

Azure Enterprise Ready Analytics Platform

The *big picture* illustrates key concepts in which Azure services in conjunction with authentication, firewalls and network integration provide the foundation for enterprise analytics.

Common data platform architecture enables data led cultures. Business users are empowered to explore and build on streamlined scalable and secure data platform

Data is **encrypted** to FIPS140 at rest and TLS enforced on all inter-service connections. Inter-region traffic travels over Azure's private internet backbone (dark fibre). Azure Policies lock configuration and alert of violations

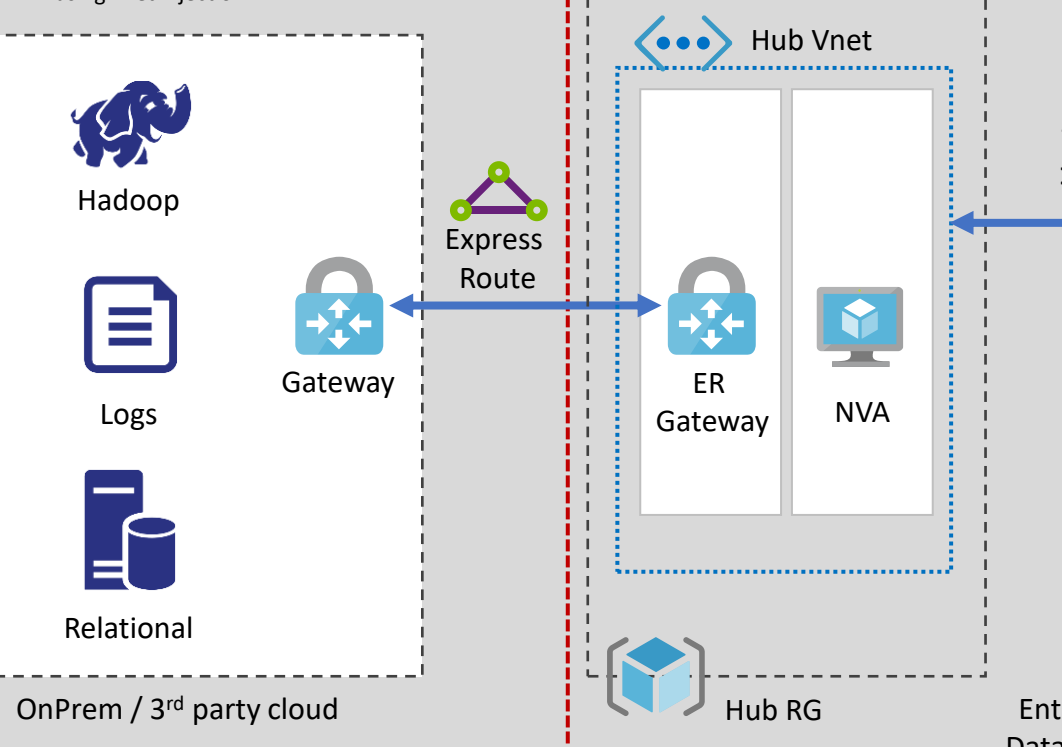
Out of box **audit logs**, monitoring, and alerts across entire estate are aggregated and presented centrally via Azure Monitoring

Active Directory authentication is interwoven throughout cloud fabric, enforcing policies, MFA, and conditional access

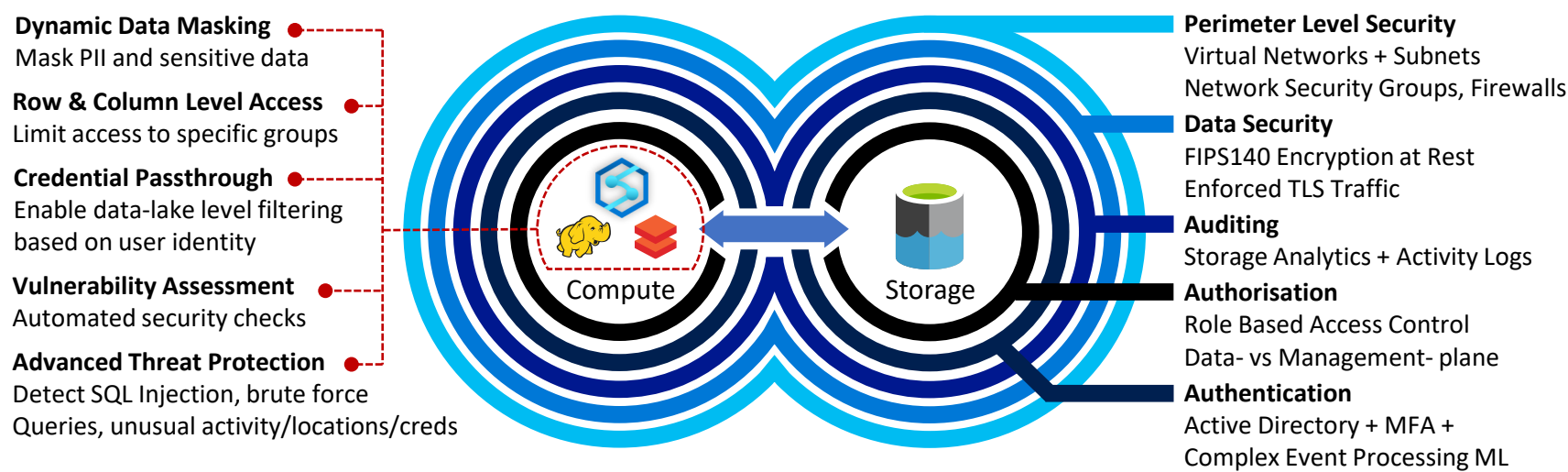
Separation of compute and storage enable agility to evolve processing. Data flows are CI/CD driven (Data DevOps) and are backed by repos that support different deployment strategies.

Microsoft John A.D. Mallinder
Cloud Solution Architect Data & AI

*1 ... vnet joined via 'private link' or 'service endpoint'
*2 ... using vnet injection



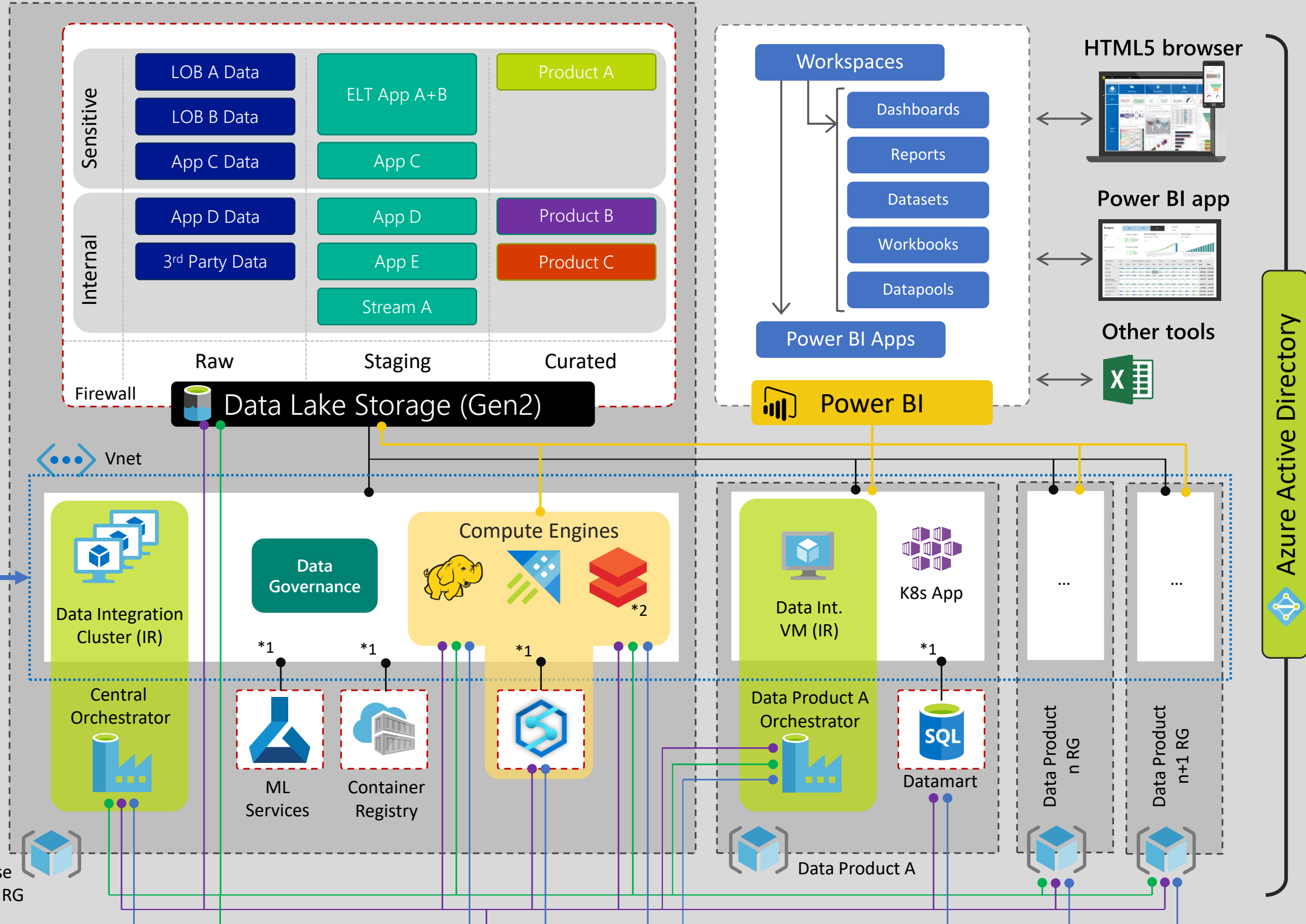
Multi-layered Security



Data Product Oriented Delivery



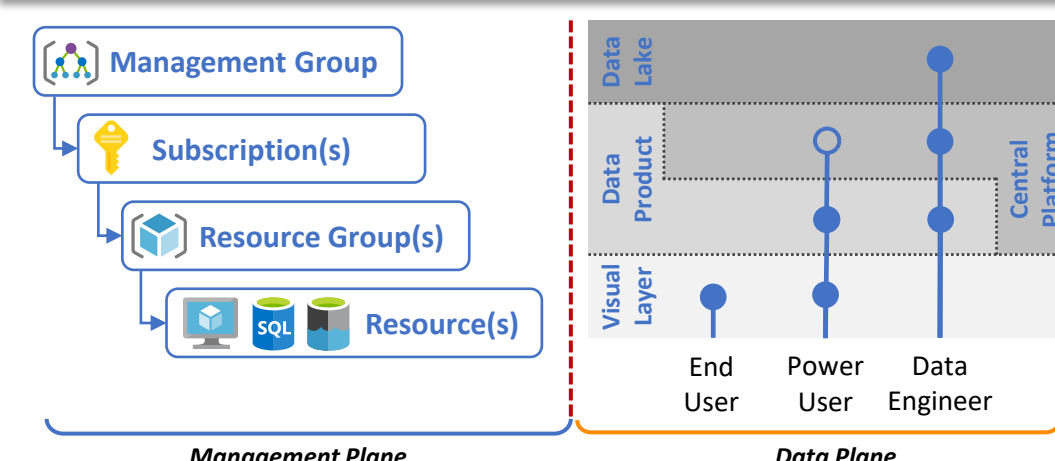
- Focus on reusability + scalability**
 - Policy enforcement
 - Data Quality + Compliance
 - Streamlined source system ingestion
 - Buildout + maintain catalogue
- Focus on driving business value**
 - Build-on core-services
 - Product delivery focused
 - Buildout + maintain catalogue



Account Types

- User Identity**
Active Directory uses employee credentials to authenticate against services, allowing admins to build fine-grained multi-layered access
- Managed Identities**
Particular Azure resources can be given a managed identity, allowing resources (i.e. SQL server, Databricks) to authenticate against other services (i.e. ADLS). Identity is embedded into Azure cloud fabric, thus no keys required reducing risk of key theft.
- Service Principals**
Conventional process automation approach. Identity created in AD and granted access to specific resources. Involves managing keys in key-vault to prevent plaintext keys appearing in code.
- Groups**
Simplify access control management using active directory groups, allowing to create standard role/access definitions.

Separation of Concerns



Abiding by principle of least privilege, support staff may have resource managing rights, however access to data plane is prohibited. Groups with data-plane access can be further restricted to different layers of data plane.

