
cisco
You make possible

Inside Cisco IT

Identity-as-a-Service: Beyond the Hype.....really

Alben Cheung, Sr. Security Software Engineer
Franky Saxena, Security Software Engineer

BRKCOC-1476

cisco Live!
Barcelona | January 27-31, 2020

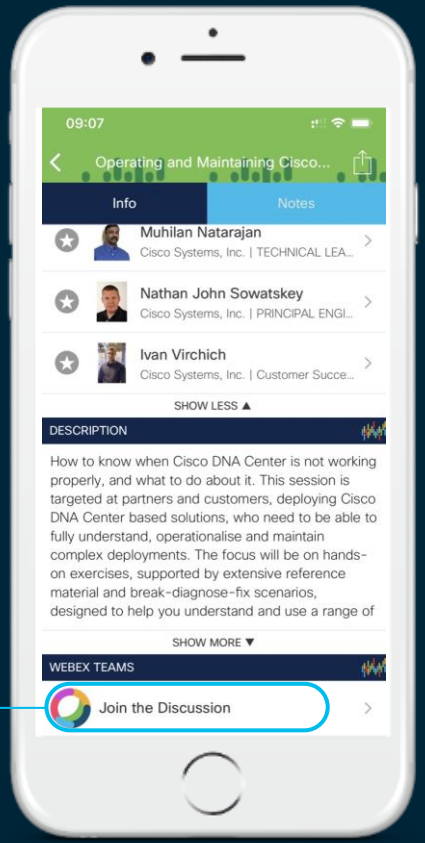
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space

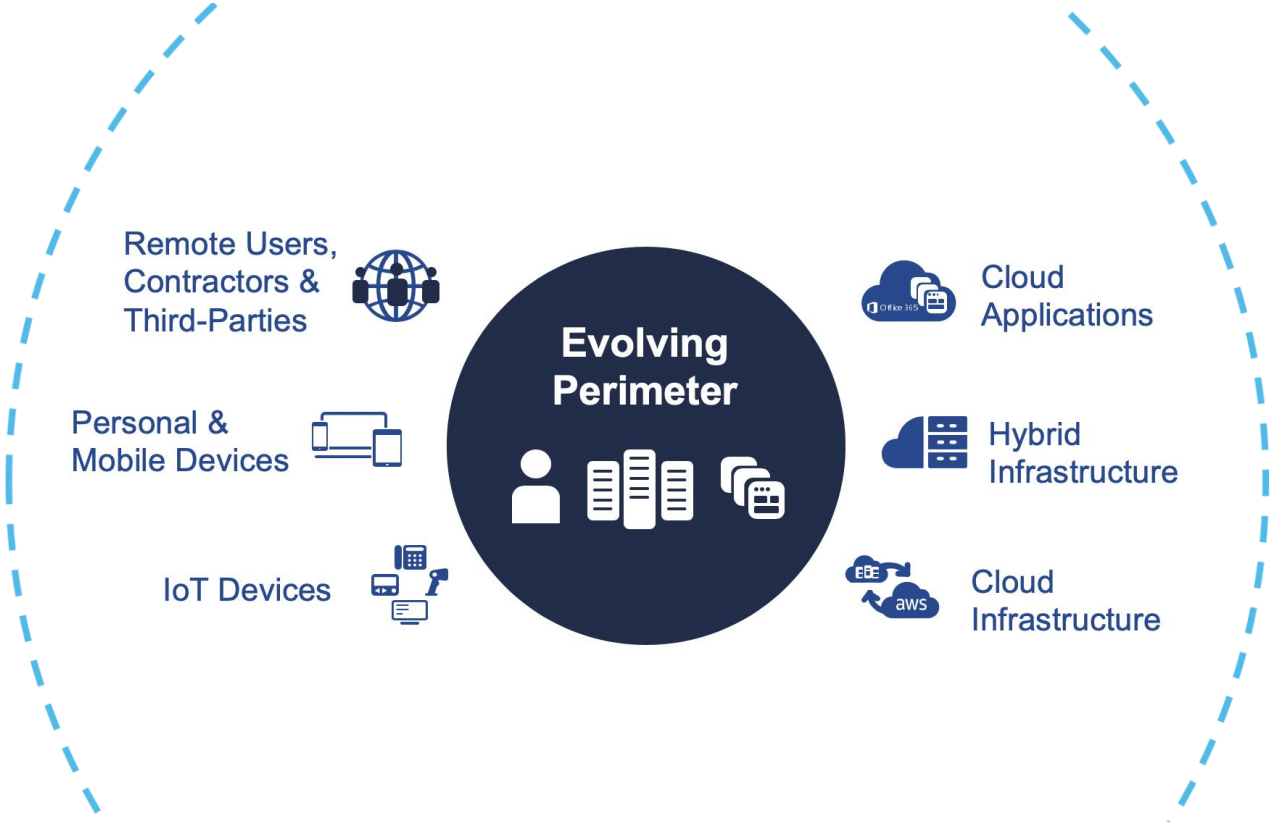


cisco Live!

Were you suspicious?

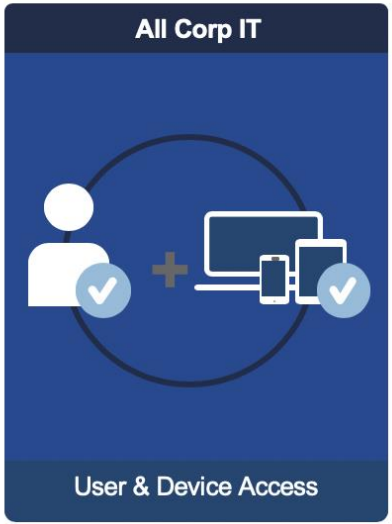
Who cares and why?

Changing IT Landscape...

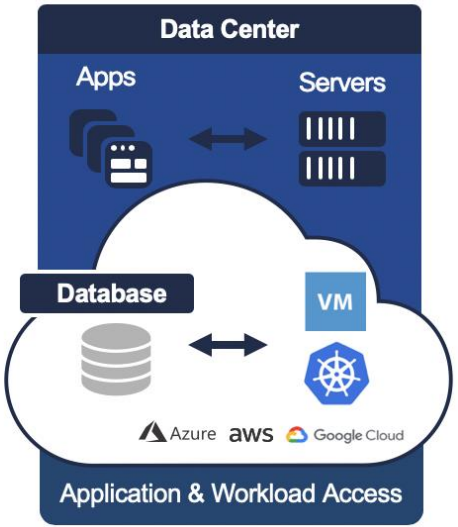


...means securing access in new ways...

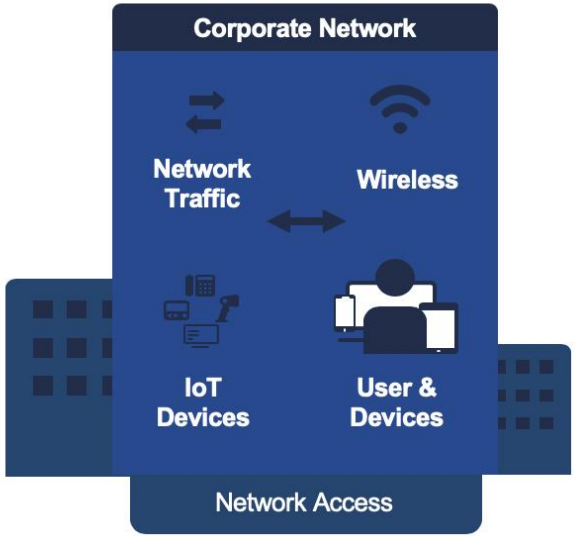
Workforce



Workload



Workplace



...bringing us these threats

Targeting Identity

81% of breaches involved compromised credentials

Targeting Apps

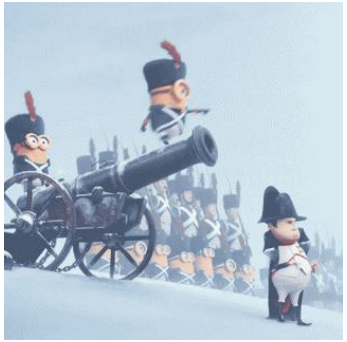
54% of web app vulnerabilities have a public exploit available

Targeting Devices

300% increase in IoT malware variants

How secure hackers think we are

How secure my CEO thinks we are



How secure I think we are

How secure we actually are

Agenda

- Goal
- Challenges
- Opportunities
- Our Approach
  - API architecture: FastFed
  - AI architecture: Applied Machine Learning
- Key Takeaways
- Questions?
  - Ask live or through Webex teams space: “Join the Discussion” @ BRKCOC-1476

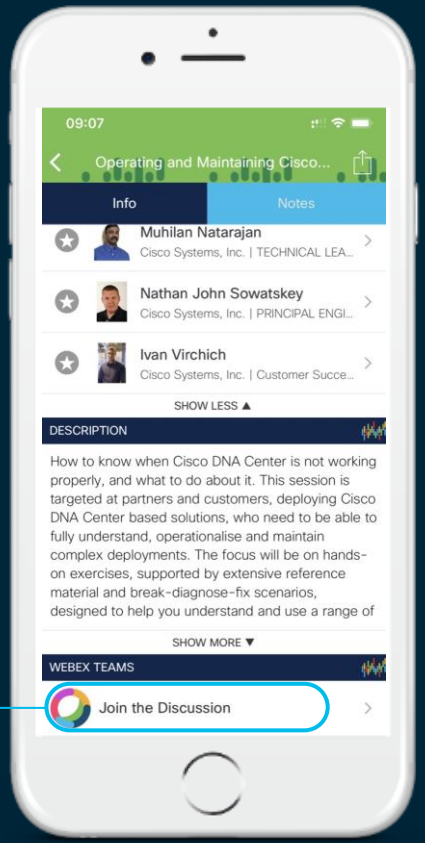
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



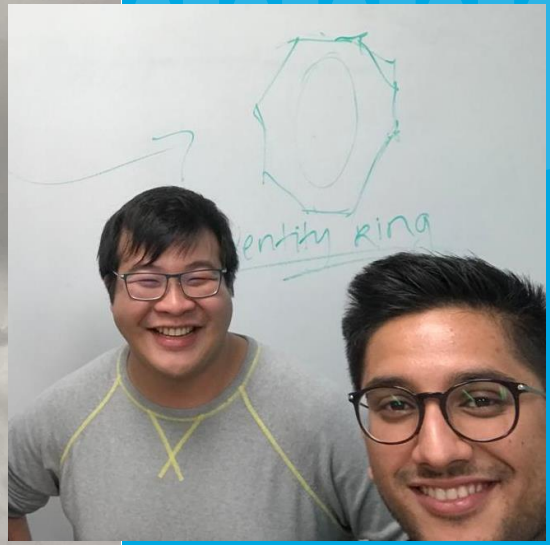
Who we are

Alan the Bubble
Automation Pro
Tea Connoisseur

Franky the Machine
Learning Guru
Tandoori Chicken
Connoisseur

BEGINNER'S GUIDE TO P1 BRIDGE SURIVAL:

1. Major incident occurs late at night (~2am)
   a. Grab a mug and break open seal the **coffee**
   b. Pour yourself a cup
2. More **4 hours** into the incident
   a. Eat a **Joi Bol**
3. More **8 hours** into the incident
   a. Pour yourself another cup of **coffee**
   b. Eat a **Joi Bol**
4. More **12 hours** into the incident
   a. Eat a **Mac N Cheese Bowl**
   b. Find a **beer mug** and place in the refrigerator
5. More **16 hours** into the incident
   a. Pour yourself another cup of **coffee**
   b. Apply **face mask** of your choice
6. More **24 hours** into the incident
   a. Pour yourself another cup of **coffee**
   b. Eat another **Mac N Cheese bowl**
   c. Apply another **face mask** of your choice
7. More **36 hours** into the incident
   a. Time to pour yourself an ice-cold **beer**
   b. Eat the **Nutella To Go**
   c. Cry
8. More **48 hours** into the incident
   a. Eat two **Joi Bol**
   b. Cry some more
   c. Time to take a swig of the good stuff (i.e. **The Jim Bean**)
9. Incident is resolved after a long haul
   a. Time to celebrate with some **Prosecco**!
   b. Apply another **face mask** of your choice
   c. Get some well-deserved sleep!



Goal

In a perfect world zero trust requires...

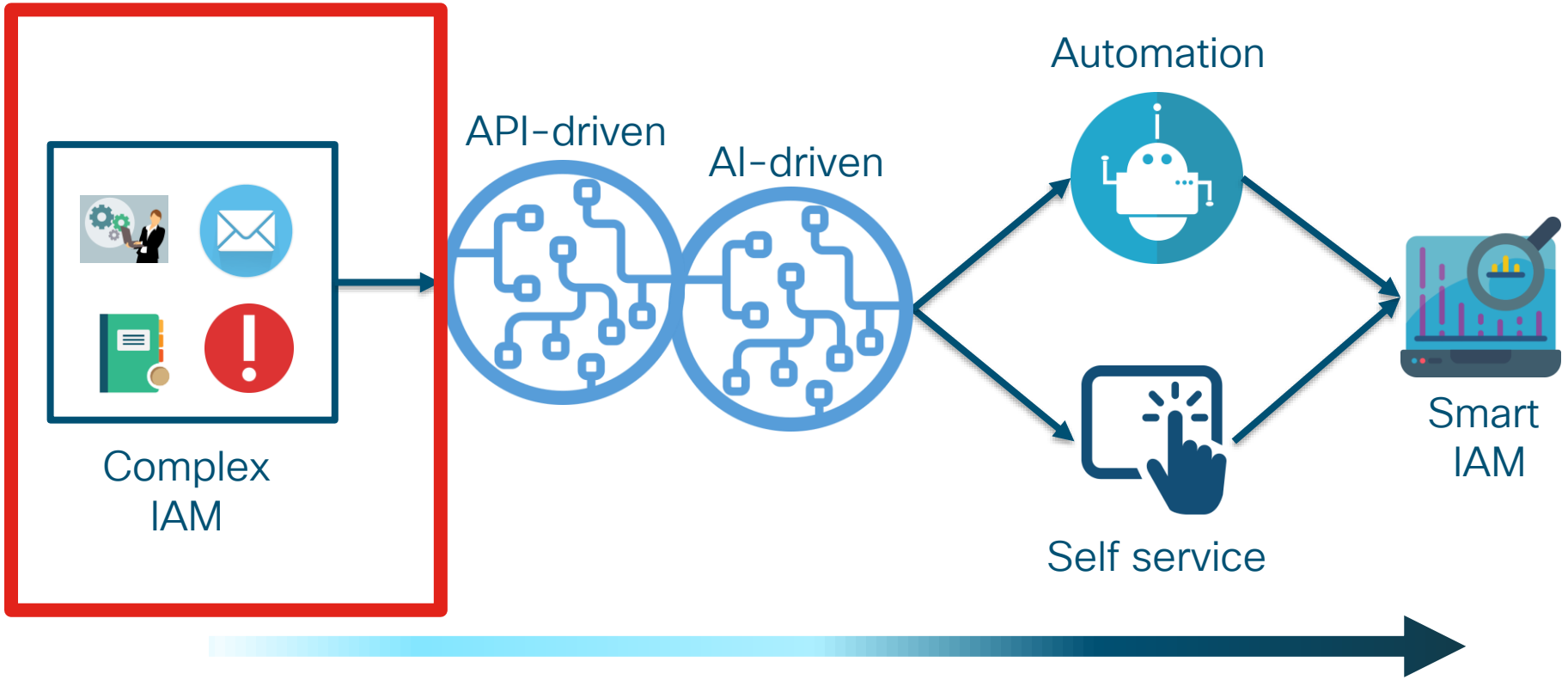
Trusted user

Trusted device

Appropriate application access

Challenges

We are future-proofing our IAM system



In an imperfect world...

- Well funded adversaries
  - State-sponsored
  - Identities available on the dark web
- Complexity of these IAM systems
  - Disorganized data
  - Custom Scripts
  - Reactive Monitoring
  - No end-to-end identity flow
- Moving to the cloud
  - Slow and inefficient
  - Security playing catch-up

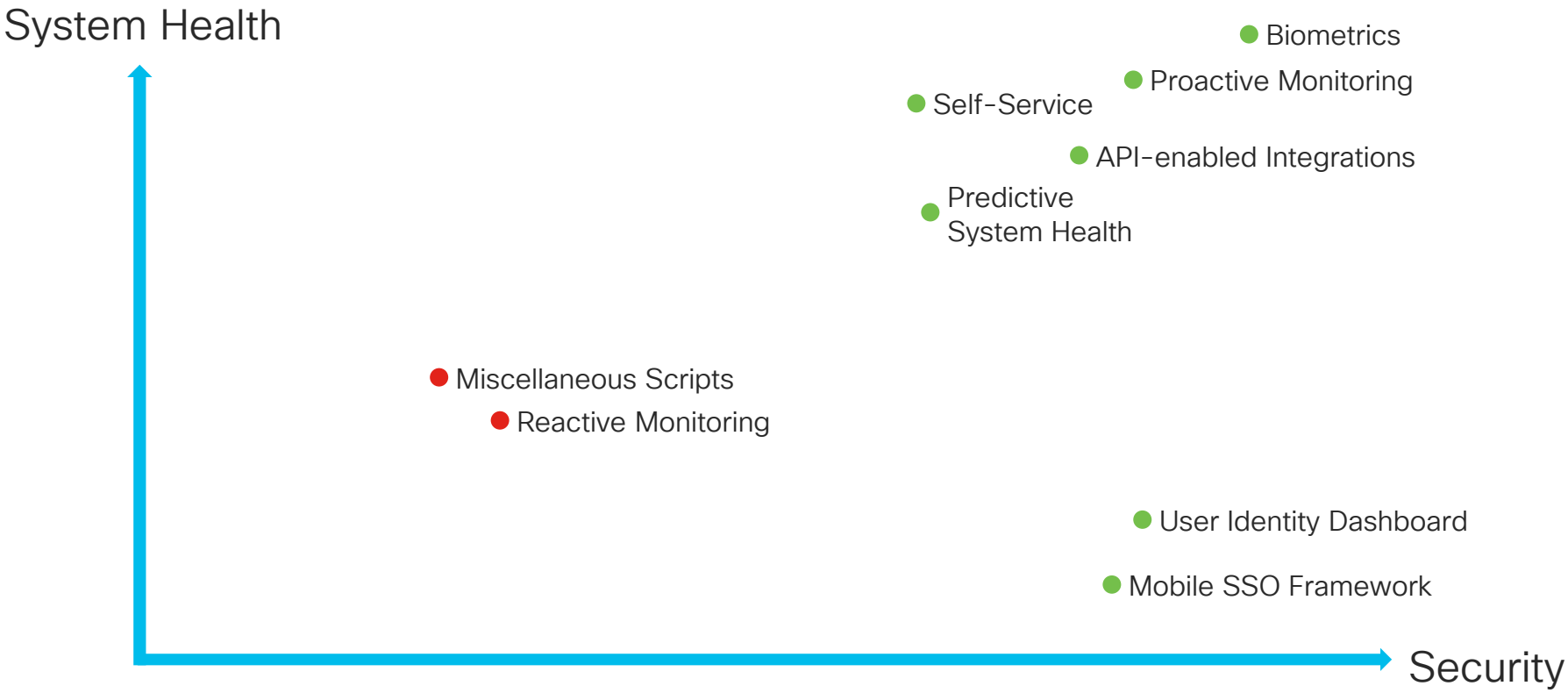
What we are and aren't

- Product that you can buy off the shelf
- Fully integrated with entirety of Cisco Security suite

- ✓ Iterating current IAM systems to make them smart
- ✓ Giving you a blueprint to get you started
- ✓ “API First” approach in Ops
- ✓ An innovative, yet generic solution that you can apply in your environment

Opportunities

You can secure and enhance IAM



Mobile SSO Framework

UOT License

("You Owe Tea" License)

CIA Framework for iOS

The CIA (Cisco Identity & Access) Mobile SSO Framework is designed to integrate SSO into mobile apps seamless without a whole lot of effort from the developer.

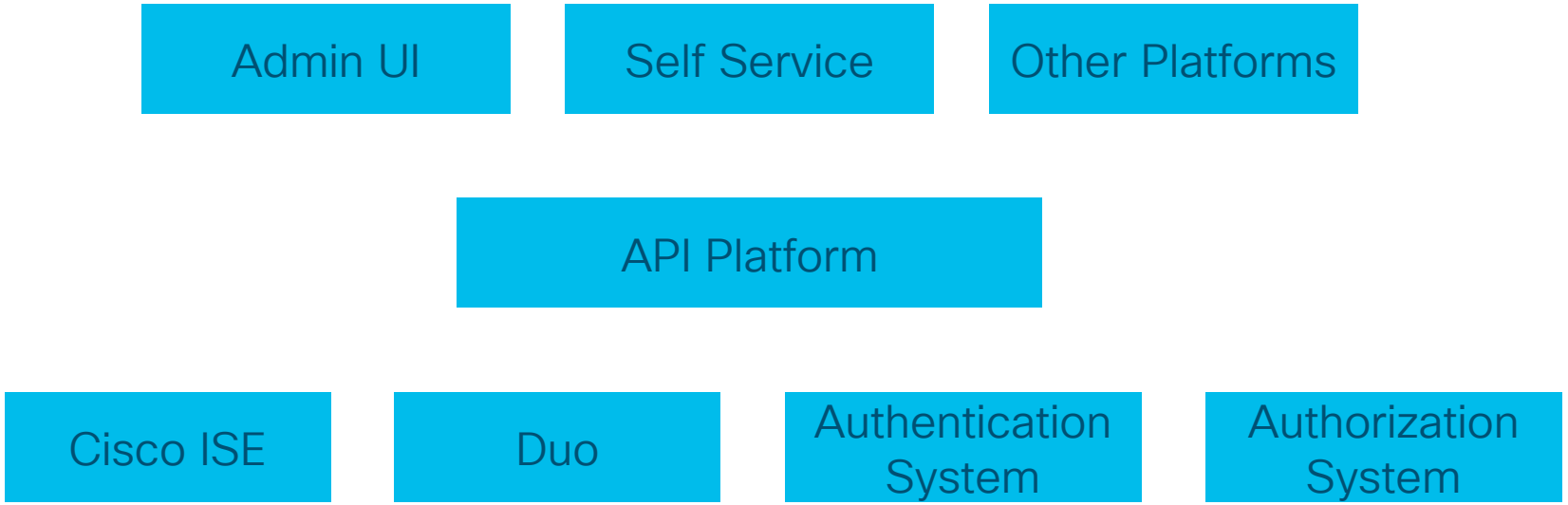
Requirements

Supported Languages: Objective-C, Swift 4, Swift 5 **Operating System:** iOS 10+

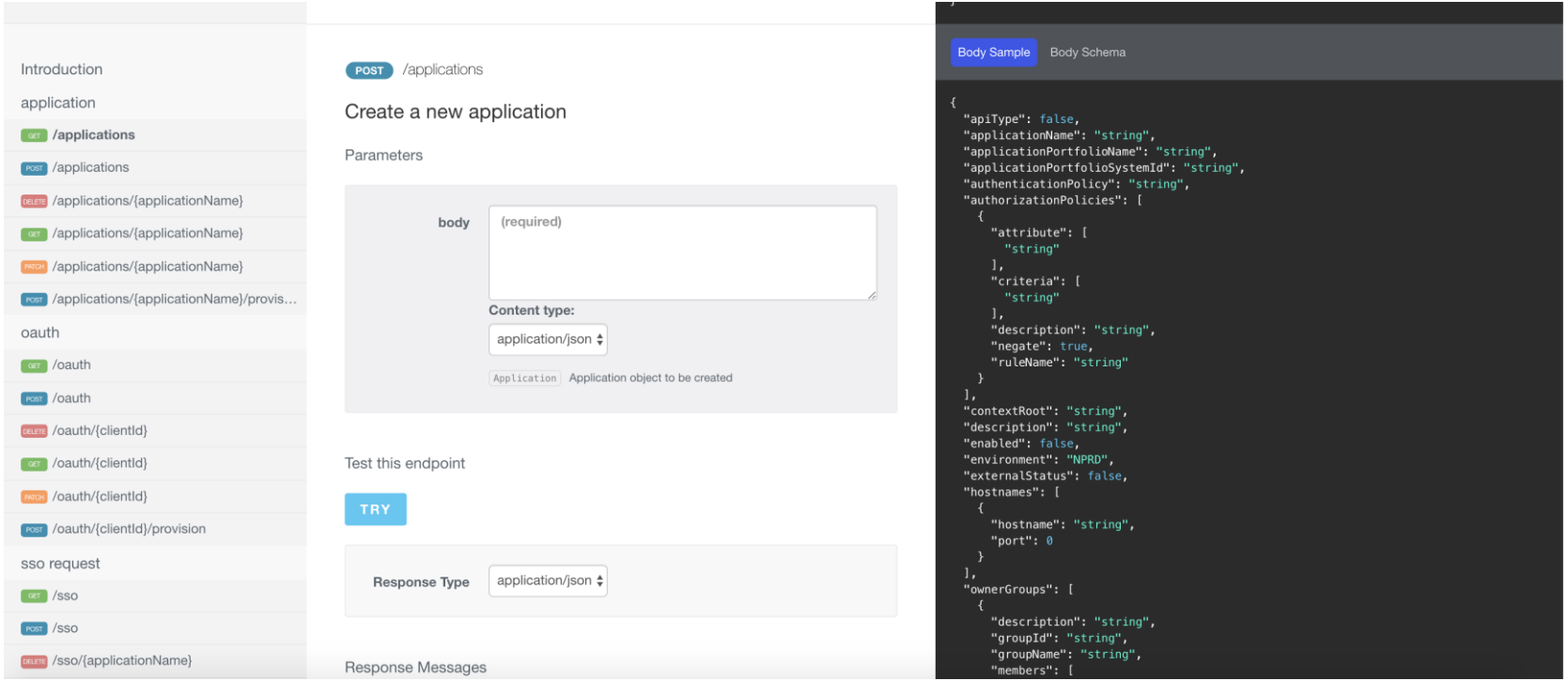
Getting Started

1. Download the latest appropriate CIA Framework zip package in the links provided in the mySSO dashboard.
2. Import the package into your Xcode project (Swift or ObjC) by dragging and dropping the cia.framework file into the Embedded Binaries section under General in Project Settings.
3. Now on to coding!

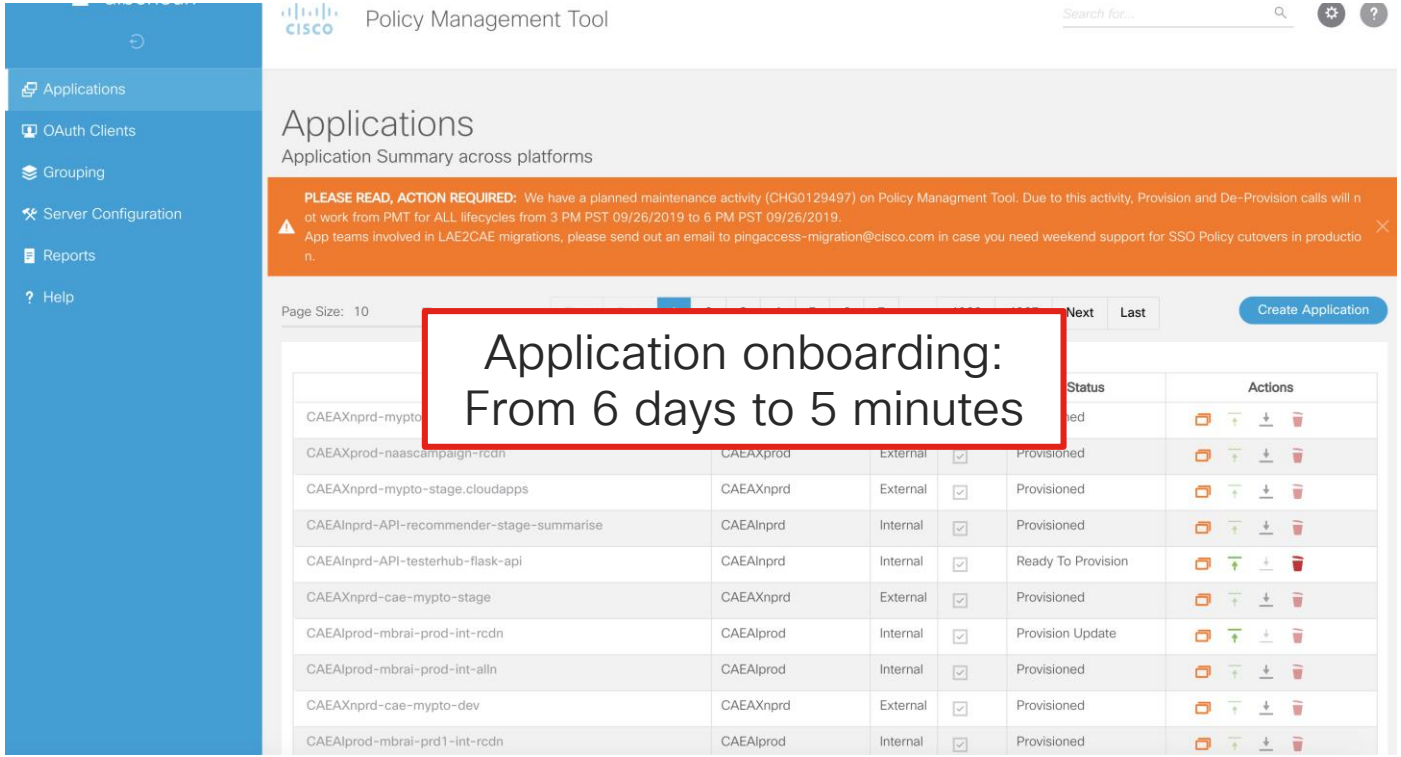
How to design versatile architecture for IAM



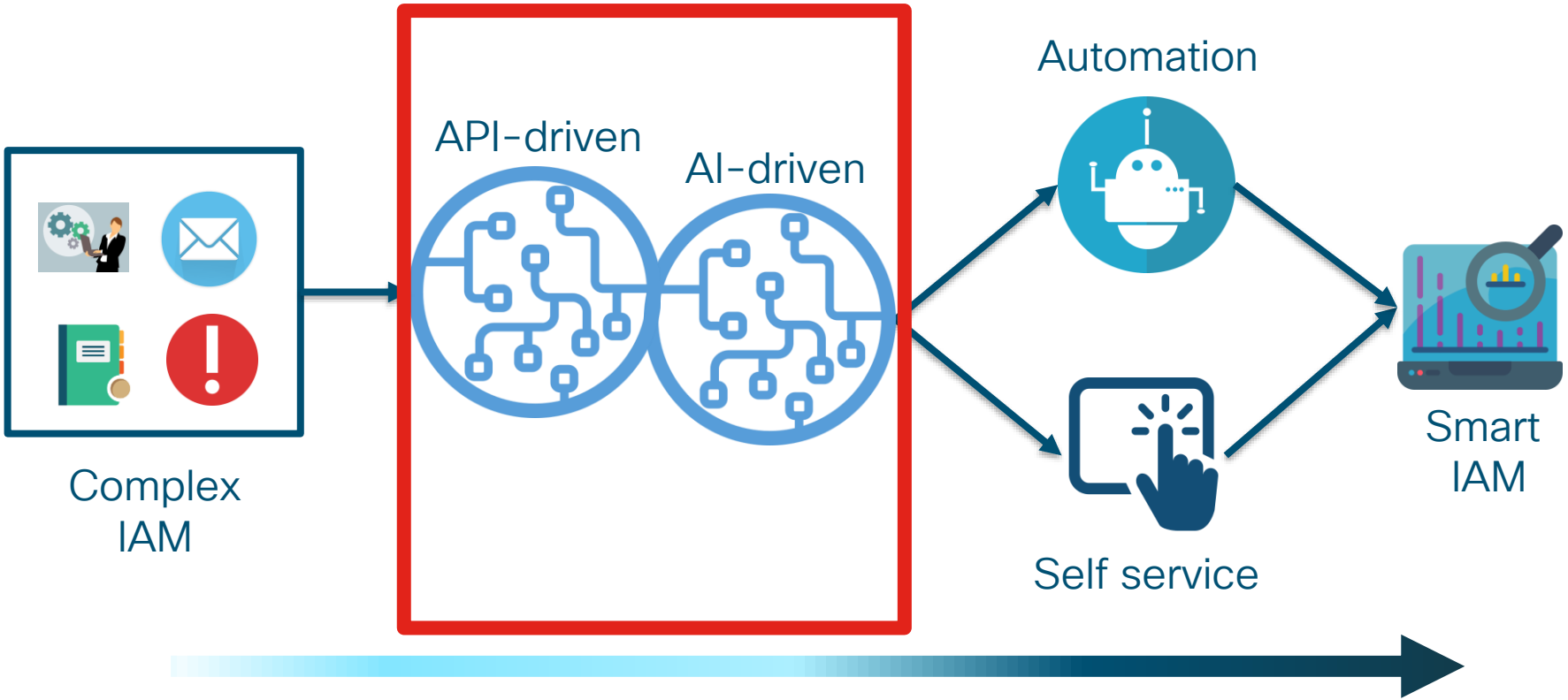
API Platform



Begin our self-service journey



We are future-proofing our IAM system



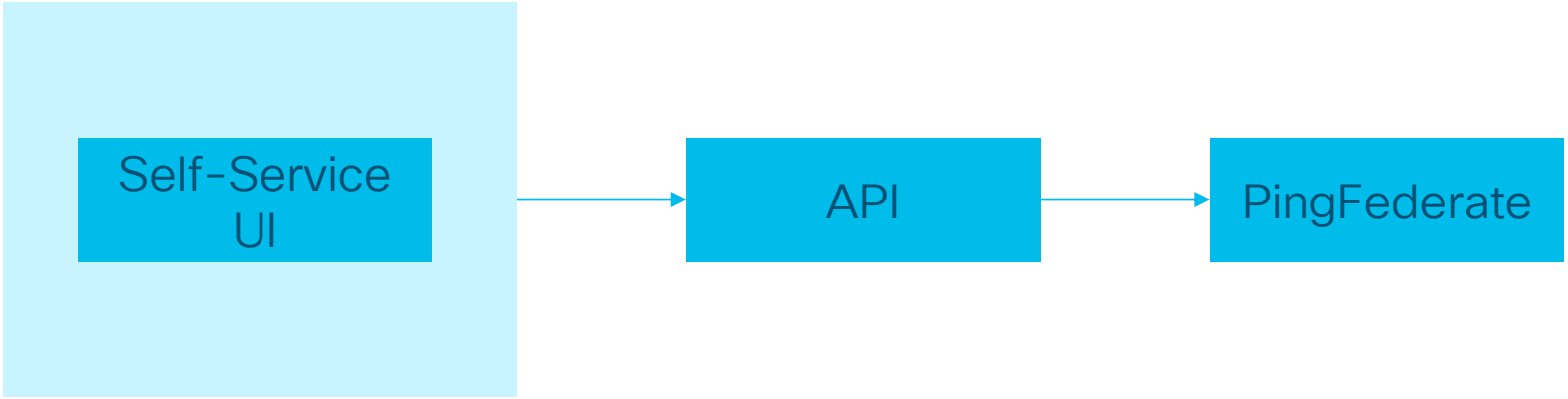
Solution #1: FastFed-like

Fastfed Protocol

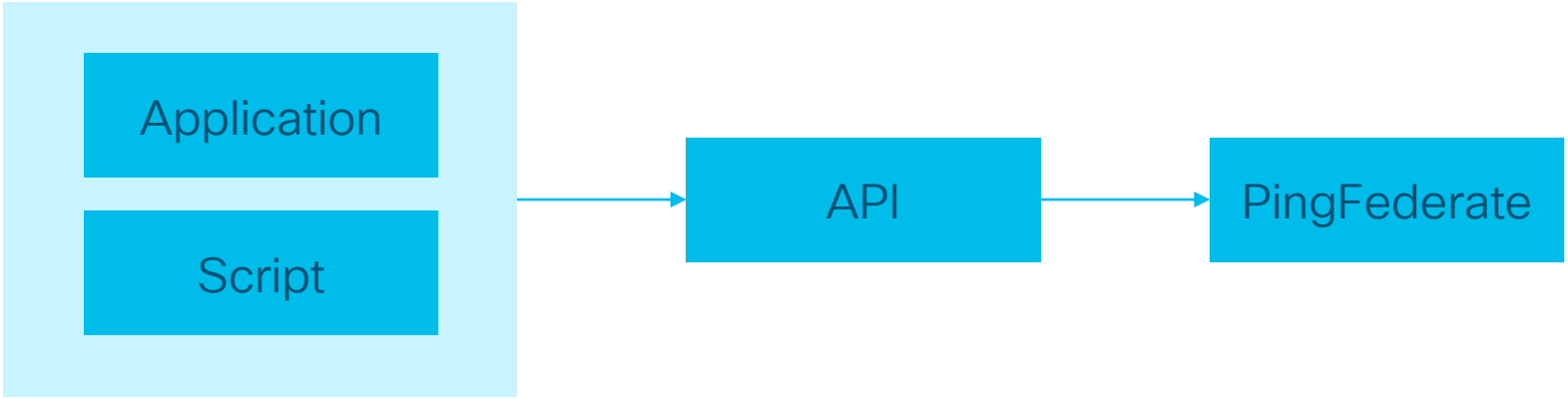
- OpenID Standard
- Status: WIP

https://openid.net/wg/fastfed/

The provisioning process via the UI



Script-based provisioning process



Demo

Solution #2:
Machine learning

"... what we want is a machine that can learn from experience"

Alan Turing

Machine learning opportunities

Availability

- Proactive monitoring
- Critical cloud infrastructure

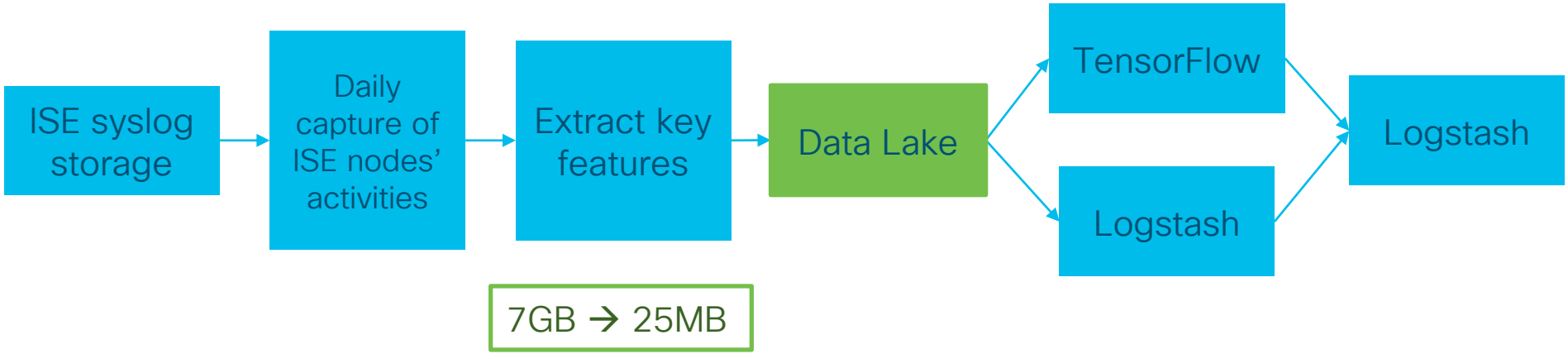
Visibility

- Identity landscape
- Who's accessing what and where

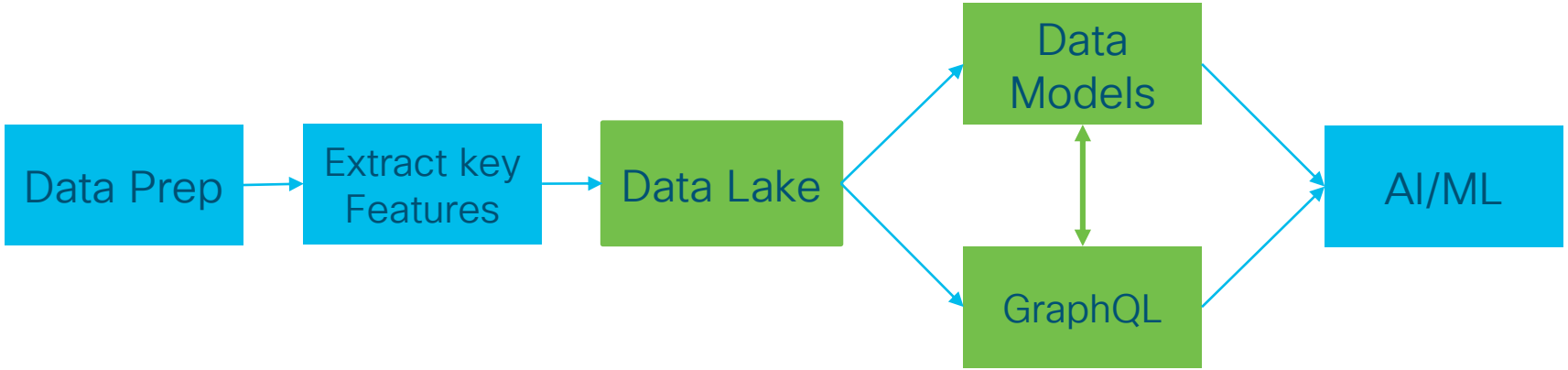
Unification

- Consolidate data from ISE, Duo, AnyConnect etc.
- Zero Trust

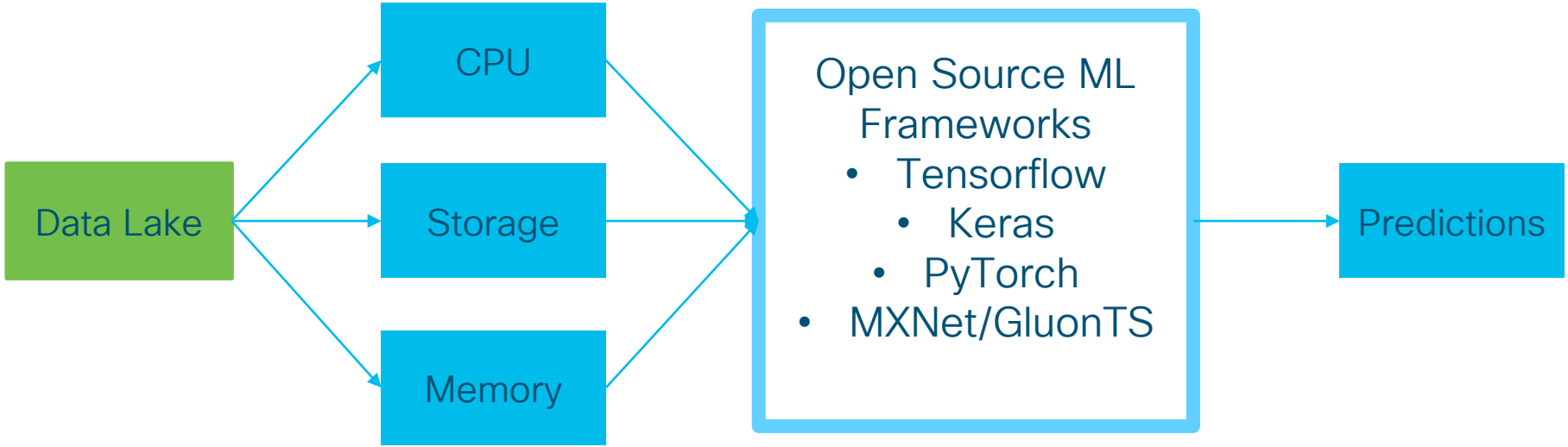
Our Approach: Proof of Concept analytics engine



Our Approach: Production analytics engine

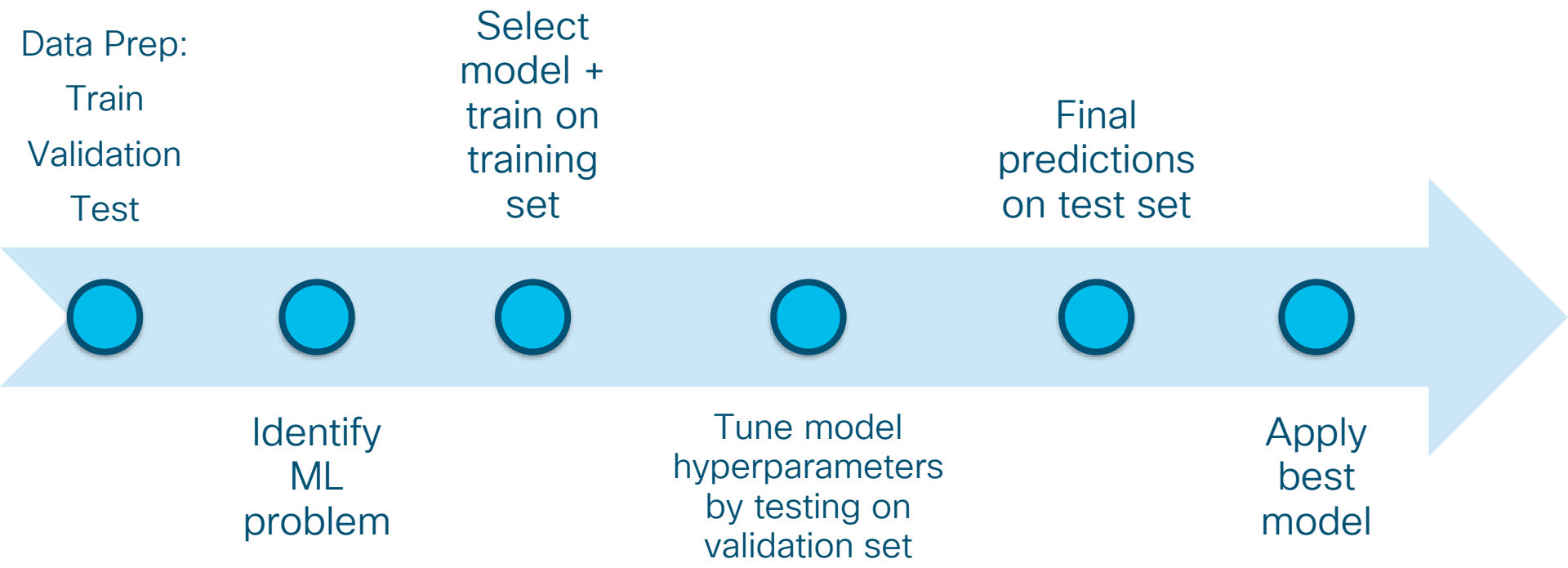


Our Approach: Proactive Monitoring data flow



Centralised repository	Operational metrics	Model dev + training	Smart Dashboard
50%	10%	30%	10%

Our Approach: Machine learning blueprint



GIS IAM | myID | JupyterLab

localhost:8888/lab?

Identity Services E... | Dashboard - Ciscol... | CCNP | Speaker Dashboard | GitHub - clovaai/Fo... | GitHub - GauthierD... | GitHub - huggingfa... | Question-Generati... | dna-ise | fambu

File Edit View Run Kernel Tabs Settings Help

/

Name

- duo_client_python
- venv
- bot.py
- CPU_prediction.ipynb
- CPU_prediction.py
- cpuPreds.csv
- cpuPreds.json
- duoAuth.py
- fakedata.py
- isemtv-prd-04_cpu_1...
- ngrok
- ngrok2
- variables.py

CPU_prediction.ipynb | Terminal 2

Code | Python 3

```
[ ]: import mxnet as mx
from mxnet import gluon
import numpy as np
import pandas as pd
import matplotlib.pyplot as plt
import json
import os
from itertools import islice
from pathlib import Path
from gluonts.dataset.common import ListDataset
from datetime import datetime, timedelta
from gluonts.model.deepar import DeepAREstimator
from gluonts.trainer import Trainer
from itertools import islice
from gluonts.evaluation.backtest import make_evaluation_predictions
from datetime import datetime

import requests
from requests.auth import HTTPBasicAuth
import variables
import json

user = variables.user
passw = variables.password
import warnings
warnings.filterwarnings('ignore')
from IPython.display import clear_output
clear_output(wait=True)
```

STEP 1: Loading dataset

Using previous 24 hours' CPU data of a random ISE node

```
[ ]: dataFile_1day = 'isemtv-prd-04_cpu_1_day'
dataset = './' + dataFile_1day

data = pd.read_csv(dataset)
total_rows = len(data)
```

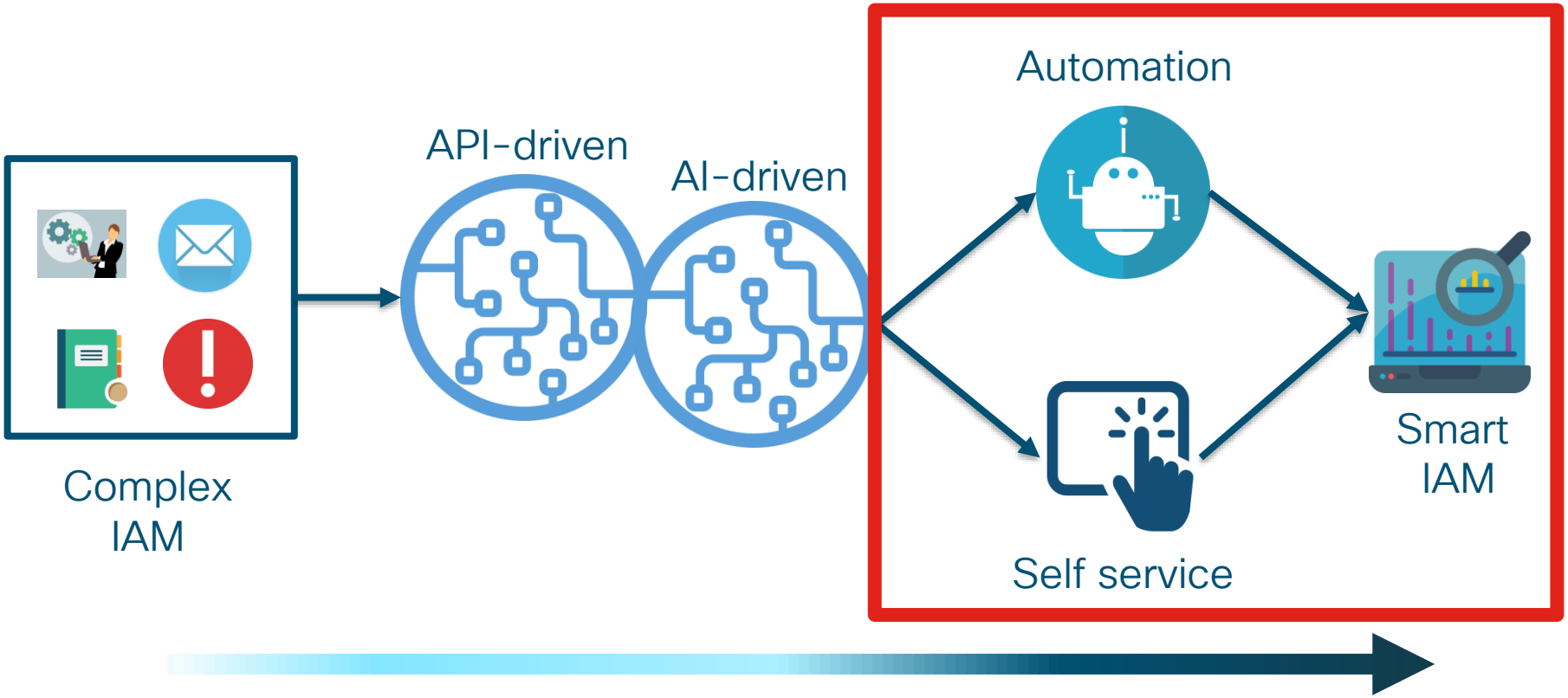
STEP 2: Making dataset iterable ¶

2 | 1 | Python 3 | Idle

Mode: Command | Ln 28, Col 24 | CPU_prediction.ipynb

Demo

We are future-proofing our IAM system



Smart IAM cookbook

Future-Proof IAM

- RESTFul API
- Role-based APIs
- Extensive Logging
- Cloud-ready

AI/ML

- Data Lake
- Visualization Tools
- AI/ML in the cloud

Key Takeaways

- Basics
  - Understand Logging
  - Build a Data Pipeline
  - Filter out noise
- RESTful APIs
- Modularity

- Advanced AI/ML
  - Data Streaming (i.e. Apache Spark)
  - Supervised
  - Unsupervised
  - ISE analytics engine

What should you do now?

Business leaders

- Skills for the future:
  - DevOps – setting up API architecture
  - AI skills – for real time analytics
- MTE sessions for Alben and Franky

Engineers

- Think API first
- Follow the blueprint
  - Set up a data lake
  - Prioritise key data features
  - Experiment with different open source models
  - Implement PoC on one key feature
  - Scale it!

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

cisco Live!

Continue your education

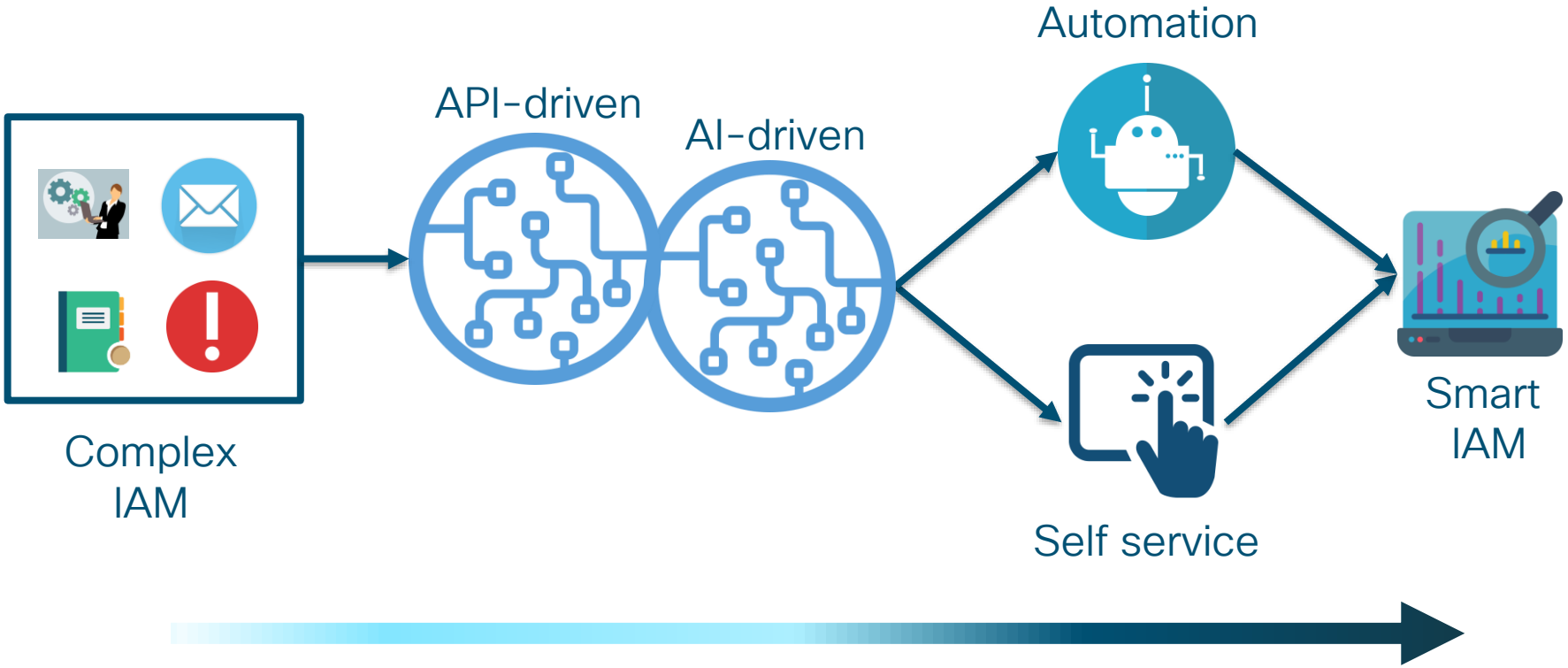
Demos in the Cisco Showcase

Walk-In Labs

Meet the Engineer 1:1 meetings

Related sessions

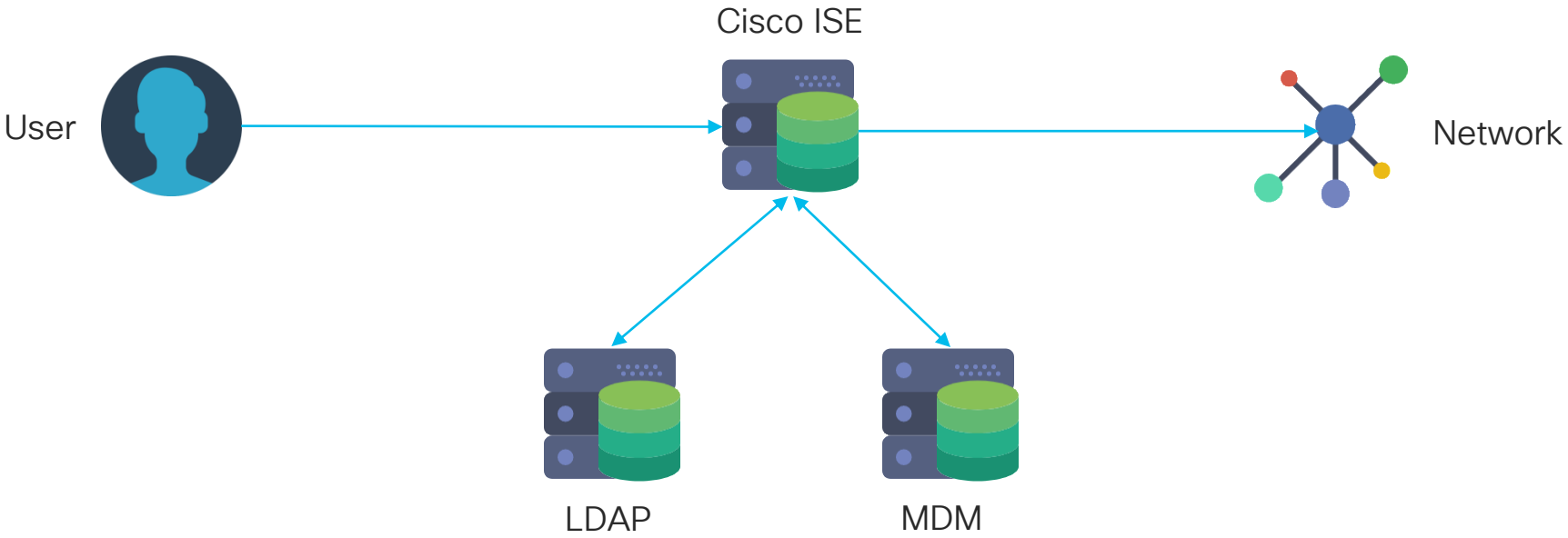
We are future-proofing our IAM system



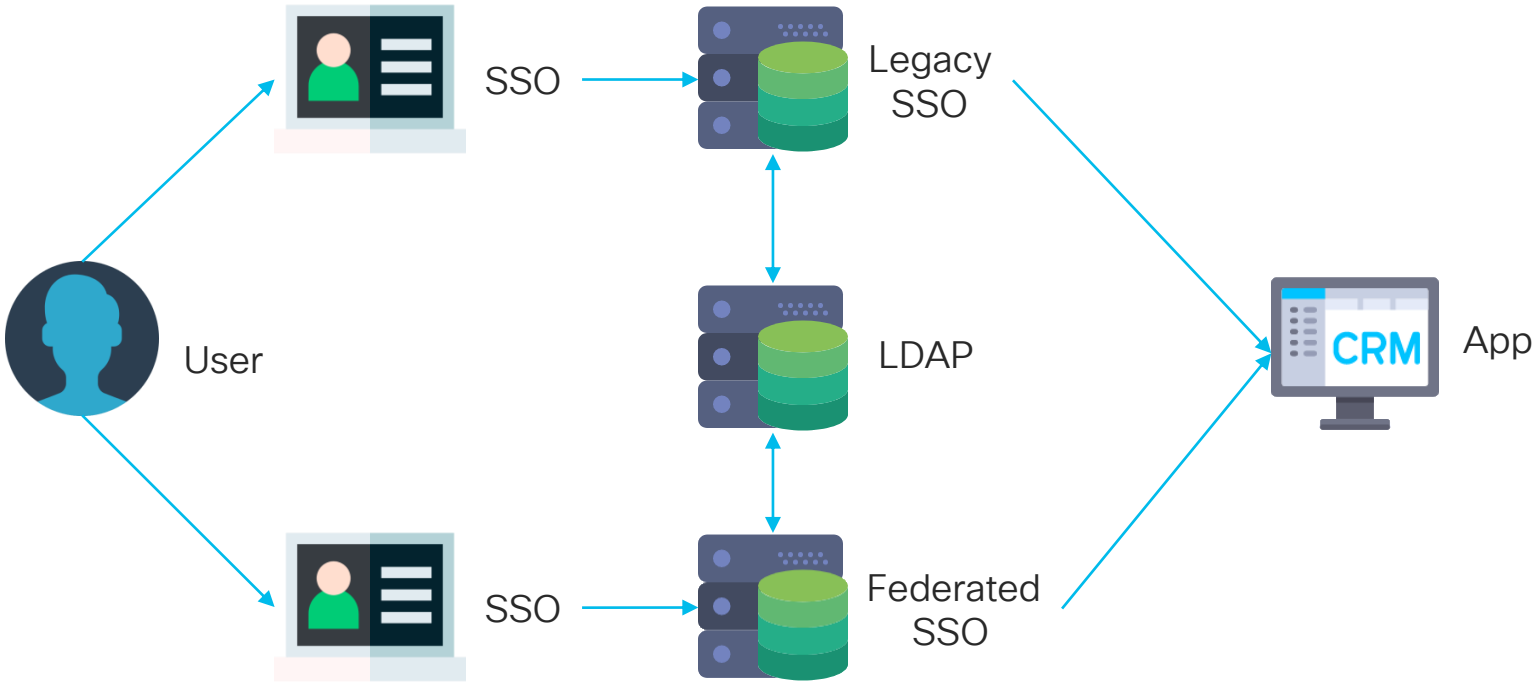
You make **possible**

Backup slides

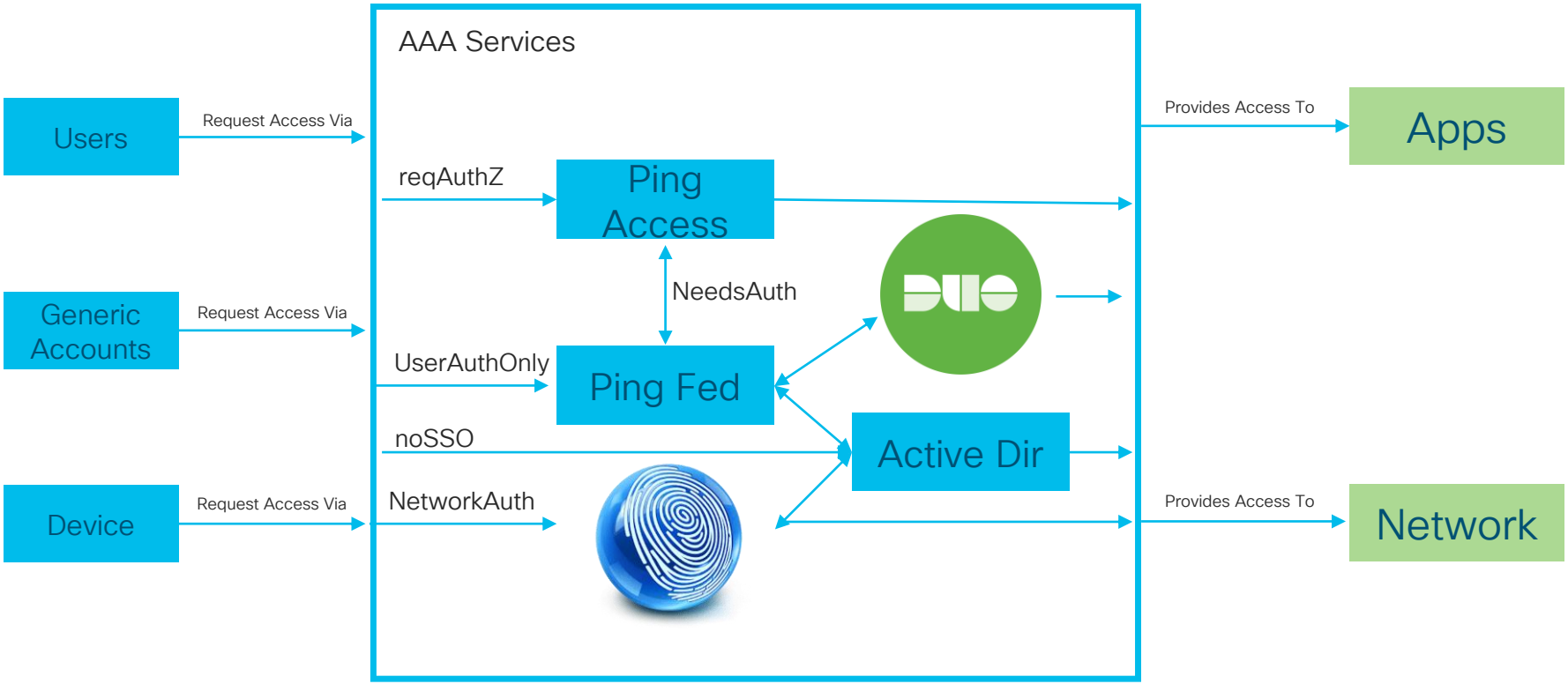
Cisco Network Access



Cisco Application Access



Identity Flow



Challenges → Opportunities

Data

Intelligent Monitoring

UX

Cloud-ready

High availability