BeyondCorp Overview

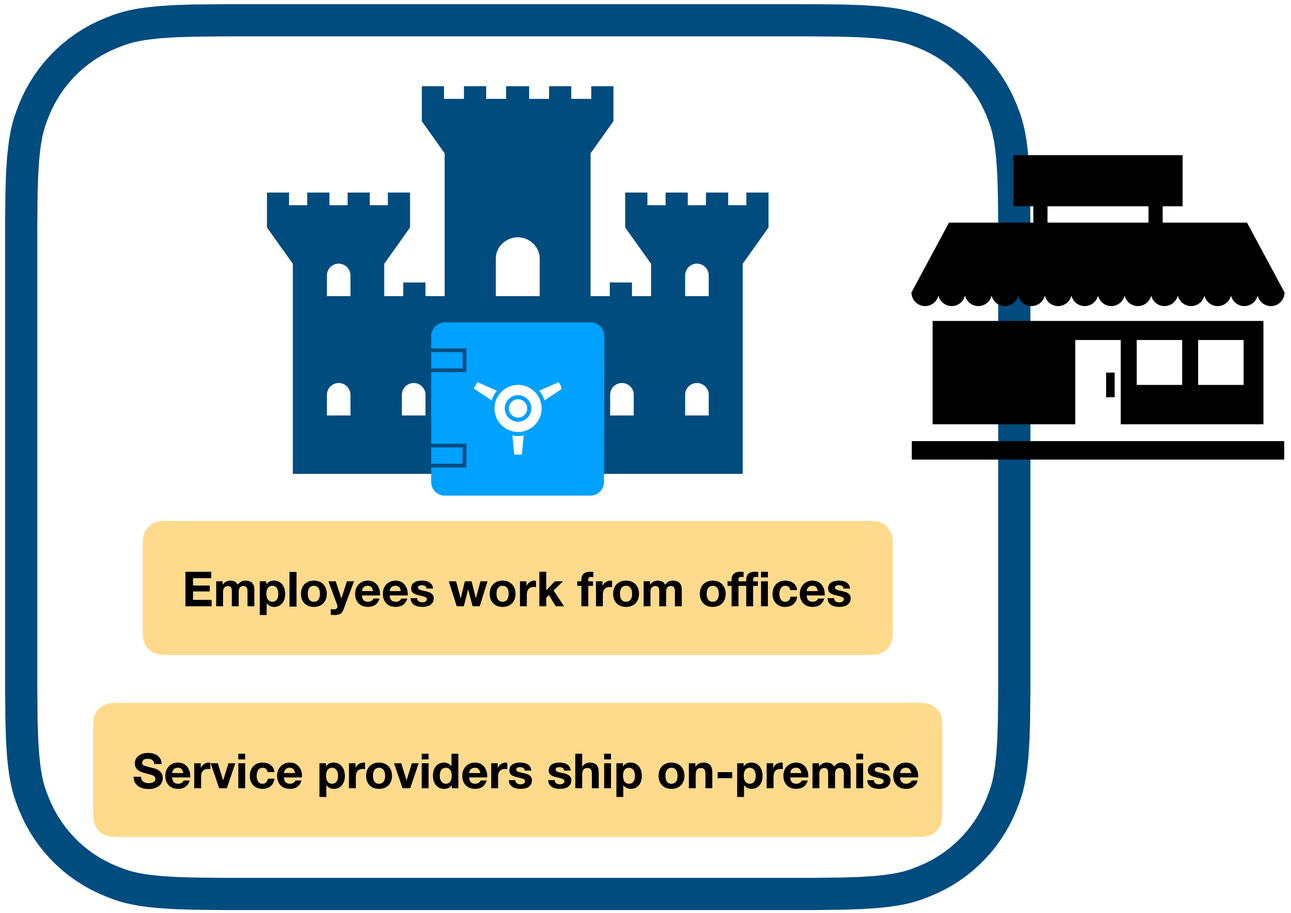
Maintaining Productivity While Improving Security

A shortlist of the Google BeyondCorp zero trust security strategy.

2021, Lukas Rieder

Traditional approach to security

The moated fortress.



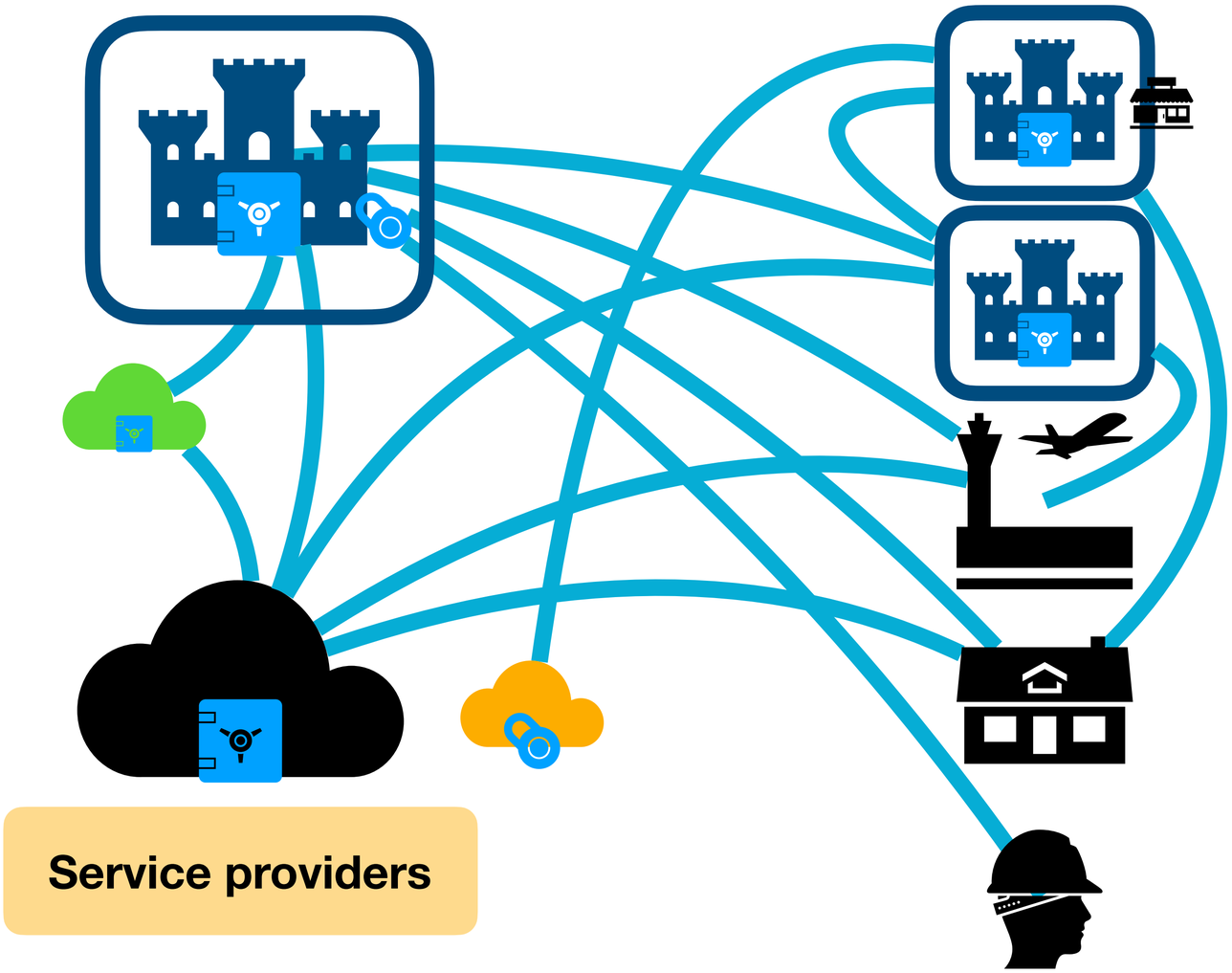
Employees work from offices

Service providers ship on-premise

Customers use public interfaces

Modern organisation

Organisations are evolving into dynamic, agile organisms.



Customers use public interfaces

Branches, subsidiaries, partners

Mobile workforce

Work from home

Externals

Service providers

A shortlist of the Google BeyondCorp zero trust security strategy.

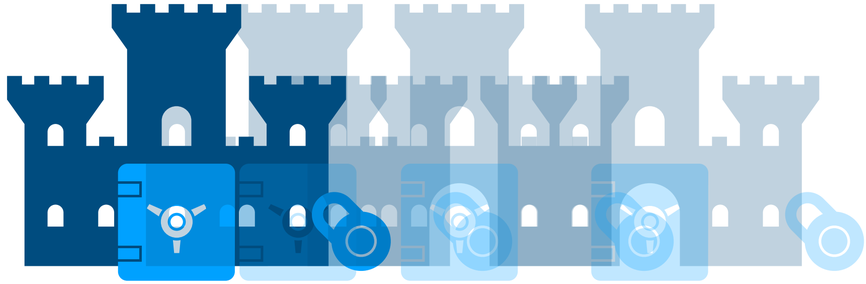
Problem: Security

The bigger problem: Productivity (or lack thereof)

- Traditional security models build upon perimeter security
- Growth, branching and size increase the complexity of traditional security models
- Adoption of cloud technologies increase the complexity of perimeter security
- Shift to dynamic mobilised work force increase complexity of security measures
- Resulting complexity suffocates productivity
- Complex perimeters are increasingly hard to master, endangering security
- One breach effects a whole perimeter, or worse, multiple
- One breach halts most productive processes, or worse, all

Problem: Scaling a fortress

Moated fortresses scale badly



- Each perimeter generally grants too much access
  - More fine grained perimeters are introduced
  - Redundant hybrid authentication solutions are introduced
- Re-centralisation efforts have increasingly higher costs, or fail, leading to partitions
- Externals cannot navigate the space, leading to silos and overly expensive solutions.
- Cross-team concerns are hindered, leading to data silos.
- Temporary grants may become permanent by accident, endangering security.
- Introducing service providers requires absorption into the organisation
  - Incompatibilities introduce follow up problems, patches and promote insecure solutions

Problem: Working with externals

Major drivers of change are hindered.

- High amount of technical on-boarding required to establish trust for externals
  - Slow expensive start due to extensive on-boarding procedures
- Projects with cross-team concerns hindered due to multiple perimeters or incompatible trust levels
- Potential to produce isolated solutions due to high cost of crossing perimeters
- Potential to produce redundant solutions, due to high cost of reusing modules from other teams
- Increasingly limited technological palette due to numerous highly regulated perimeters

BeyondCorp

Beyond the traditional security model

- Remove trust from the network perimeter
  - Zero trust to networks and network clients
- Securely identify devices
  - Device inventory databases with change tracking and metadata services
  - Device identity through certification
- Securely identify individuals
  - User and group management tightly integrated with HR
  - Single Sign-On System

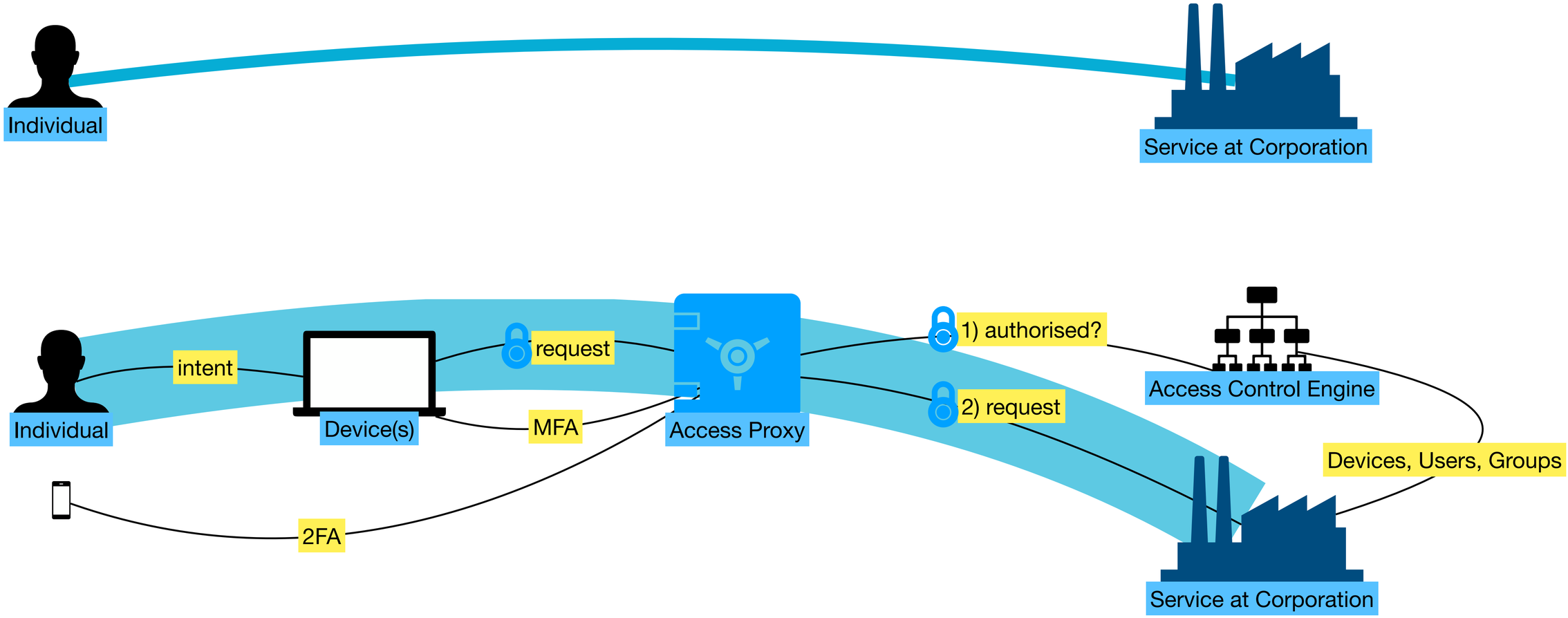
BeyondCorp

Beyond the traditional security model

- Externalise services to the internet
  - Public DNS, HTTPS
  - Internet-facing Access Proxies
- Implement access control on all endpoints
  - Access control engine handles access on a *per request basis*
  - Roles promote least privilege functional security grants
  - Inference of trust based on multiple data sources and many factors (inventory, users, groups)
  - Constant updates from data sources and factors to access control engine

BeyondCorp

Anatomy of an interaction



Securing externals

- BYOD or MDM
  - MDM, streamline MDM device availability
  - BYOD with multiple factors streaming into ACL Engine
- Central access control governs on- and off-boarding
- Small embedded self-sufficient teams in collaboration with the whole organisation
- Constantly transfer functional knowledge to employees
  - Avoid external silos and proprietary buy-ins
- Allow for rapid prototyping, but demand proper re-integration into the existing eco-system
  - Respect existing ACL services
  - Expose new services early with the same Access proxies
  - Quickly structure new services into existing user, group systems

References

- BeyondCorp: A New Approach to Enterprise Security
  Rory Ward, Betsy Beyer, ;login:, vol. Vol. 39, No. 6 (2014), pp. 6-11
  https://research.google/pubs/pub43231.pdf

- Migrating to BeyondCorp: Maintaining Productivity While Improving Security
  Betsy (Adrienne Elizabeth) Beyer Colin McCormick Beske Jeff Peck Max Saltonstall, Login, vol. Summer 2017, VOl 42, No 2 (2017)
  https://research.google/pubs/pub46134.pdf

- https://beyondcorp.com