Case Study #5

Exploration	Strategizing and planning	Execution and iterations	Release and assessment
Shaping the problem space	Foundational strategic direction	Tactical and evaluative	Measuring impact and benchmarking
Defining markets	Competitive Intelligence		
Product positioning	Feature prioritization and definition		

Opportunity Discovery

(Continuous strategic research)

IBM Cloud Access Governance

Evaluating proposed concepts to help users govern sensitive resources based on where they are being accessed from

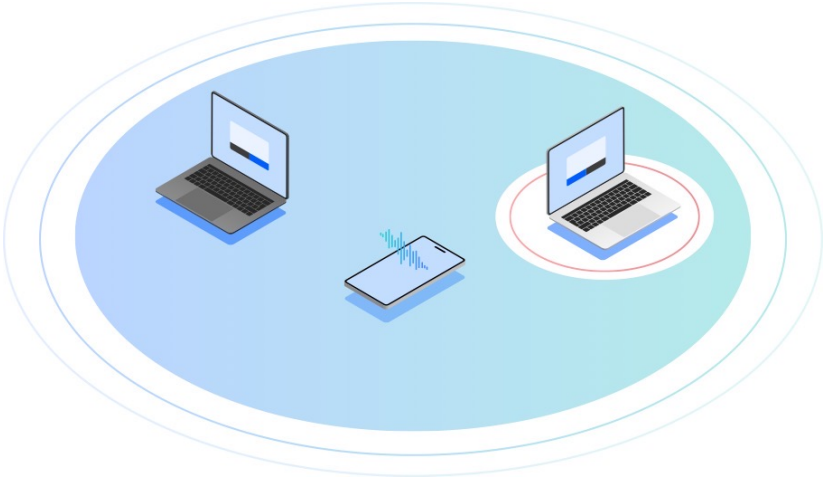
Tactical evaluations and strategic explorations

Helping development and design leads test the performance of proposed concepts and uncover opportunities for enhancement

Background

When I first joined the IAM organization:

1. This project was already committed due to a client request
2. The architecture was already proposed and APIS were being developed
3. Initial design proposals were created based on technical requirements and proposed architecture
4. Designers and developers needed to test their proposed concept (an access governance feature they called "*network policy*" which they assumed it must live in IAM console)



Client Request:

As an admin, I want to be able to restrict access to resources based on what IP addresses they are being accessed from) so that I can mitigate the risks of privileged access through compromised accounts

I did not have the time to conduct foundational explorations on the original customer requirement and assumptions and needed to proceed with concept testing

“Does this concept make sense to our users? Do they find it useful?"

Development Manager, IBM Cloud Security Services

“Can users successfully and confidently complete the tasks? Is the UX intuitive?”

Design Manager, IBM Cloud

Research Design Overview

Research Objective:

- To validate the design direction, flow and architecture proposal
- To validate that the design proposal can communicate the purpose of the feature to a first-time user
- To understand if users feel confident in understanding the steps required to complete their tasks
- To identify opportunities for improvements

Research Design

- Concept testing X2 (n=~10/test)
- Competitive Audit
- Interviews (n=6)
- Terminology Testing (n=25)

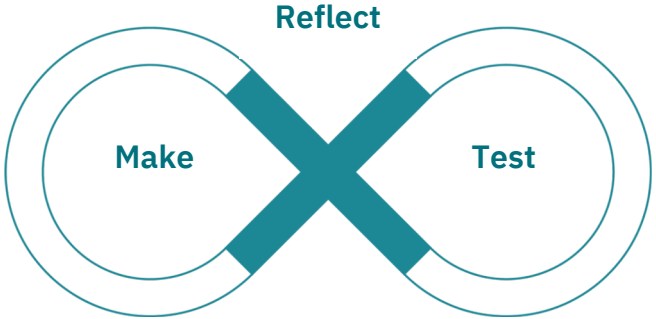
Participants

Screening criteria assumption:

- Identity and access management admins, engineers and architects
- Company size 1000+ , Regulated industries

Research Design

Due to time constraints a foundational exploration was not conducted prior to concept testing so concepts were merely informed by assumptions from SMEs



2 rounds of concept testing and iterations

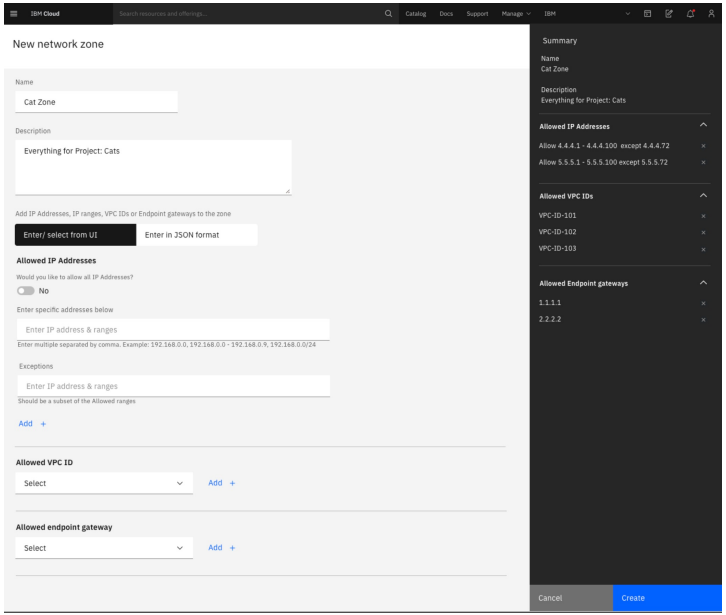
Secondary Research

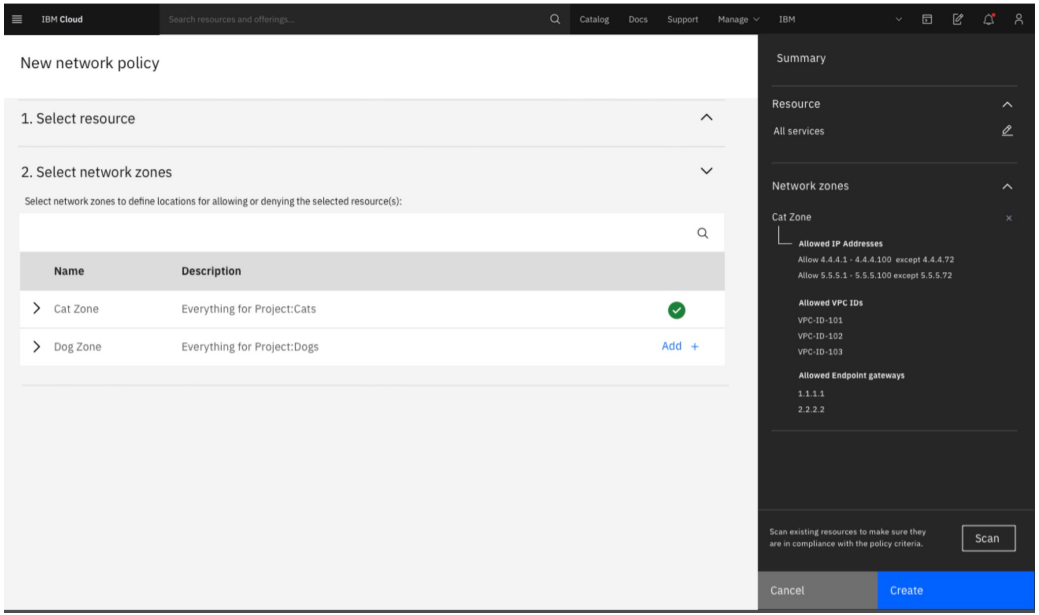
Lean deep dive With SMEs

Terminology surveys

Top Research Findings

Sample Screens





2 rounds of concept testing

There were several blockers in conveying the full story of this new concept during both rounds

- Majority of participants did not understand or misunderstood the purpose of this new concept even after they went through the entire policy creation process
- Users' interpretation of each element how they work together were vastly inconsistent
- The overall flow did not fully match expectations and user mental models
- Users expressed that this task is normally a cloud admin or enterprise or security admin task
- Since this concept was in IAM console and was being tested with IAM SMEs they were looking for IAM elements in the flow (entities, auth, etc.)

"It would be beneficial in the first page to explain what a network policy or network Zones are. It could mean different things in different contexts. I really don't understand this at all, it's too networky, I'm not the one normally taking care of these things"

IAM engineer, Central IT, Banking

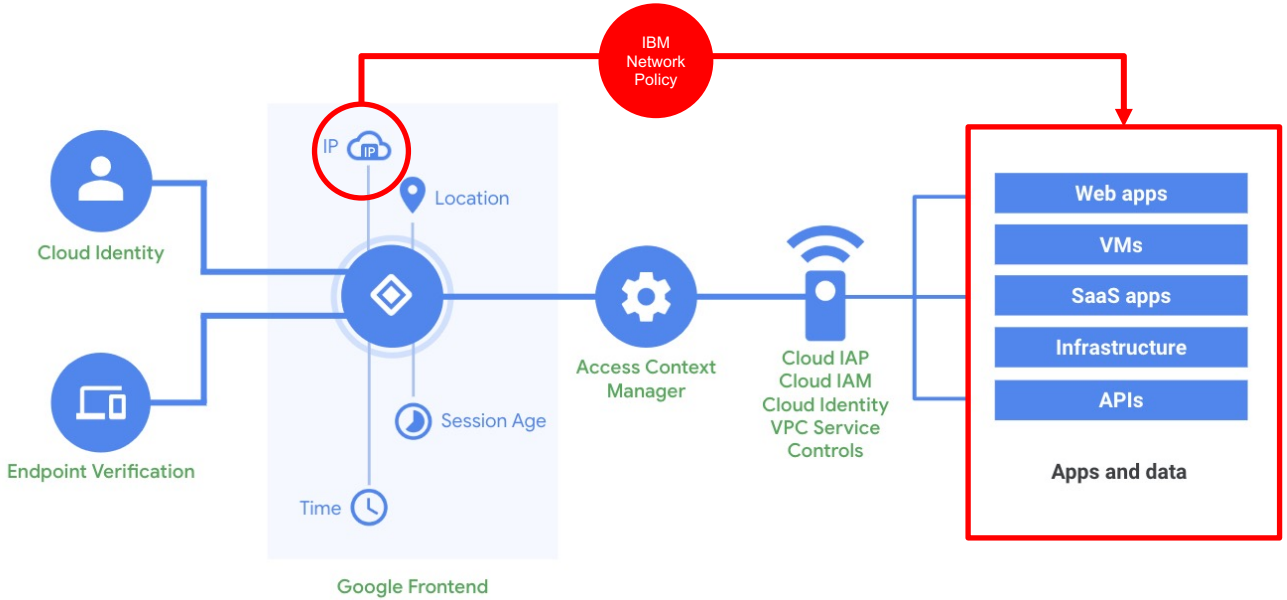
"I don't really understand this. I was expecting to see IAM related elements such as authentication or users in here"

IAM admin, Central IT, Telecom

Secondary Research

Competitive audit showed that the closest concept to our proposal was GCP's Access Context Manager which produced "access levels" that were based on various types of context

This concept is a feature that lives under GCP security Center



Recommendations

I expressed my concerns with the team and shared footage of some risky behavior that I observed along with direct user quotes.

Shared competitive intelligence and discussed potentials for expansion

I recommended to my team to postpone release so we can conduct a lean generative study with the appropriate persona (cloud, system, or security admins) to gain more understand on their expectations from this capability.

Luckily due to some last-minute roadmap reprioritization and the severity of observed issues the team was able to accommodate this recommendation

Lean Study: SME interviews

After conducting interviews with 6 SMEs it was evident that we needed to rethink the scope, direction and terminology for this new feature

- Cloud and enterprise admins expect a much larger scope from this tool. Restricting access only based on network location was not enough for an entire feature
- They used terminology similar to GCP Access context manager and expected to be able to restrict access based on “context” which goes beyond “network”

“ I want to see a broader scope as you should be able to add the user or application's context to the authorization to access the resource”

Cloud Admin, Fintech

Recommendations

I recommended to my team to rework the future vision for this feature to match users' mental model and differentiate from our competitors

I proposed a new scope and architecture but also proposed an MVP that could use majority of already build components and needed minimal change to accommodate an easy future transition to the “wedding cake” version of this concept

I suggested to work with the content team to run a terminology survey and gain some confidence on content and terminology strategy

Future vision recommendation

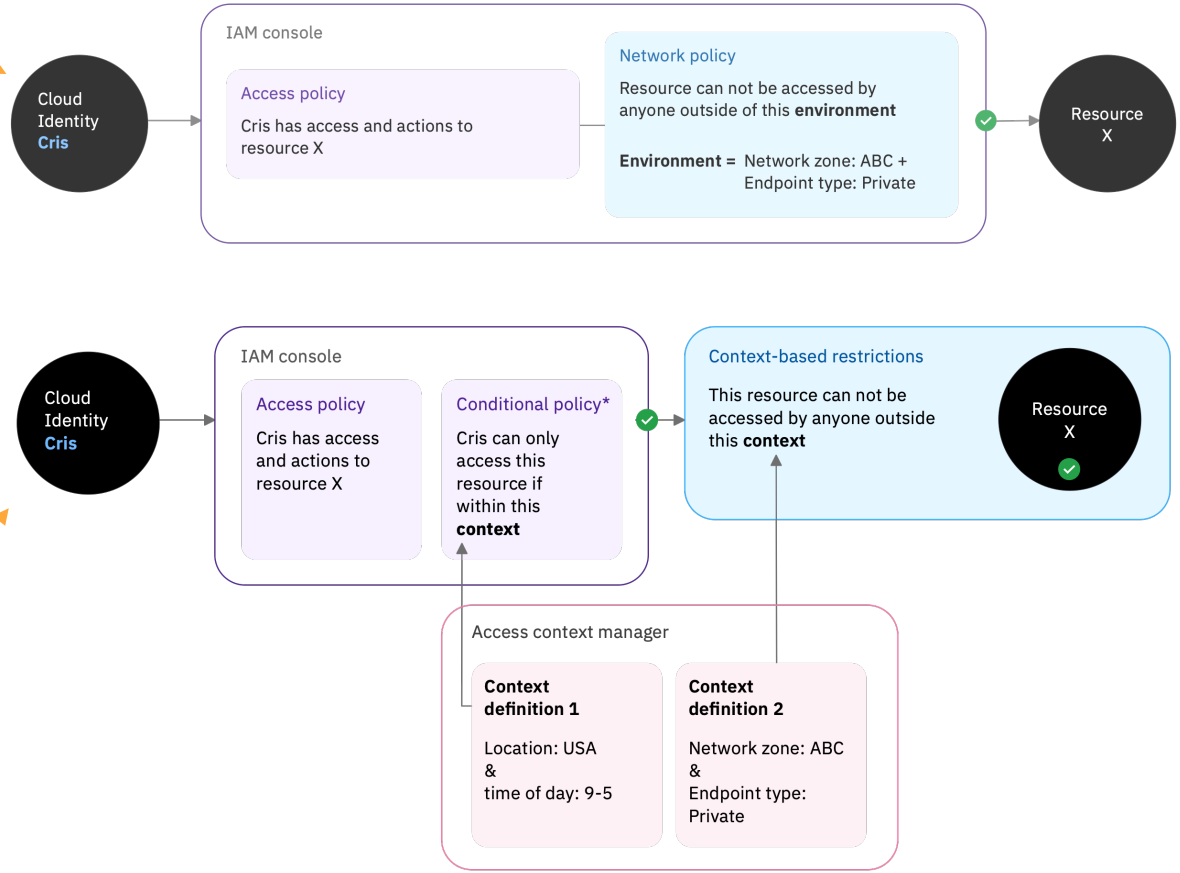
Project starting point:
Network Policy

Research

3 rounds of concept testing and interviews in addition to Terminology surveys

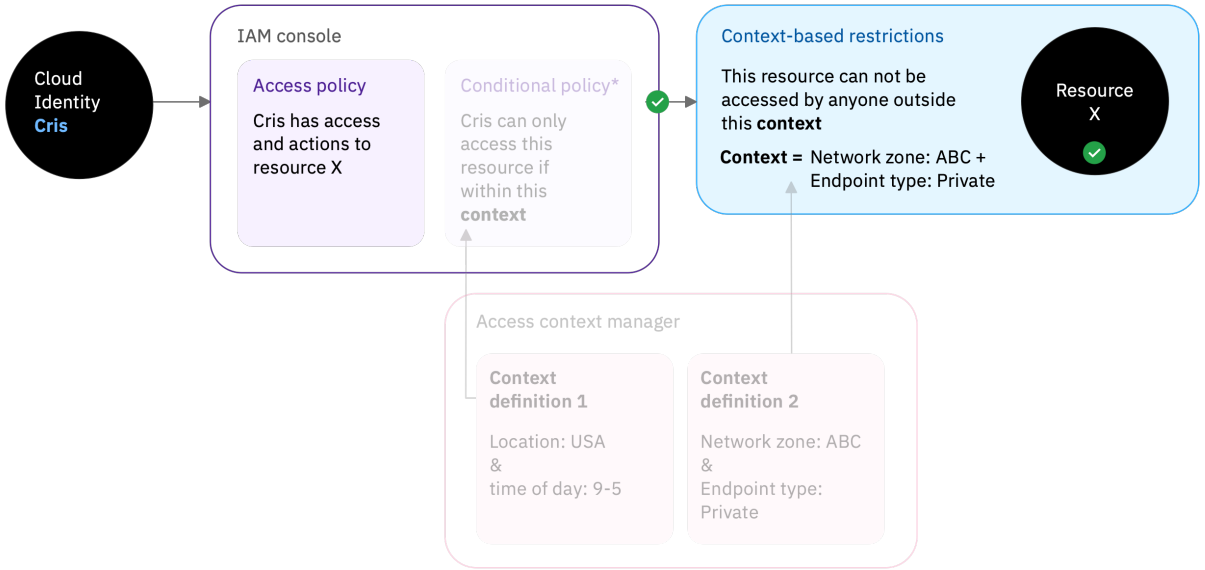
What users want:
Access context manager

Cloud administrators and IAM admins want to achieve an added layer of security beyond IAM access levels by restricting access to cloud resources based on user's context, such as IP addresses, VPCs, time of day, and device integrity.



MVP Recommendation

Release for Q3:
Context-based restrictions



Top business outcomes

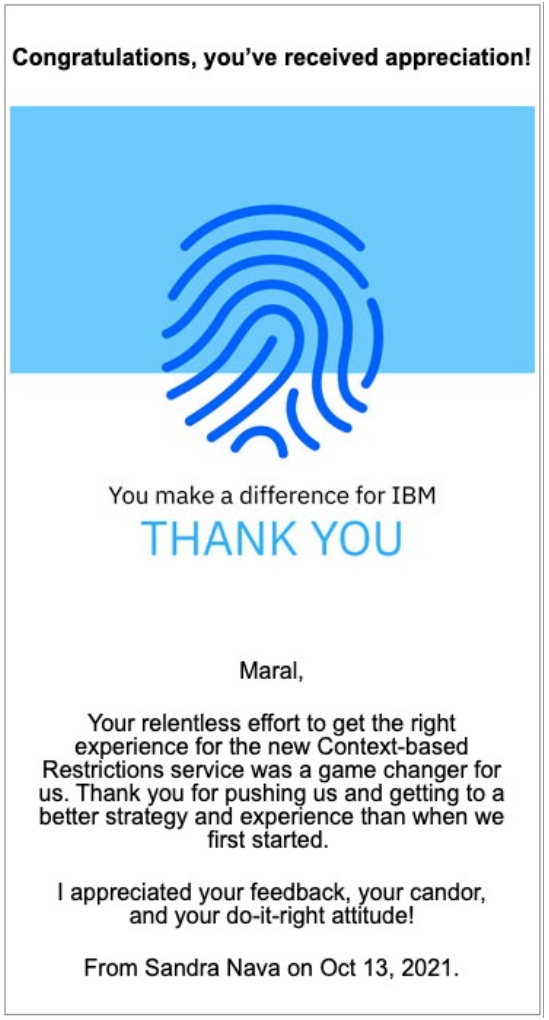
De-risked assumptions and gained insight into opportunities:

De-risked the original decisions
We were able to avoid potential risky behavior that could expose sensitive company information to public or disrupt processes due to the lack of knowledge of users we assumed would be using this feature

Gained insight into an opportunity to differentiate and bring value to our regulated enterprise users
Were able to uncover an opportunity to expand the scope of this feature to really differentiate our offering compared to competition

Actions taken to date

All MVP recommendations were implemented
This feature was released in October 2021 considering all recommended changes to design and terminology



Thank you