Operations Principles

Securely deploying the graph to production at scale

8. Access and Demand Control

> Grant access to the graph on a **per-client basis**, and manage **what** and **how** clients can access it.

Authorization in a data graph has two equally important aspects: access control, which dictates which objects and fields a user is allowed to access, and demand control, which dictates how (and how much) the user is allowed to access those resources. While access control is often talked about, attention also needs to be given to demand control, since it is critical in any production deployment of GraphQL. It is a mistake to allow users to perform any possible query regardless of cost, with no ability to manage its impact on production systems. Both access and demand control must be performed with full awareness of the semantics and performance of the data graph. It's not sufficient to limit a user to particular number of queries per minute without an analysis of the queries actually being sent, as a query could access a wide universe of services and the cost of a query can vary over multiple orders of magnitude.

Authentication in a data graph also has two aspects: the app that is requesting the operation, and the person that is using