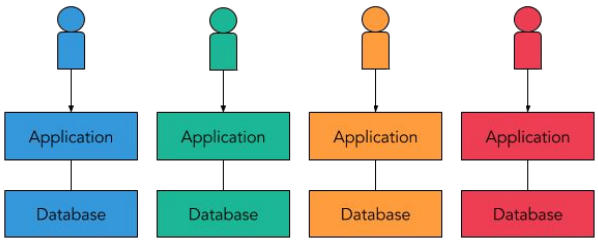
Single-Tenant vs. Multi-Tenant Enterprise Software

Choosing between single-tenancy and multi-tenancy comes down to an organization's business objectives and requirements. Which trade-offs are you willing to make?

SINGLE-TENANT



In a single-tenant architecture each company, or tenant, has their own instance, separate from any other customer. With a single-tenant solution the risk of another business accidentally receiving another customer's user data is eliminated.

Benefits

Enhanced security

Single-tenancy delivers true data isolation resulting in maximum privacy and enhanced security. The possibility of data leakage between tenants, whether accidentally or through sabotage, is removed making this architecture a popular choice for large enterprises. To increase security, customers can implement a firewall at any layer to protect data. For example, the identity provider APIs can be located behind a firewall while the OAuth login system resides in the public facing network.

Regulatory compliance

Enforcing regulatory requirements is easier due to complete control of the environment. If your company policy does not allow data to be transmitted outside of your country (i.e. German Data Regulations or GDPR regulations) a multi-tenant solution needs to be specifically designed for this. A single-tenant solution makes this as simple as installing the software on a server in Germany. Similarly, compliance with regulations such as PCI, HIPAA and SOC2 is simplified because data is secured, encrypted and protected separately for each tenant.

Single-Tenant Key Benefits

- Security
- Compliance
- Customization
- Upgrade control
- Data recovery
- Performance
- Failure isolation

Multi-Tenant Key Benefits

- Cost
- Automatic upgrades
- Instant on-boarding

Customization

With a single-tenant architecture, the software environment can be customized to meet customer's business needs; robust plugins can be installed to maximize personalization without limitation.

Upgrade control

Customers have decision authority over the upgrade cycle. Customers can choose what updates they want to install and when. This adds flexibility for scheduling maintenance windows and downtime without impacting others.

Data recovery

Data extraction is an important consideration that is often overlooked. If a service is acquired or shutdown it's wise to consider how you will retrieve your data in advance; it is easier to export data from an isolated, single-tenant cloud.

Drawbacks

Cost

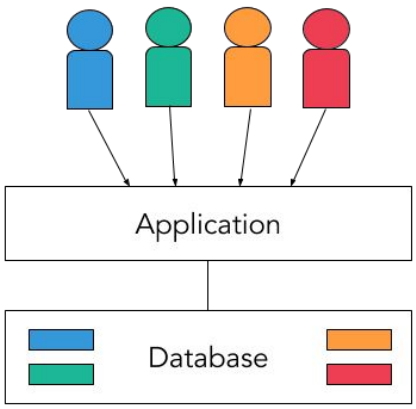
Since this is not a shared infrastructure, customers have to pay the cost of the entire system (hardware and software). However, with the rise of low-cost hosting providers, like AWS and Azure, the cost for single-tenant solutions is becoming more affordable.

Provisioning

To set up new customers, servers must be provisioned and the software must be installed on each server. This process has been made simpler through the use of APIs provided by hosting providers and tools such as Kubernetes and Chef.

MULTI-TENANT

Multi-tenant is an architecture where multiple companies store their data within the same infrastructure. The entire system can span multiple servers and data centers, but most commonly data is co-mingled in a single database.



Benefits

Cost reduction

One of the big drivers is cost. The sharing of infrastructure and resources significantly reduces the overhead of the service provider, and as a result, lowers the costs imposed on customers.

Automatic upgrades

Multi-tenant systems ensure that software updates, including security patches, are rolled out to all customers simultaneously. This standardizes software versions utilized by customers and eliminates version control issues.

Instant on-boarding

In most cases, new customers can be setup by creating a new logical tenant. No new servers are provisioned and software installation is not required, which makes this process instantaneous.

> The instances (tenants) are logically isolated, but physically integrated.
>
> Gartner

Drawbacks

Performance

One tenant's heavy use or load spike may impact the quality of service provided to other tenants. In addition, when software or hardware issues are found on a multi-tenant database, it can cause an outage for all customers.

Security risk

If a hacker gains access to one tenant's data, they can access data from every tenant because all data resides in a single database.

Single point of failure

If the multi-tenant system goes down, **EVERYONE** goes down. In contrast, failure can be isolated with a single-tenant system.

DATA LEAK: Office 365

A multi-tenant architecture enables tenants to share the same infrastructure, but any interaction between tenants should be prevented. The ability to access another customer's data is a breach of security and can destroy confidence in multi-tenant environments.

In August 2017, Microsoft leaked Office 365 usage data, names and email addresses across the multi-tenant Admin Center. The breach affected users in multiple Office 365 data center regions, including both the United States and EMEA, according to Petri.

While this data breach was handled quickly, "the regulations are clear that this is a leak. As such, the EU could fine Microsoft up to 4% of its global revenue, which is enough to make your eyes water."

> System vulnerabilities, or exploitable bugs in programs, are not new, but they've become a bigger problem with the advent of multi-tenancy in cloud computing. Organizations share memory, databases, and other resources in close proximity to one another, creating new attack surfaces.
>
> InfoWorld

CONCLUSION

There are benefits and drawbacks to both single-tenant and multi-tenant systems. Ultimately, a company must decide what is most important to their business and what can be sacrificed. Choosing your deployment environment depends on a variety of factors.

Is cost a primary driver? Does your industry vertical have unique regulatory constraints? Is security critical for the type of data you are storing? Do you want a system that you can customize without limitations? Or are you happy using a one-size-fits-all system?

At FusionAuth, we believe that each customer has unique business cases that often require customization to solve. Security is a core focus of our business. Therefore, FusionAuth, unlike other CIAM solutions, is single-tenant. This architecture provides each of our customers with their own infrastructure. They remain in complete control of their data, upgrade schedule and can rest assured their data is separate and secure.

> Concerns over security in multi-tenant environments have led to many organizations choosing to switch to single tenant infrastructure as a service to mitigate the risks of co-located data. Despite the extra cost, this is a sensible and advisable solution.
>
> TechTarget

About FusionAuth

FusionAuth was designed and built by security and identity experts with over 50 combined years experience developing software for Fortune 500 companies. It installs in minutes and delivers Customer Identity and Access Management including login, registration, SSO, MFA, emails, localization, reporting and powerful user management features.

FusionAuth has been battle-tested in high-volume industries from finance to gaming and deployed on servers around the globe. For more information, visit fusionauth.io.