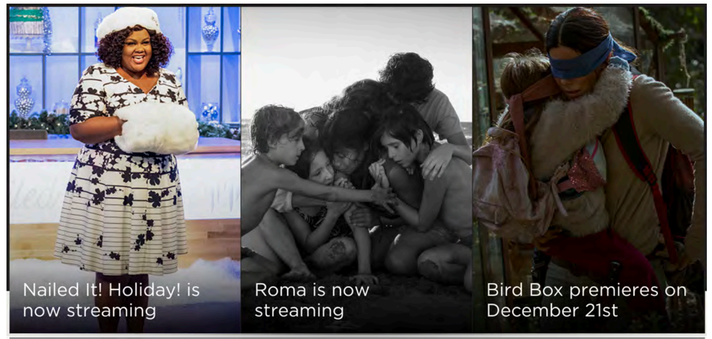
workday.

zendesk

Corporate



Engineering



Media Partners

Location Independent Security Approach (LISA)

NETFLIX

BeyondCorp

Google

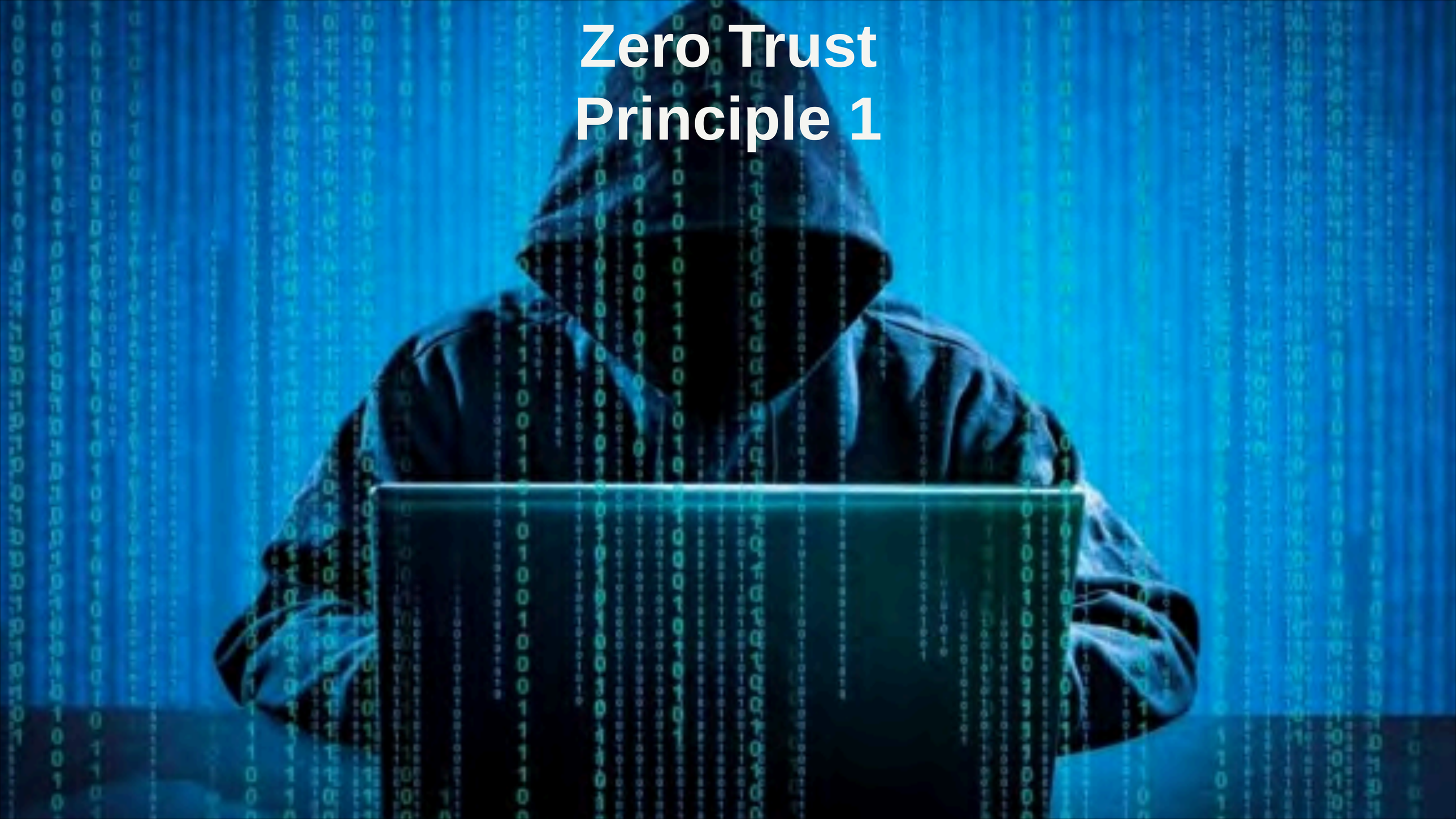
Beyond the Edge

intel

Zero Trust

FORRESTER®

Zero Trust Principle 1



Zero Trust Principle 1

Netflix Identity Platform (aka Meechum)

Federation

SSO

Standards (OpenId, OAuth 2.0, SAML)

Layered Security

Signed and Verifiable Identity Information

User Experience

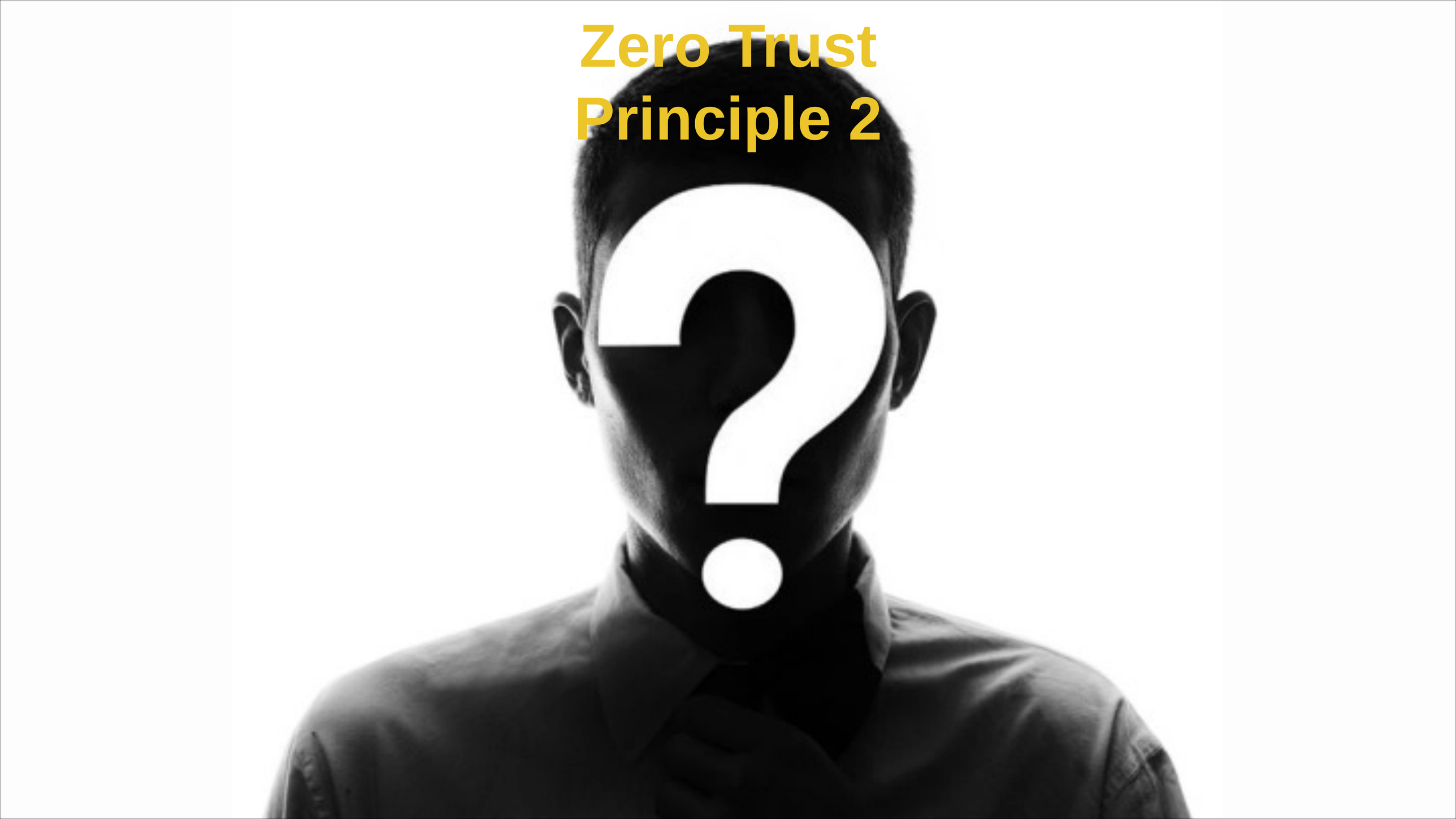
Delegate AuthN & AuthZ

Signed and Verifiable Identity Information

Self-service

Pluggable

Zero Trust
Principle 2



OpenLDAP™
http://www.OpenLDAP.org

Microsoft Active Directory

MySQL®

Crowd

cassandra

NETFLIX

Google

workday.

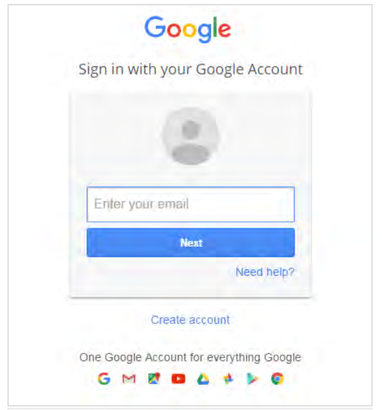
STUDIO NETWORK

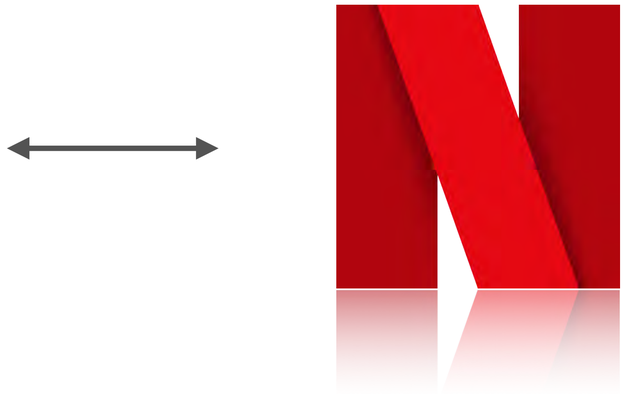
Provisioning/
De-provisioning

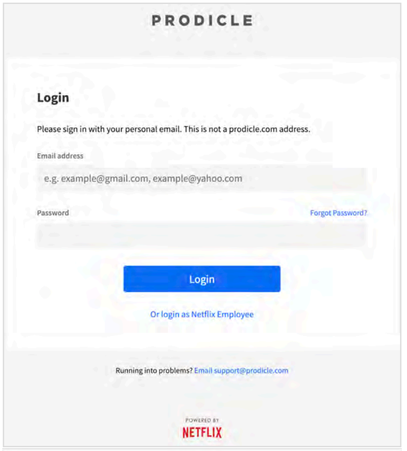
NETFLIX

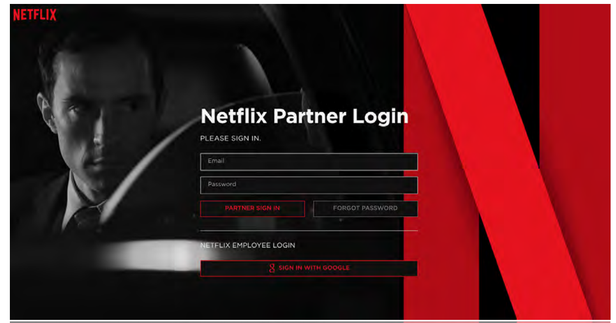
Zero Trust
Principle 3

Federation Hub (Layered Security)



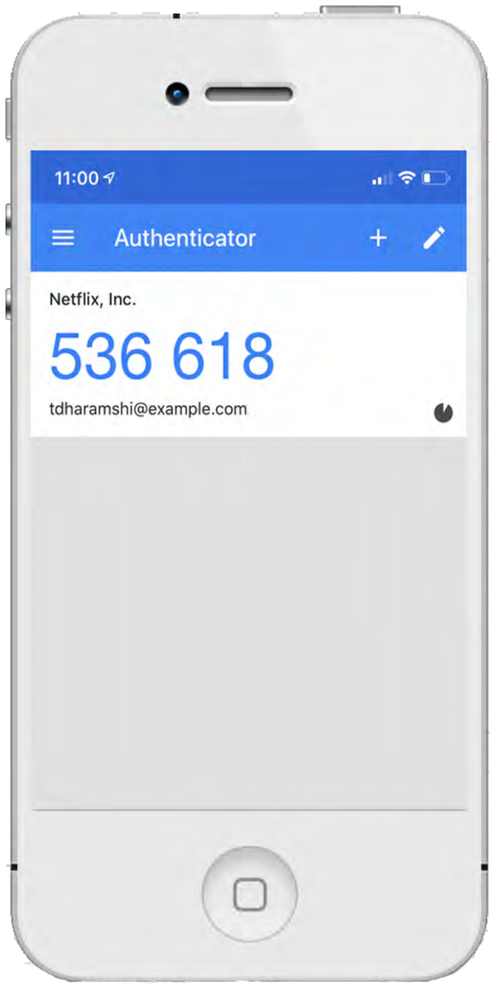


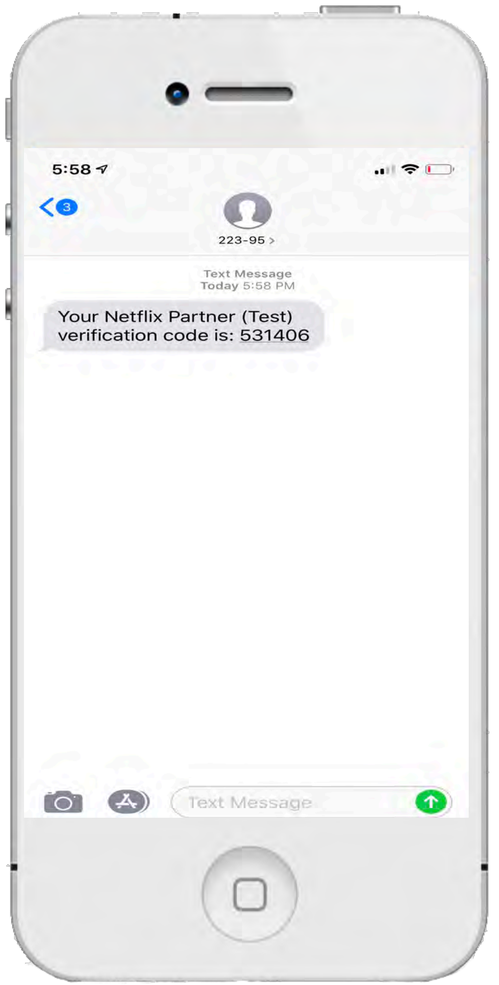




- Telesign Research
- Verizon 2017 Data Breach Investigation Report

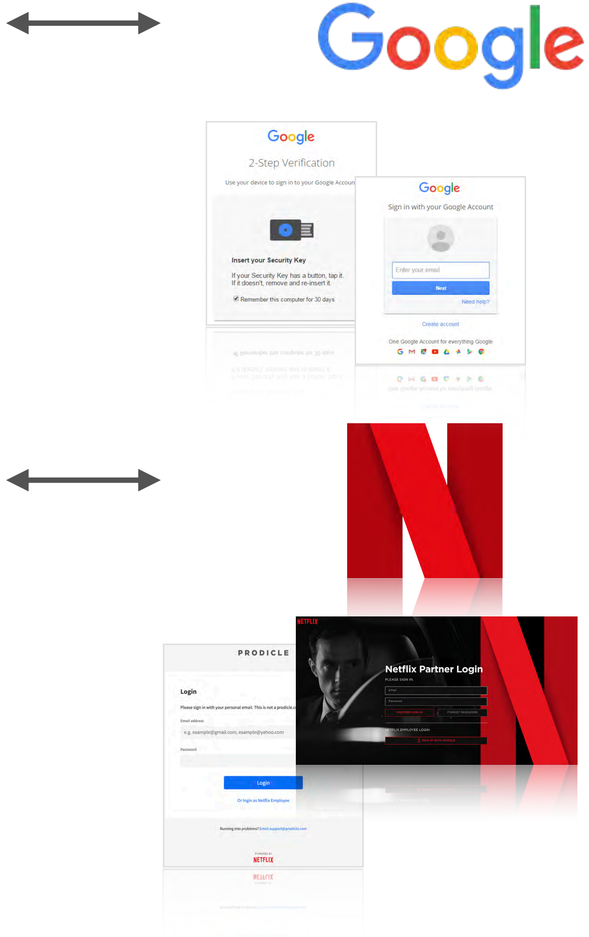
Multi-factor Authentication

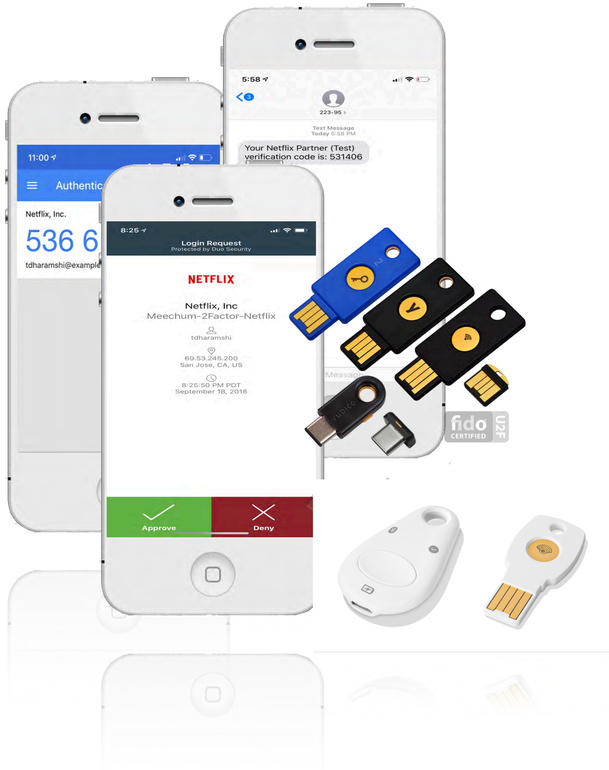




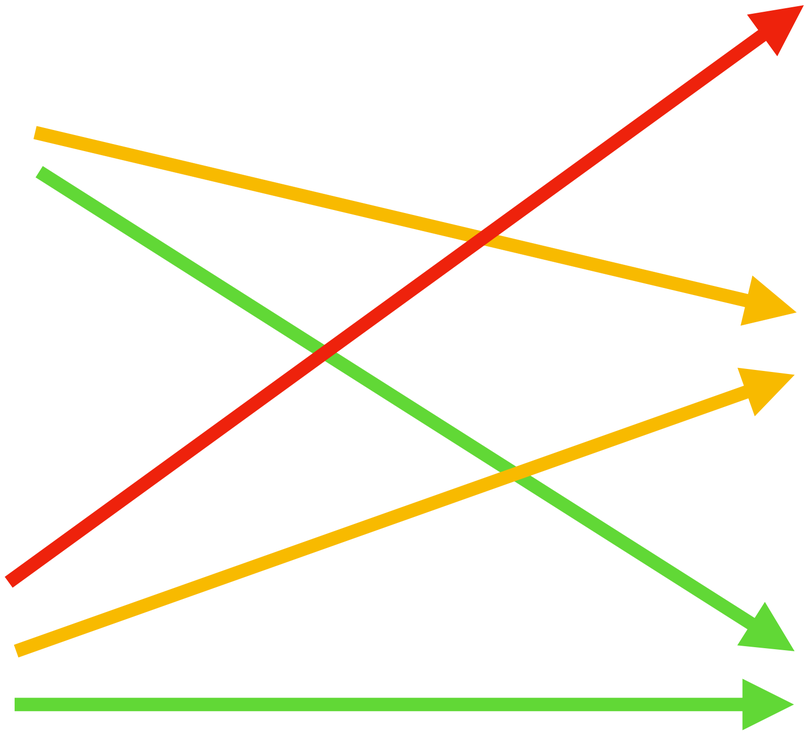
Multi-factor Authentication

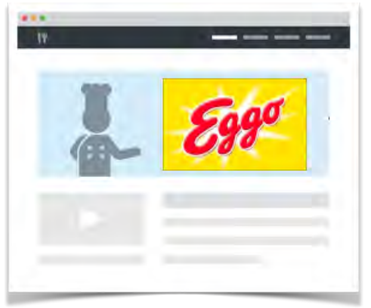
Federation Hub (Layered Security)

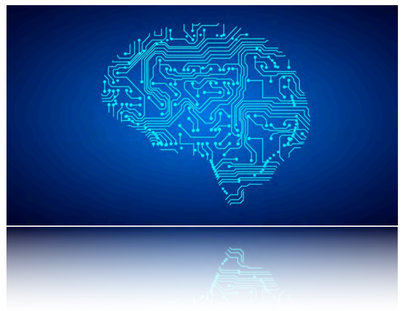




Are all access patterns the same?



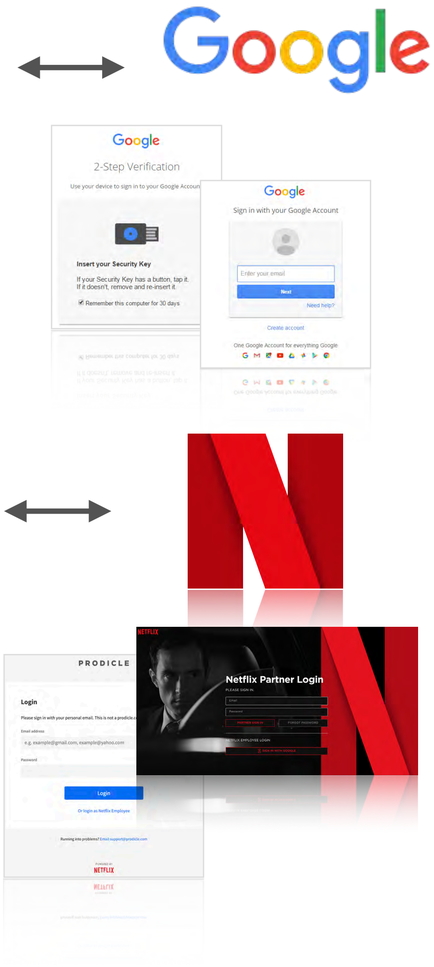


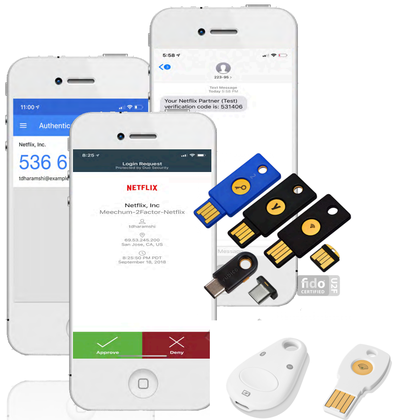


Adaptive Authentication

NETFLIX

Federation Hub (Layered Security)






Zero Trust
Principle 4


Bitdefender


eset
ENJOY SAFER TECHNOLOGY™

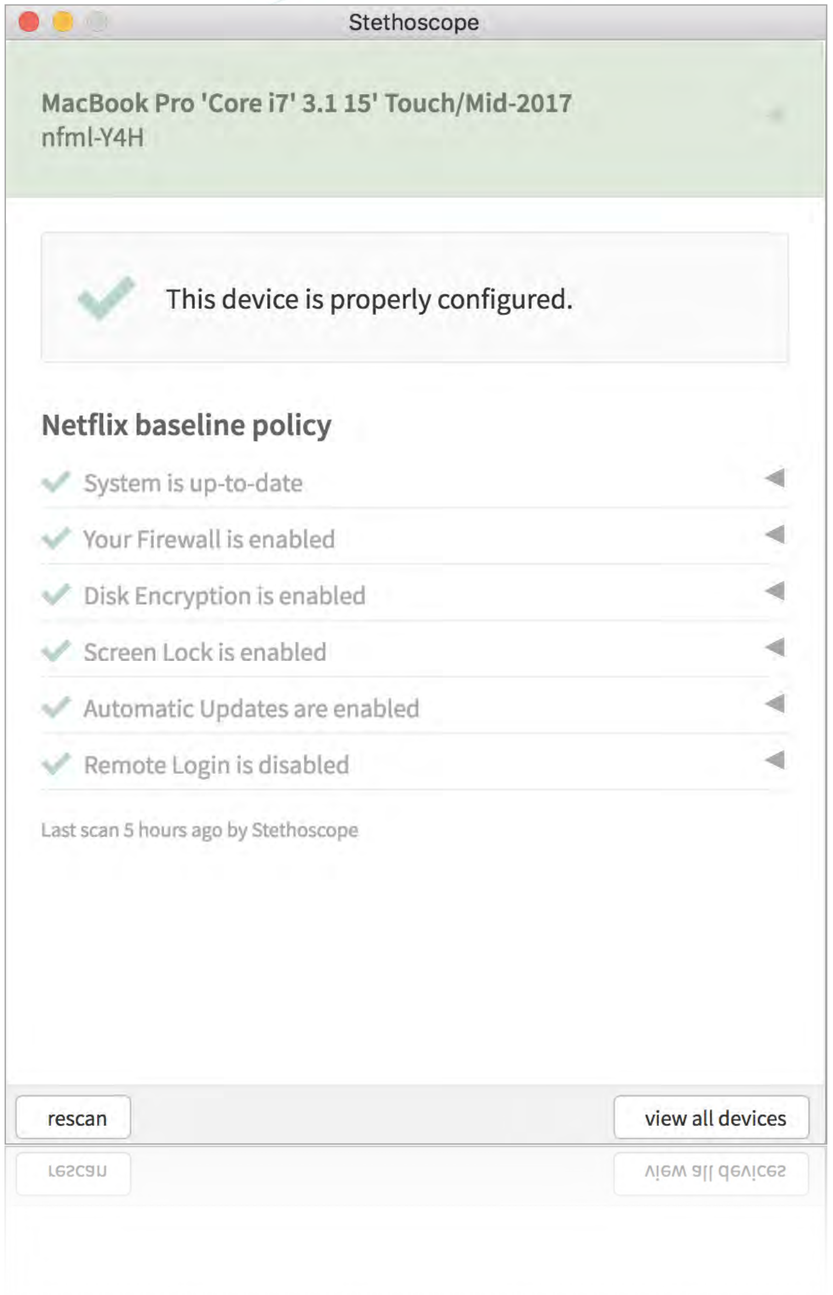

Symantec.


F-Secure


ivanti

NETFLIX


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
rescan
view all devices

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

Stethoscope

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

rescan | view all devices

Authenticate

CHECKING DEVICE SECURITY

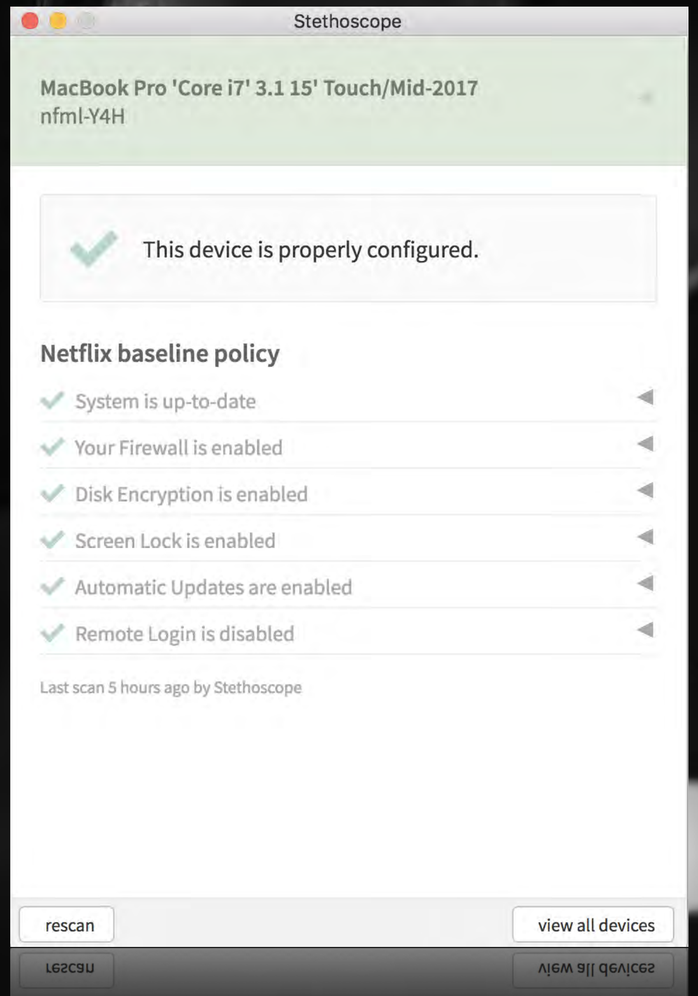
The OS X device you are using does not match our recommended security settings.

Please follow the directions to make your device more secure.

Check again

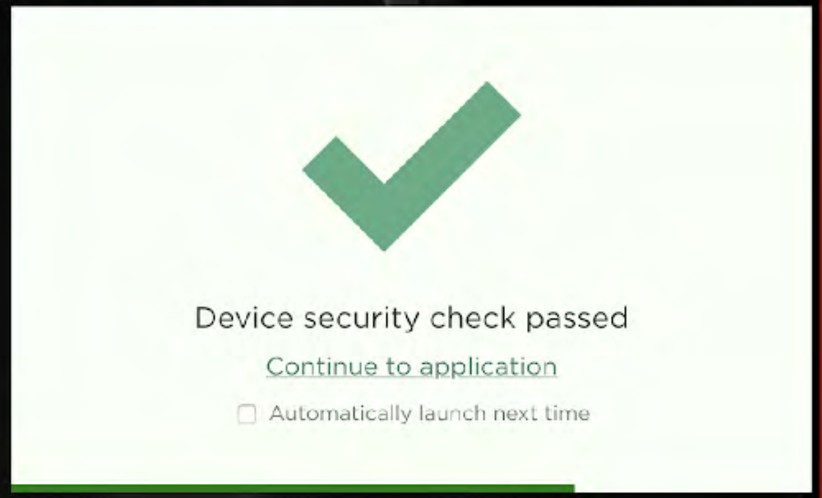
CONTINUE ▶

NETFLIX



Authenticate

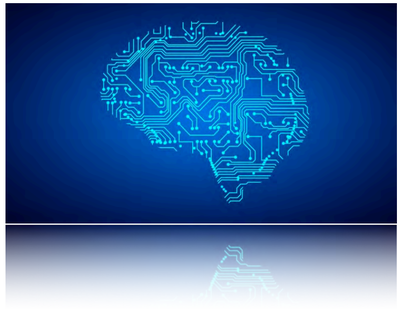
CHECKING DEVICE SECURITY



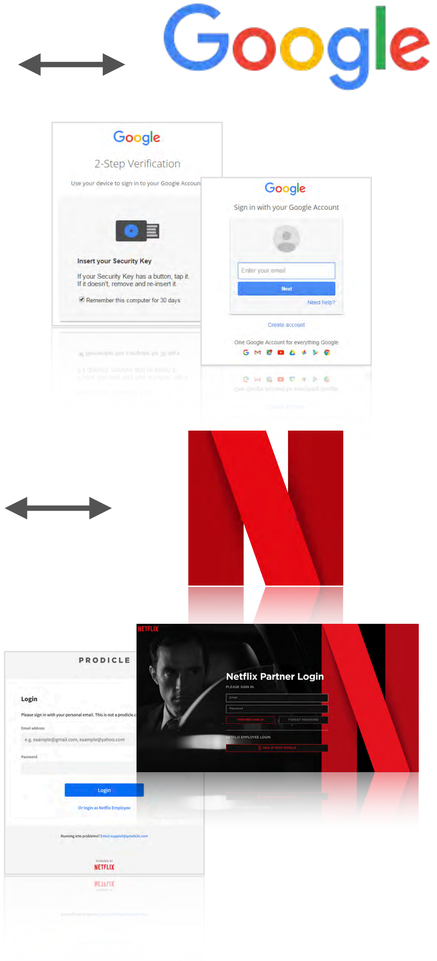

NETFLIX
Big Data Portal
NETFLIX
HOUSE of CARDS
NETFLIX
NETFLIX
Lemur
360
NETFLIX
Employee Landing Page
NETFLIX
NARCOS
NETFLIX
workday.
zendesk

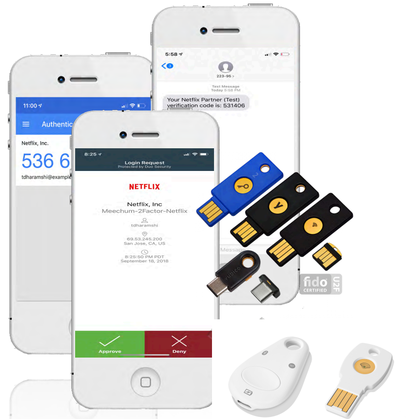

R
I
S
K

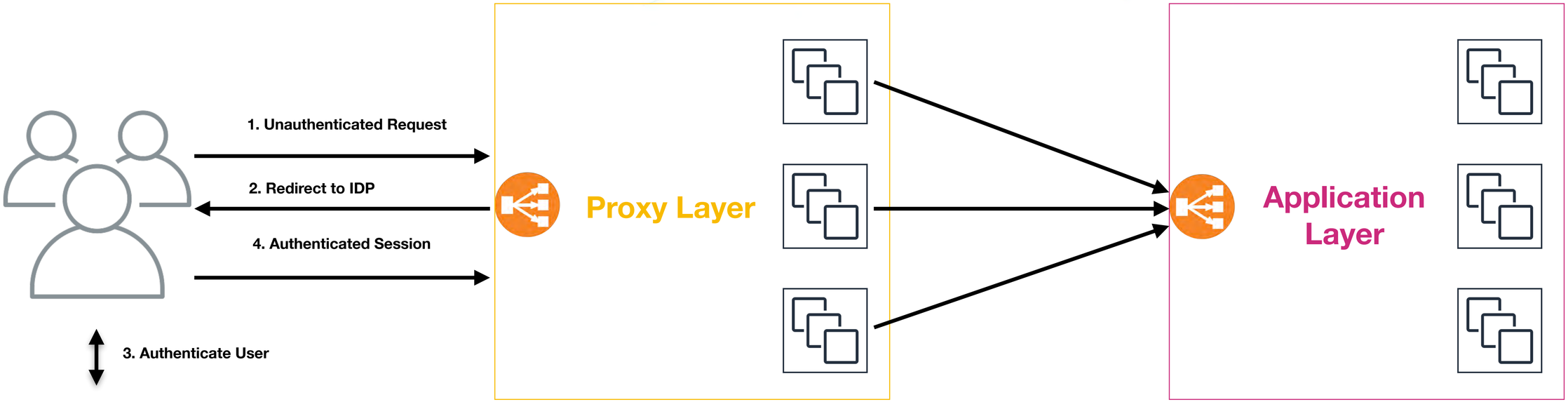

VERY LOW
LOW
MODERATE
HIGH
VERY HIGH

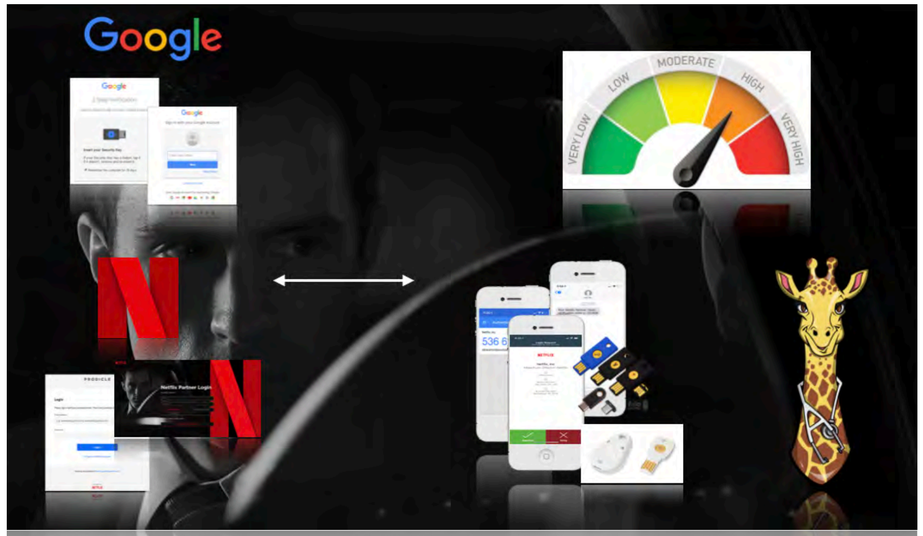


Federation Hub (Layered Security)



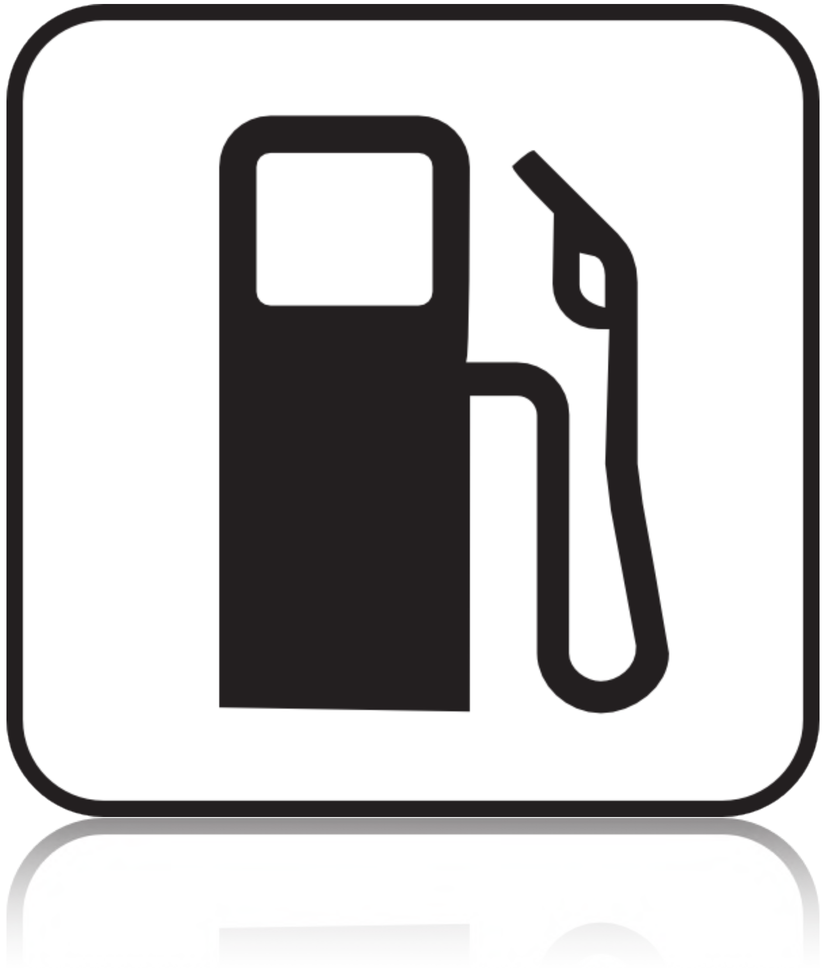






Identity Provider

NETFLIX



EDWARD

Search for: applications, scopes

Tejas Dharamshi

Edit

Configuration

Regenerate Secret

Delete

Help

Help

security help

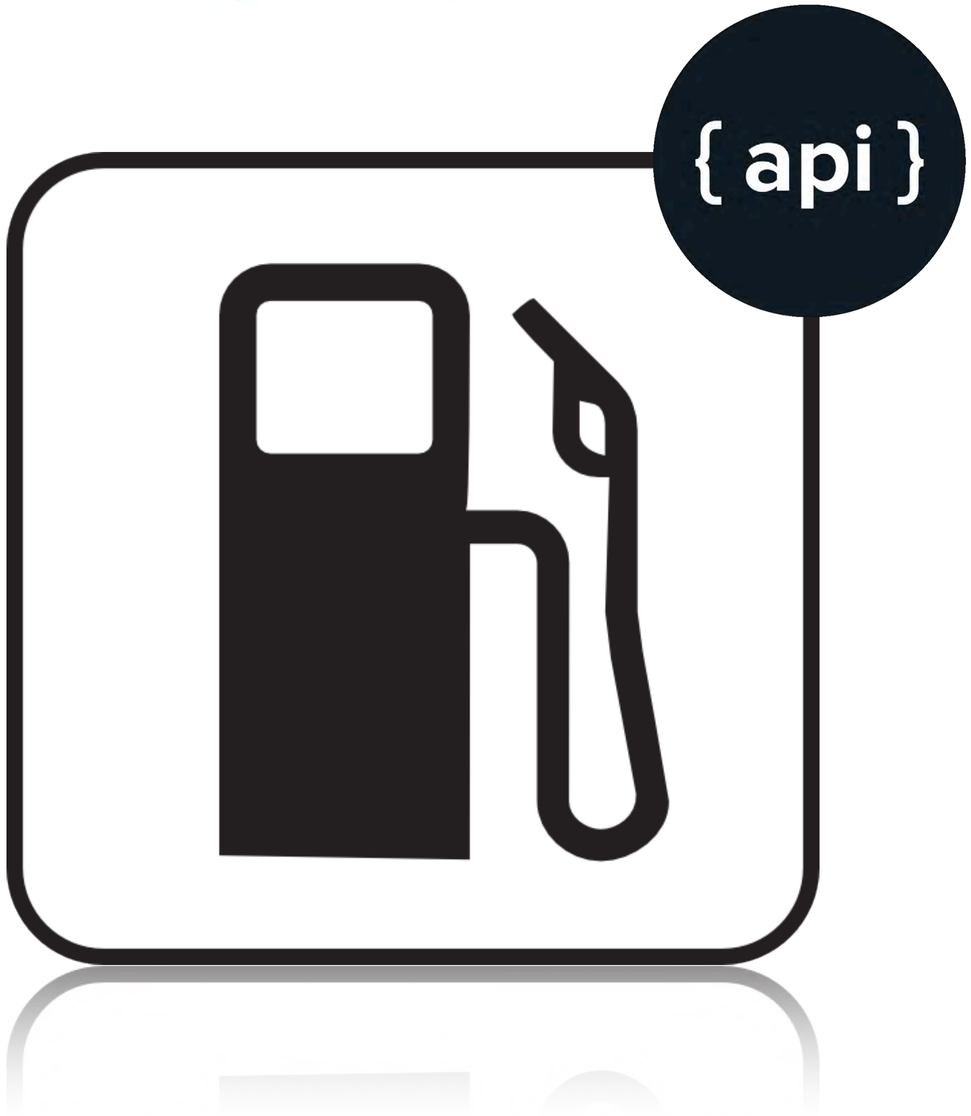
FINISHED

Configuration

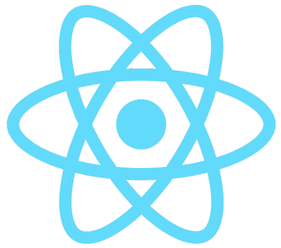
EZ Configuration

```
APACHE_MEECHUM = enabled
APACHE_MEECHUM_CLIENT = iaetester-java
APACHE_MEECHUM_SECRET = /run/metatron/decrypted/iaetester-java-secret
APACHE_MEECHUM_ADDITIONAL_SCOPES = allgooglegroups default iaetester-java

# Hostname for your application
APACHE_HTTPS_HOSTNAME = myapp.netflix.com

##################
# Locations
##################

# URLs requiring authentication. By DEFAULT, authenticate everything not
# explicitly whitelisted in APACHE_PLAINLOCATIONS. This expression must
# be in Apache LocationMatch compatible format. Note that if
# APACHE_LOCATIONS_FILE is set then APACHE_MEECHUM_LOCATIONS has no effect.
APACHE_MEECHUM_LOCATIONS = ^/

# URLs requiring oauth authentication. By DEFAULT, authenticate nothing.
```

Close


{ api }

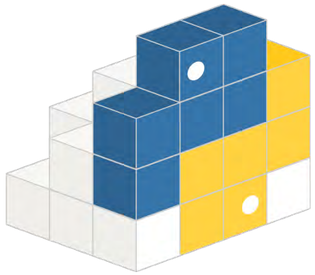

JS

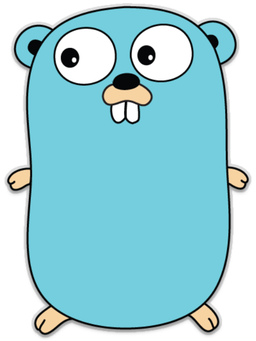



A

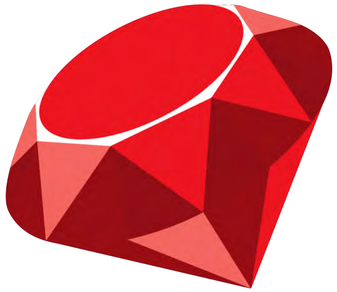

npm


RAILS






node
JS



Paved Road

build passing | code quality: c/c++ A+ | lgtm 0 alerts

OpenID CERTIFIED

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).

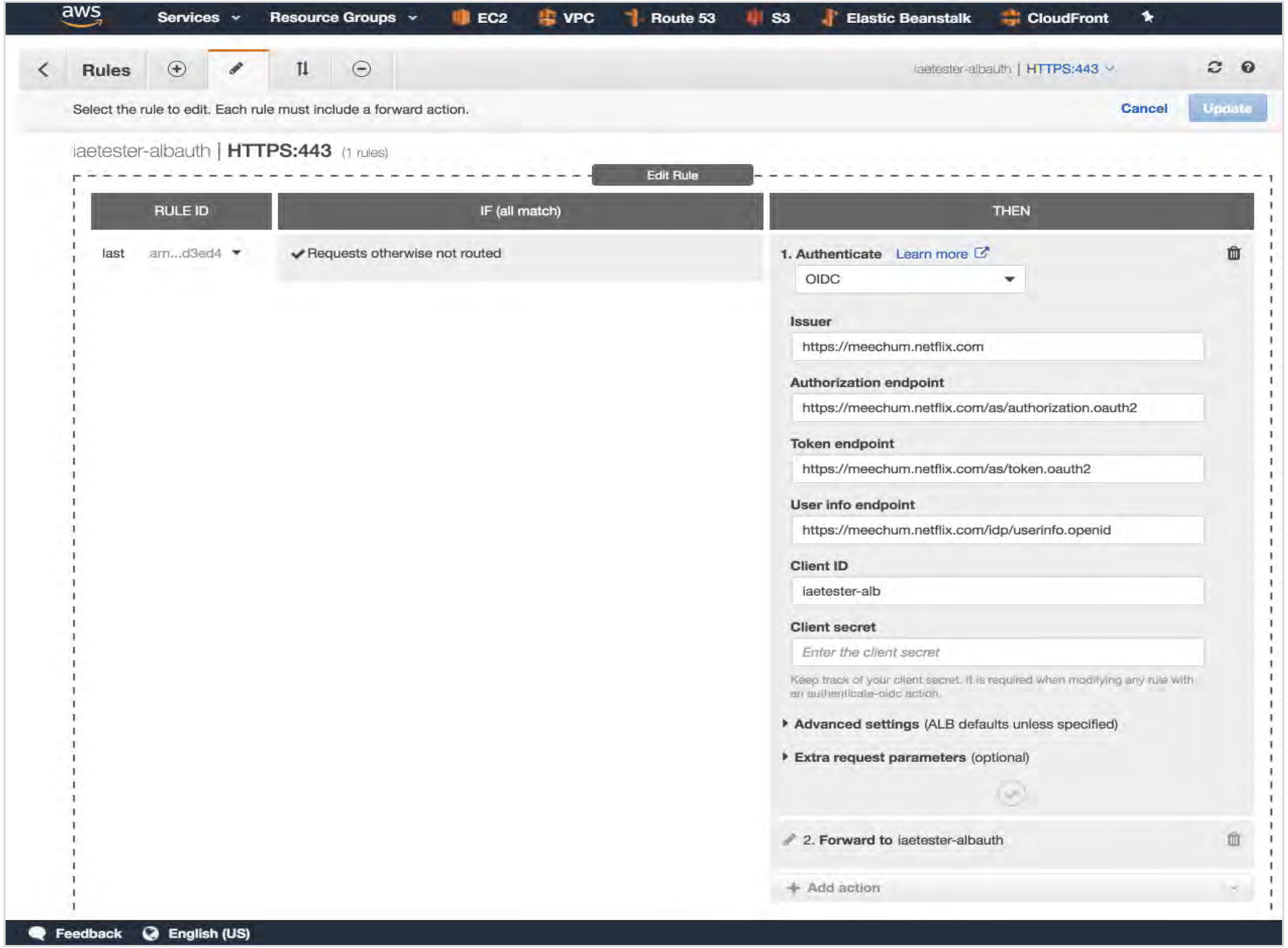
By default the module sets the `REMOTE_USER` variable to the `id_token [sub]` claim, concatenated with the OP's Issuer identifier (`[sub]@[iss]`). Other `id_token` claims are passed in HTTP headers and/or environment variables together with those (optionally) obtained from the UserInfo endpoint.

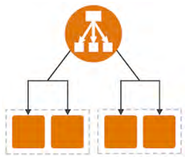
It allows for authorization rules (based on standard Apache `Require` primitives) that can be matched against the set of claims provided in the `id_token` / `userinfo` claims.

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

Netflix / zuul

Watch 817 | Star 6,618 | Fork 1,280

Code | Issues 105 | Pull requests 12 | Projects 0 | Wiki | Insights

Join GitHub today

GitHub is home to over 28 million developers working together to host and review code, manage projects, and build software together.

Sign up

Dismiss

Zuul is a gateway service that provides dynamic routing, monitoring, resiliency, security, and more.

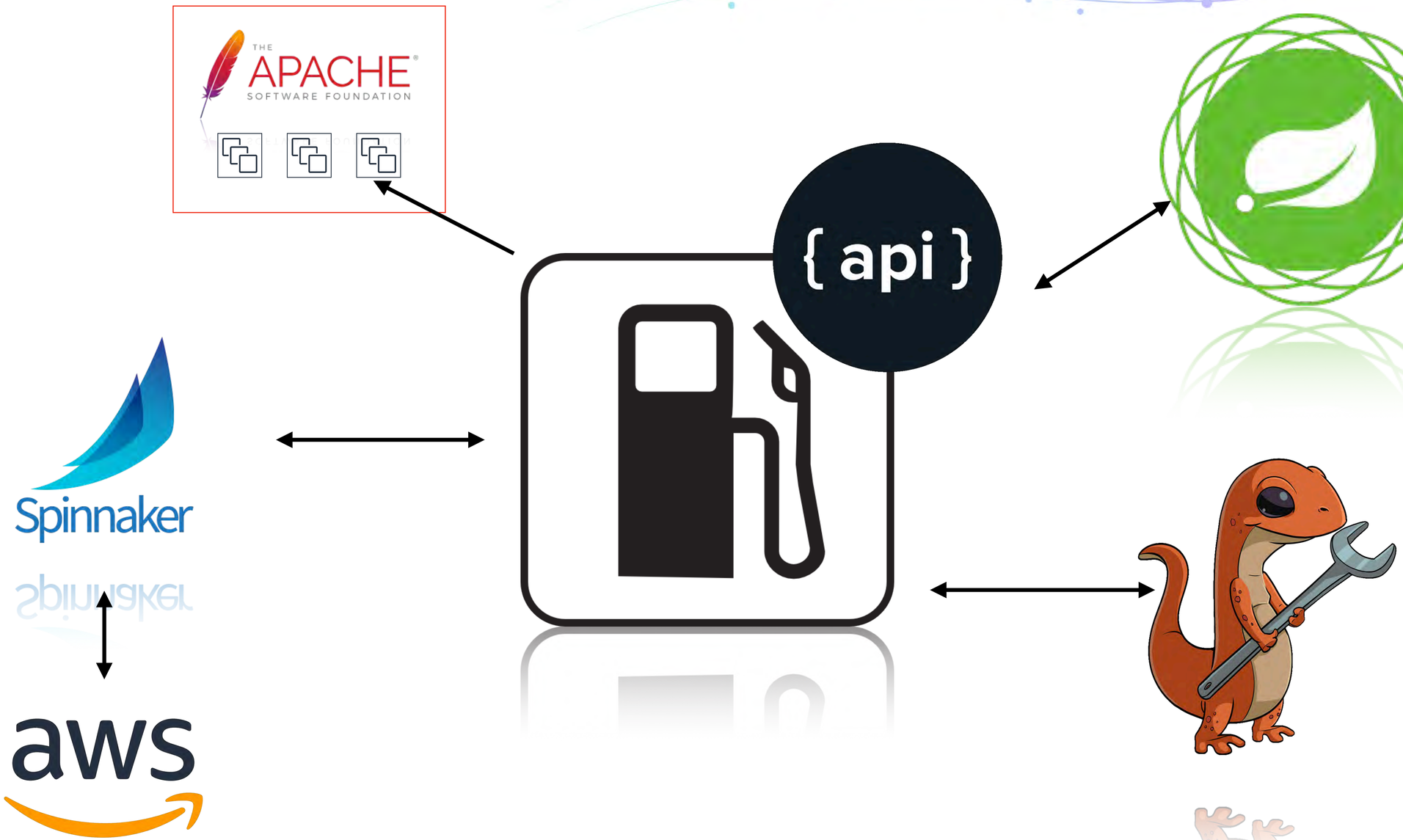
672 commits | 15 branches | 51 releases | 30 contributors | Apache-2.0

Branch: 2.1 | New pull request | Find file | Clone or download

artgon make origin server connection extensible — Latest commit d8166a5 3 days ago

codequality	Remove unneeded files	4 years ago
gradle	GH-428 add ssl support for netty client	7 months ago
zuul-core	make origin server connection extensible	3 days ago
zuul-sample	secure token changes	a month ago
.gitignore	Added isAvailable()	3 years ago

Spinnaker


THE
APACHE
SOFTWARE FOUNDATION
{ api }
Spinnaker
aws

Zero Trust
Principle 5

Role Based Access Control (RBAC)

- Groups
- Organizations
- User attributes

General
Grants
Redirect Uri's
Scopes
Access Control
Attributes
Summary

Actions
Update Token Manager
Configuration
Regenerate Secret
Delete

Help
Help
security-help

iaetester-java (Client ID: iaetester-java)

PROGRESS FINISHED

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:

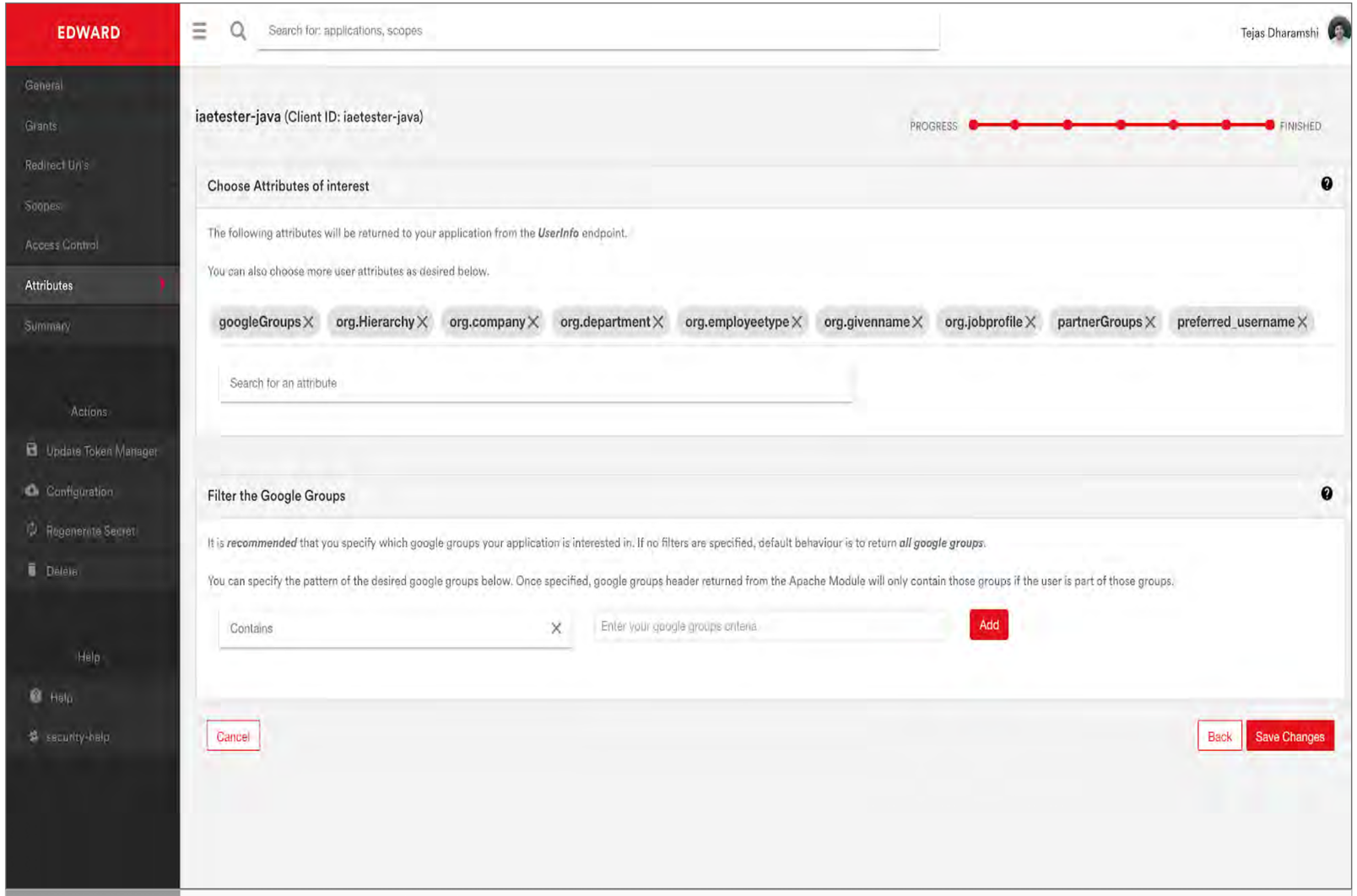
- [x] Netflix.com (employee's only)
- [ ] NetflixContractors.com (contractors and vendors only)
- [ ] NetflixCS.com (customer service only)
- [ ] Svc.netflix.net (service accounts only)
- [x] Pandora Prod (Partner Directories)
- [ ] Pandora Test (Partner Directories)
- [ ] Moon.film (Prodicle production)

N

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

iae@

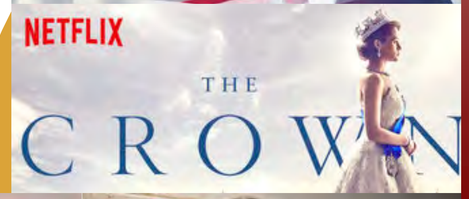
```
{
  "sub": "tdharamshi@netflix.com",
  "preferred_username": "tdharamshi",
  "given_name": "Tejas",
  "org.description": "Sr. Security Software Engineer",
  "org.Hierarchy": "President's Office (Reed Hastings) :: Product Mana
  "authFlow": "GoogleNetflixEmployee",
  "picture": "https://plus.google.com/_/focus/photos/public/AIbEiAIAA
  "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"
}
```

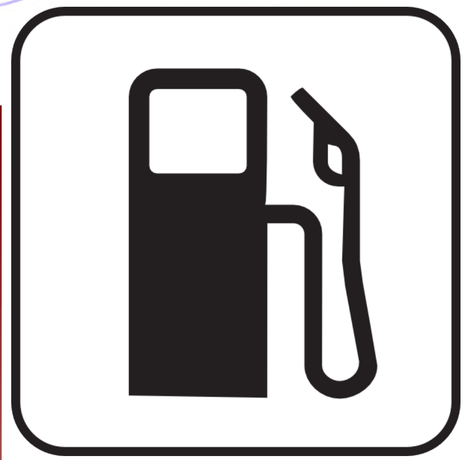
Recap


NETFLIX
STRANGER THINGS
A NETFLIX ORIGINAL SERIES


NETFLIX
HOUSE of CARDS

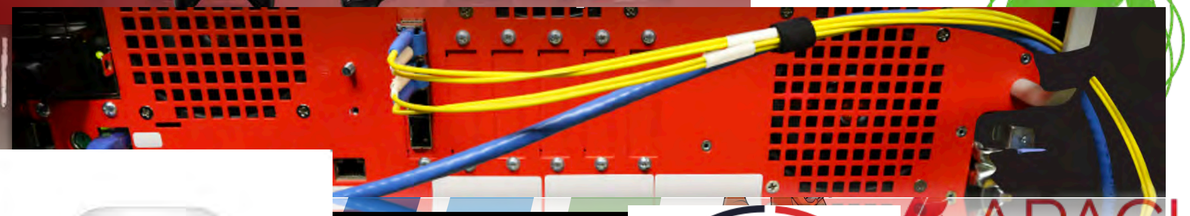

NETFLIX
THE
CROWN


NETFLIX
NETFLIX ORIGINAL
HOUSE of CARDS
ORANGE is the new BLACK

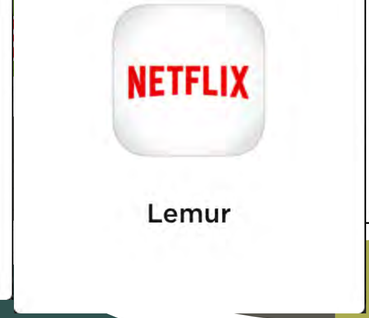


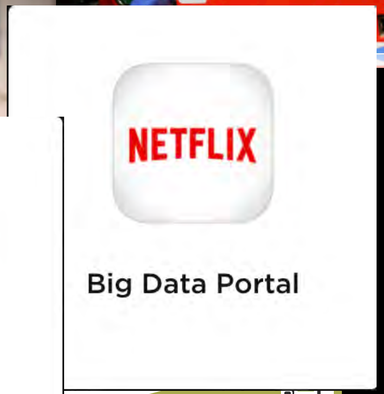

NETFLIX
NARCOS


NETFLIX
ORANGE is the new BLACK




NETFLIX
Employee Landing Page


NETFLIX
Lemur


NETFLIX
Big Data Portal


spinnaker

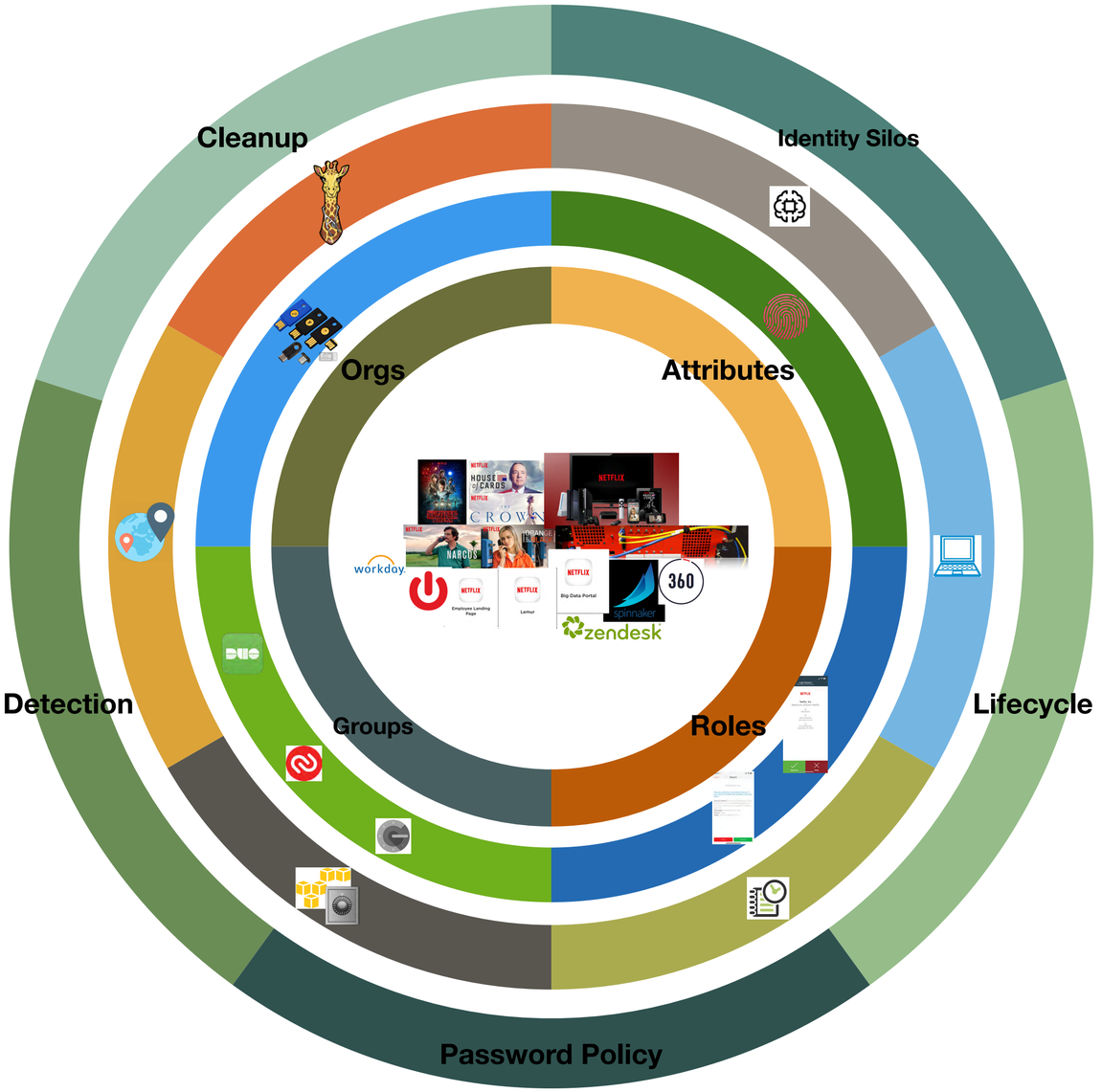

360


APACHE
SOFTWARE FOUNDATION


Spinnaker


zendesk

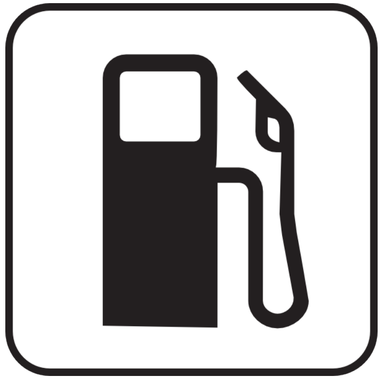
Identity as the Security Perimeter



OpenID

OAUTH 2

SAML



Immediate Action Items

- Identify if your organization has privileged corporate network?
  - What access do users get as a result of this implied trust?
- Identify gaps in the provisioning and de-provisioning process in your organizations
  - Are you tapping into event sources?
  - What about de-provisioning?
- If you liked anything which is not open-sourced yet. Please email me @tdharamshi@netflix.com.

How to apply what we learnt today

- Adopt standards OpenId, OAuth 2.0, SAML and leverage IDP’s like PingFederate, Okta, Auth0 etc.
- See if apache module, alb authentication fits your organization needs.
- Adopt multi-factor authentication and adaptive authentication for stronger authentication
- How does your endpoint security strategy looks like?
  - Does your organization adopt BYOD?
  - Checkout Stethoscope app

RSAConference2019

Q&A

Tejas Dharamshi

Senior Security Software Engineer
Netflix, Inc.
@tejasdharamshi