FORTIT
SECURE DIGITAL BUSINESS

All you need to know about applied Zero Trust

Zero Trust: Because perimeter security isn't enough.

Zero trust is a framework that assumes an organization's security is always at risk to external and internal threats:

- Business processes are strongly driven by digital transformation. Classic security concepts reach their limits.
- Users, applications and data increasingly move outside the corporate perimeter and sphere of control.
- Advanced threats move within the perimeter - the "trust but verify" approach is no longer an option.
- Cyber threats continuously increase. Companies are forced to increase their resilience against cyber threats.

Assume breach, never trust, always verify.

Embrace the benefits of a Zero Trust Architecture

A Zero Trust Architecture provides several benefits and leads to a more efficient and effective IT-Landscape. It reduces cyber security risks, and acts as a business enabler for new access use cases in a digitized enterprise.

Increased security

- Visibility on activities around your resources for an effective detection of suspicious behaviour or security breaches.
- Closing security gaps and minimizing the risk of lateral movement and thus protecting company and customer data.

Business enabler

Anywhere, anytime access
Employees and customers have secure access to data from anywhere, at any time, via any device.

Cloud & Digital Transformation
Enables digital transformation with intelligent security measures in complex distributed environments.

Reduced complexity

Reduction of the security stack

- Removal of overlapping security measures and minimization of complexity in policy implementation.
- Consolidated policy management
- Access Policies for can be efficiently created and managed in a common policy language for all resources.

Cost reduction

Efficiency increase for analysis and response

- Complete visibility of devices in your network which are constantly tracked for faster detection, response after a security incident.
- Higher audit efficiency
- Central verification of access rights for efficient audit and re-certification of access rights.

Overcome typical challenges

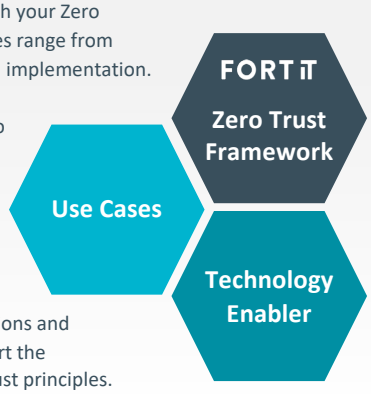
Implementing a zero trust approach throughout an enterprise comes along with several challenges. FortIT can support you on your journey.

Strategy
Unclear strategies make the company-wide introduction of zero trust principles difficult.
Zero trust target architecture as an overall implementation concept is not aligned with corporate strategy.

Awareness
Lack of knowledge and expertise, often influenced by security solution providers.
Lack of common understanding and misaligned approaches on different levels.

Complexity
Heterogeneous IT infrastructure with legacy components.
Multitude of existing technologies and lack of orchestration.

- ✓ FortIT can guide you through your Zero Trust Life-Cycle. Our services range from analysis and conception to implementation.
- ✓ Our framework helps you to align the architecture with 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 journey to a successful ZeroTrust Implementation

Analyse as-is state
Analyse existing IT architecture and processes to understand current Zero Trust maturity
- Target maturity determination

Define strategy
- Set goals & define strategy to meet target maturity
- Determine scope of application
- Develop a high-level roadmap

1 2 3 4

Build foundation
- Create common understanding
- Ensure management support

Design
- Define Zero Trust Model / Design Patterns
- Develop architecture
- Determine organization and processes
- Roadmap for continuous maturity increase

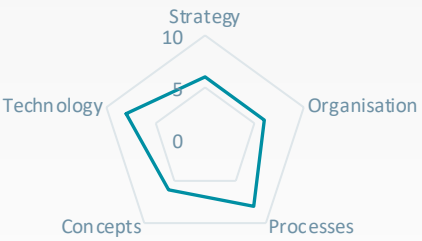
FORTIT

Maturity assessment

Starting point
- Unclear understanding of the existing situation regarding Zero Trust.
- Lack of know-how in the implementation of Zero Trust.
- Unclear understanding of readiness to implement Zero Trust.

FortIT services
- Conduct workshops, interviews and document analysis.
- Analyse the IT architecture taking into account all systems.
- Evaluate existing relevant Zero Trust processes.
- Examine ongoing activities and in-flight initiatives
- Ascertain zero trust maturity applying FortIT Zero Trust Framework based on the analysis results.
- Decide on the Zero Trust target maturity.

Sample deliverables
- Architectural overview (current situation)
- Process map (current situation)
- Overview of all ongoing activities
- Current Zero Trust maturity and proposed target maturity



Sample zero trust maturity spider diagram

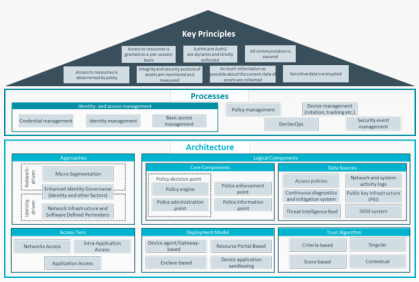
Your added value
- ✓ Fact-based view of your current situation, taking into account all people, process and technology measures.
- ✓ Qualitative analysis about the maturity of Zero Trust.
- ✓ Basis for initialization Zero Trust implementation activities and roadmap.

Strategy and design

Starting point
- Existing overview of the actual situation.
- First vision on the implementation of Zero Trust.
- Lack of Zero Trust strategy.

FortIT services
- Definition of the scope: system and process boundaries, surrounding systems, delimitations.
- Determine the use cases, goals and requirements, derive a zero trust strategy.
- Development of zero trust processes, design patterns (building blocks) and architecture variants.
- Definition of a Zero Trust Roadmap as a planning basis for an iterative increase in maturity.

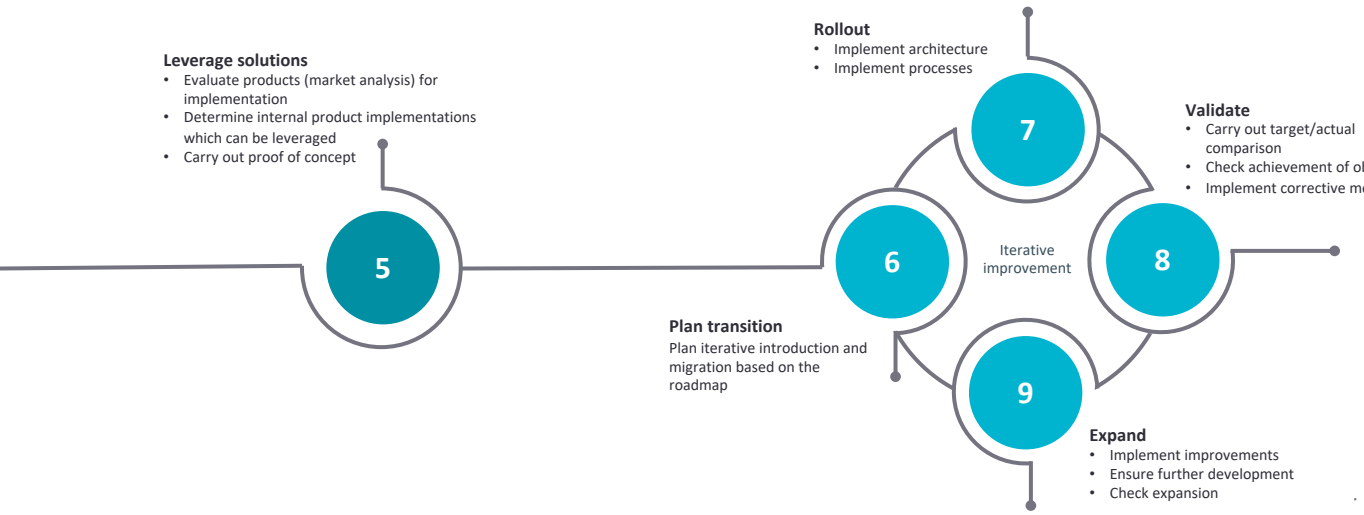
Sample deliverables
- Zero Trust Strategy
- Process map (target situation)
- Zero Trust Model / Design Patterns
- Target architecture



FortIT Zero Trust Architecture Building Blocks

Your added value
- ✓ Common understanding of Zero Trust.
- ✓ Unified Zero Trust Strategy.
- ✓ Implementable target architecture.
- ✓ Zero Trust know-how.

A clear path to your desired Zero Trust maturity level



Product enabler

Starting point

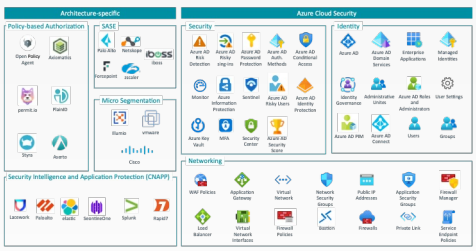
- Existing Zero Trust strategy and design
- Precise idea about the implementation of Zero Trust
- Specific project plan

FortIT services

- Carrying out market analyses.
- Definition of implementation options (SWOT) with recommendations for action.
- Developing the target picture for implementation.
- Conduct a concept validation:
  Specify, plan and implement a proof of concept (PoC).

Sample deliverables

- Market analysis and product comparison
- Implementation variants
- Proof of concept



FortIT Zero Trust Technology Enabler Map

Your added value

- ✓ Independent clarity on enabling products
- ✓ Planning and quality confidence for implementation.
- ✓ Clarity on feasibility of Zero Trust architecture.

Implementation

Starting point

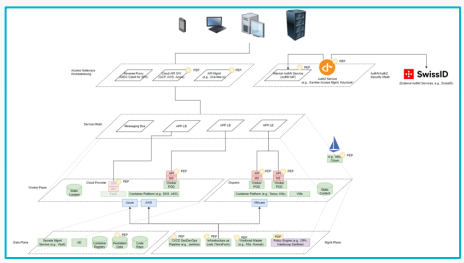
- Validated Zero Trust concept.
- Defined product strategy.
- Detail specification.

FortIT services

- Determine an iterative implementation plan based on the selected implementation option.
- Implementation of the procurement.
- Create a migration, operation and training concept.
- Support with the implementation (rollout).
- Carry out validation to ensure correct implementation and correct implementation and achievement of objectives.
- Support for improvement and further development.

Sample deliverables

- Transition planning and Detail specification
- Migration, operation and training concept
- Implementation validation
- Improvement and further development measures



Sample Zero Trust deployment architecture for microservices

Your added value

- ✓ Implemented Zero Trust concept in line with the strategy
- ✓ Clearly regulated responsibilities and processes

Success stories

Design of Zero Trust architecture patterns

Background: A large Swiss banking group is increasingly focusing on cloud technologies and cloud native development. To complement the on-premises PaaS solution based on Openshift, it will also be possible to run workloads on hyperscalers (Azure, AWS, GCP) in the future. They have a strong interest for access policy automatization in cloud native applications and a seamless integration into their Dev(Sec)Ops Lifecycle.

Role of FortIT: Analysis of baseline architecture and documentation of existing access control systems. Design and implementation management of policy management processes for central governance and dynamic control of access authorizations. Market analysis of current technology enablers for fine grained access control. Design architecture patterns on how to secure communication between frontend and backend systems (Machine to Machine) with policy-based access control according to Zero Trust principles.

Added value for our client: Awareness and common understanding of Zero Trust Architecture. Automation and central control of authorizations by using a policy engine (Open Policy Agent). Clear processes and responsibilities for policy management.

Conceptualise Zero Trust access management

Background: A large Swiss Logistics Corporation's hybrid multi-cloud led to increasingly more different systems and workloads being scaled elastically in different environments. The distribution of workloads made it difficult to verify whether specifications and directives are adequately implemented. FortIT was asked to develop a concept for Externalized Authorization Management.

Role of FortIT: Creation of a target architecture for policy-based access to services and corporate resources based on the FortIT Applied Zero Trust architecture blueprint. Based on the defined target architecture, a policy management and deployment solution for the central administration and monitoring (compliance) of access was evaluated and introduced. Definition of processes and responsibilities for the administration (creation, mutation) of policies in consultation with different stakeholders, including training of staff.

Added value for our client: Modern access control based on policies. Central overview (compliance) and management of policies. Clearly defined responsibilities and processes for creating and managing policies.

Develop Zero Trust architecture 2025

Background: A large Swiss Bank Group was trying to reduce the risk from cyber attacks and, at the same time, to take into account an increasingly emerging hybrid way of working and hybrid infrastructure. The implementation of various measures in the area of zero trust is intended to increase resilience to cyber attacks and at the same time serve as a business enabler by enabling a hybrid way of working.

Role of FortIT: Structural analysis of the entire IT infrastructure, processes and existing access control systems. Determination of the current Zero Trust maturity and definition of the target maturity. Analysis of the risks arising from current state. Design of a Zero Trust target architecture and implementation plan based on FortIT's Applied Zero Trust framework. Develop prioritised measures showing the cost-benefit ratio. Market analysis of different technologies for the implementation of the target architecture.

Added value for our client: Company wide, common definition of Zero Trust. Show the current risk-based threat level due to the lack of zero trust measures. Strategy for the step-by-step improvement of Zero Trust Maturity.

Key take aways

Why Zero Trust?

- ✓ Secure access through adaptive access management: authentication & authorization based on contextual information and risks.
- ✓ Appropriate protection of cloud resources: Dynamic segmentation based on policies (per workload)
- ✓ Minimize security incidents through Security Operation: Continuously identify, analyse and respond to suspicious activity.

Increasing your Zero Trust maturity brings you the following added value

Why FortIT?

Our expertise and experience help you succeed

- Our team has 10+ years of experience in the applied implementation of zero-trust architectures and implementations.
- Partnership in the academic environment in terms of zero trust and application security.
- Comprehensive expertise on areas impacting Zero Trust: Cloud Security, IAM (Identity and Access Management) and DevSecOps.

Contact us

FORTIT
SECURE DIGITAL BUSINESS

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