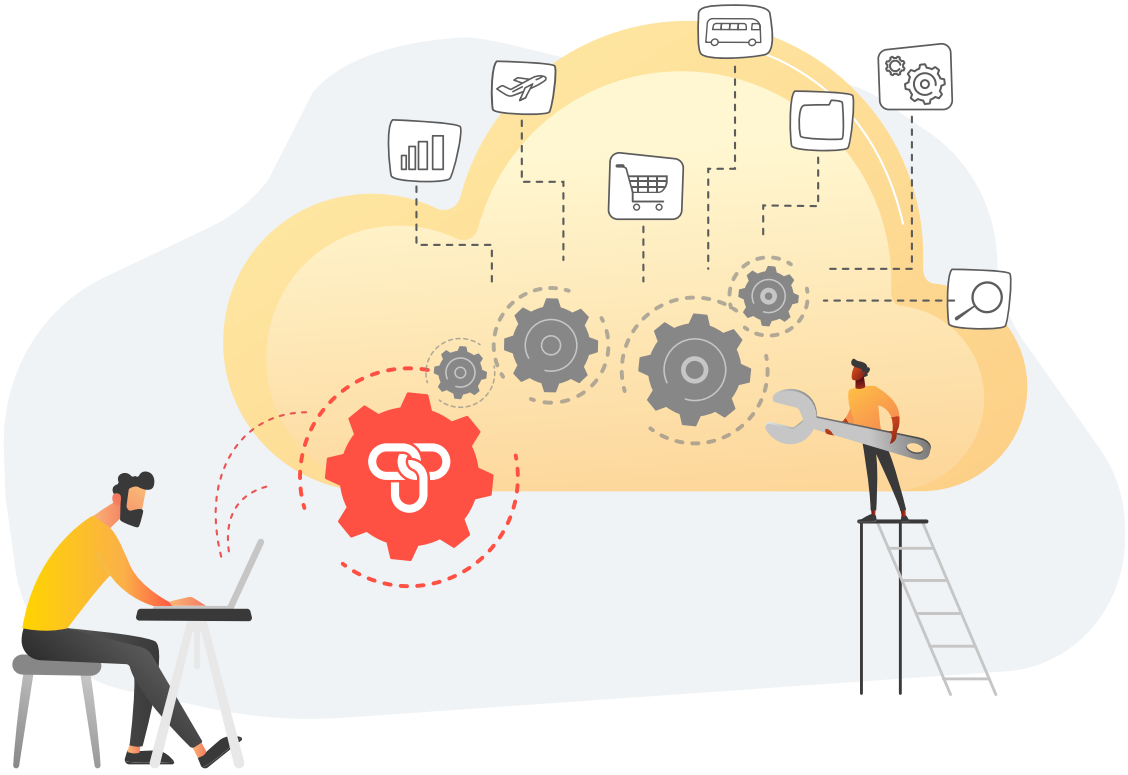
Securing the microservices ecosystem

TrustBuilder®

Microservices are hot. Market researcher IDC estimates that microservices architectures will account for 80% of application development on cloud platforms by the year 2021. The microservices architecture differs radically from the traditional 'monolithic' applications which are built and deployed as a single unit. Microservices are small, independently versioned and scalable services. Each of these services fulfills a specific goal. Using interfaces and standard protocols, they work together to address a more complex business goal.

Microservices allow development teams to work separately on these smaller fragments, rather than orchestrating everything they do with their colleagues. Developers can build microservices faster and get more flexibility in making changes without affecting the rest of the architecture.

While microservices are heaven to developers, they might be hell to anyone involved in security. Whereas monolithic apps usually have just a few access points, microservices have many, which all need airtight security to protect them against the outside world. TrustBuilder Identity Hub offers unique functionality to address these security issues and, in doing so, combines customer experience with complete security.



An ecosystem of APIs

- Access to applications has increasingly become a matter of system-to-system communication, where applications access each other on behalf of a human user.
- Companies are forging partnerships, offering third-party applications and allowing their customers access to these applications through Application Programmable Interfaces (APIs).
- This has given rise to an ecosystem of APIs and microservices that should not be exposed to the outside world, unprotected.
- API attacks have long stayed under the radar, but some recent high-profile breaches have made API security more prominent.
- The ability to control API access is the cornerstone of effective API and microservice security.

Security does not stop at the edge

- While API Gateways take care of basic security, only an IAM system such as TrustBuilder provides adequate security in complex environments with hundreds of APIs.
- Many IAM systems secure microservices only at the edge, not between the microservices themselves.
- TrustBuilder Identity Hub addresses security of these APIs on an individual level, authenticating identity and privileges at each hop. Whenever a token is passed on from one microservice to another, the user context defines the user access to different microservices.
- TrustBuilder acts as a single entry point, invoking multiple back-end servers and aggregates the results in attributes that can be customized and returned to the requester along with the appropriate authorization.
- Contrary to many other IAM systems that only consider users, TrustBuilder provides security for both users and APIs in one single system.

Find out more on www.TrustBuilder.com or drop us a line at info@TrustBuilder.com

Growing the business, securely

- Thanks to TrustBuilder's centralized policies, we secure both monolithic applications and microservices, no matter where they reside: in the cloud or on-premise.
- Acting as a token exchange, TrustBuilder Identity Hub allows easy integration with multiple third-party applications, thus enabling the ecosystem to be developed.
- Adding a new provider to the ecosystem is enabled by extending standard policies. Following that integration, the customer and other applications can interact with the newly added application, including microservices. New microservices can be added easily, benefitting from the existing security mechanism.
- TrustBuilder Identity Hub hides the complexity for end-users, thus increasing customer experience. Once a user is authenticated, TrustBuilder captures the user context to allow access to those microservices that the user has privileges to.

The best of both worlds

Organizations that deploy TrustBuilder Identity Hub to secure their microservices get the best of both worlds: they continue agile development, gain maximum security and maintain seamless customer experience.