

# Zero Trust: Because perimeter security isn't enough anymore



## Assume breach. Never trust. Always verify.

Zero trust is a framework that assumes that an organization's security is always at risk to internal and external threats. It addresses security challenges related to cloud adoption and hybrid and remote workforces.

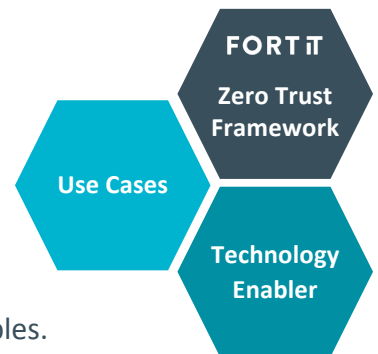


## FortIT supports you in the strategy, architecture design and implementation of a Zero Trust approach for your business

FortIT guides you through your Zero Trust life cycle – from analysis to implementation.

Our framework helps you align the Zero Trust architecture to your organization's use cases for successful implementation.

10 years of average team experience in proven solutions and technology enablers support the implementation of Zero Trust principles.



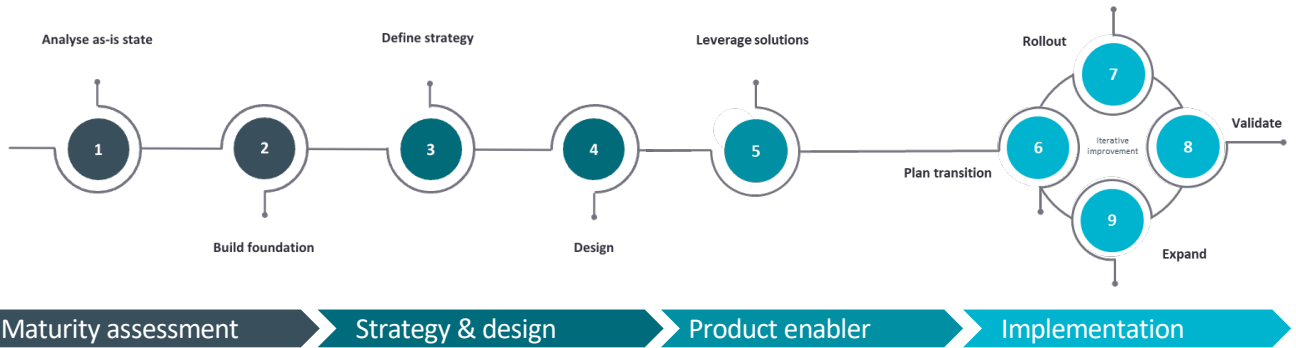
## Your benefits

- ✓ **Increased security:** Mitigate risks by closing security gaps and curtailing lateral movement, effectively protecting both company and customer data.
- ✓ **Enhanced flexibility:** Enable secure remote work, BYOD policies, and the use of cloud services for a modern, adaptable work environment.
- ✓ **Reduced complexity:** Streamline your security posture by eliminating redundant measures and simplifying policy implementation.
- ✓ **Lower costs:** Centrally manage access rights for a more efficient audit process and re-certification of access rights, thereby lowering operational costs.
- ✓ **Business enabler:** Empower your business operations with a robust security framework that not only protects, but also enhances operational efficiency and regulatory compliance.

# Expert guidance and support every step of the way to Zero Trust



Implementing a Zero Trust approach across an enterprise is a challenging undertaking. FortIT supports you through every stage of your journey.






**Maturity assessment:** We support you in determining your current Zero Trust maturity via workshops, interviews and architecture analysis. Together we define a target level of maturity.

**Strategy & design:** We outline system boundaries, use cases, goals, and requirements, subsequently crafting a Zero Trust strategy and a roadmap for iterative maturity growth.

**Product enabler:** Market analyses and SWOT review guide us in defining the ideal Zero Trust model. A proof of concept is conducted to validate this target.

**Implementation:** We detail an iterative implementation plan, assist in vendor selection, and design training modules. Post-implementation, we validate and support further development.

## Leverage our expertise and experience for your success

-  10+ years' experience in the applied implementation of Zero Trust
-  Partnerships in the academic environment for Zero Trust and application security
-  Comprehensive expertise on Cloud Security, IAM (Identity and Access Management) and DevSecOps.

Contact us today!

[www.fort-it.ch](http://www.fort-it.ch)



**Michael Schläpfer**  
CEO  
michael.schlaepfer@fort-it.ch



**Saner Çelebi**  
Head Consulting Services  
saner.celebi@fort-it.ch



**Chris Venetz**  
Zero Trust Lead  
chris.venetz@fort-it.ch

