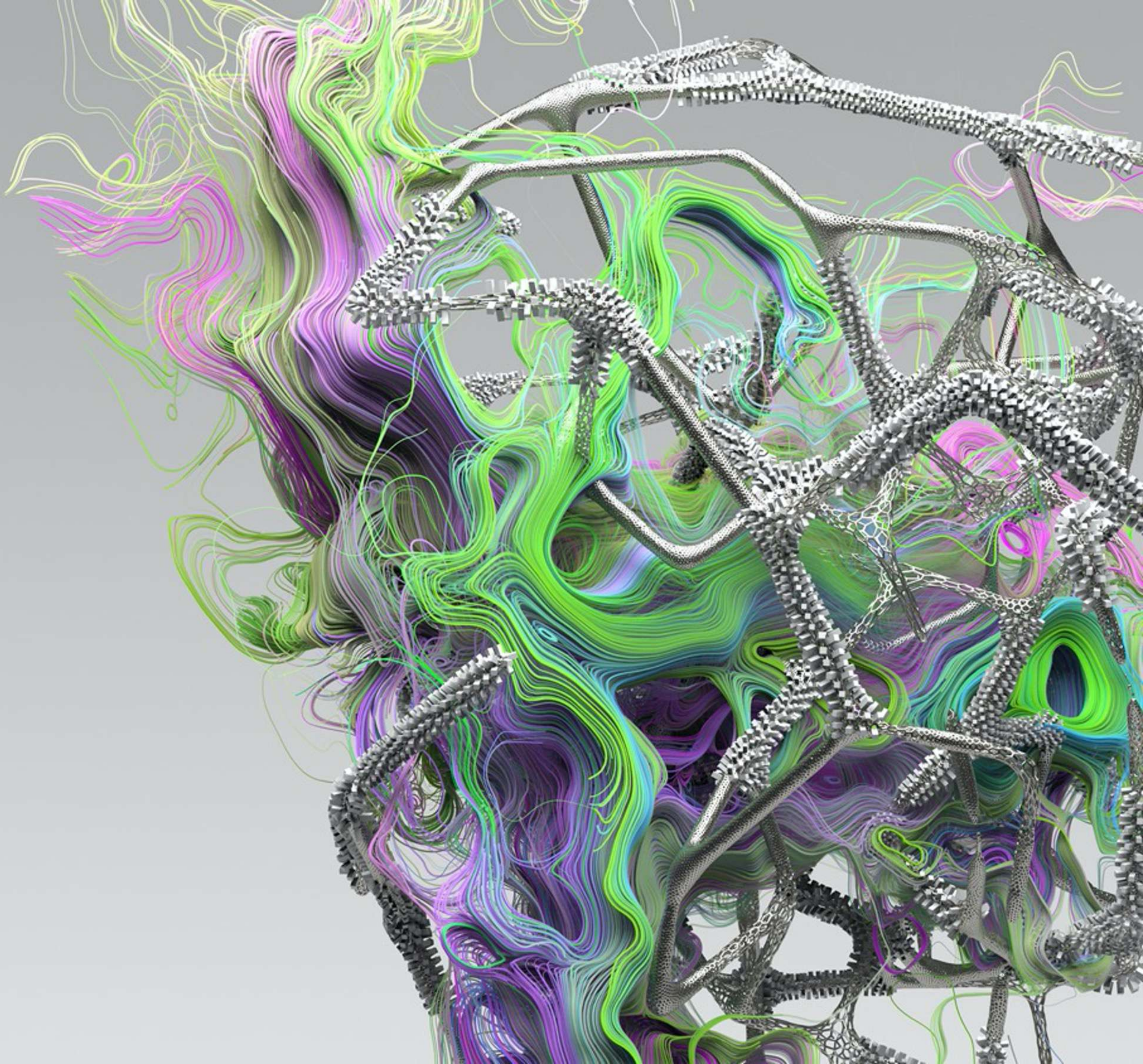




Network Security Future First-time Experience

Takahiro Ishii (UX design intern)

05-21-2020



1.

Introduction

Introduction ●

Competitive Analysis ○

Persona ○

User Journeys ○

Information Architecture ○

Wireframes ○

Mockups ○

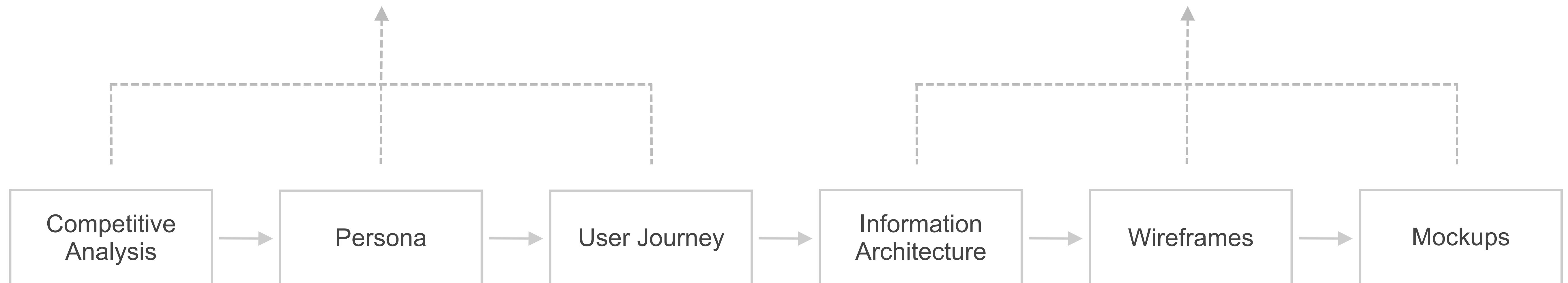
- 1. The first-time users can clearly understand the product features and values quickly**
- 2. The first-time users can easily deploy a Network Security instance and set policies for their environments**



1. We don't know users in cloud network security

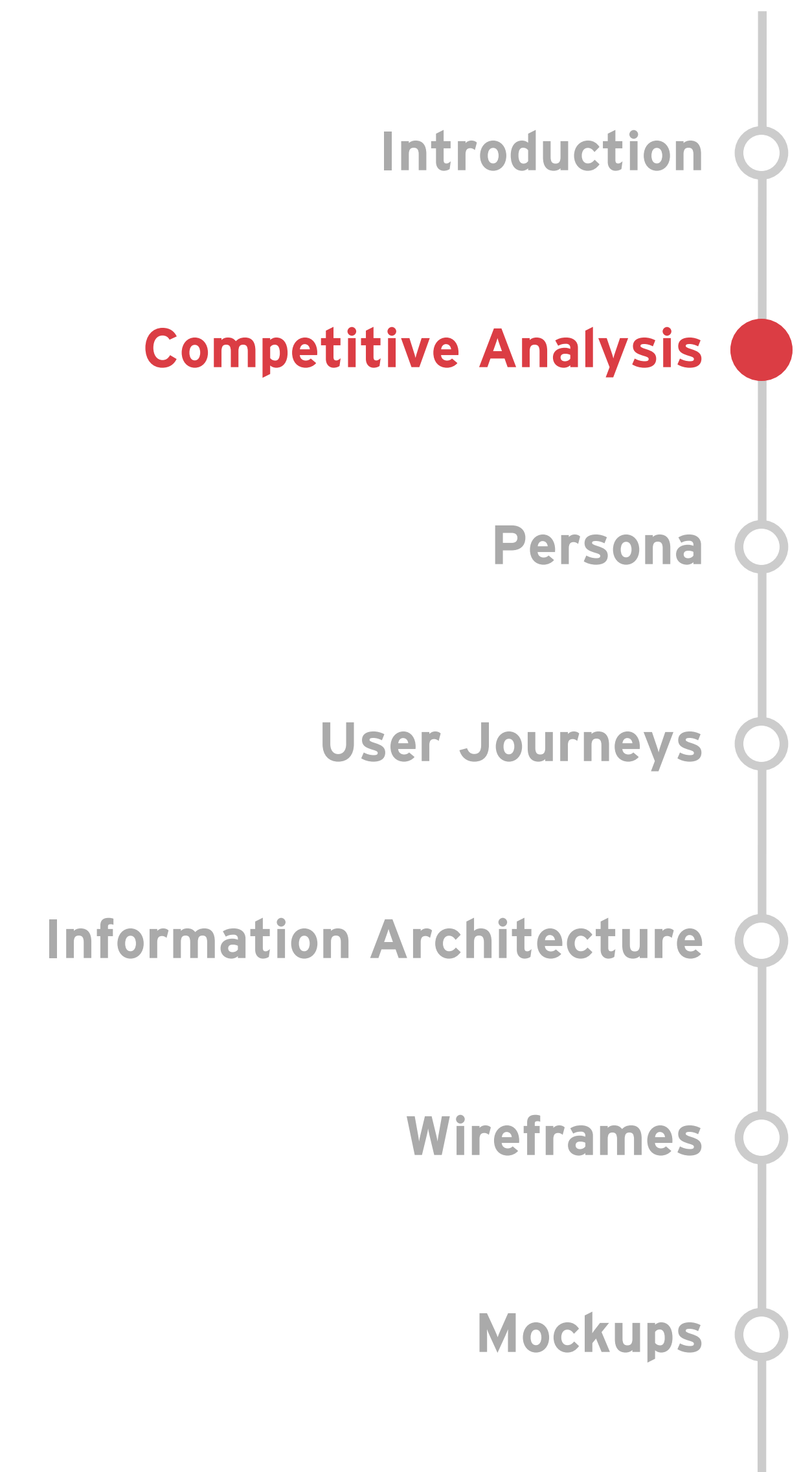


2. The traditional first-time experience is painful



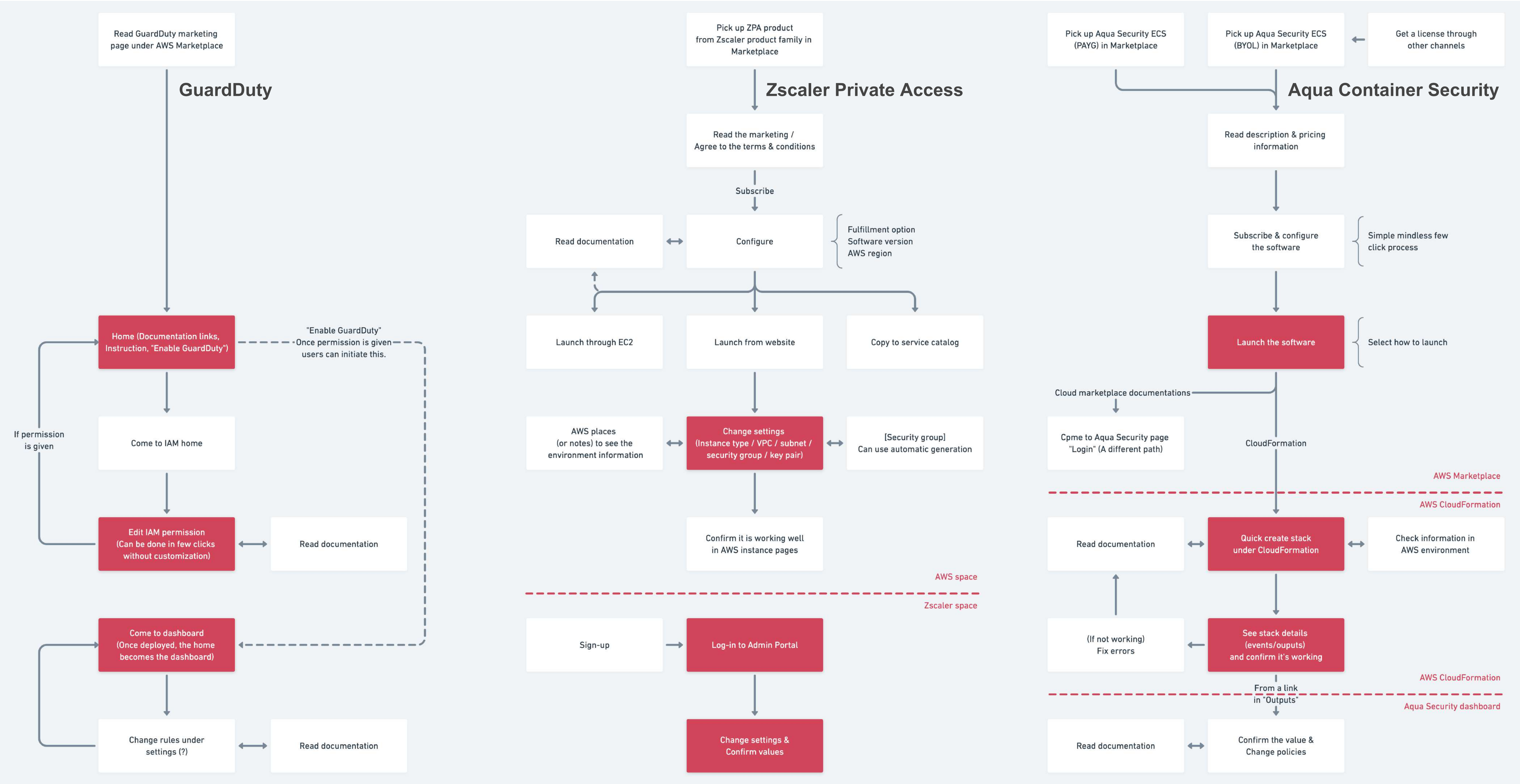
2.

Competitive Analysis

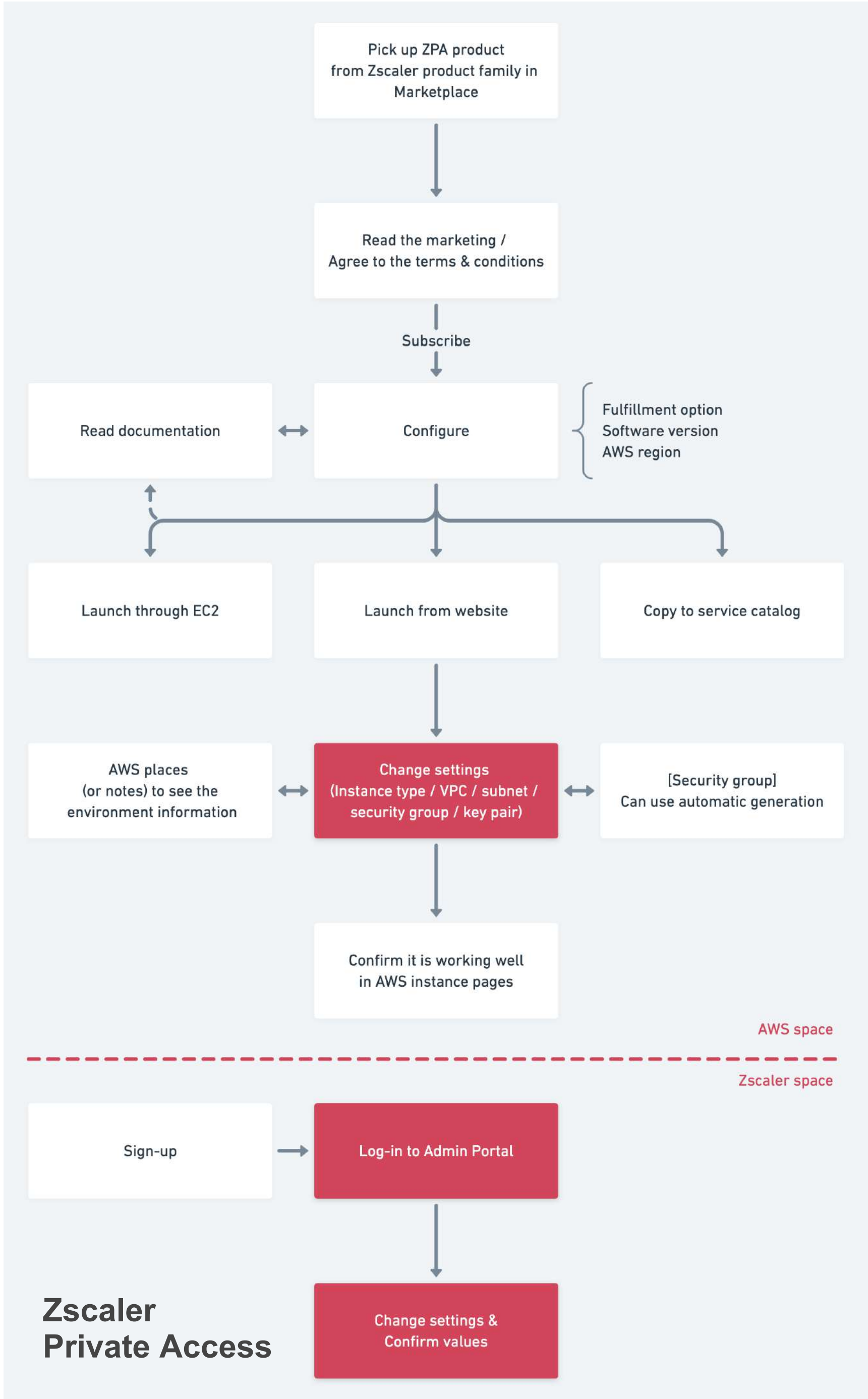


User flow of FTX on three different cloud security products

Competitive Analysis



Zscaler provides both a “Happy Path” and a customization option



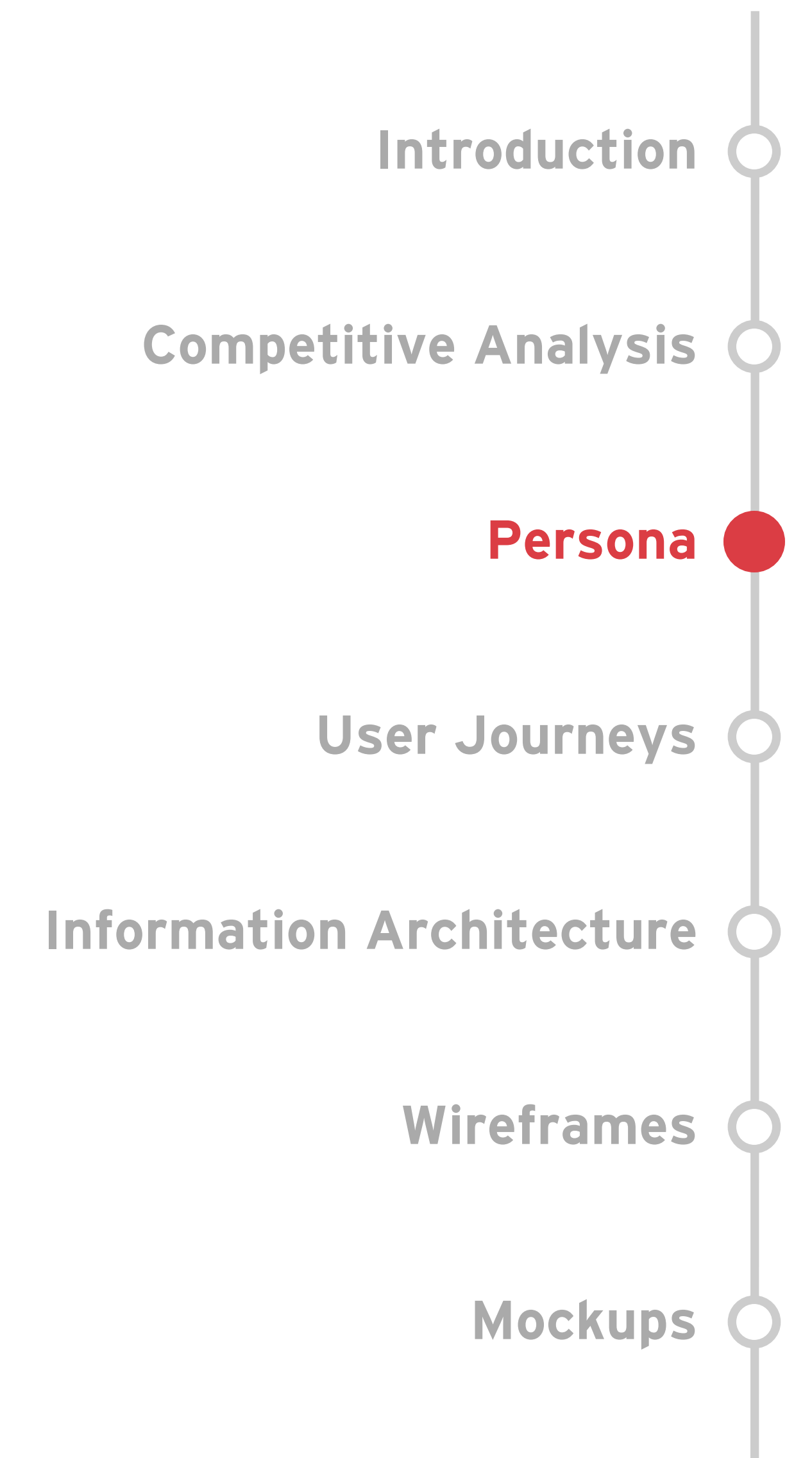
Key Takeaways

Some of the products provide users two options for the initial deployment:

- Happy path (Recommendation):** If users don't want to spend much time, they can use the recommended or default settings. Users can just review and click to proceed.
- Customization option:** If users want to customize deployment or other settings for their environment, they can read documentations, use command line interfaces, and adjust settings to deploy manually.

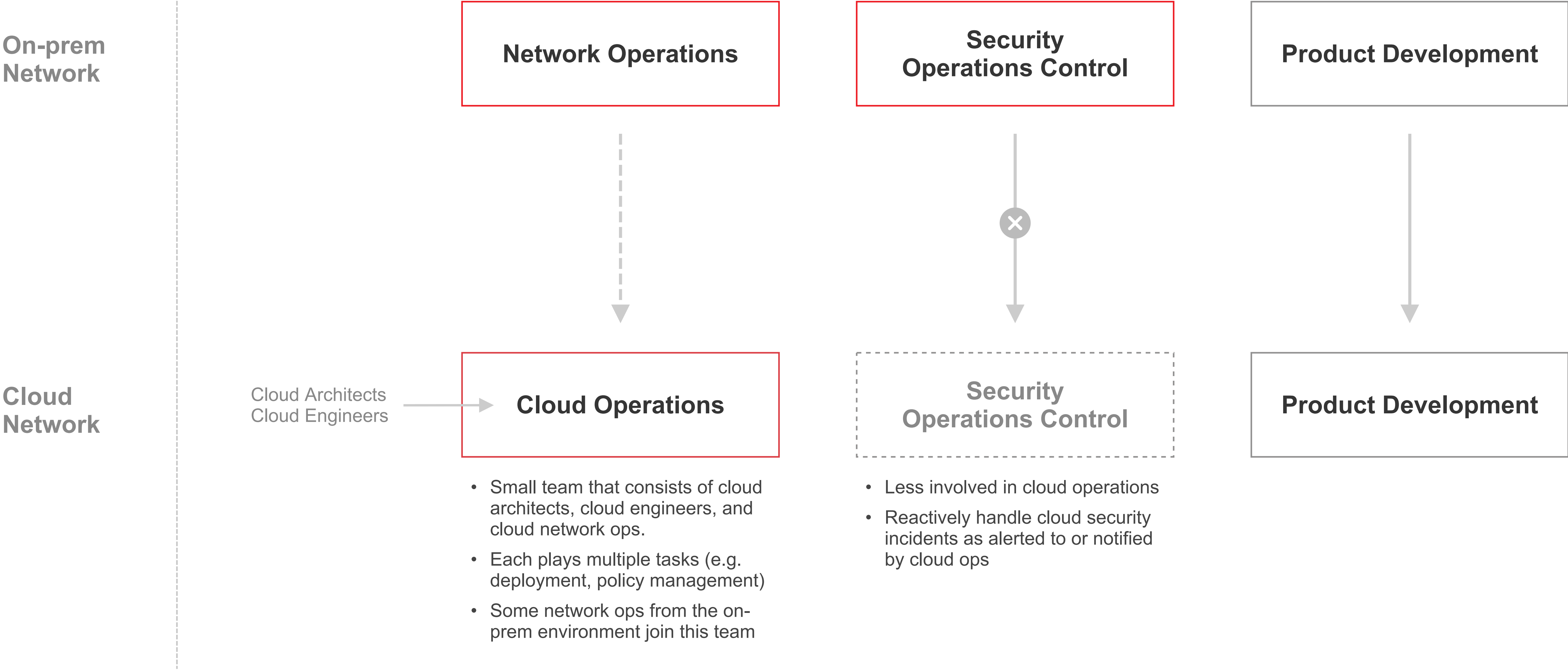
3.

Persona













Cloud One’s target will be a multifunctional cloud ops team

Persona



FTX focuses on cloud ops architects, engineers and especially network ops

Persona

Job role	Cloud Ops Architect	Cloud Ops Engineer	Cloud Network Ops	Security Engineer	Network Ops
Stage	ARCHITECTURE	DEVELOPMENT DAILY MONITORING	DEPLOYMENT INCIDENT HANDLING		ON-PREM
Team	Cloud ops	Cloud ops	Cloud ops <- Network ops	Security operations control	Network ops
Team size	Large	Large	Large	Large	Large
Job tasks	<ul style="list-style-type: none">Design and maintain cloud architectureAssess viability of different cloud servicesManage related billing	<ul style="list-style-type: none">Develop environments by referring to API and automation documentationBuild POCs with vendor support	<ul style="list-style-type: none">Converted to cloud network opsConfigure third-party security productsMonitor networks	<ul style="list-style-type: none">Respond to security incidents as alerted to or notified by cloud opsAssess vulnerabilities in security posture and stay on top of it	<ul style="list-style-type: none">Responsible for on-prem networks, including deployment and policy managementSome converted to cloud network ops
Security experience	 Low	 Low	 High	 High	 High
Cloud ops experience	 Med~High	 Med~High	 Low	 Low	 Low
Painpoints	<ul style="list-style-type: none">Ever-increasing complexityLimited resources (budget, human)	<ul style="list-style-type: none">Limited knowledge in network securityTime it takes for configuration and deployment	<ul style="list-style-type: none">Limited knowledge in cloud operationsStruggles for troubleshooting	<ul style="list-style-type: none">Time and effort it takes to investigate the incident causes	<ul style="list-style-type: none">Extensive SMS trainingTime consuming deployment and policy management



Job role: Cloud network operator

Tenure: Mid-level

Work experience: 5 years

Team: Cloud ops <- Network ops

Team size: Large (XXX+)

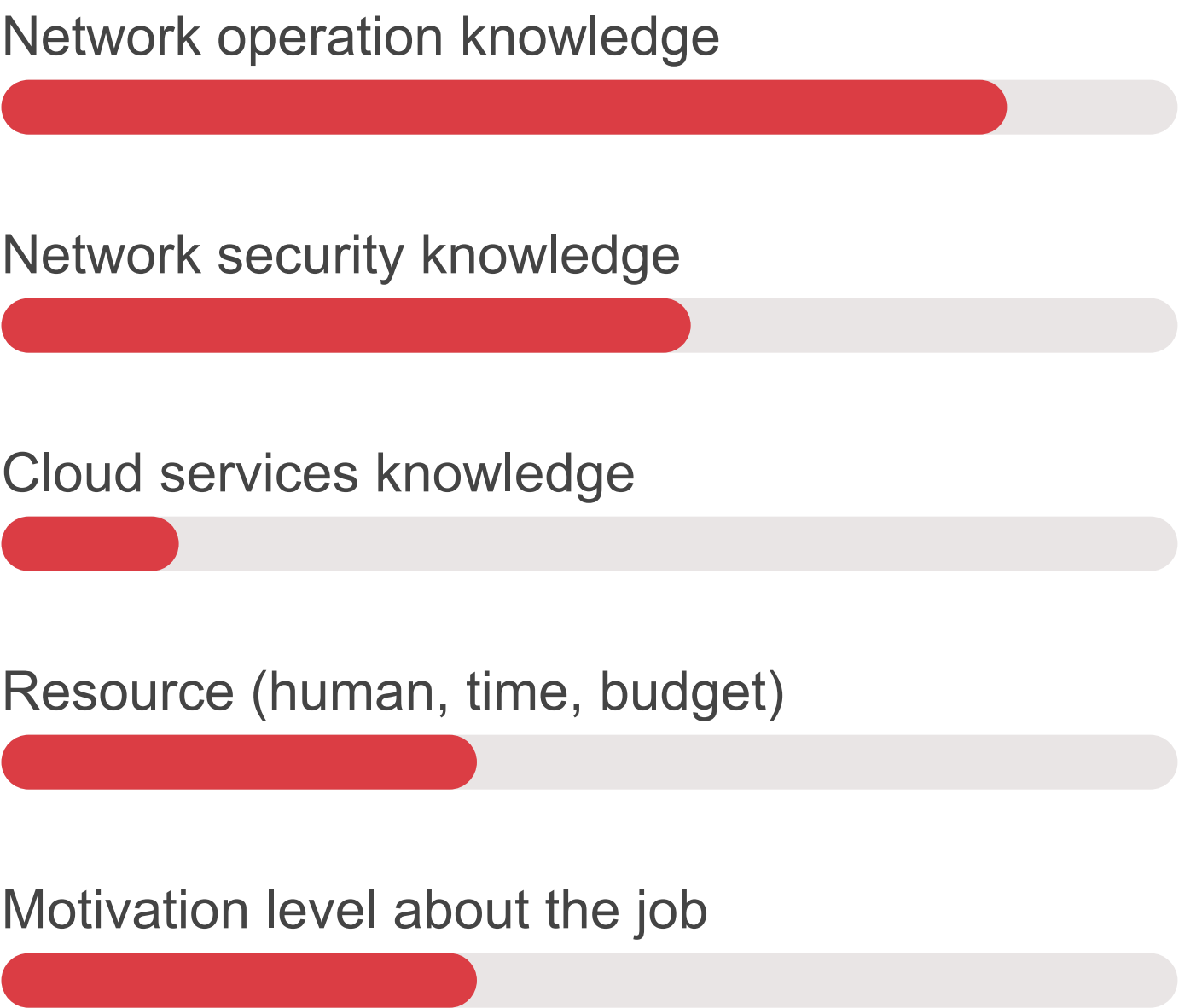
Education level: Bachelor in STEM

Description: Converted to a cloud ops from a traditional network ops. Responsible for monitoring networks and handling issues in the cloud space

Job tasks



Proficiency / Resources



User goals

- Quickly learn cloud operations
- Easily figure out what is wrong in the cloud for incident handling
- Easily set policies
- Learn about which products work best to protect networks

Pain points

- Unfamiliar with cloud operations
- Takes time to check every filter for incident handling
- Don't know what network security software is available in the cloud space
- Not easy to keep the software stay updated



Job role: Cloud-Ops engineer

Tenure: Mid-level

Work experience: 5 years

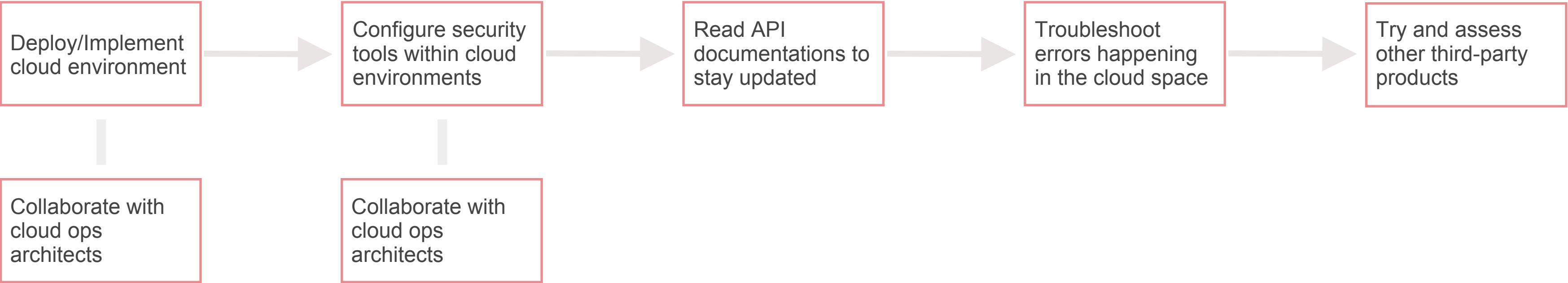
Team: Cloud Ops

Team size: Large

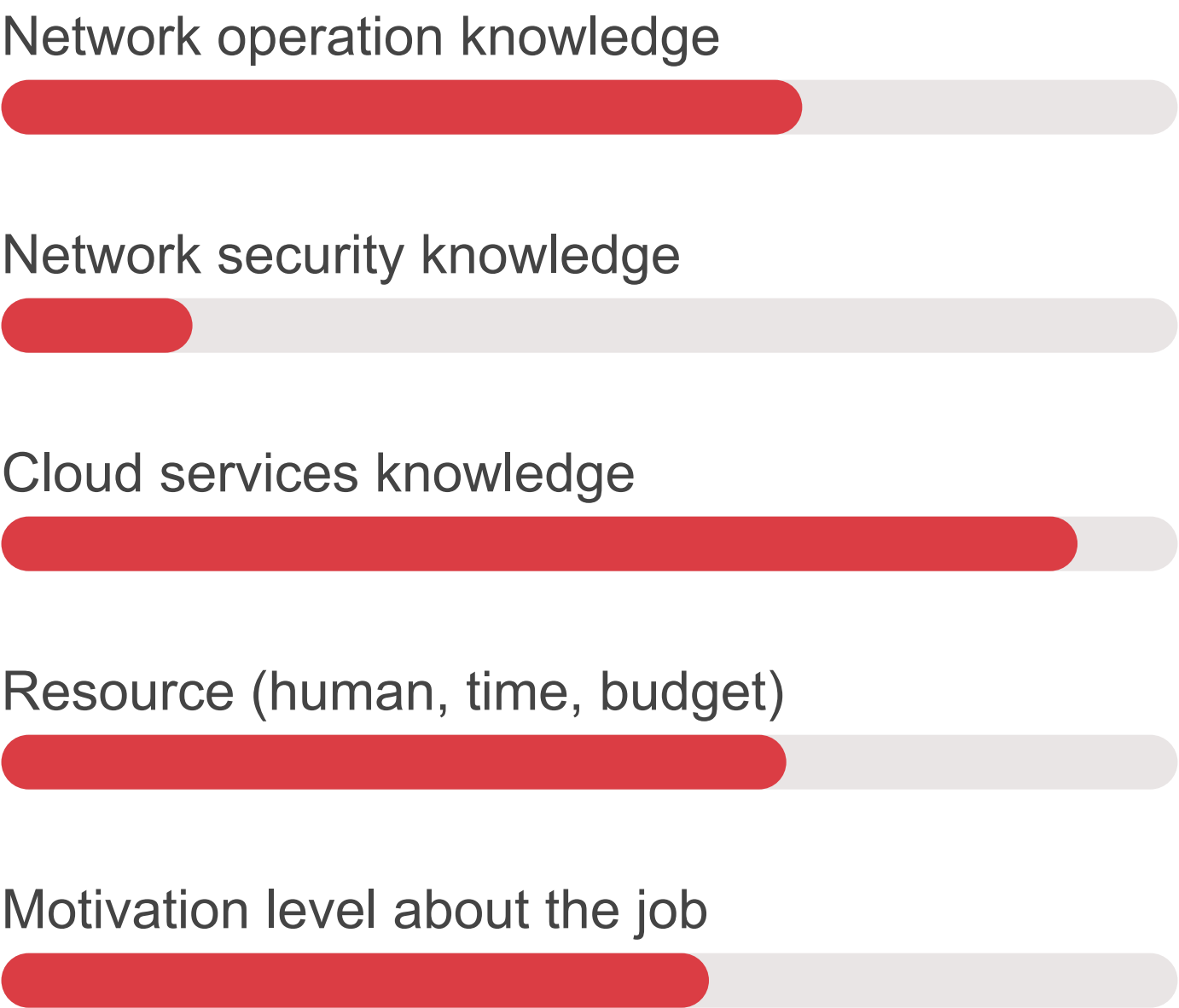
Education level: Master’s in STEM

Description: Responsible for implementing the cloud environments, and configuring third-party software.

Job tasks



Proficiency / Resource



User goals

- Want a simplified security deployment experience for our complex AWS environment
- Learn network security with less effort and time
- Confirm that Network Security works well to protect our environments
- Easily troubleshoot and fix issues

Pain points

- Unfamiliar with cloud network security
- It takes time to fix issues. Also difficult to find related information (documentation, forum, etc)
- Our AWS environment is so complex that it’s hard to configure it for Network Security deployment
- Not easy to test if the deployment has gone well



Job role: Cloud-Ops architect

Tenure: Mid-level

Work experience: 5 years

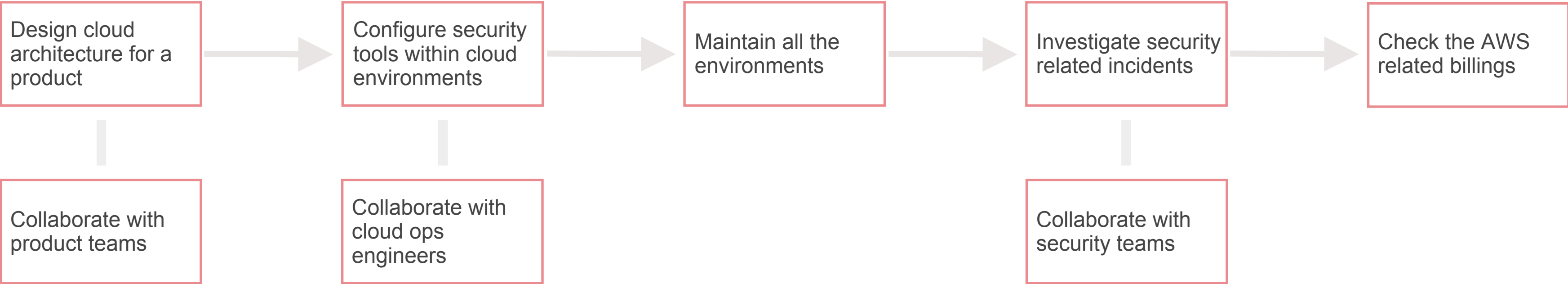
Team: Cloud Ops

Team size: Large

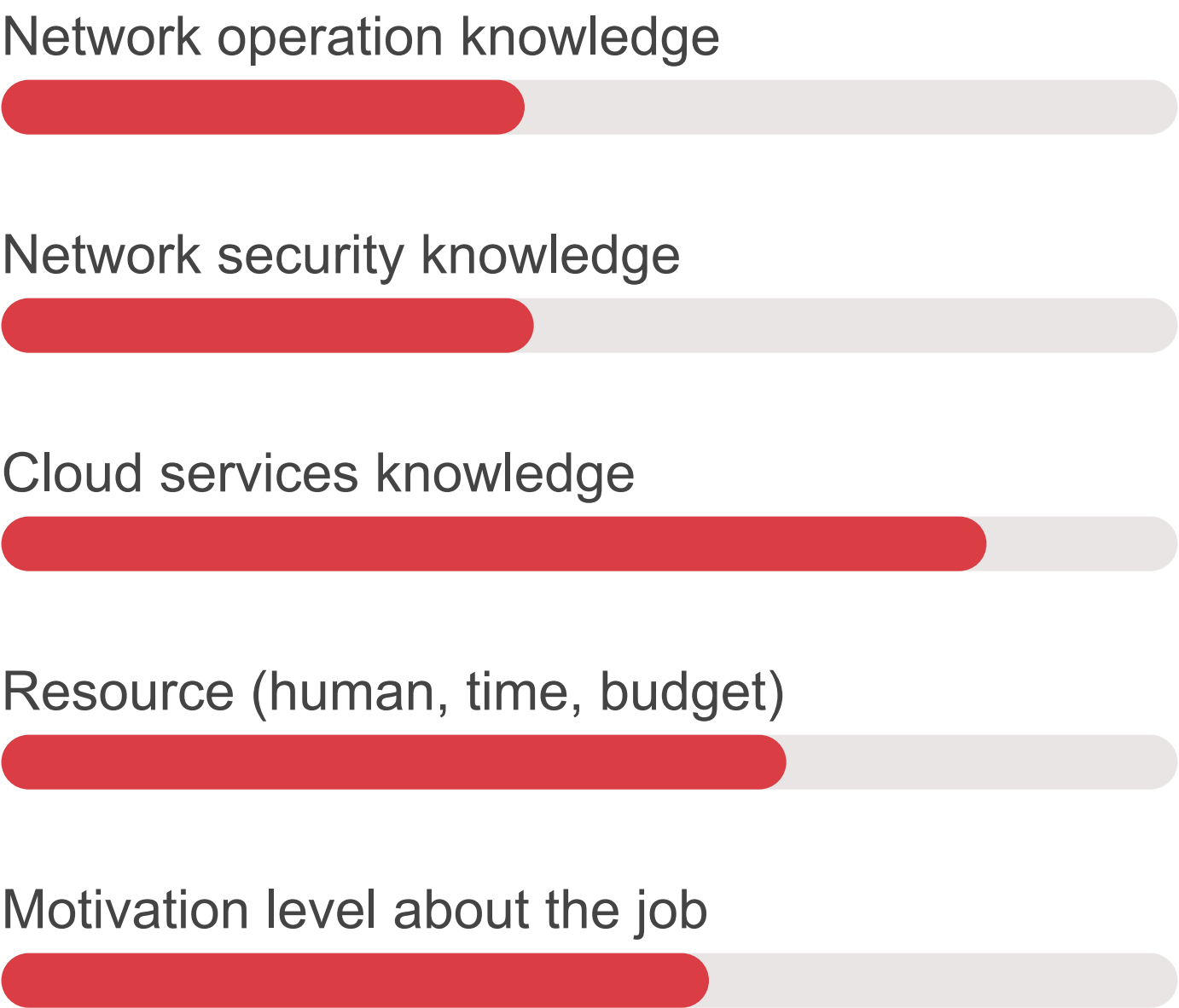
Education level: Master’s in STEM

Description: Responsible for designing the cloud architecture, and the entire environment, including maintenance and billing.

Job tasks



Proficiency / Resource



User goals

- Want a simplified security deployment experience for our complex AWS environment
- Learn network security with less effort and time
- Want a consolidated platforms, products, and services
- See the integrated billing

Pain points

- Unfamiliar with cloud network security
- Struggle to see the value of different cloud network security product due to the limited domain knowledge
- Not easy to meet SOC’s security requirement
- The architecture can easily get very complex

4.

User Journeys

Introduction ○

Competitive Analysis ○

Persona ○

User Journeys ●

Information Architecture ○

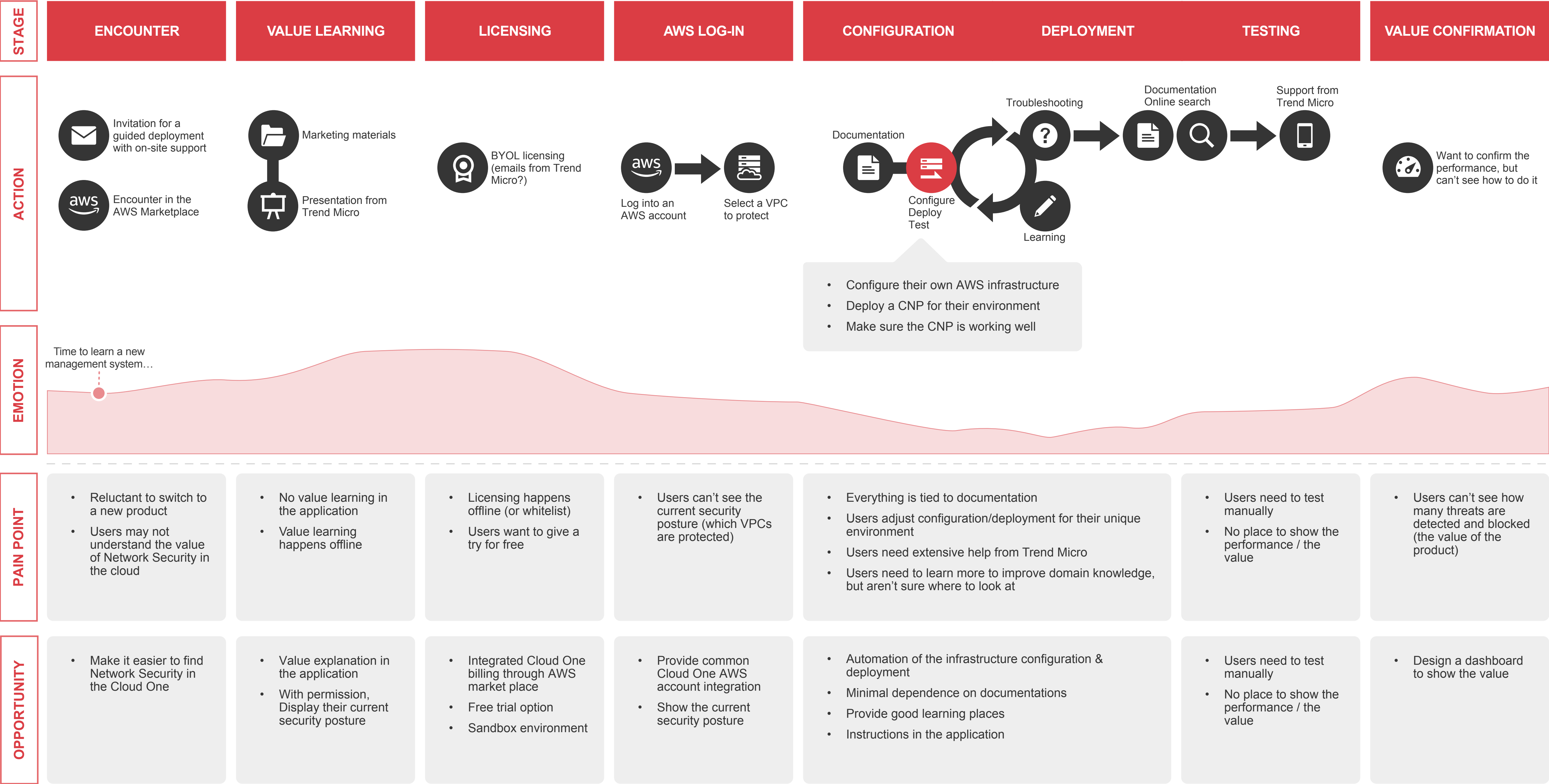
Wireframes ○

Mockups ○

Current first-time experience

From encounter to value confirmation

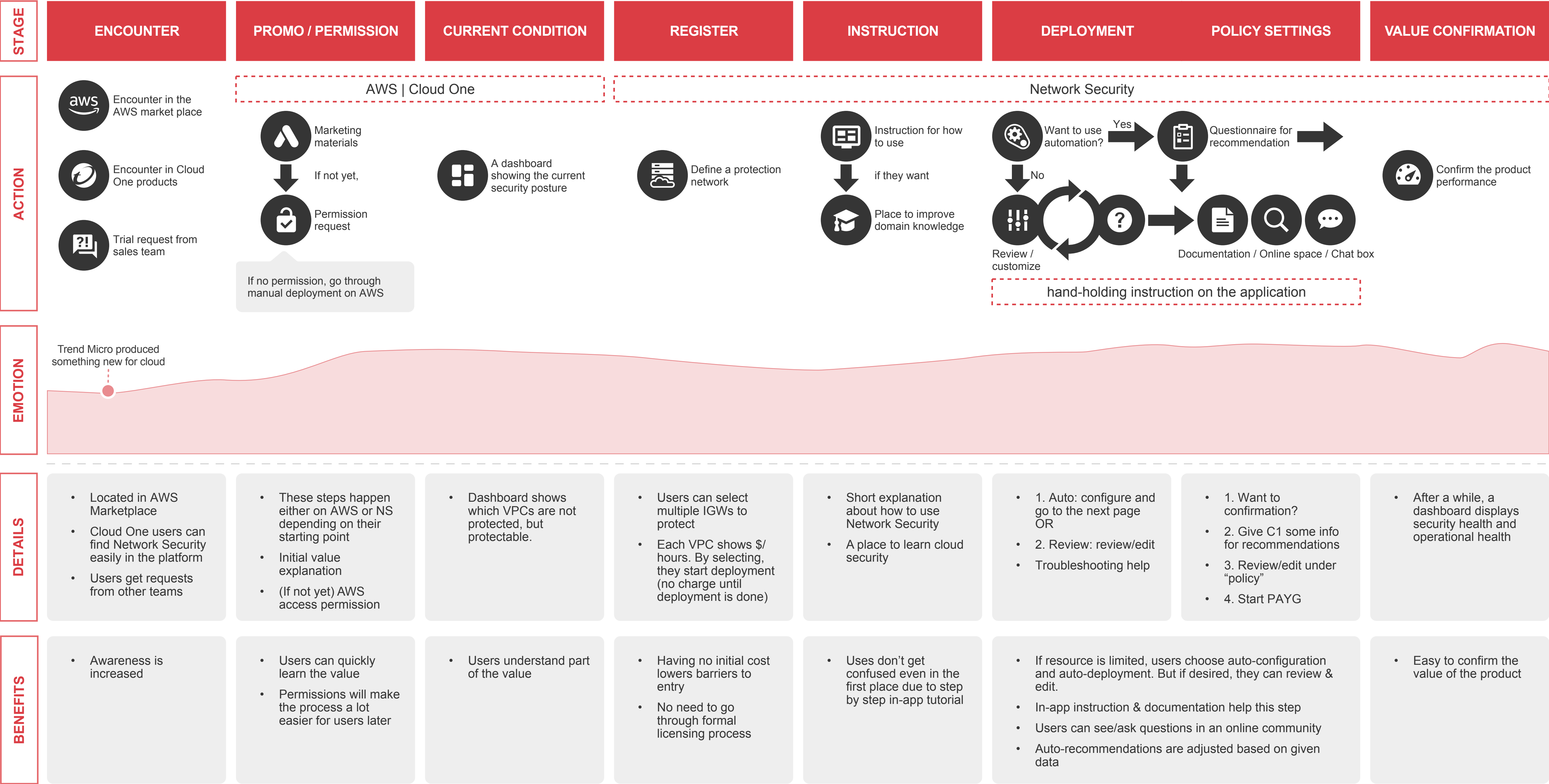
User Journeys



Future first-time experience

From encounter to value confirmation

User Journeys



Current user journey

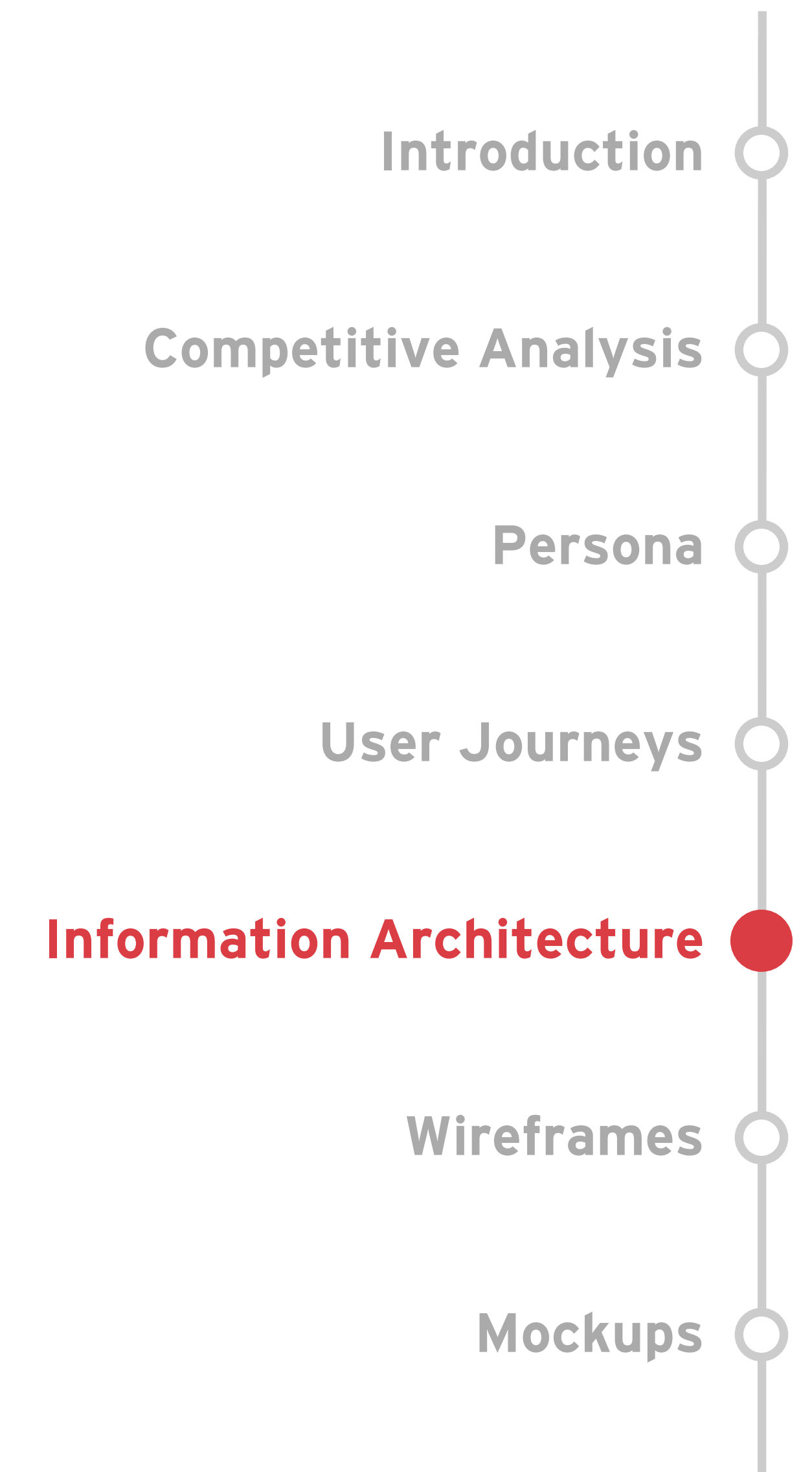
1. **Manual deployment:** Users need to understand the steps and fill out input fields on AWS by themselves.
2. **Heavily tied to documentation:** Users need to read the documentation carefully on every step. If they receive an error, they read it once more to manually fix it.
3. **Many switches between different places:** Users need to switch among documentations, different places on AWS, and Network Security to complete the first-time experience.
4. **No value confirmation:** It's not easy to see if Network Security is working as expected. Also, users struggle to see how well their environment is protected.

Future user journey

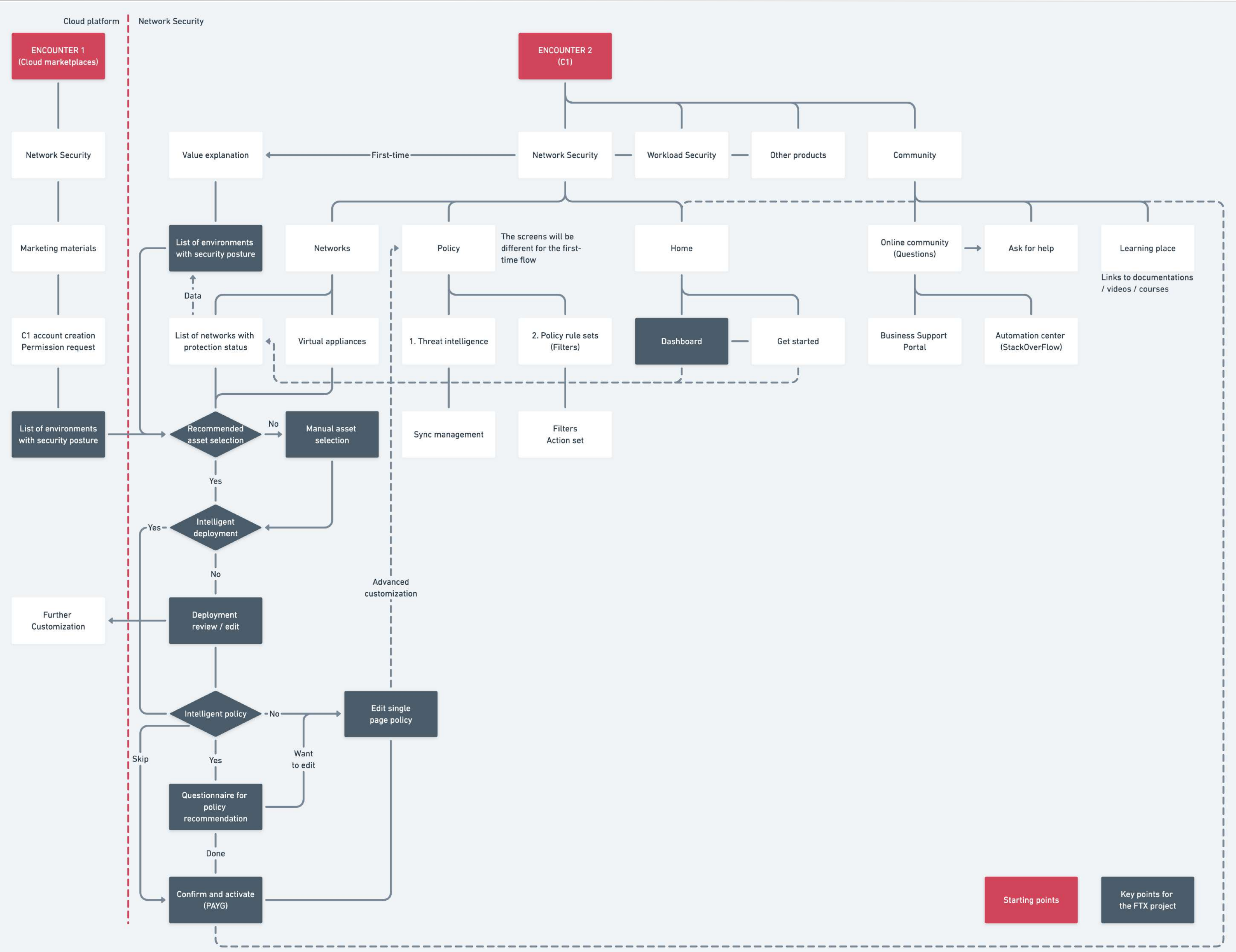
1. **Default / Recommendation:** Users can use default settings to deploy an NS instance and set policies. If so, they just need to review and click.
2. **Customization:** Users still can customize deployment and policy settings. But the UI and the instruction will minimize the dependence on documentation.
3. **Actions on Network Security:** Most of the actions can be completed on Network Security.
4. **Dashboard:** It shows the performance, operational health, and security health of their environment.

5.

Information Architecture



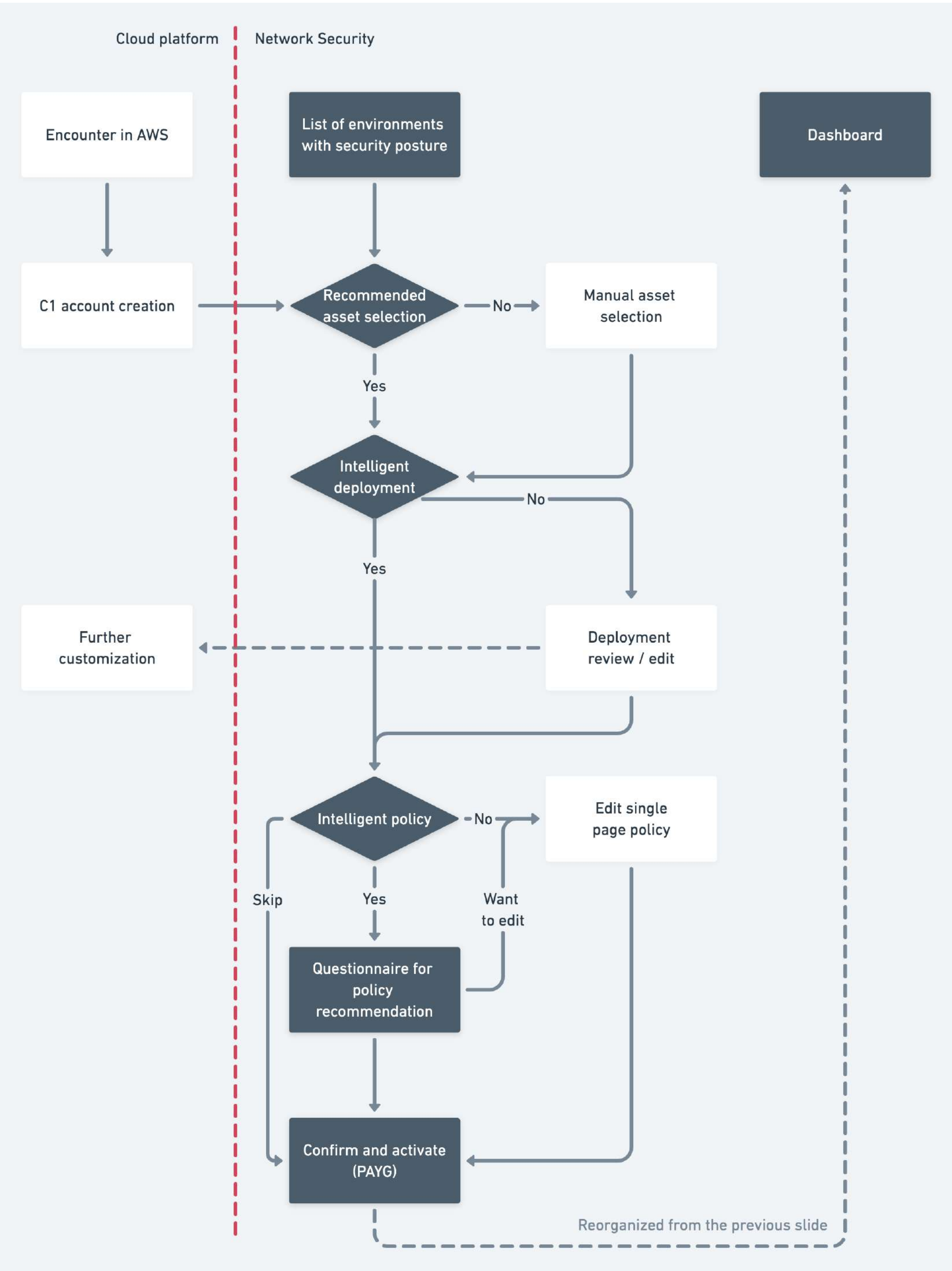
New Site Map for Network Security



Key points

- Two entry points:** Users can initiate the first-time experience either from AWS Marketplace or Cloud One
- No jump:** Unlike the current experience, users don't need to jump among different pages.

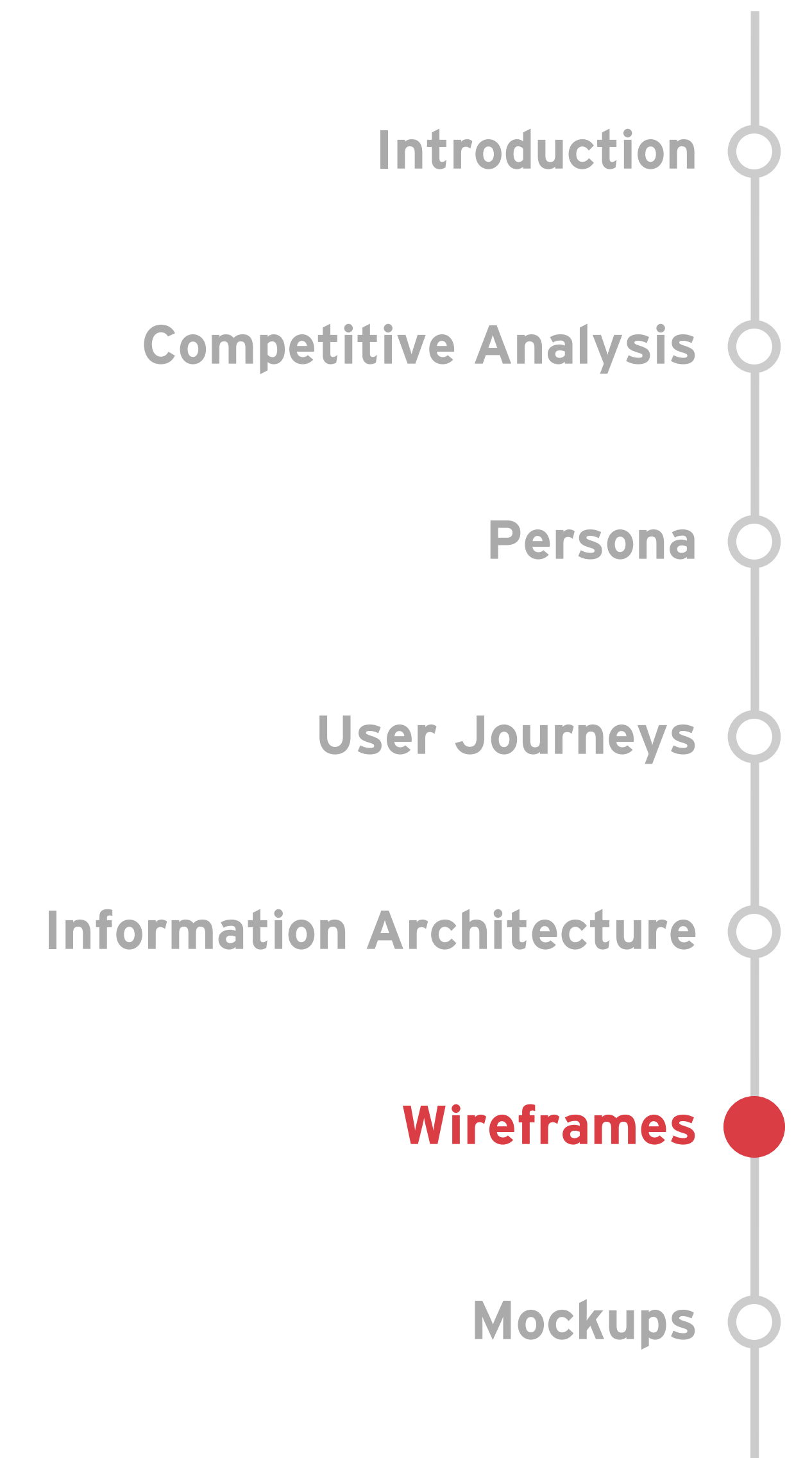
This sitemap is a living document, and will always evolve. So, please use this just as a reference. (05/10/2020)



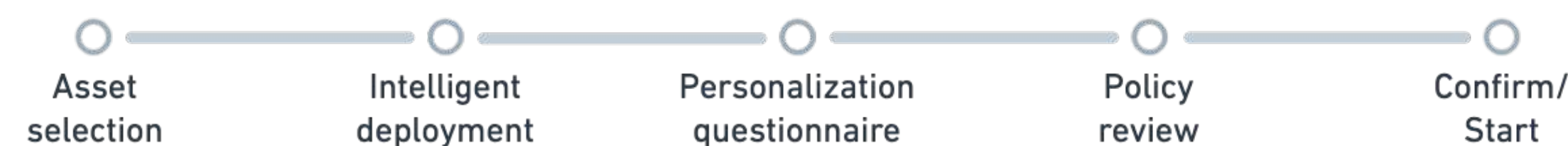
Key points

- Recommendation:** If users want to spend much time, they can use the recommended settings. The recommendation process is streamlined. (Filled boxes)
- Customization:** This user flow still allows users to customize for their environment. Most of the customization can be done in the GUI of Network Security.
- Dashboard:** At the end of the flow, users can confirm the value of Network Security through a dashboard.

6. Wireframes



5 steps to complete the first-time experience



1. **Asset selection:** select multiple assets users want to protect
2. **Intelligent deployment:** select a deployment model or manually customize it
3. **Personalization questionnaire:** fill out a questionnaire to use a better policy settings recommendation
4. **Policy review:** Review and edit the policy
5. **Confirm / Start:** Review the summary and start

Test settings (3 participants)

I gave participants two scenarios of the first-time experience. This sessions are conducted to find design issues.

1. **Default / Recommendation:** Your resource is limited, so you would like to deploy an NS instance and set policies as quickly as possible.
2. **Customization:** You need to follow the cloud security rules of your company. So, you need to customize deployment and policy settings.
(Details provided in the testings)

Default / Recommendation

Customization

Wireframes

TREND
MICRO

Cloud One

Network Security

Help

Lab User 1

Asset selection

Intelligent deployment

Personalization questionnaire

Policy review

Confirm/Start

Recommended asset selection

Total assets selected: 472

VPC

Assets selected: 148

Lab user 1: 91

Lab user 2: 35

Lab test user: 34

Shared public user: 32

Temp test account: 20

Implementation lab: 17

Lab user 3: 15

Test intern account: 12

Acme-checking: 11

Temp test: 7

Load more

Internet Gateway

Assets selected: 103

Subnet

Assets selected: 71

Transit Gateway

Assets selected: 57

NAT Gateways

Assets selected: 32

Back

Proceed

Next step

Asset Selection

TREND
MICRO

Cloud One

Network Security

Help

Lab User 1

Asset selection

Intelligent deployment

Personalization questionnaire

Policy review

Confirm/Start

You can customize the asset selection: 472 assets selected

Cancel

Completed

All assets shown

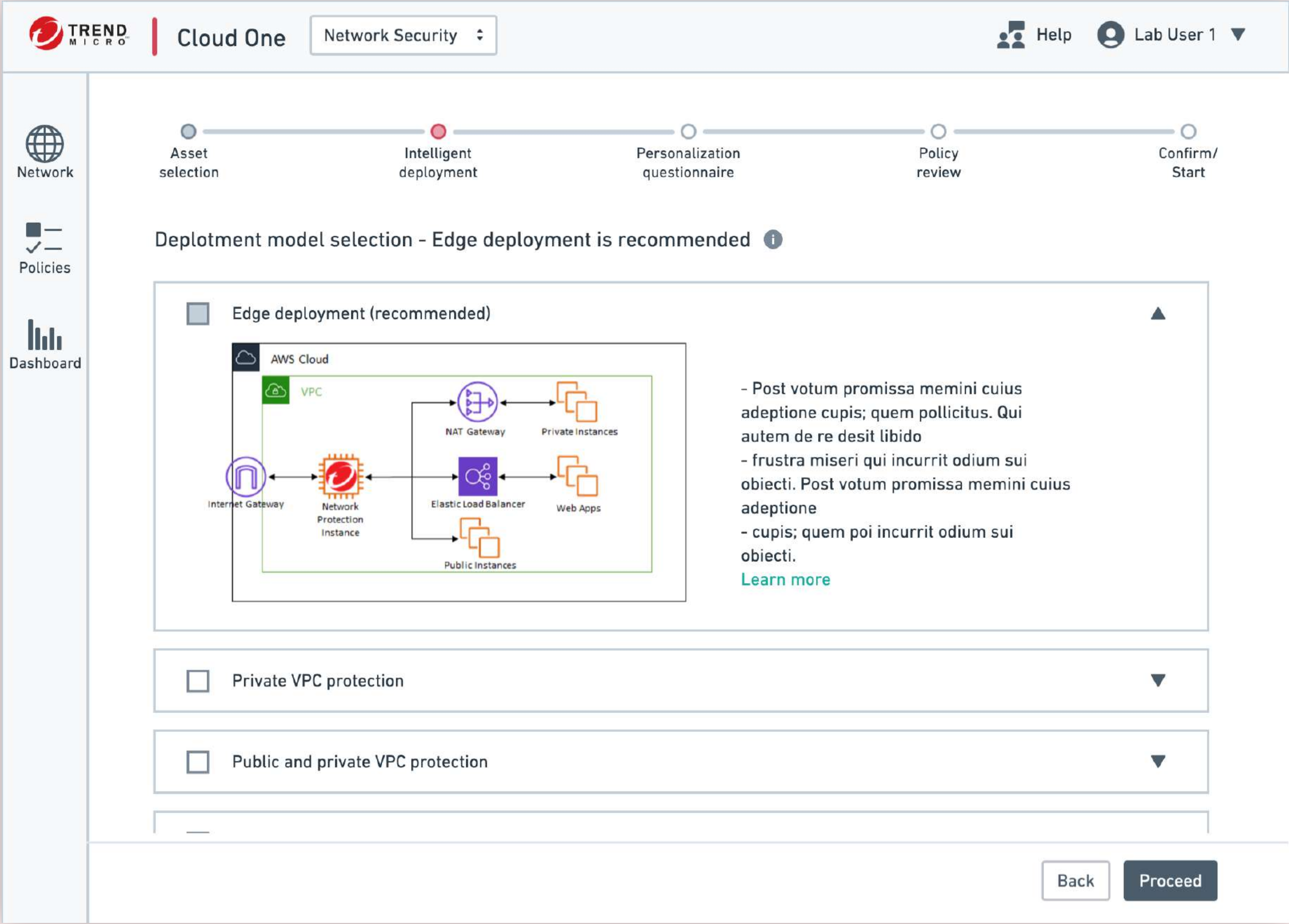
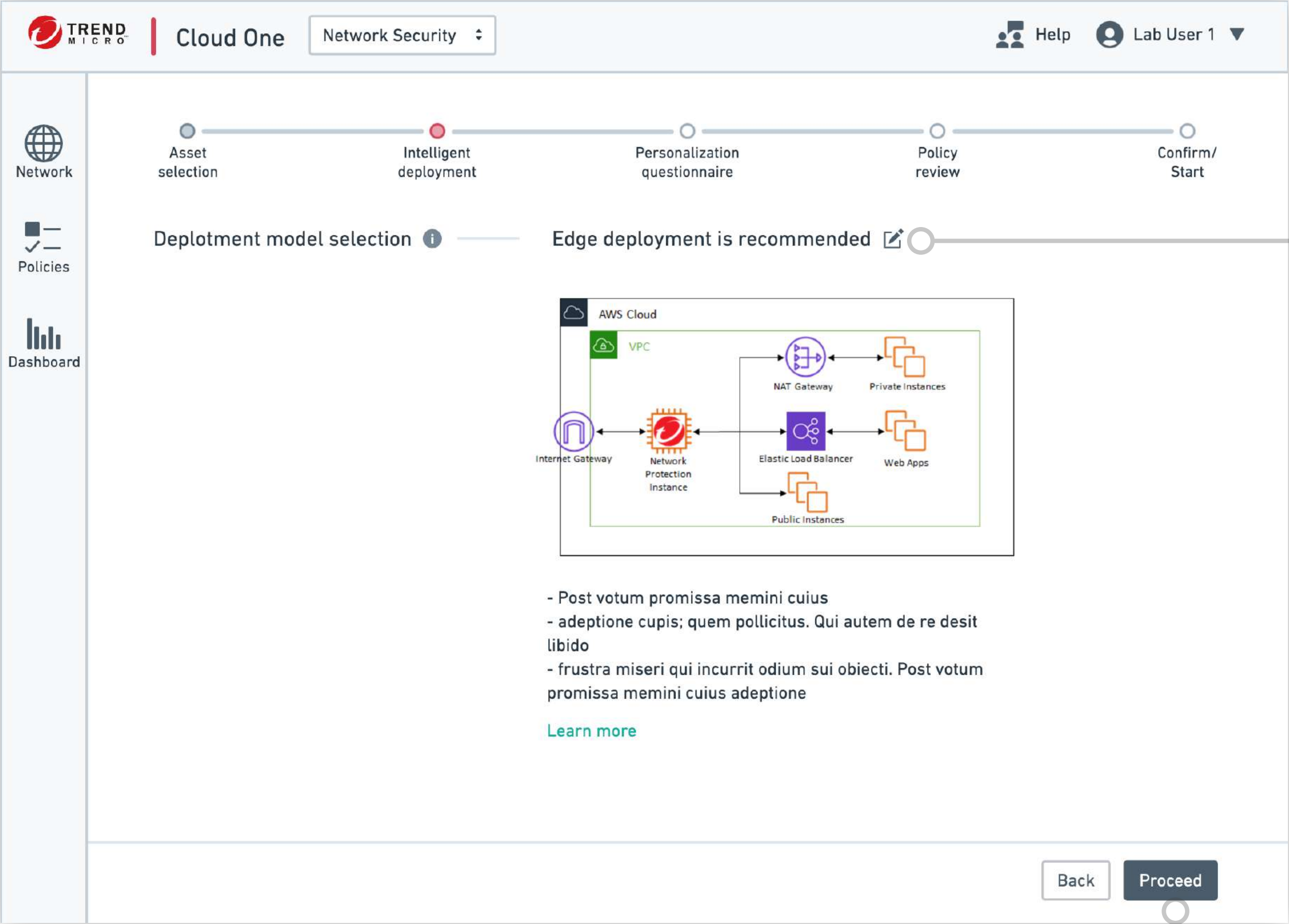
VPC: 148 unprotected assets selected

	Account name	Asset name	ID	Region
	Lab user 1	vpc-acme-public-1	012ab3cd456de-vpc	West (N. California)
	Lab user 1	vpc-acme-public-2	vpc-31014t89sLi180	West (Oregon)
	Lab user 1	test-vpc-intern	vpc-12qwe34rt56zq	East (Ohio)
	Lab user 1	vpc-pricate-connect	vpc-q13049-wfaplzc	West (Oregon)
	Lab user 1	[N/A]	vpc-98zy76xv5w4ut	West (N. California)
	Lab user 1	public-implementation	012ab3cd456de-vpc	West (N. California)
	Lab user 1	[N/A]	vpc-31014t89sLi180	West (Oregon)
	Lab user 1	vpc-acme-public	vpc-12qwe34rt56zq	East (Ohio)
	Shared public user	vpc-private-mgmt	vpc-q13049-wfaplzc	West (Oregon)
	Shared public user	mgmt-acme-trend	vpc-98zy76xv5w4ut	West (N. California)

Load more

Internet Gateway : 103 unprotected assets are selected

Subnet : 71 unprotected assets are selected



Next step

Intelligent Deployment

TREND
MICRO

Cloud One

Network Security

Help

Lab User 1

Network

Policies

Dashboard

Asset selection

Intelligent deployment

Personalization questionnaire

Policy review

Confirm/Start

Questionnaire for personalized policy recommendations (optional)

Skip

1. Which industry is your business in?

2. What is the primary purpose of using AWS?

3. What kind of sensitive data does this AWS environment handle? - Multiple

☐ Personal data (e.g. name, birthday, gender)

☐ Identification data (e.g. passport, social security number)

☐ Financial data (e.g. credit card number, PayPal accounts)

☐ Social media data (e.g. Facebook account information)

☐ Medical data (e.g. medicine history, physical data)

☐ Conversational data (e.g. messages on the chat)

☐ Shopping history (e.g. online shopping data)

☐ Others:

4. How much inbound and outbound traffice does this AWS environment have?

Inbound:

gb / second

Outbound:

gb / second

5. Does this AWS environment need to block certain countries or regions?

Back

Proceed

Next step

Integrated into policy settings.

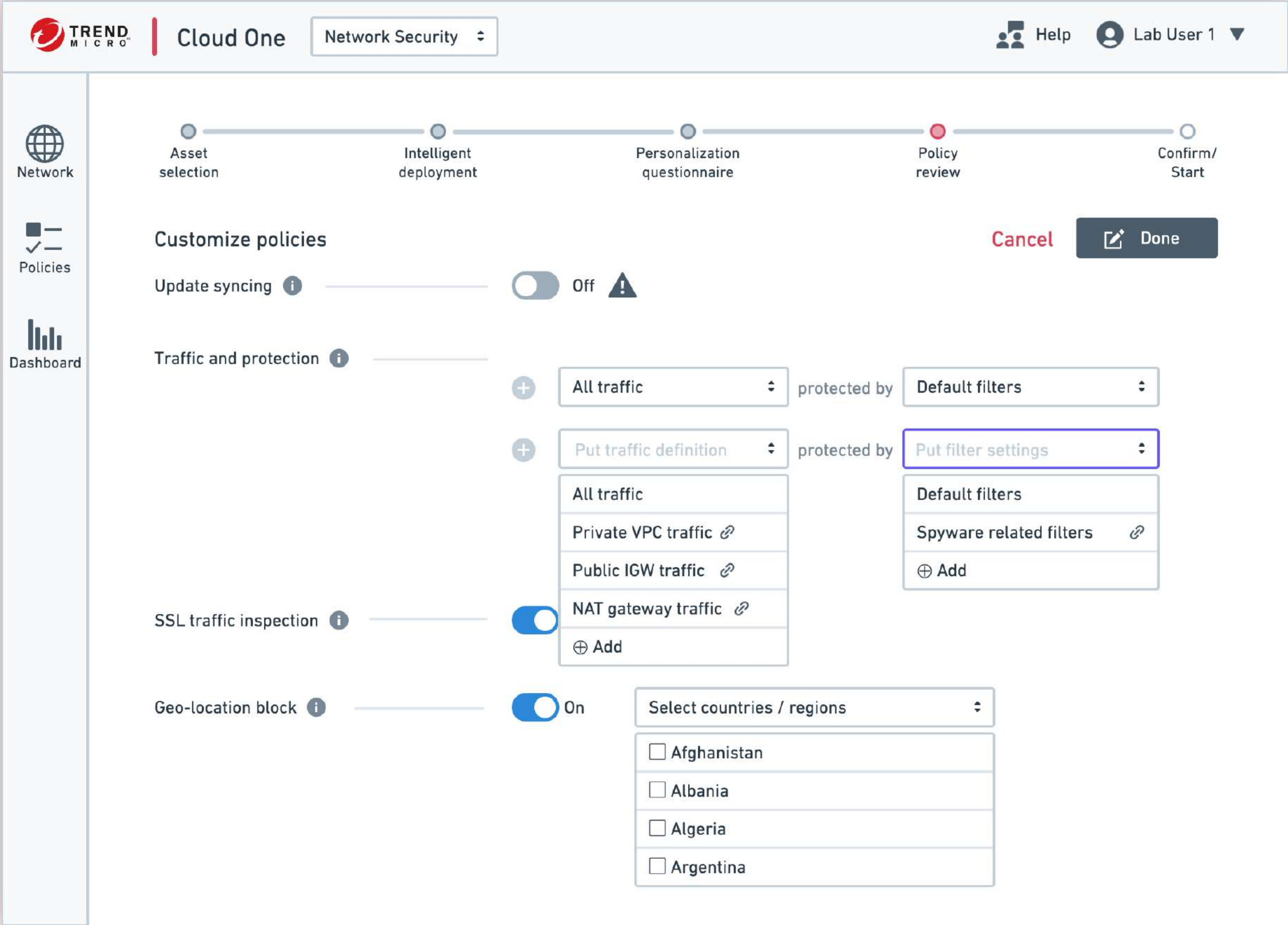
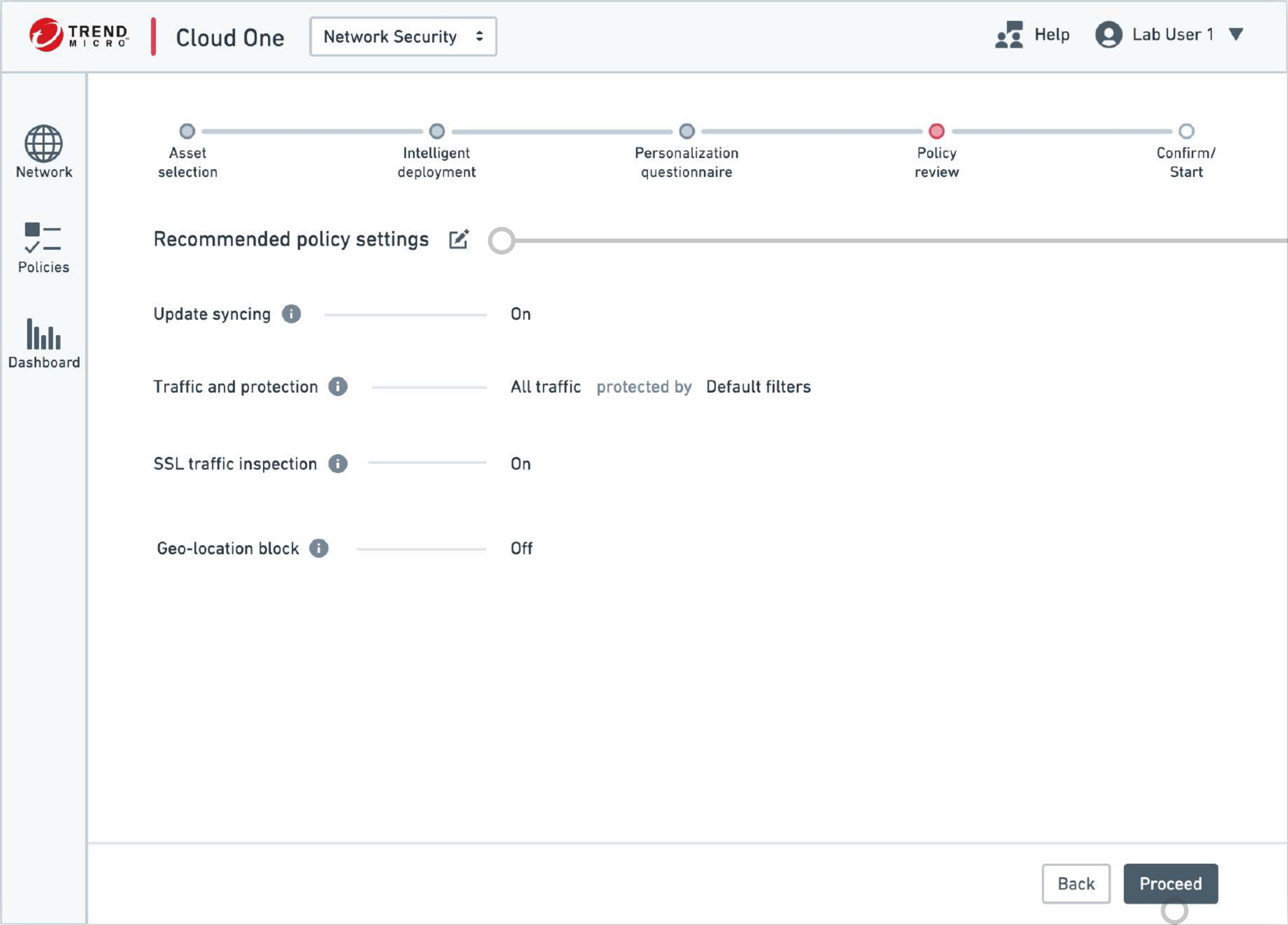
Next step

Questionnaire

Default / Recommendation

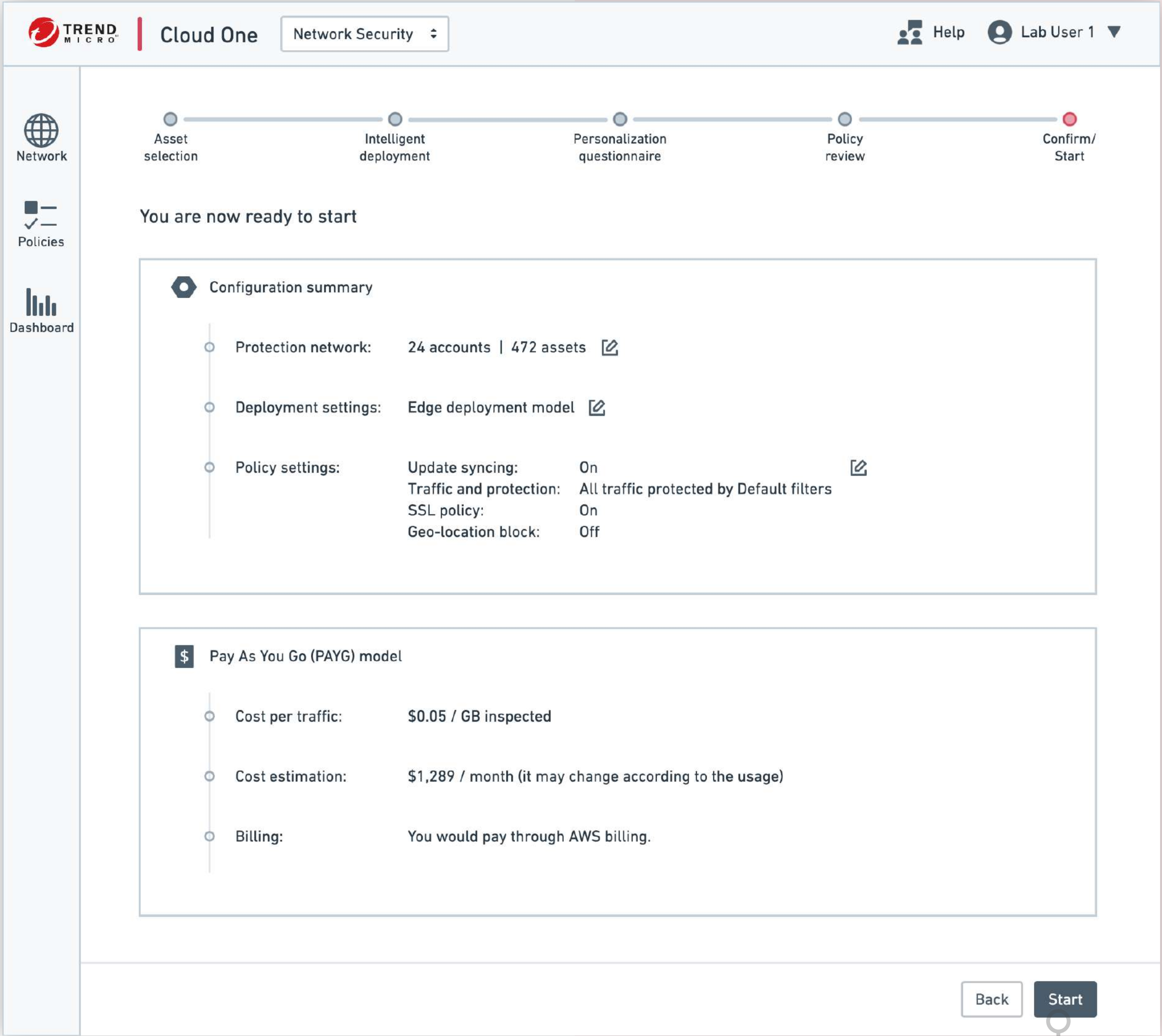
Customization

Wireframes



Next step

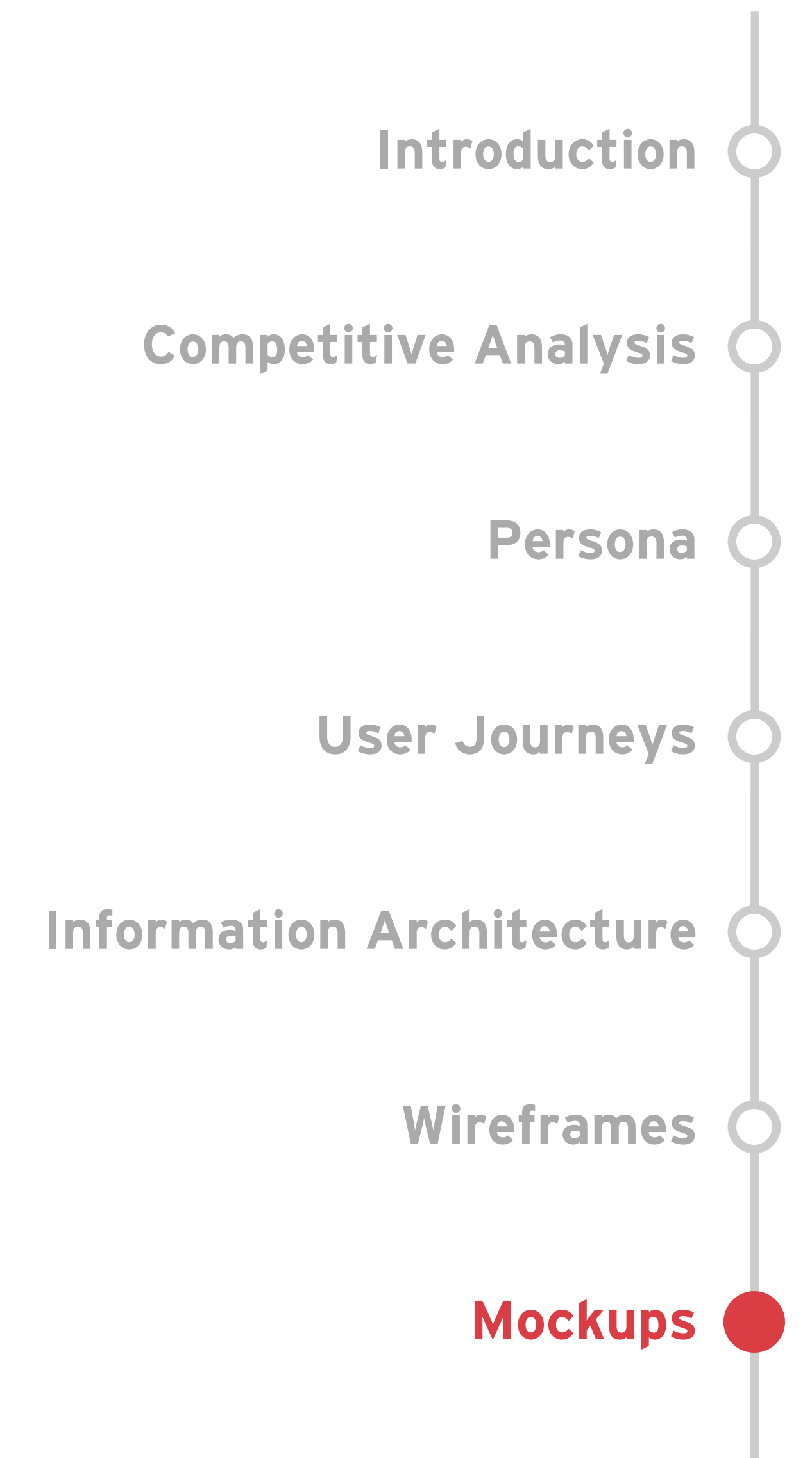
Policy review

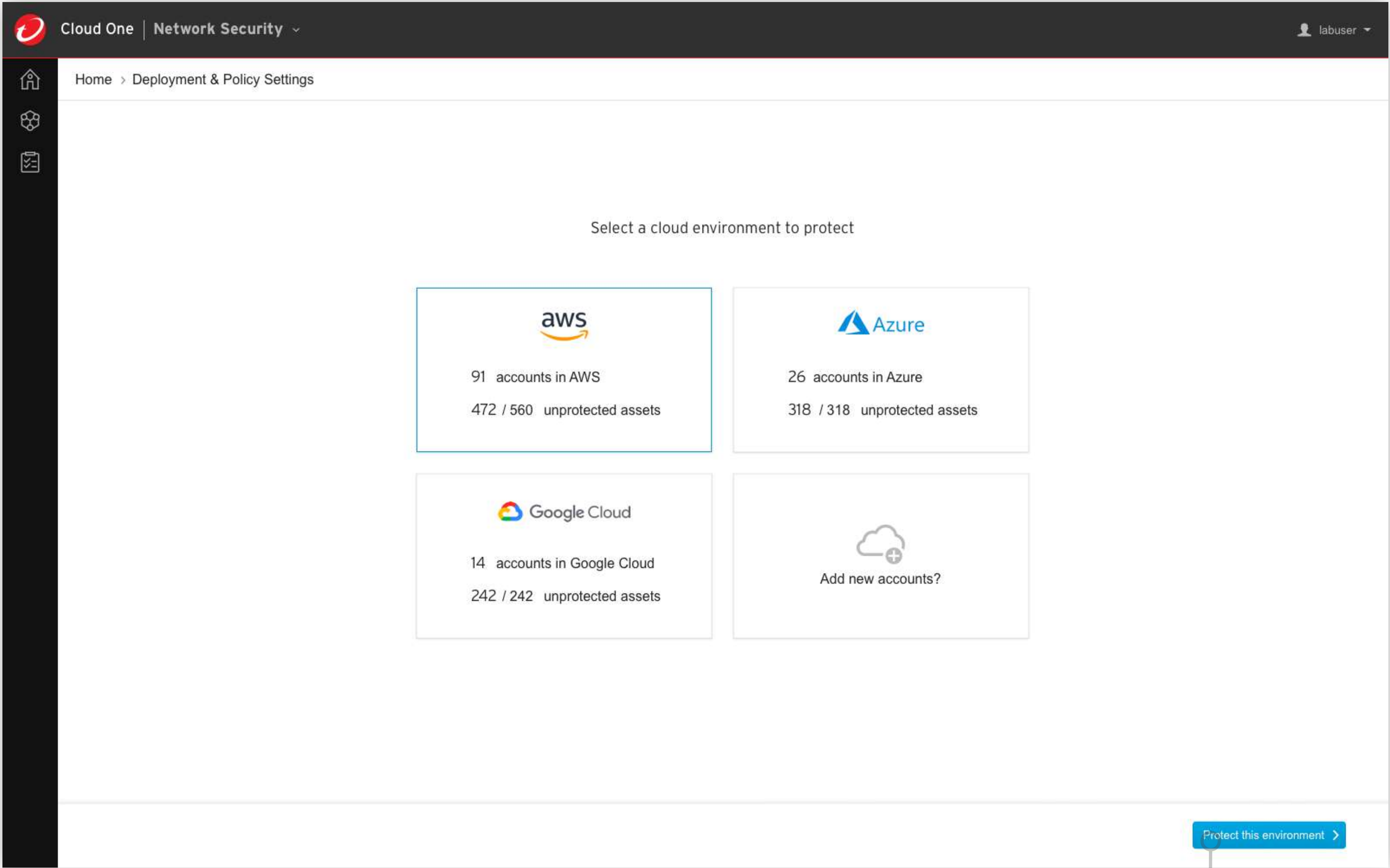


Summary

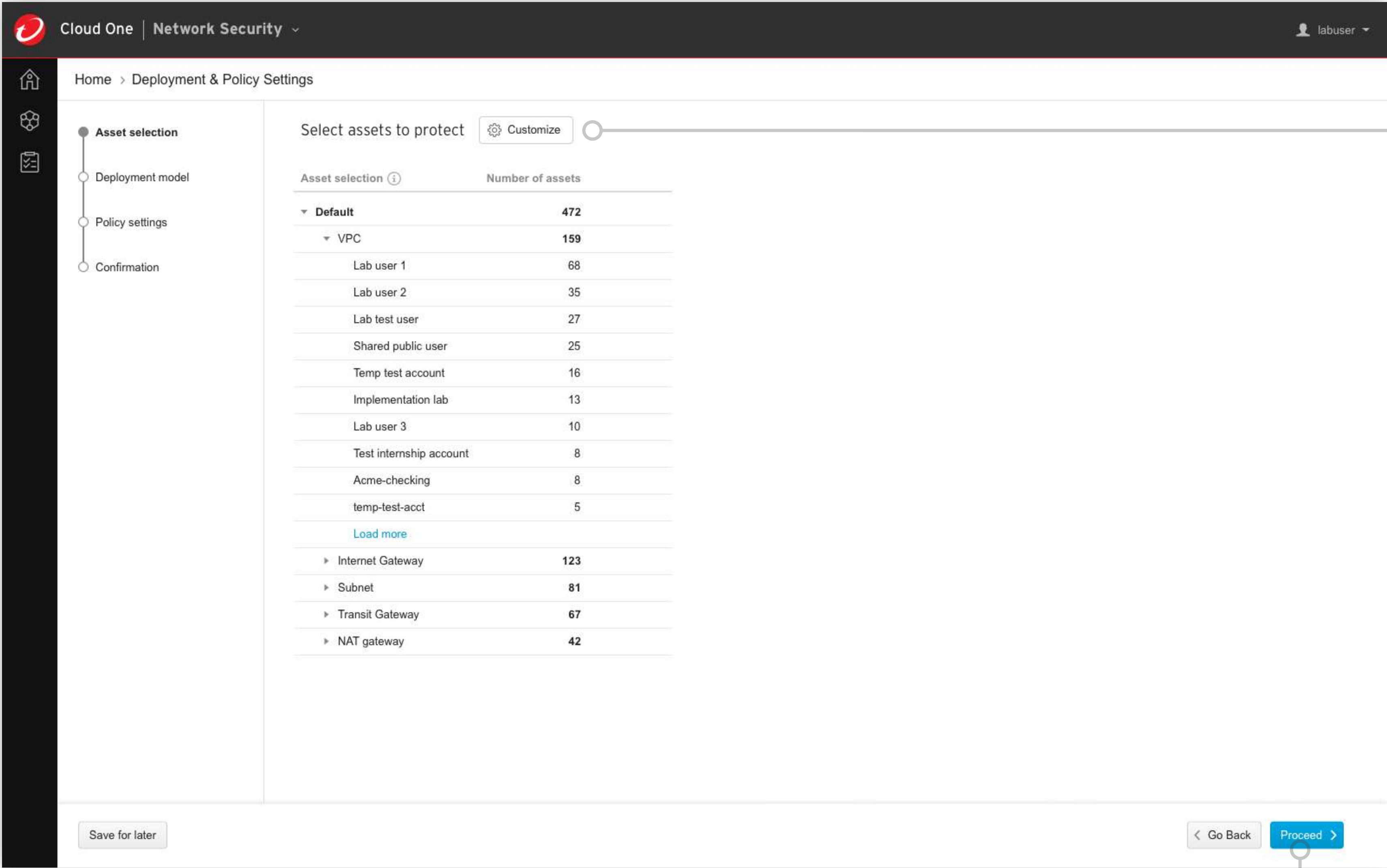
Next step

7. Mockups



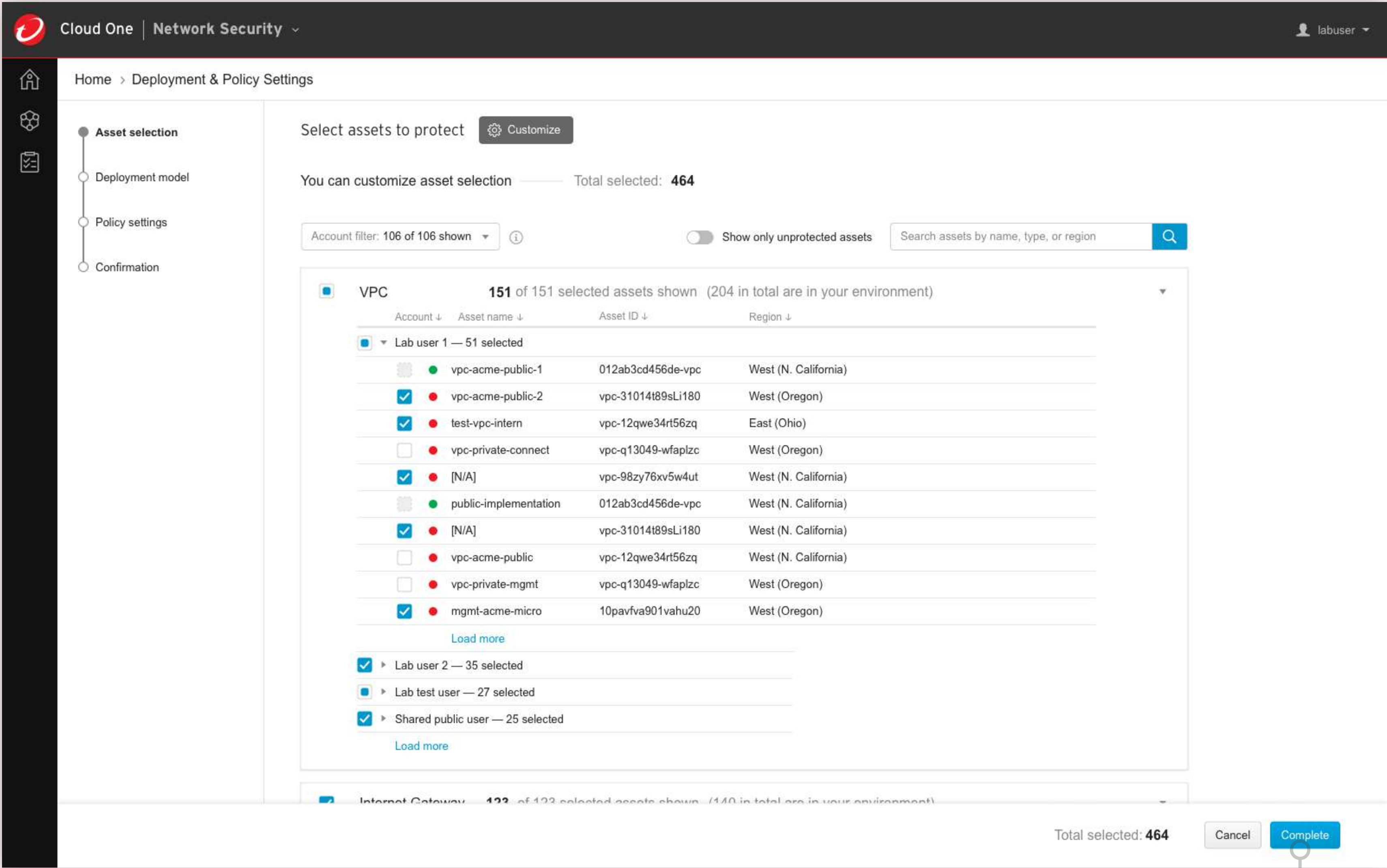


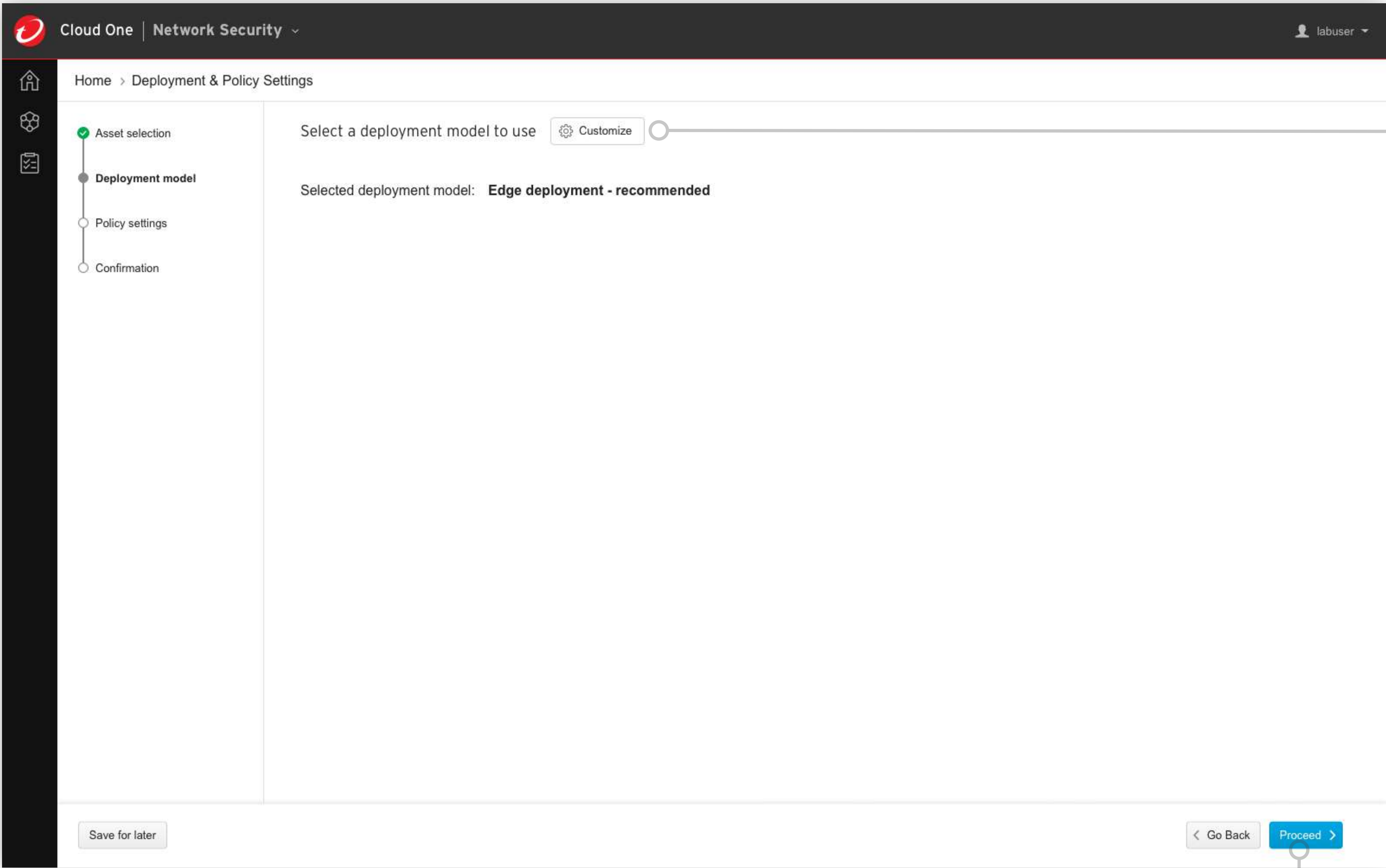
Next step



Customization

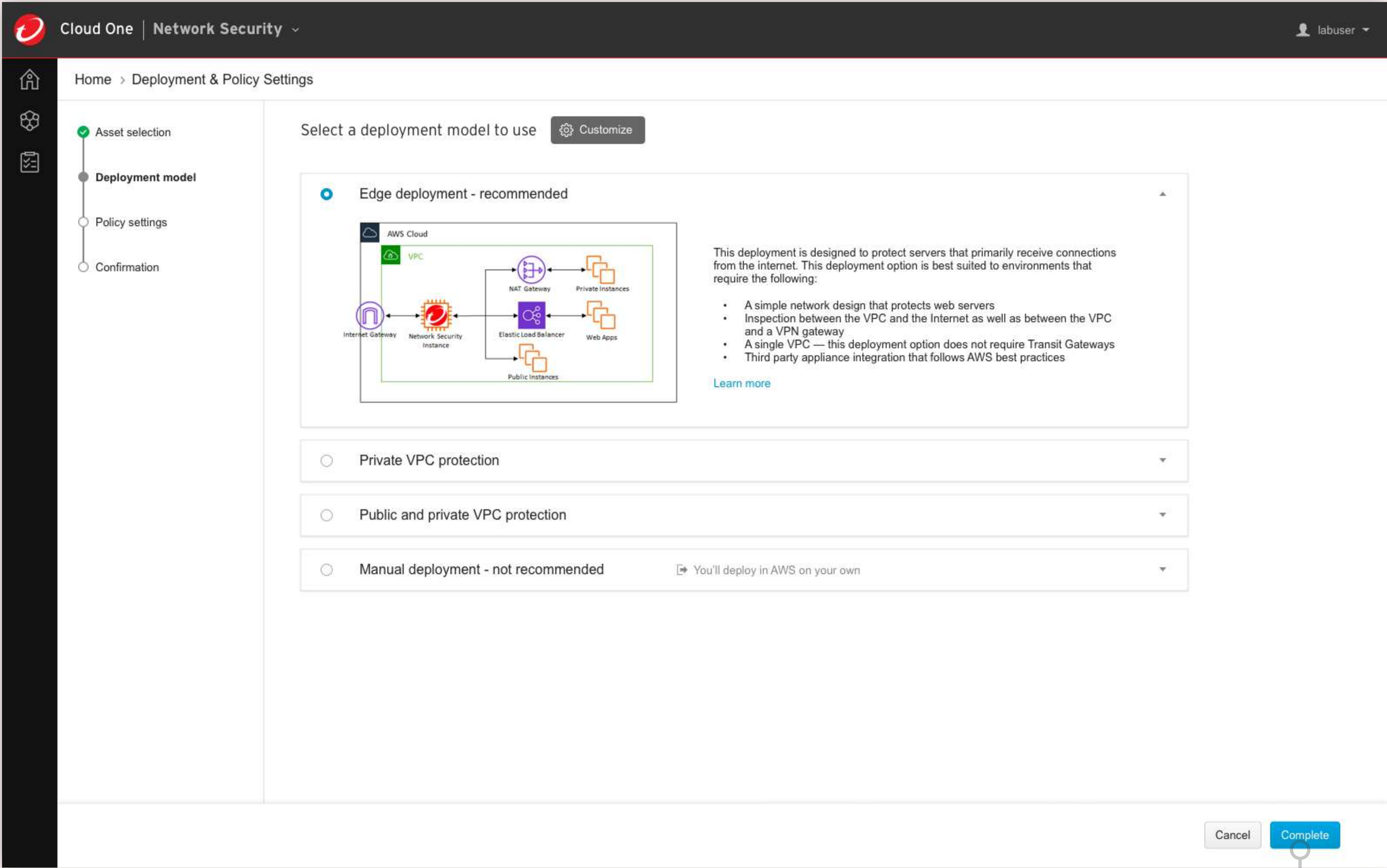
Next step







Customization

Next step



Next step

 Cloud One | Network Security

 labuser

Home > Deployment & Policy Settings

Asset selection

Deployment model

Policy settings

Confirmation

Review and set a policy

Policy setting options:

☒ Default

☐ Customization

☐ Dynamic recommendation

You can choose the default settings and customize it later.

Please customize on your own below.

Please take this questionnaire to adjust recommendations.

Fill out a questionnaire

Summary of policy settings:

Default

Update syncing

On

Traffic and protection

All traffic

protected by

Default filters

SSL traffic inspection

On

Geo-location block

Off


Save for later


< Go Back

Proceed >

Customization

Next step

 Cloud One | Network Security

 labuser

Home > Deployment & Policy Settings

Asset selection

Deployment model

Policy settings

Confirmation

Review and set a policy

Policy setting options:

☐ Default

☒ Customization

☐ Dynamic recommendation

You can choose the default settings and customize it later.

Please customize on your own below.

Please take this questionnaire to adjust recommendations.

Fill out a questionnaire

Summary of policy settings:

Customization

Update syncing

☒ On

Traffic and protection

+ All traffic

protected by

Default filters

SSL traffic inspection

☒ On

Geo-location block

☐ Off

Save for later

< Go Back

Proceed >

Last step

Cloud One | Network Security

labuser

Home > Deployment & Policy Settings

Asset selection

Deployment model

Policy settings

Confirmation

Review and set a policy

Policy setting options:

Default

Customization

Dynamic recommendation

Fill out a questionnaire

Completed

Summary of policy settings:

Dynamic recommendation

Update syncing

On

Traffic and protection

All traffic

Internet gateways

protected by

Default filters

protected by

Malware filters

See details

SSL traffic inspection

On

Geo-location block

Off

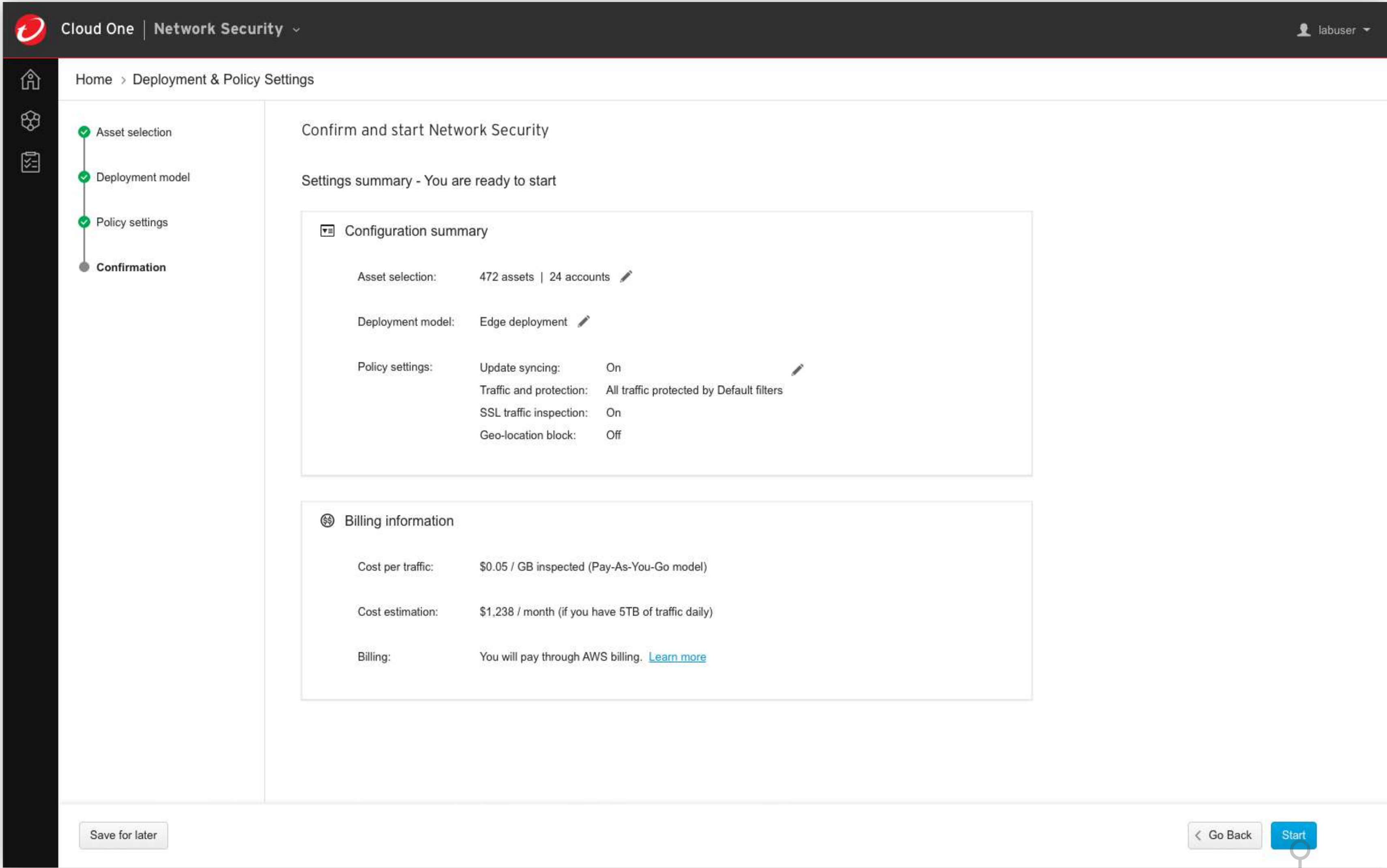
Save for later

Go Back

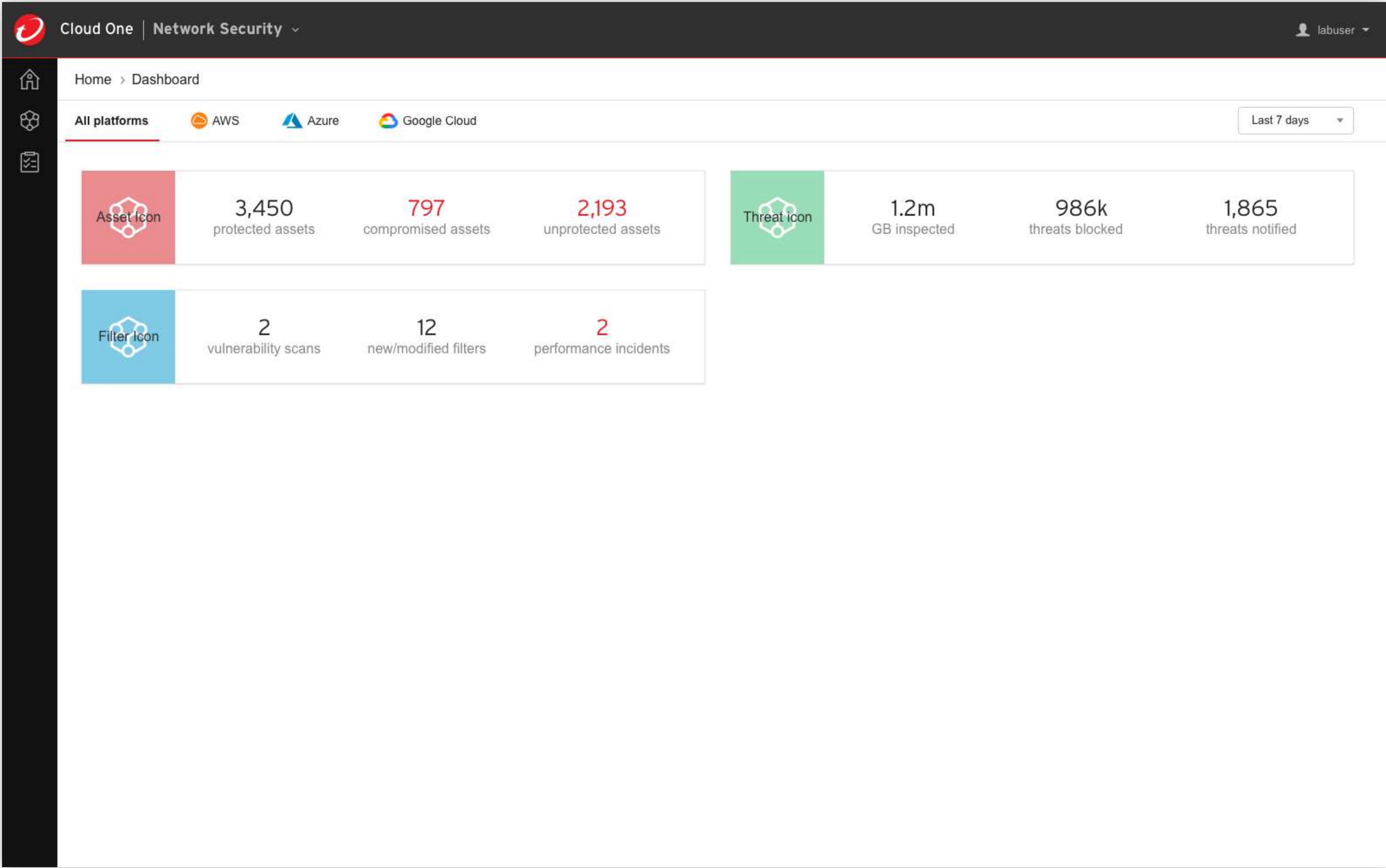
Proceed

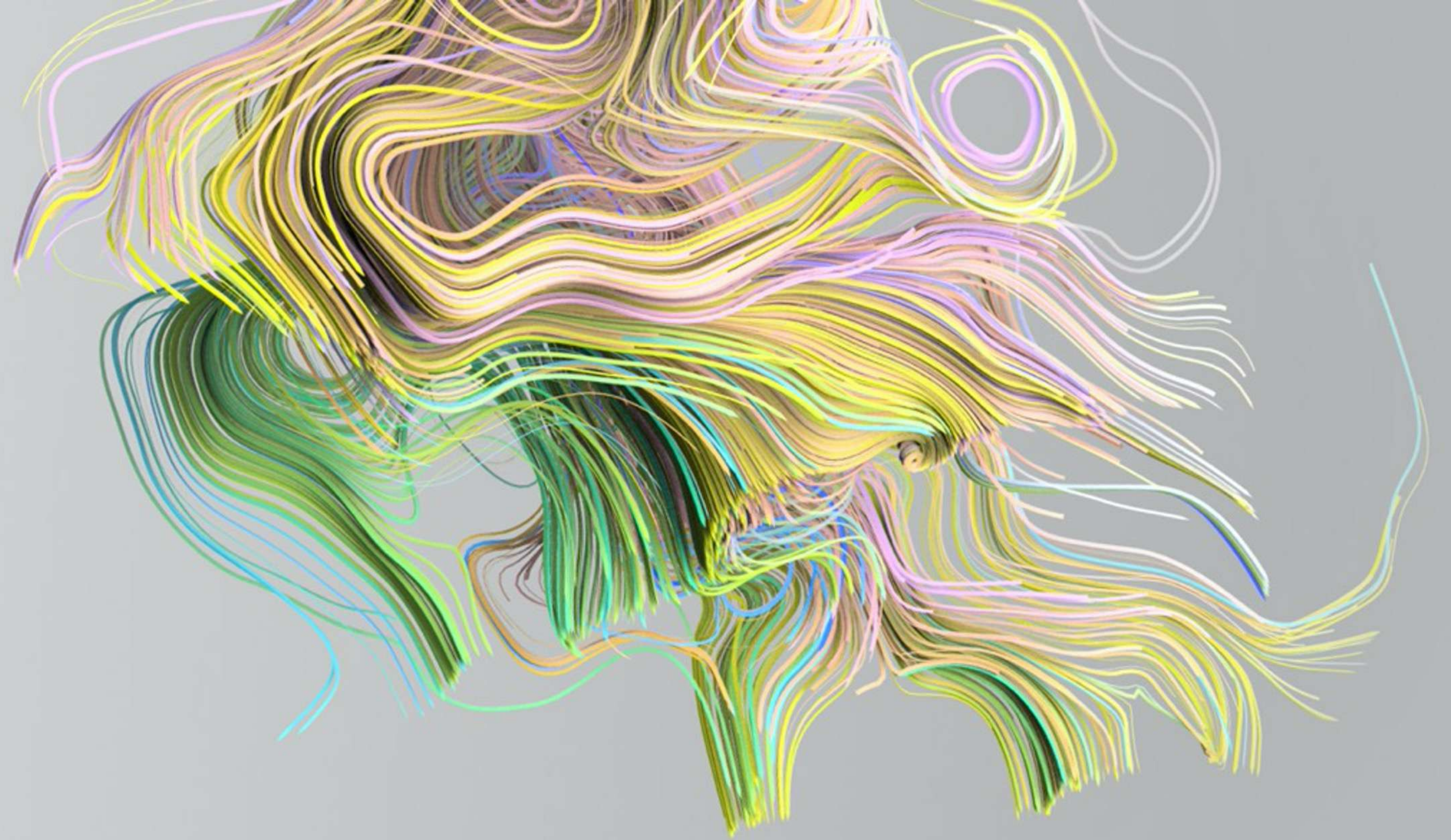
Questionnaire

Last step



Complete&Start





Thank you / Arigatō