

# How Zero Trust enables the *everywhere* office

Marco Kolbas

José Torre

# Who we are.

José Torre



Information Security Manager  
@fiskaly GmbH






Marco Kolbas

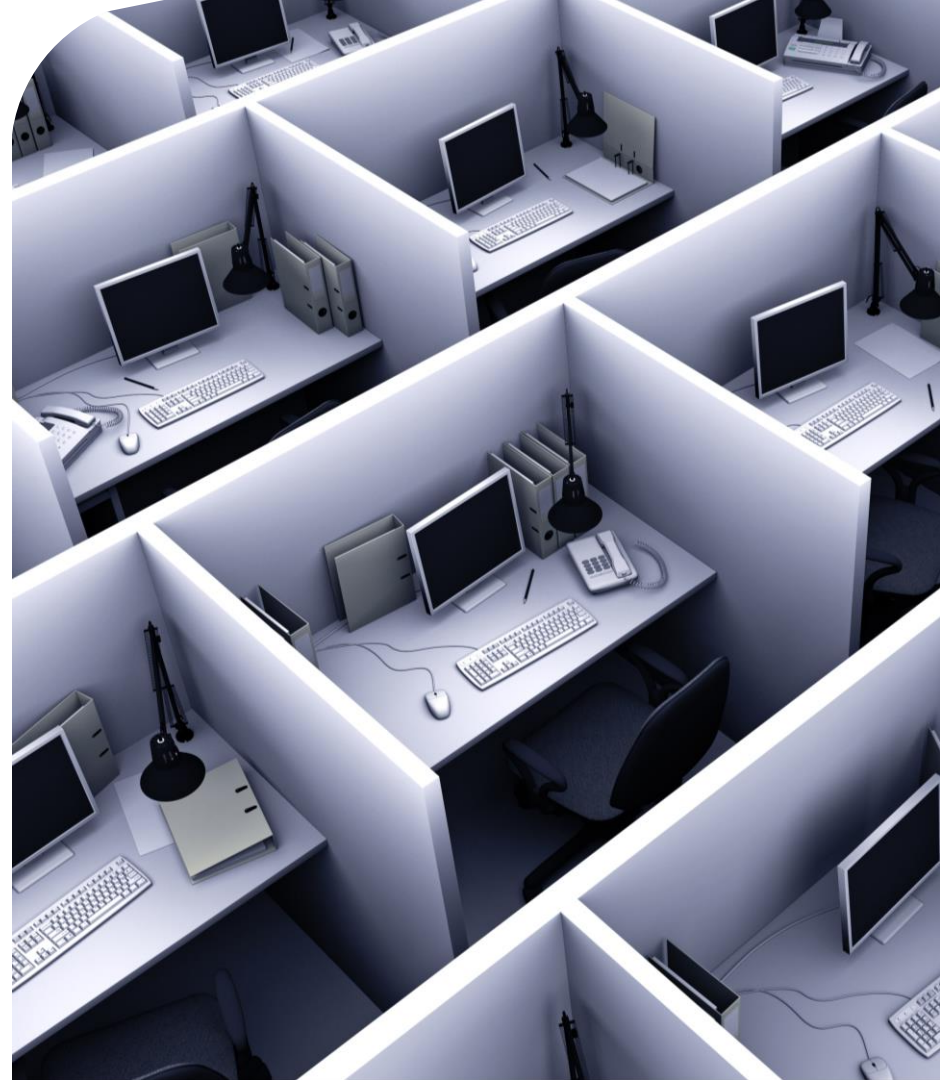


Senior System Administrator  
@fiskaly GmbH



# The feudal mindset

- Castle & Moat 
- Trust but Verify 
- Focus only on physical security 



# What made us **change**?

the Technology.

**WHAT IS WI-FI?** “Wireless fidelity” is a high-frequency radio signal that’s broadcast throughout a home, office or business. It allows people to connect to the Internet without using wires.

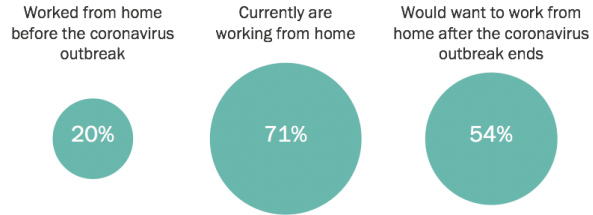
## Wireless Net links spread



Steven M. Hirsch/The Olympic

**Many workers would like to telework after the pandemic is over; transition to working from home has been relatively easy for many**

*Among employed adults who say that, for the most part, the responsibilities of their job can be done from home, % saying they \_\_\_ all or most of the time*



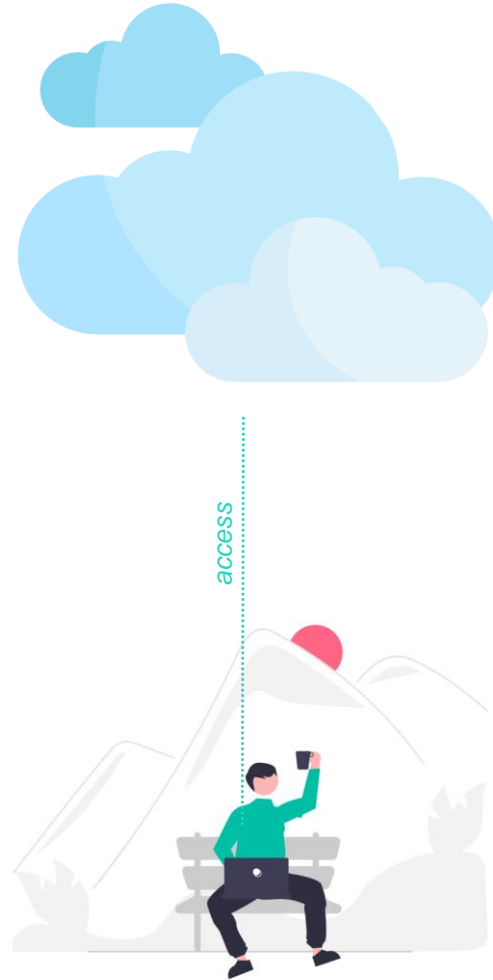
Pew Research Center, December 4, 2020

*How the coronavirus outbreak has – and hasn’t – changed the way Americans work*



the Catalyst.

The *everywhere* office.



# The Jungle

## "out there"



- Shadow IT



- Unsecure network connections



- Unauthorized access



- Theft



- Shoulder surfing



- Bringing security culture *out there*

# Zero Trust

security model

*/'ze:ro/ /'trʌst/*

*"never trust; always verify"*

*"never trust (by default); always verify"*

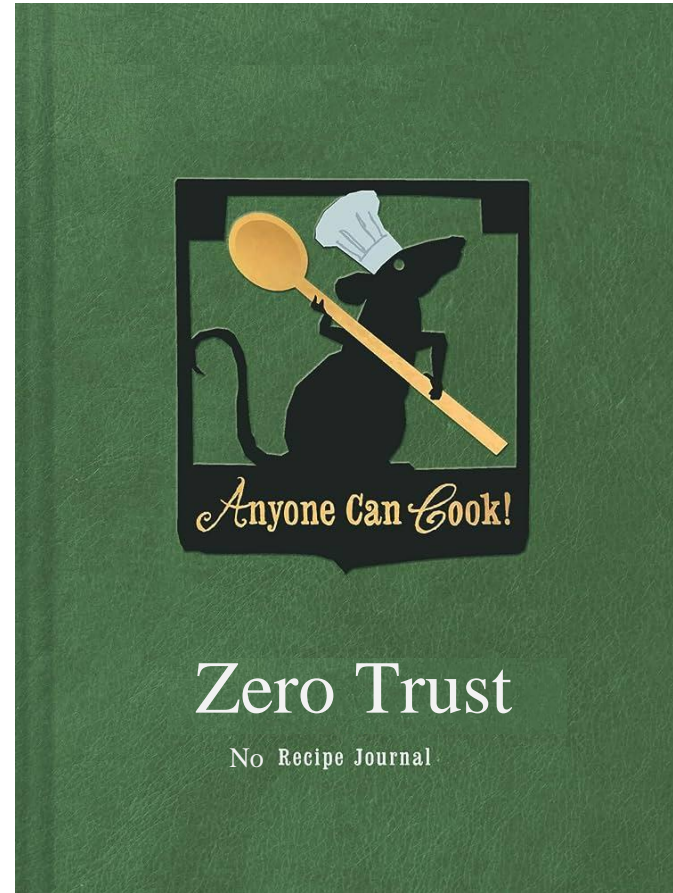




**Zero Trust is some trust;**  
it is just the **token** that is different for which  
trust is **exchanged**.

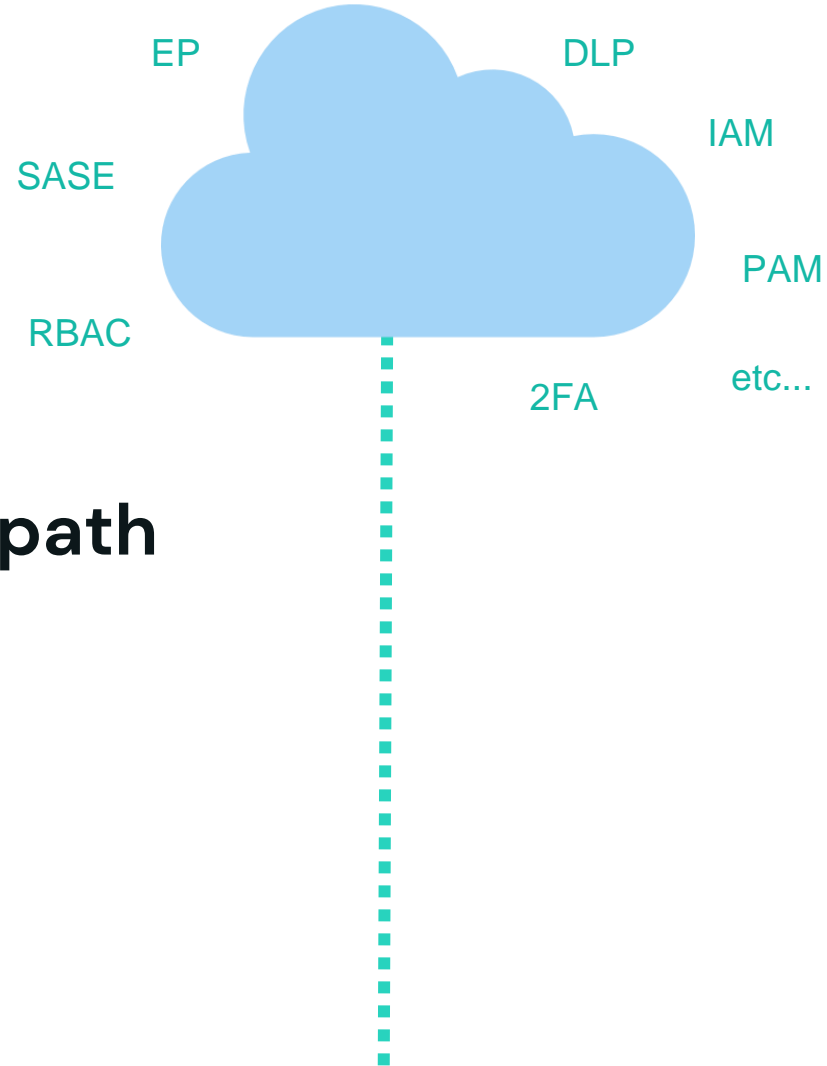


There's not a single way.



It's not a silver bullet.





# Synergy as a path to Zero Trust.

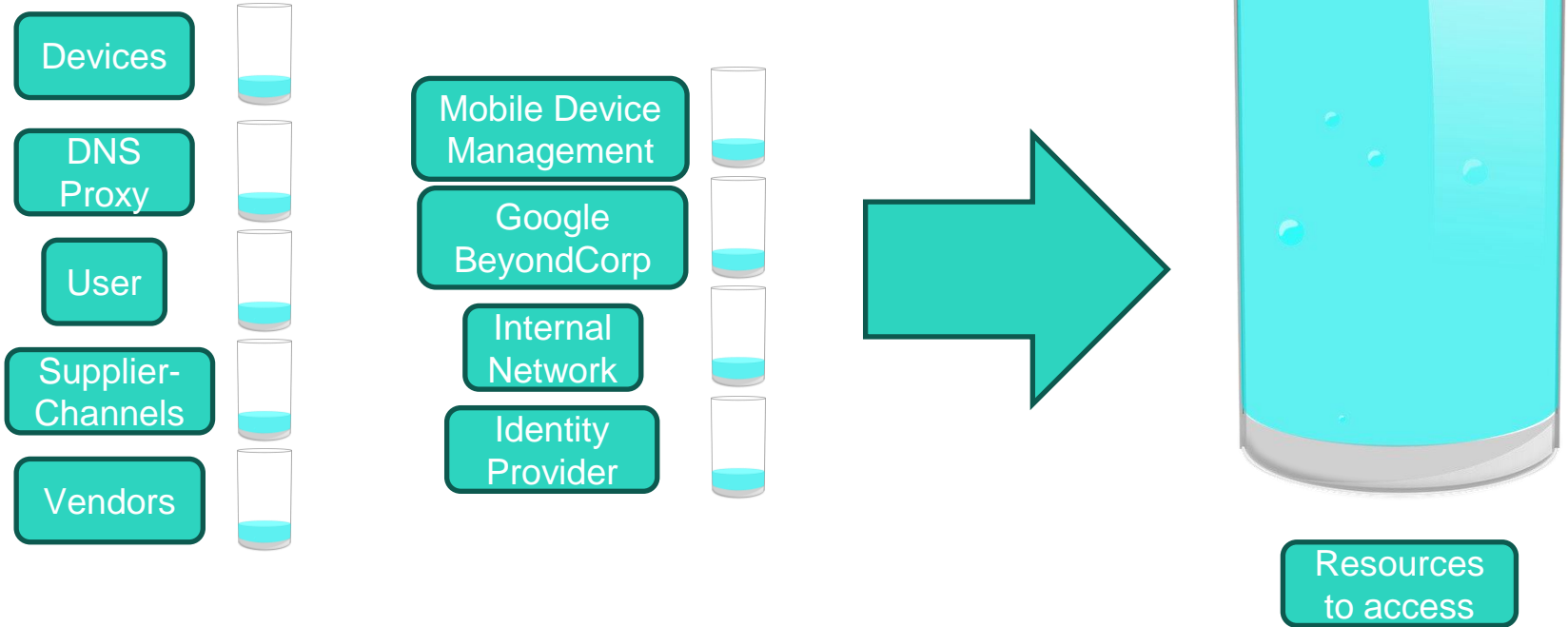


# Zero Trust @fiskaly.

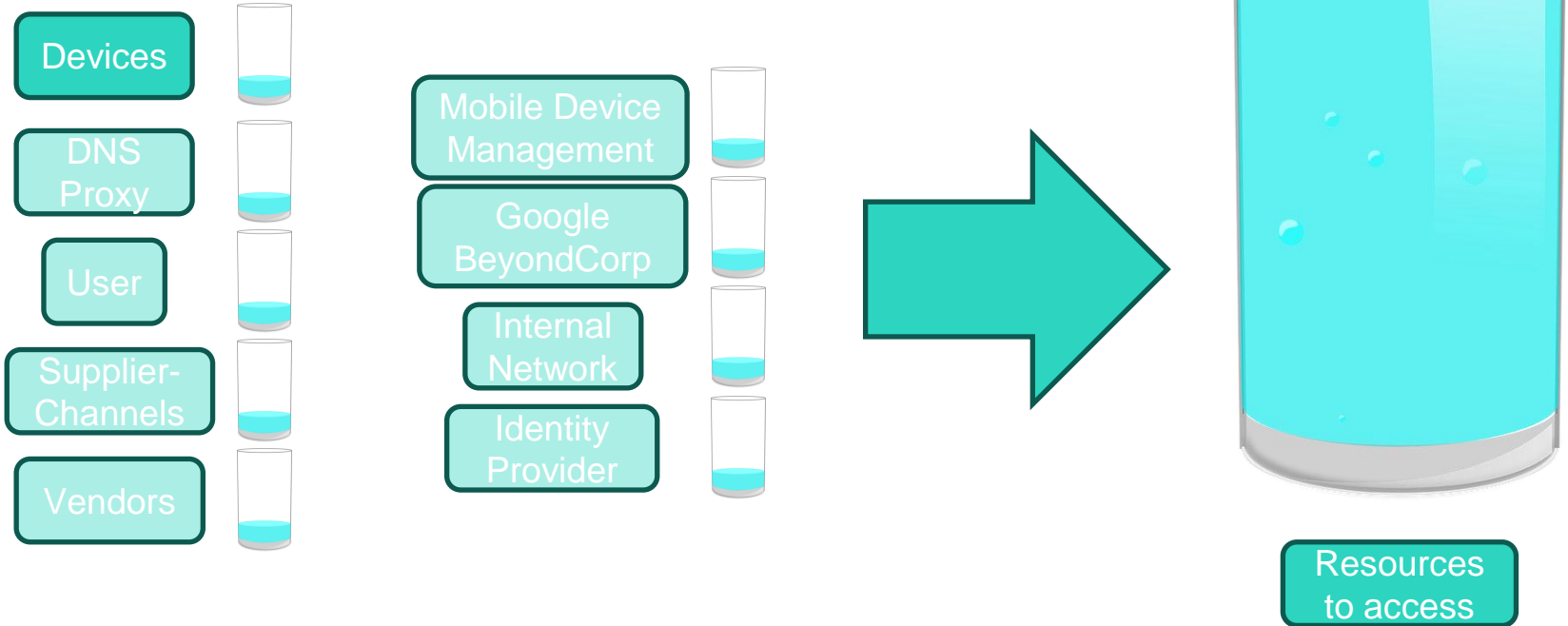
No part of the system can be seen as trustworthy on its own.

*All* parts must come together, to establish trust.

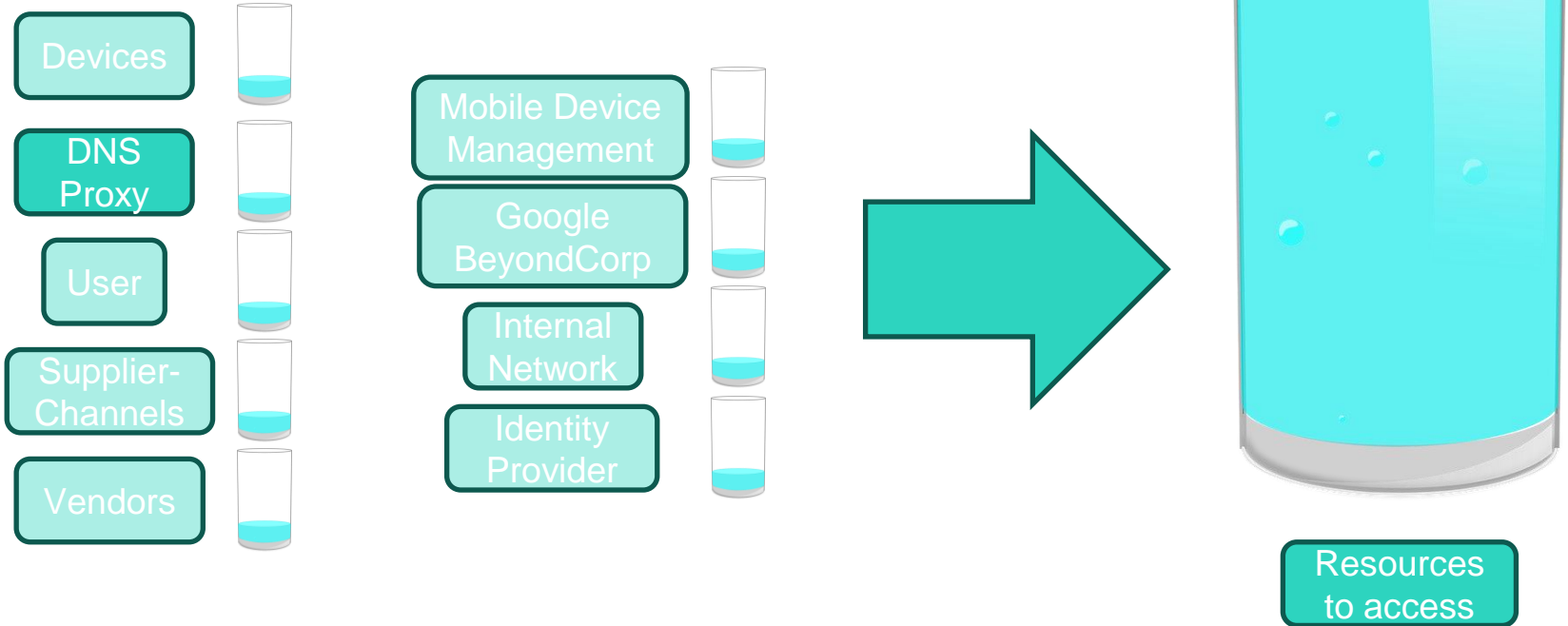
# System Components.



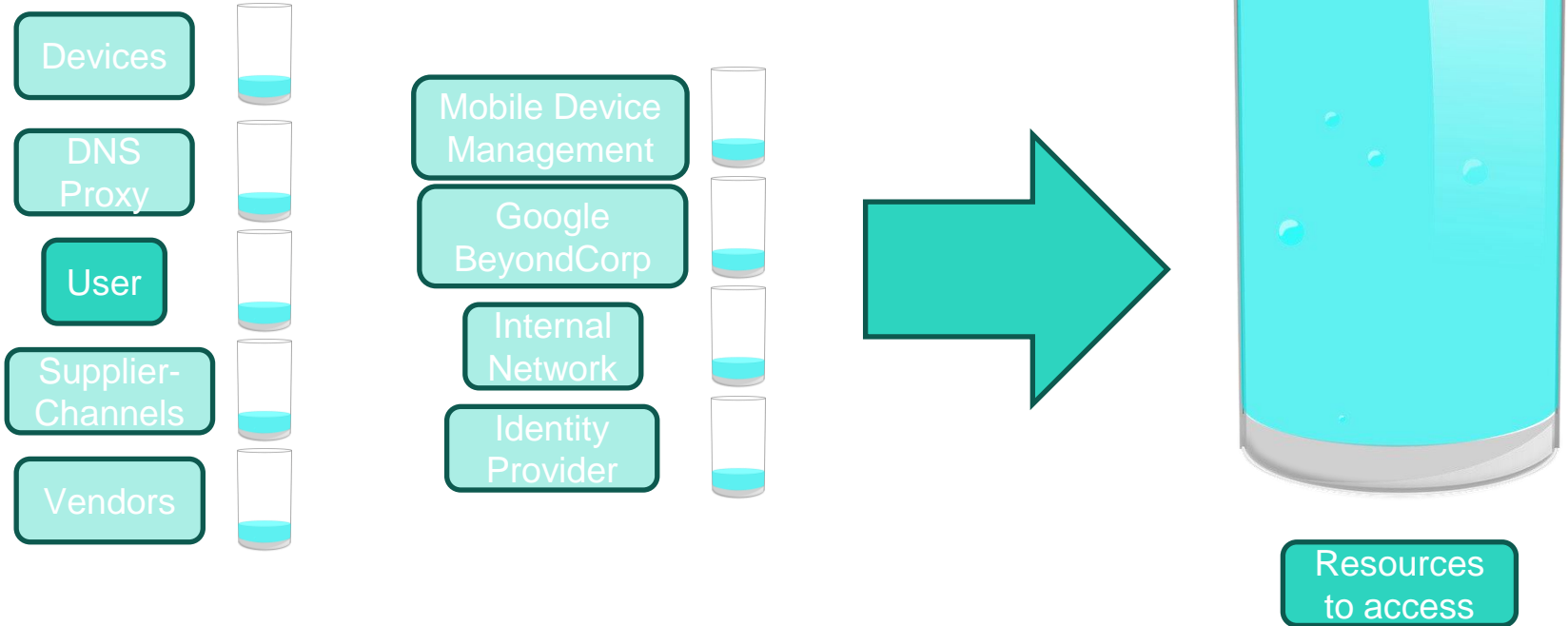
# System Components.



# System Components.

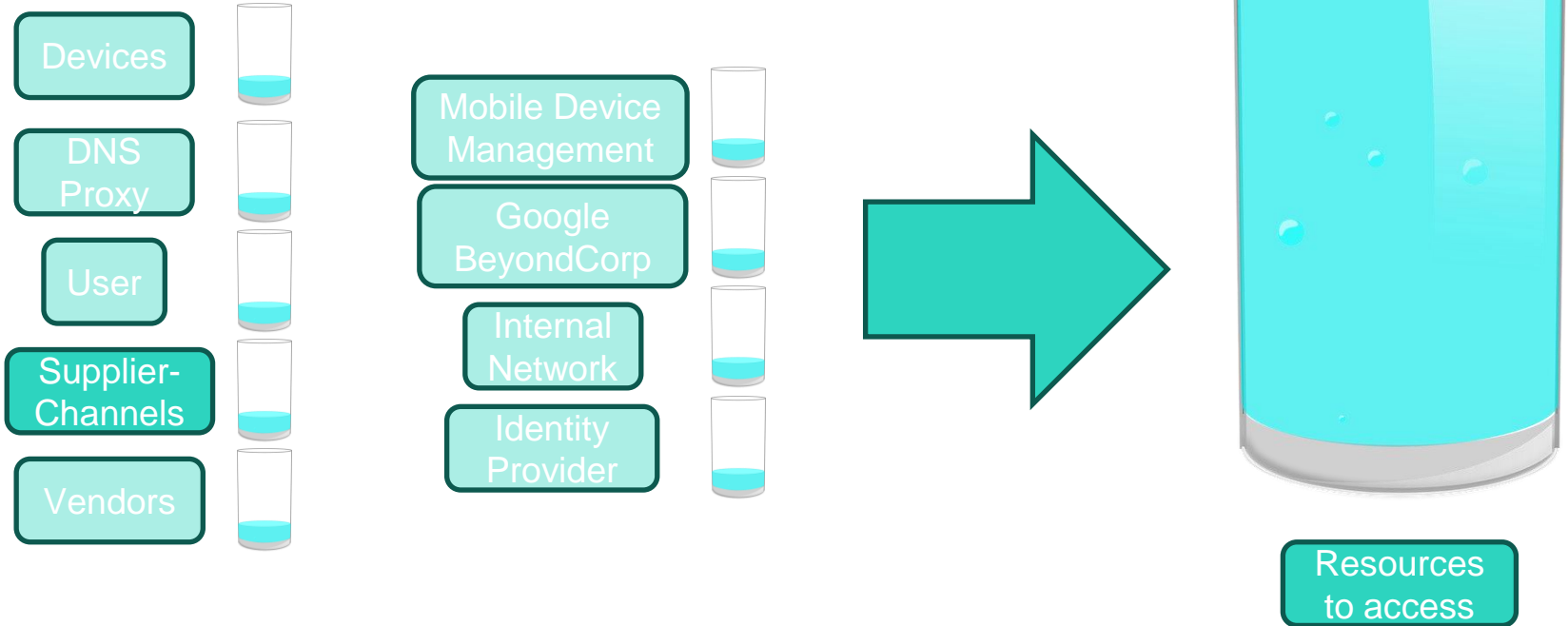


# System Components.

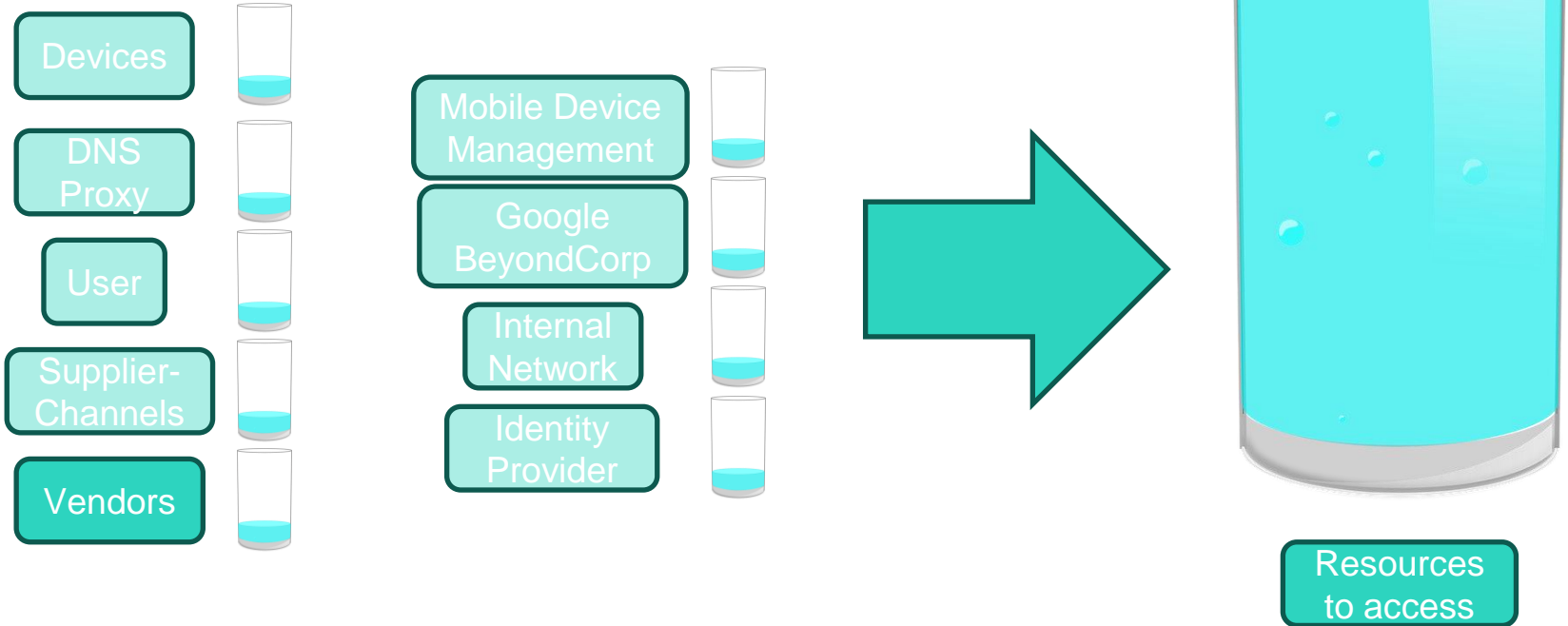




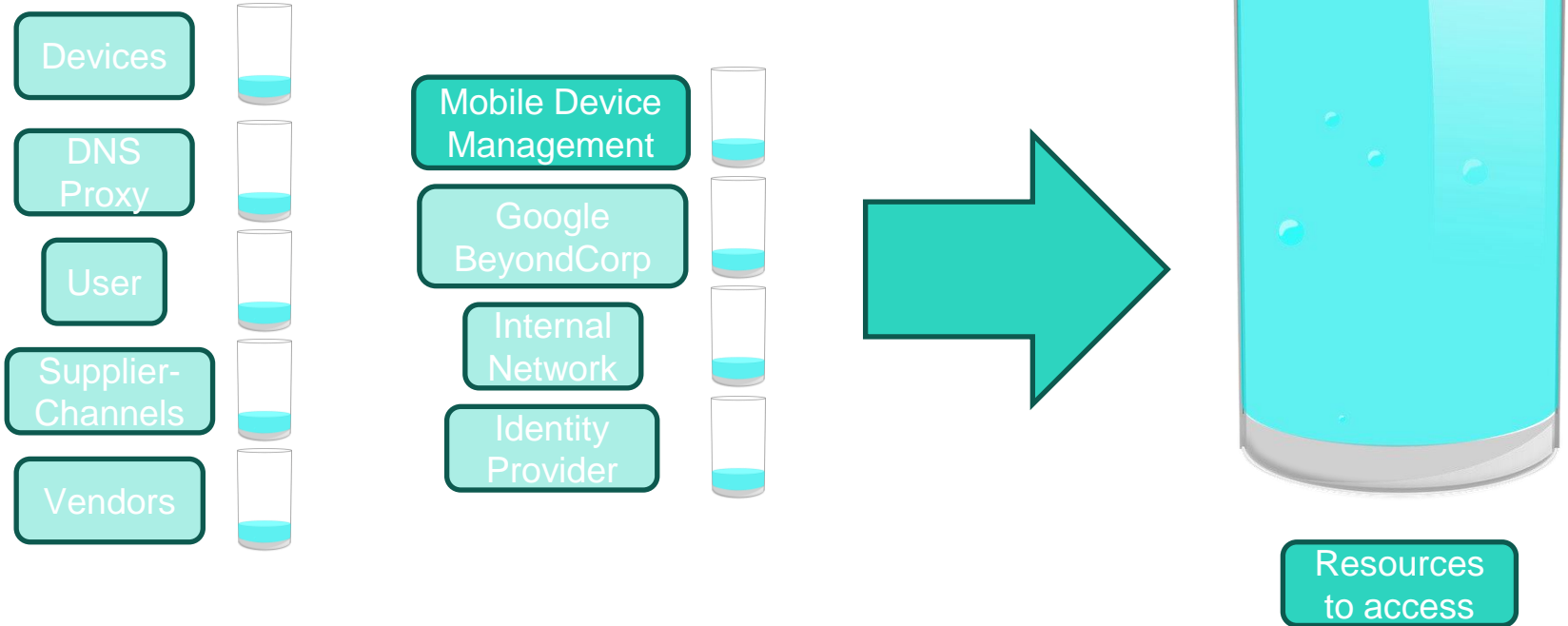
# System Components.



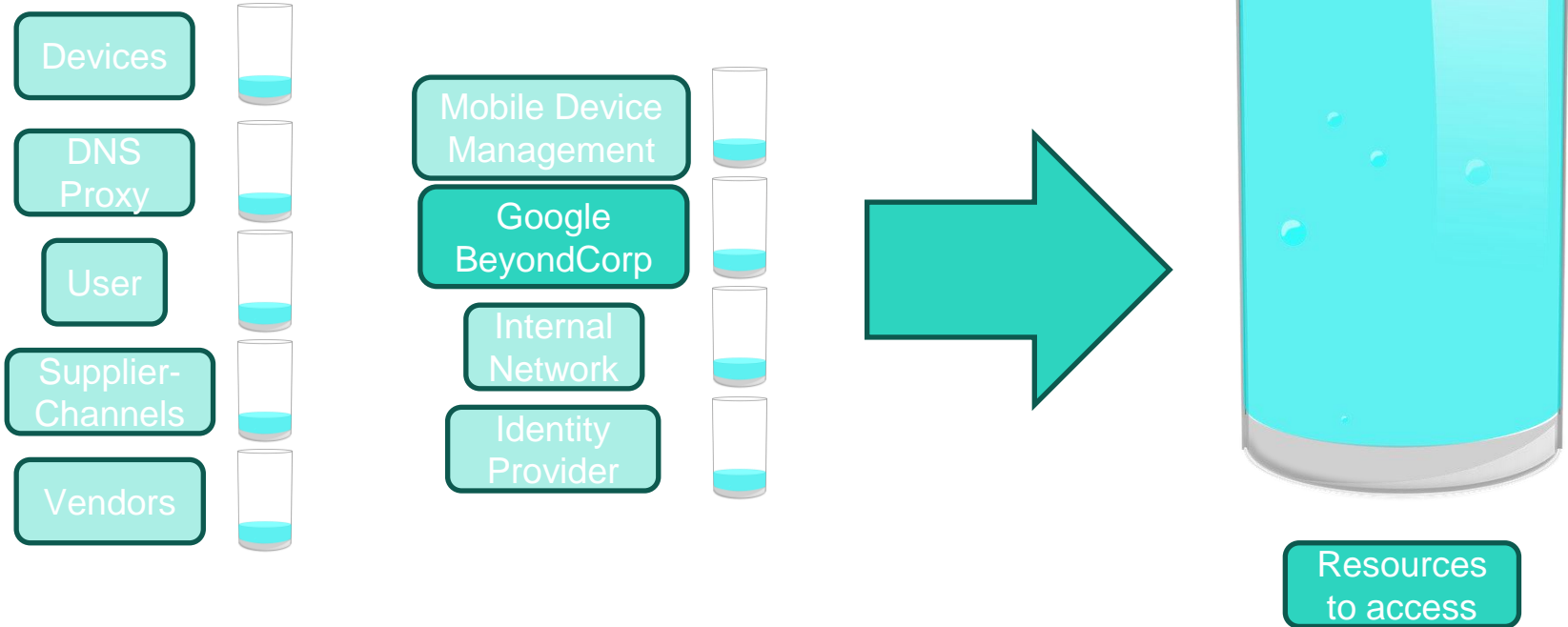
# System Components.



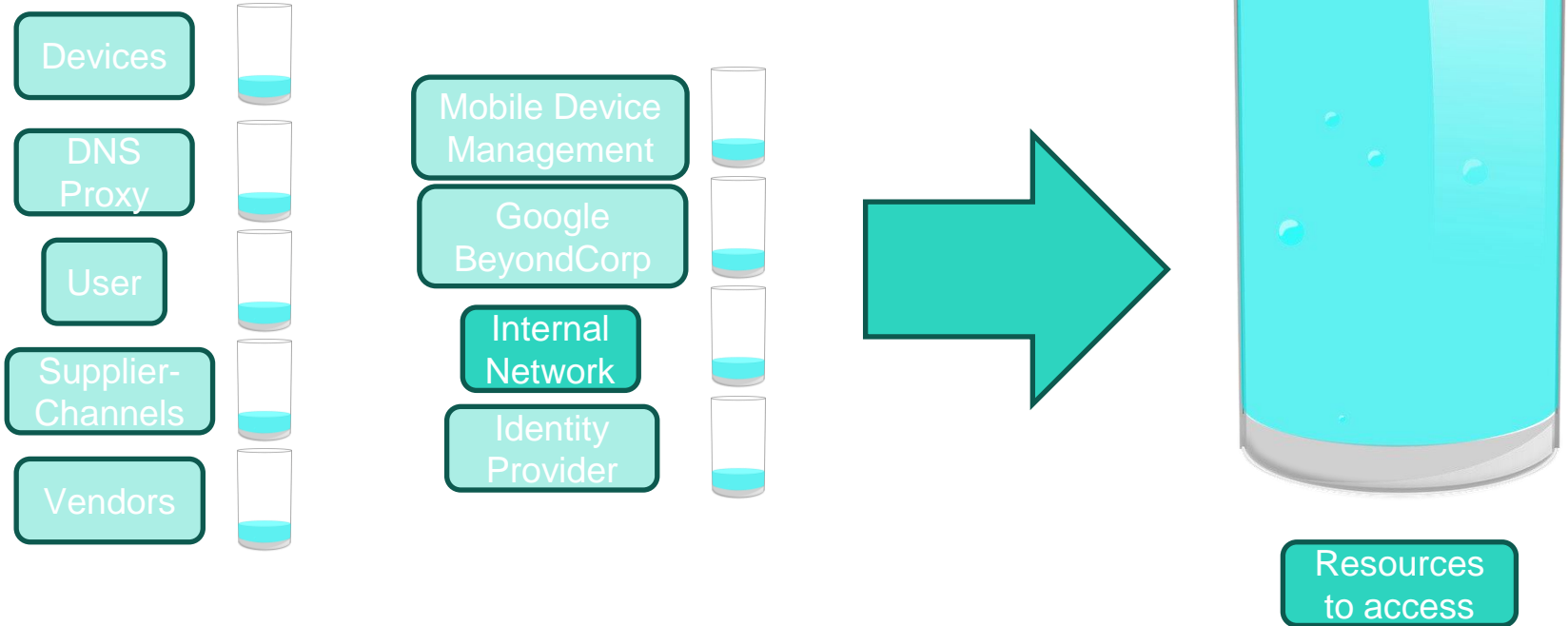
# System Components.



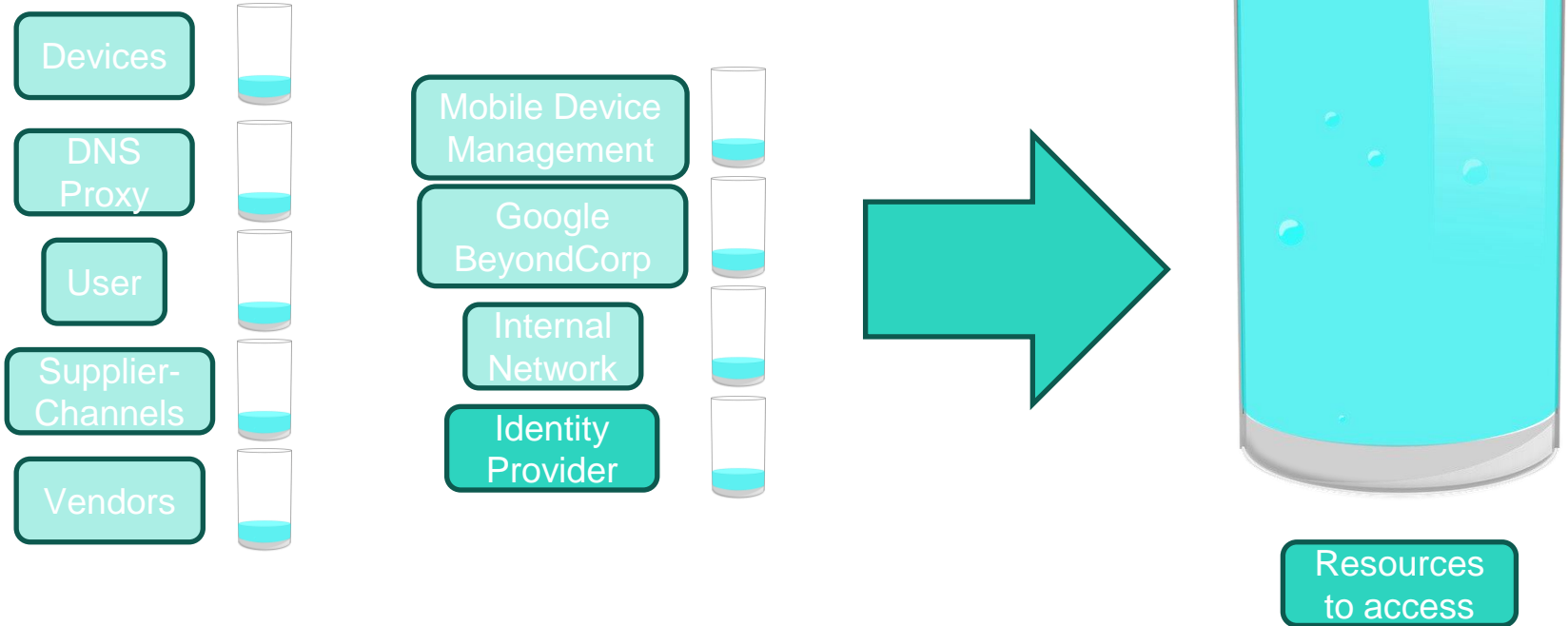
# System Components.



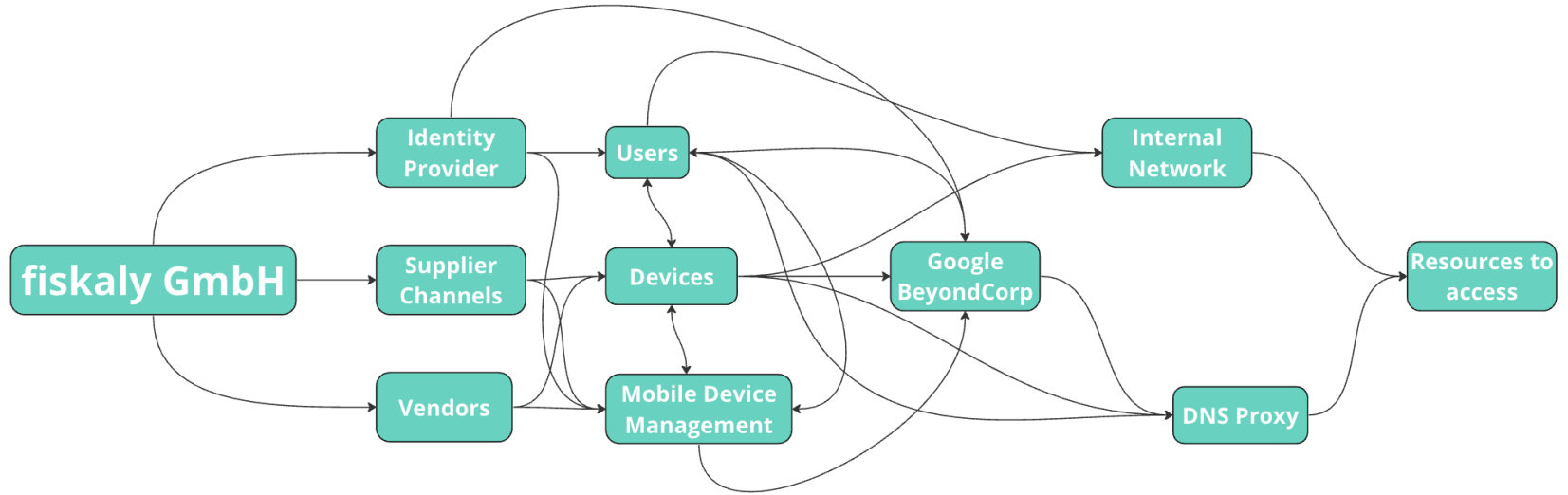
# System Components.



# System Components.



# The flow of trust.



# 7 Hacks for Zero Trust.







Know what  
you have.

*be a positive pessimist.*



**Lurphy's  
Maw.**

An aerial photograph of a snowy mountain slope with numerous skiers. The skiers are scattered across the frame, leaving tracks in the snow. The lighting is bright, creating distinct shadows for each skier. The overall scene is dynamic and active.

**Another**

**pillar**

**of Zero**

**Trust.**

# Risk Appetite.





Less is more.

*Sufficient stress can hardly be laid  
on the advantages of simplicity.*

*Alfred Holt*

# Processes.



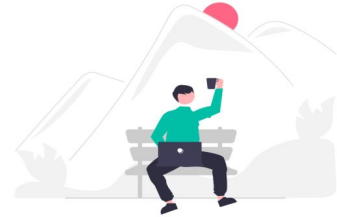


# Culture.

Zero Trust should  
make people feel  
secure.

# The *everywhere* office.

- We can *trust*, that resources only can be accessed if **all** parts of the system are trustworthy:
  - Only a **user** we trust...
  - ...from a **device** we trust...
  - ...which was delivered through a **supplier** we trust...
  - ...and is therefore managed by an **MDM** we trust...
  - ...can connect to an internal **network** or **DNS-proxy** we trust...
  - ...which **authenticates** only trustworthy users with trustworthy devices...
  - ... allows **access to resources**, as they come from a trustworthy **IP-range** and again authenticate themselves with trustworthy users from trustworthy devices.
- All communication in between different parts of the system is **encrypted**
  - Eliminates the need for a classic VPN
- Additional **supporting components**
  - Anti-Virus / Threat Prevention / Data Loss Prevention / 2FA / Role-based limited access / ...





Thanks!

Q&A?

