

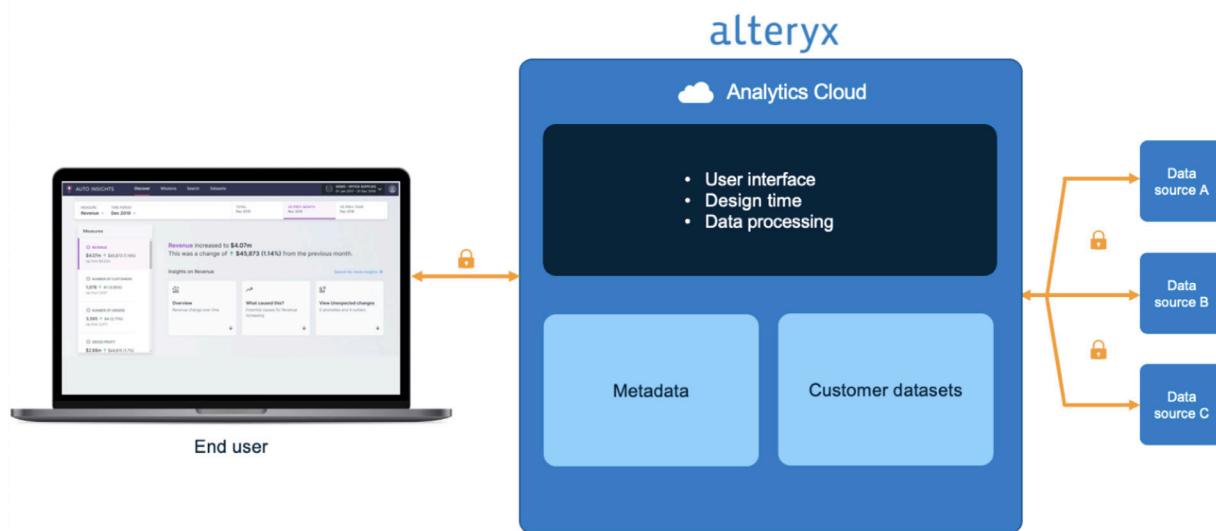
SOLUTIONS BRIEF

# Private Data Handling

An on-premises deployment model had been the de facto standard for enterprise software vendors for decades. Organizations maintained control and ownership of the software and their data. In theory, by keeping data in the organization’s environment, an on-prem architecture exposes no external connectivity. The obvious benefit of this approach was security and compliance.

A significant downside to this approach was large overhead investments in infrastructure and hardware and substantial reliance on IT departments to manage hardware and software. Users were also rarely getting the latest and greatest features because IT had to confirm compatibility with existing systems, and upgrades could take years in some cases.

The SaaS approach flipped this model on its head. Software vendors would host the software in their environment, and users would access it through a browser. This enabled quick deployments, painless software updates, reduced burden on IT departments, and in general, lower costs for organizations. Organizations rapidly adopted this model because of the scalability and flexibility it provided.



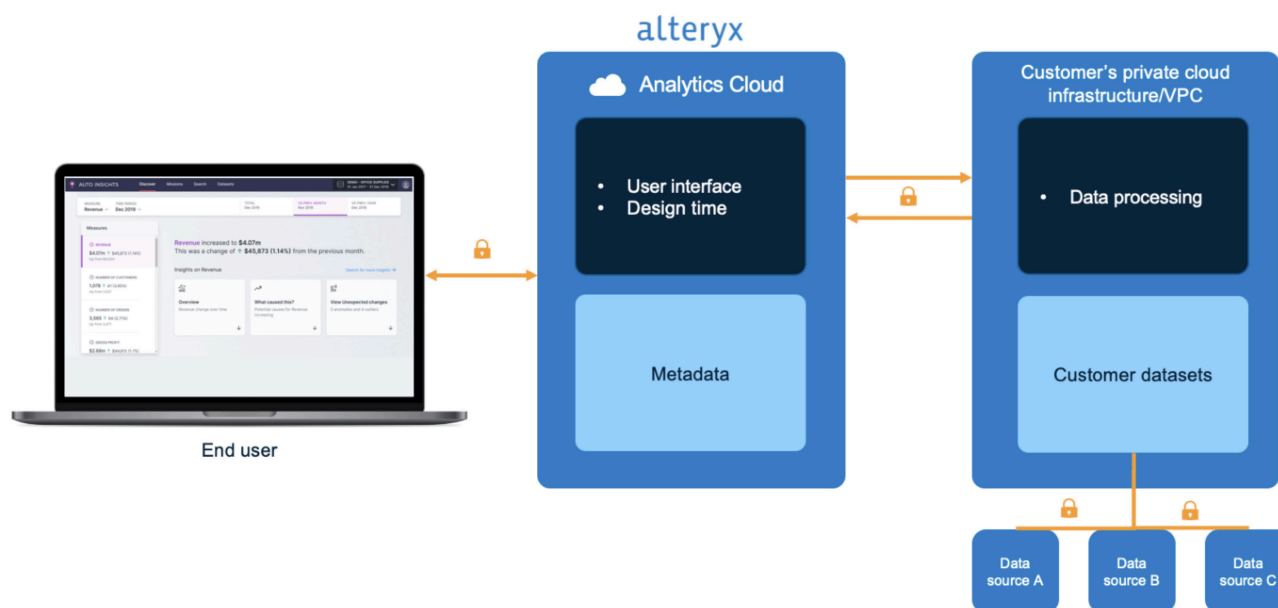
This model has become the new standard, but there was one complication – data. SaaS vendors have robust security in place to encrypt and protect an organization’s data, but the data is still in the vendor’s environment. As organizations generated and captured more and more data and increasingly leveraged the cloud and SaaS applications, serious security concerns were raised along with increased scrutiny around how this data is accessed and used.

In the age of the GDPR, CCPA, HIPAA, and other rules and regulations on data protection, keeping track of and securing data is a priority. In some cases, the SaaS model doesn’t work for many organizations.

How do you get the security and governance of an on-premises solution with the ease of deployment and convenience of SaaS?

## Private Data Handling

Alteryx believes many customers are best served with a hybrid approach: private data handling, which enables private storage and processing in a SaaS-based solution. Application experiences and metadata stay in the hosted SaaS application, while customer content stays in the organization’s environment.



The Alteryx Analytics Cloud encapsulates data storage and data processing into modules that customers can run in their own private cloud infrastructure. Private data handling leverages best practices and architecture improvements to combine the security and governance of on-premises solutions with the ease of a SaaS deployment.

When customers configure private data handling, Alteryx Analytics Cloud continues to provide the “control plane,” which hosts the user interface, powers users’ design-time experience, provides user management, and enables sharing and scheduling capabilities.

The control plane interacts with the organization’s “data plane” in running its virtual private cloud. Data runtime operations (such as accessing, processing, and storing customer data) are delegated to this private data plane. Alteryx offers customers the agility of a SaaS offering with the compliance, security, and governance of an on-premises solution. No customer content is stored or persisted on Alteryx-owned infrastructure.

Hosting the user interface in Alteryx’s environment means that organizations get access to new, innovative features and functions as they are released. Customer IT teams don’t have to manage different software versions and slow upgrade cycles – they can rest assured that internal users will be updated to the latest and greatest release.

Finally, another benefit is that this architecture enables organizations to deploy software quickly and accelerate time to value, deriving immediate impact from Alteryx Analytics Cloud.