FORTIT
SECURE DIGITAL BUSINESS

Alles, was Sie über angewandtes Zero Trust wissen müssen

Zero Trust: Weil die Perimetersicherheit nicht mehr ausreicht

Zero Trust ist ein Rahmewerk, das davon ausgeht, dass die Sicherheit einer Organisation ständig von externen und internen Bedrohungen gefährdet ist. Geschäftsprozesse werden zunehmend von der Cloud-Transformation beeinflusst, wodurch Nutzer, Anwendungen und Daten immer häufiger ausserhalb des Perimeters agieren. Klassische Sicherheitskonzepte stossen daher an ihre Grenzen. Da Bedrohungen auch innerhalb des Perimeters auftreten, ist der Ansatz "trust but verify" nicht mehr ausreichend, weshalb Unternehmen ihre Cyber-Resilienz weiter stärken müssen.

Von den Vorteilen einer Zero Trust Architektur profitieren

Eine Zero-Trust-Architektur führt zu einer effizienteren und effektiveren IT-Landschaft. Sie reduziert Cybersicherheitsrisiken und ermöglicht neue Anwendungsfälle in einem digitalisierten Unternehmen.

Erhöhte Sicherheit

- Sichtbarkeit der Aktivitäten zur effektiven Erkennung von verdächtigem Verhalten oder Sicherheitsverletzungen.
- Risiken von Seitwärtsbewegungen reduzieren und damit Unternehmens- sowie Kundendaten schützen.

Befähigung der Geschäftsaktivitäten

- Mitarbeitende und Kunden haben jederzeit und überall über jedes Gerät sicheren Datenzugriff.
- Unterstützt die digitale Transformation durch intelligente Sicherheitsmassnahmen in verteilter IT-Landschaft.

Reduzierte Komplexität

- Entfernung überlappender Sicherheitsmassnahmen; einfachere Richtliniensumsetzung.
- Effiziente Erstellung und Verwaltung von Zugriffsrichtlinien.

Kostensenkung

- Vollständige Sicht auf Netzwerkgeräte für schnelle Reaktionszeiten nach Vorfällen.
- Zentrale Überprüfung von Zugriffsrechten für effiziente Audits und Rezertifizierung.

Typische Herausforderungen überwinden

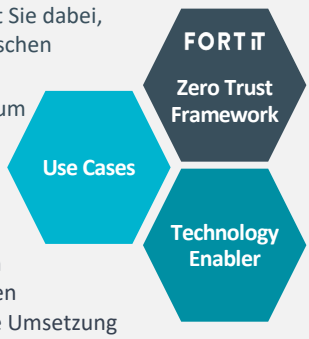
FortIT unterstützt Sie aktiv bei der Umsetzung des Zero Trust Ansatzes, trotz der damit verbundenen Herausforderungen.

Strategie
Unklare Strategien erschweren die unternehmensweite Einführung von Zero Trust-Prinzipien.
Die Zielarchitektur von Zero Trust ist nicht mit der Unternehmensstrategie abgestimmt.

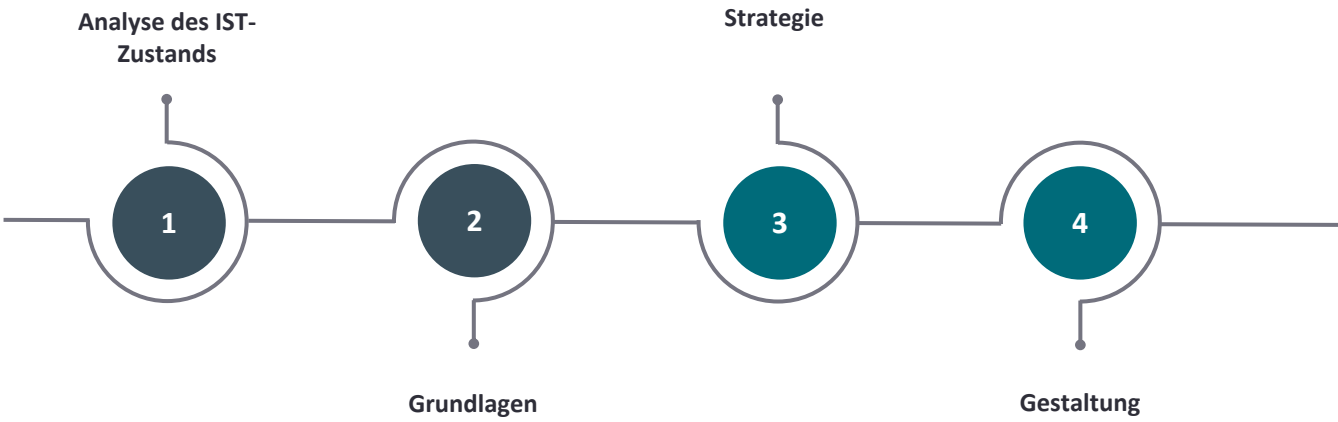
Bewusstsein
Mangel an Wissen und Expertise, oft beeinflusst von Sicherheitslösungsanbietern.
Fehlendes gemeinsames Verständnis und unterschiedliche Ansätze auf verschiedenen Ebenen.

Komplexität
Heterogene IT-Infrastruktur mit Legacy-Komponenten.
Vielzahl von vorhandenen Technologien und fehlende Orchestrierung.

- ✓ FortIT führt Sie durch Ihren Zero Trust Lebenszyklus. Unsere Dienstleistungen reichen von der Analyse und Konzeption bis zur Umsetzung.
- ✓ Unser Framework unterstützt Sie dabei, die Architektur an die spezifischen Anwendungsfälle Ihres Unternehmens anzupassen, um eine erfolgreiche Umsetzung zu gewährleisten.
- ✓ 10 Jahre durchschnittliche Teamerfahrung in bewährten Lösungen und technologischen Hilfsmitteln, unterstützen die Umsetzung von Zero Trust Prinzipien.



Ihr Weg zu einer erfolgreichen Zero Trust Implementierung



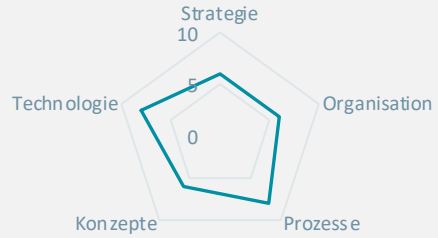
FORTIT

Bewertung des Reifegrads

Ausgangslage
- Unklare Kenntnisse über Ihren aktuellen Zero Trust Stand
- Fehlendes Know-how bei der Umsetzung von Zero Trust
- Unklare Bereitschaft zur Implementierung von Zero Trust

FortIT Dienstleistungen
- Workshops, Interviews und Dokumentenanalysen
- Analyse der aktuellen IT-Architektur
- Bewertung bestehender relevanter Zero Trust Prozesse
- Untersuchung laufender Aktivitäten und aktueller Initiativen
- Bestimmung der Zero Trust Reifegrad mit dem FortIT Zero Trust Framework nach Analyseergebnissen
- Entscheidung über die Zero Trust Zielreifegrad

Beispielhafte Lieferobjekte
- Aktueller Zero Trust Reifegrad und vorgeschlagener Zielreifegrad
- Aktuelle Architekturübersicht
- Aktuelle Prozesslandkarte und Überblick laufender Aktivitäten



Muster eines Zero Trust Reifegrad Spinnendiagramms

Ihr Mehrwert

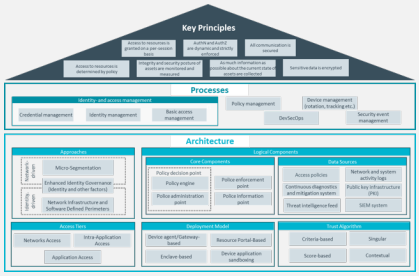
- ✓ Faktenbasierte Sicht Ihres aktuellen Zero Trust-Reifegrads
- ✓ Grundlage für den Start Ihrer Zero Trust-Roadmap

Strategie und Gestaltung

Ausgangslage
- Übersicht über die aktuelle Situation
- Erste Vision zur Implementierung von Zero Trust
- Fehlende Zero Trust Strategie

FortIT Dienstleistungen
- Definition des Umfangs: System- und Prozessgrenzen, Umsysteme, Abgrenzungen
- Bestimmung der Anwendungsfälle, Ziele und Anforderungen, Ableitung einer Zero Trust Strategie
- Entwicklung von Zero Trust Prozessen, Design Patterns (Bausteinen) und Architekturvarianten
- Definition einer Zero Trust Roadmap als Planungsgrundlage für eine iterative Steigerung der Reife

Beispielhafte Lieferobjekte
- Zero Trust Strategie und Implementierungs-Roadmap
- Prozesslandkarte (Zielsituation)
- Zero Trust Zielarchitektur und Design Patterns

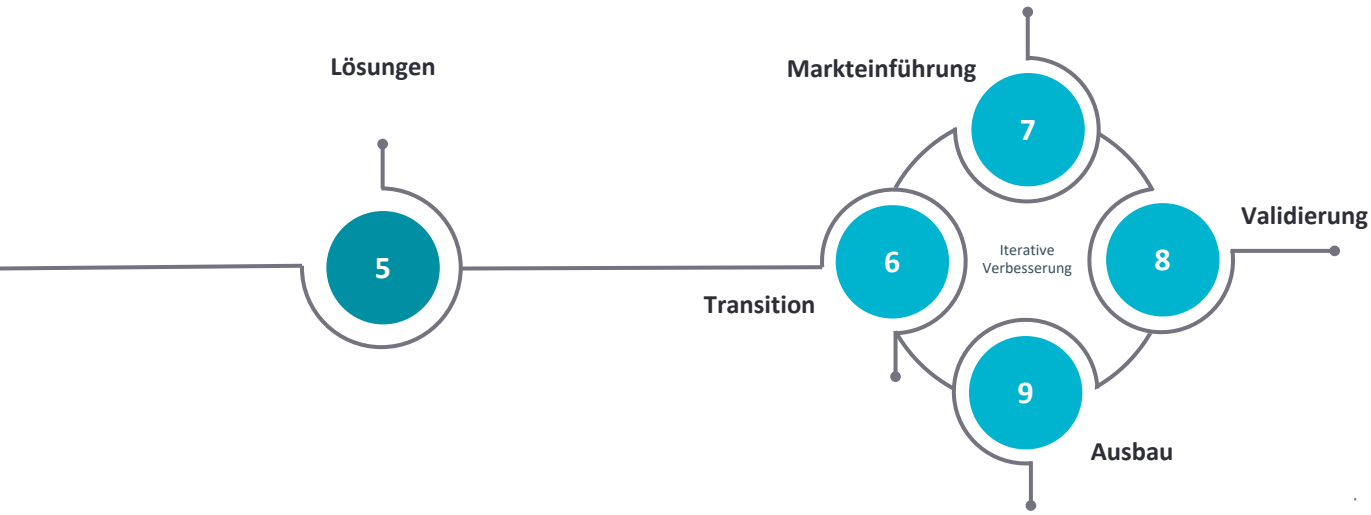


Bausteine der FortIT Zero Trust Architektur

Ihr Mehrwert

- ✓ Gemeinsames Verständnis und Vision von Zero Trust
- ✓ Umsetzbare Zielarchitektur

Ein klarer Weg zu Ihrem gewünschten Zero Trust-Reifegrad

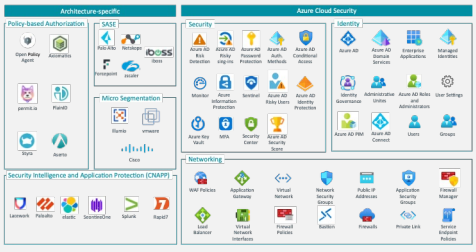


Product enabler

Ausgangslage
- Bestehende Zero Trust Strategie und Design
- Klare Vorstellung zur Umsetzung von Zero Trust
- Konkreter Projektplan

FortIT Dienstleistungen
- Marktanalysen durchführen
- Definition von Umsetzungsoptionen (SWOT) mit Handlungsempfehlungen
- Zielbild für die Implementierung entwickeln
- Konzeptvalidierung durchführen: Details festlegen, Planung und Durchführung eines Proof of Concept (PoC)

Beispielhafte Lieferobjekte
- Marktanalyse und Produktvergleich
- Implementierungsvarianten
- Proof of Concept



FortIT Zero Trust Technology Enabler Karte

Ihr Mehrwert

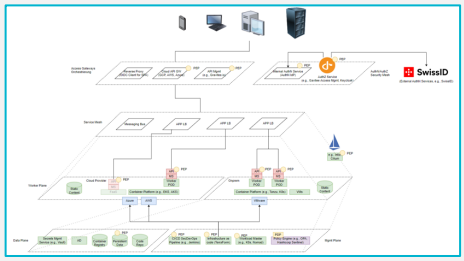
✓ Unabhängige Sicht über Product Enabler
✓ Klarheit zur Machbarkeit einer Zero Trust Architektur

Umsetzung

Ausgangslage
- Validiertes Zero Trust Konzept
- Definierte Produktstrategie
- Detail-Spezifikation

FortIT Dienstleistungen
- Einen iterativen Implementierungsplan festlegen
- Anbieterauswahl und -Beschaffung
- Migrations-, Betriebs- und Schulungskonzept erstellen
- Rollout- und Implementierungsunterstützung
- Validierung durchführen, um korrekte Implementierung und Zielerreichung sicherzustellen
- Unterstützung bei Verbesserung und Weiterentwicklung

Beispielhafte Lieferobjekte
- Übergangsplanung und Detail-Spezifikation
- Migrations-, Betriebs- und Schulungskonzept
- Implementierungsvalidierung
- Massnahmen zur Verbesserung und Weiterentwicklung



Beispiel einer Zero Trust Deployment Architecture für Microservices

Ihr Mehrwert

✓ Umgesetztes Zero Trust Konzept gemäss Strategie
✓ Klare Verantwortlichkeiten und Prozesse

Erfolgsgeschichten

Entwicklung von Zero Trust Architekturmuster

Hintergrund: Eine Schweizer Bankengruppe setzt auf Cloud-Technologien und Cloud Native Development. Neben On-Premises PaaS-Lösung auf Basis von Openshift laufen Workloads auch auf Hyperscalern (Azure, AWS, GCP).
Sie haben ein starkes Interesse an der Automatisierung von Zugriffsrichtlinien in nativen Cloud-Anwendungen und an einer nahtlosen Integration in ihren Dev(Sec)Ops Lifecycle.

Die Rolle von FortIT: Analyse der grundlegenden Architektur und bestehenden Zugangskontrollsysteme. Entwurf und Implementierung von Richtlinienprozessen für zentrale Zugangsberechtigungen. Marktanalyse aktueller Technologie für feinkörnige Zugangskontrolle. Architekturmuster zur Sicherung der Frontend-Backend-Kommunikation mit Zero Trust.

Mehrwert für unseren Kunden: Gemeinsames Verständnis der Zero Trust Architektur. Automatisierung und zentrale Kontrolle von Berechtigungen durch eine Policy-Engine. Klare Prozesse und Zuständigkeiten für Richtlinienverwaltung.

Konzeptualisierung des Zero Trust Zugriffsmanagements

Hintergrund: Die hybride Multi-Cloud eines grossen Schweizer Logistikunternehmens führte dazu, dass immer mehr Systeme und Workloads in unterschiedlichen Umgebungen skaliert wurden. Die Verteilung der Workloads erschwerte die Überprüfung, ob die Kontrollen angemessen umgesetzt wurden.
FortIT wurde beauftragt, ein Konzept für das Externalized Authorization Management zu entwickeln.

Die Rolle von FortIT: Erstellung einer Zielarchitektur für den richtlinienbasierten Zugriff. Darauf basierend wurde eine Lösung für zentrales Zugriffsmanagement evaluiert und implementiert. Definition von Prozessen und Zuständigkeiten für die Verwaltung von Richtlinien in Absprache mit verschiedenen Stakeholdern, einschliesslich Schulung des Personals.

Mehrwert für unseren Kunden: Modernes Zugriffskontrollsystem mit Richtlinien. Zentrale Übersicht und Verwaltung von Zugriffsrichtlinien. Eindeutig definierte Verantwortlichkeiten und Prozesse.

Entwicklung der Zero Trust Architektur für 2025

Hintergrund: Eine grosse Schweizer Bankengruppe suchte nach Wegen, Cyber-Risiken zu minimieren und gleichzeitig eine immer stärker werdende hybride Arbeitsweise und Infrastruktur zu berücksichtigen. Die Umsetzung von Zero Trust soll die Widerstandsfähigkeit gegenüber Cyber-Angriffen erhöhen und gleichzeitig als Geschäftstreiber dienen, indem sie eine hybride Arbeitsweise ermöglicht.

Die Rolle von FortIT: Strukturanalyse der IT-Infrastruktur, Prozesse und Zugangskontrollsysteme. Analyse der aktuellen Zero Trust Reifegrads und Definition der Zielreife. Risikoanalyse des aktuellen Zustands. Entwurf einer Zielarchitektur für Zero Trust und eines Implementierungsplan. Entwicklung priorisierter Massnahmen mit Kosten-Nutzen-Verhältnis. Marktanalyse relevanter Technologien für die Zielarchitektur.

Mehrwert für unseren Kunden: Unternehmensweite Definition von Zero Trust. Darstellung des aktuellen, risikobasierten Bedrohungsniveaus. Strategie zur schrittweisen Verbesserung der Zero Trust Reife.

Key Takeaways

Warum Zero Trust?

- ✓ Sicherer Zugriff durch adaptives Zugriffsmanagement: Authentifizierung & Autorisierung basierend auf Kontextinformationen und Risiken.
- ✓ Angemessener Schutz von Cloud-Ressourcen: Dynamische Segmentierung basierend auf Richtlinien (pro Workload).
- ✓ Sicherheitsvorfälle minimieren durch Security Operations: Kontinuierliches Erkennen, Analysieren und Reagieren auf verdächtige Aktivitäten.

Die Steigerung Ihrer Zero Trust-Reife bietet Ihnen folgenden Mehrwert

Warum FortIT?

Setzen Sie auf unsere Expertise und Erfahrung für Ihren Erfolg

- 10+ Jahre Erfahrung in der angewandten Umsetzung von Zero Trust Architekturen
- Partnerschaft im akademischen Umfeld für Zero Trust und Applikationssicherheit.
- Umfassende Expertise rund um das Thema Zero Trust: Cloud Sicherheit, IAM (Identitäts- und Zugriffsmanagement) sowie DevSecOps.

Kontaktieren Sie uns

FORT iT
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