Google BeyondCorp

- company network has the same security level than the Internet
- workers can access the company services from everywhere
- they use managed devices
- access control on application / connection level
- access control also takes patch level and client location into account
Problems Solved by BeyondCorp

- the network that is secured by the perimeter is too large
- no clear perimeter in the cloud and datacenters anymore:
  -> example: vhosts, hosting providers
- when security relies only on the perimeter it is weak and should be considered as being broken.

Analogy:
  a) security by obscurity
  b) security by design
  -> perimeter = a)
Make the perimeter smaller!

- easier to grasp what is inside the perimeter
- higher confidence whether the perimeter is correct or not
- Analogy: trusted code base
- BUT: it is not disappearing
Focus on end points

- device management instead of perimeter security
- don't spend your time with putting up more and more perimeters
- keep your devices secure
SDN for Legacy

• * What happens with legacy devices like printers?  
  - in a completely open network these devices are accessible from the internet  
  - possibly unsupported with old patch levels

* SDN for protecting legacy devices  
  - security is implemented in the controller  
  - managed devices need adaptations as well  
  - but most devices could still be used in this scenario
What does this mean for the network? Two different solutions:

1. - simple network as infrastructure, security is provided end-to-end by the managed device and the server
   - access control at the end points
2. - network enforces security rules with SDN access control in the network by the controller
   - usable with legacy devices as well

* large perimeter at network edges is still useful for monitoring and additional security, but should not be the only source of security