AUSTIN ELLIOT

Case Study

Zero Trust Architecture (ZTA)

Challenge

The government client is migrating to a hybrid cloud platform. The platform is needed to enable architecture for 36 Government departments across many domains. To enable this, it is essential that there is a Zero Trust Architecture (ZTA) to underpin the platform, moving from the traditional methodology of access management on the boundary. With the ZTA the access management will be done at the application layer or data set. This will enable a federated ICAM approach with interoperability across all disparate architectures. Ultimately it will allow data of different security classification to be accessible on one network. Applications and data can be shared using Fine Grained Security.

Solution

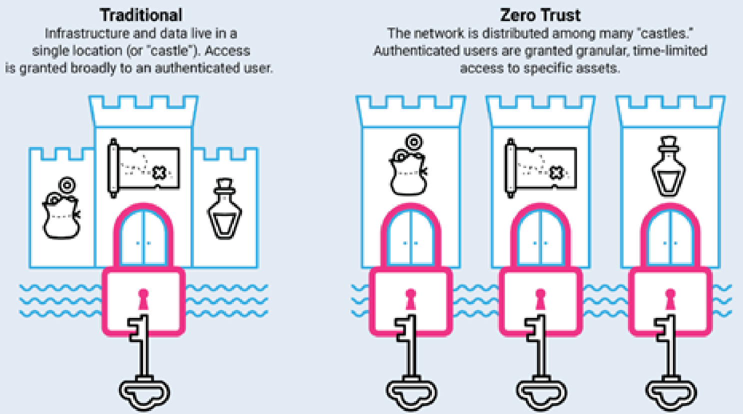
The team of Business Analysts and Systems Architects conducted a discovery, investigation and research piece on the existing architecture and available technology to understand how best to implement ZTA and a federated ICAM approach. This was done firstly across 3 agency domains then across 36 departments. We conducted technical focus groups and workshops to understand the As Is State and then to agree collegiately on the future vision, roadmap and concept of operations. This revolved around agreement on corporate directory services and attribute-based access control (DCS), orchestrated by Security Policy Enforcement Engine. We evaluated policy decision points, policy execution points and evolutionary capabilities.

System Design

Results

The team created a report recommending a vision of what the future architecture should look like along with roadmaps and a concept of operations to provide the ZTA as a service.

The developed roadmaps and CONOPS enabled the client to have a clear understanding of the architecture required with common agreement across the domain partners. They were then able to make an informed decision to establish the platform and deliver it to all sites.


Traditional
Infrastructure and data live in a single location (or "castle"). Access is granted broadly to an authenticated user.
Zero Trust
The network is distributed among many "castles." Authenticated users are granted granular, time-limited access to specific assets.