INSEYA
simply secure

Zero Trust & SASE

Das Wichtigste in Kürze.

Was ist Zero Trust?

Zero Trust ist ein **Sicherheitskonzept** welches auf dem Grundsatz basiert, dass keinem Benutzer, Gerät oder Prozess vertraut wird.

Aufgrund der Bedrohungslage ist es nur eine Frage der Zeit, bis ein Angriff erfolgt. Die Sicherheitsstrategie ist so auszurichten, dass ein Angriff erwartet wird: **«assume breach»**.

Zero Trust Prinzipien

«never trust, always verify»
Jede Anfrage erfordert eine neue Verifizierung anhand von unterschiedlichen Parametern.

«least privilege»
Jeder Zugriff erfolgt mit der minimal notwendigen Berechtigung. Diese wird situativ gewährt und wieder entzogen.

«microsegmentation»
Um jede Ressource wird ein adäquater Schutzperimeter definiert, welcher bei jedem Zugriff verifiziert wird. Nach erfolgreicher Verifizierung, wird ein policybasierter, begrenzter Zugang zu der Ressource gewährt.

Gründe für Zero Trust

Klassische Sicherheitskonzepte können folgende Anforderungen nicht mehr erfüllen:

Cloud Services: Immer mehr Dienste aus der Cloud

Work from home: Mitarbeitende arbeiten ausserhalb des Unternehmens.

Digitalisierung: Prozesse werden digitalisiert und mobil zur Verfügung gestellt.

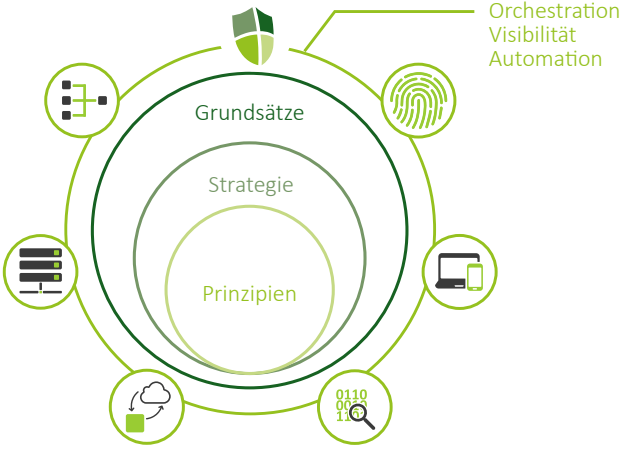
Zero Trust Mehrwert

- **Resilienz:** Stärkung der Abwehrfähigkeiten gegen aktuelle und kommende Cyber-Risiken.
- **Visibilität:** Mehr Informationen über Netzwerkaktivitäten erhalten.
- **Automation:** Abstimmen der Sicherheitswerkzeuge durch passende Schnittstellen (APIs).
- **Reputation:** Innovativer, zukunftsorientierter IT-Sicherheitsansatz.
- **Effizienz:** Reduktion der Komplexität durch Optimierung von Einzellösungen/Silos.
- **Skalierbarkeit:** Situative Anpassung nach Sicherheitsanforderungen und Anzahl Nutzer.

Zero Trust planen

Zero Trust umfasst sechs verschiedene Domänen: **Identity, Endpoint, Data, Application, Infrastructure** und **Network.** Eine Zero Trust Strategie berücksichtigt jede dieser Domänen.

1. Definieren Sie eine Zero Trust Strategie, welche auf den Zero Trust **Prinzipien** aufbaut.
2. Leiten Sie von dieser Strategie Ihre **Grundsätze** für jede der sechs Domänen ab.
3. Für die Umsetzung dieser Grundsätze wählen Sie die passenden technischen Lösungen.



Zero Trust umsetzen

Bei der Umsetzung von Zero Trust ist «Technik» nur die Spitze des Eisberges. Beachten Sie weitere Ebenen wie z.B. Kultur, Organisation oder Prozesse. Bestimmen Sie den Reifegrad jeder Ebene und setzen Sie Prioritäten. Eine Bewertungshilfe für den Reifegrad finden Sie bei den QR-Codes.

Zero Trust Umsetzung in Schritten

Discover: Bestimmen Sie zuerst Ihren Zero Trust Reifegrad. Definieren Sie schützenswerte Ressourcen und prüfen Sie den Datenfluss.

Control: Legen Sie Ihre Zero Trust Architektur fest und definieren Sie die durchzusetzenden Regeln bevor Sie technische Lösungen einbauen.

Detect: Überwachung und Analyse des Netzwerkverkehrs ermöglicht eine schnelle Reaktion auf Angriffe.

Zero Trust & SASE

SASE führt alle Elemente von Zero Trust in einer zentralen Plattform zusammen mit folgenden Vorteilen:

- ✓ **Optimale Integration**
  Die Sicherheitskomponenten sind aufeinander abgestimmt.
- ✓ **Weniger Betriebsaufwand**
  Der Anbieter sorgt für koordinierte Aktualisierung und Kompatibilität.
- ✓ **Volle Kontrolle**
  Visibility und Orchestrierung sind bereits eingebaut.

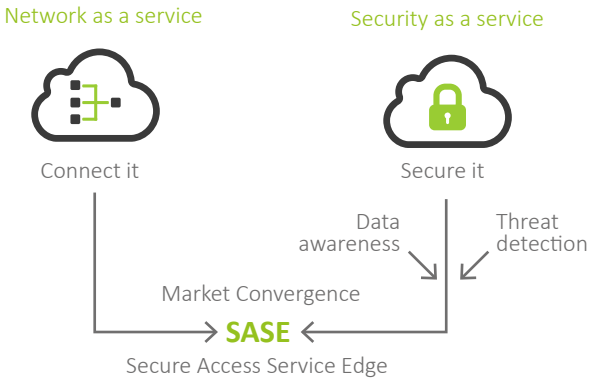
Data protection ist der Treiber, **warum** es neue Konzepte und Lösungsansätze braucht.

Zero Trust ist das Konzept, **wie** zukünftigen Cyber-Risiken begegnet werden kann.

SASE ist ein **konkreter Lösungsansatz,** um ein Zero Trust Konzept umzusetzen.

Was ist SASE?

Secure Access Service Edge (SASE) kombiniert WAN-Funktionalitäten (z.B. SD-WAN, Traffic-Optimierung) mit Security-Funktionen (z.B. CASB, NGFW), um die dynamischen Zugriffsanforderungen zu erfüllen. SASE ist besonders geeignet, um eine **Zero Trust Sicherheitsarchitektur** aufzubauen.



Mit einer SASE Lösung etablieren Sie im Sinne von Zero Trust eine zentrale Steuerungskomponente **(PDP – policy decision point)**, welche die Sicherheit und den Netzwerkzugriff auf ihre Ressourcen steuert und volle Visibilität in ihrem Netzwerk schafft.

Mehrwerte von SASE

✓ **Agilität**
SASE ermöglicht ein optimiertes Netzwerk und hohe Sicherheit für alle Standorte, Anwendungen und Benutzer in einer Plattform, unabhängig davon, wo sie sich befinden sowie eine schnelle Reaktion auf Standortveränderungen.

✓ **Konvergenz**
Dank der Konvergenz von Netzwerk und Sicherheit können alle Funktionen und Richtlinien in einer einzigen Oberfläche verwalten werden. Dies ermöglicht einen tiefen Einblick in Netzwerk- und Sicherheitsereignisse.

✓ **Effizienz**
SASE reduziert die Komplexität und vereinfacht die Wartung/Pflege der gesamten Infrastruktur und damit auch das Risiko von Fehlkonfigurationen. Physikalische Topologie, Skalierungs- und Wartungsaufwand werden drastisch reduziert. Alle Regeln werden automatisch weltweit angewendet.

✓ **Kostenoptimierung**
Durch Vereinfachung des Netzwerk- und Sicherheitsstacks, zusammen mit der Konsolidierung mehrerer Einzelprodukte/Anbieter, sinken die Gesamtkosten für den Betrieb der Umgebung.

SASE Indikatoren

Fehlende Flexibilität
Ihr Netzwerk ist nicht flexibel genug, um sich an Veränderungen und zukünftige Initiativen anzupassen. Beispiele dafür sind die fehlende Unterstützung neuer Cloud-Workloads, wachsende Zahl mobiler Mitarbeiter und die schnelle Erschliessung von Niederlassungen.

Fragmentierte Sicherheitslösungen
Sie haben fragmentierte Sicherheitslösungen und müssen immer mehr Sicherheitsprodukte implementieren, um neue oder bestehende Services, Anwendungen, Daten und Benutzer zu schützen.

Fehlende Bandbreite
Die Mitarbeitenden beschweren sich über langsame Geschäftsanwendungen. Besonders bei empfindlichen Anwendungen wie Sprache und Video.

Fehlende Visibilität
Ihnen fehlt ein vollständiger Einblick in Ihr Netzwerk, was Ihnen verunmöglicht, die Sicherheit und Leistung Ihres Netzwerks zu optimieren. Sie sind nicht in der Lage, Cyber-Angriffe rasch zu erkennen und deren Auswirkungen einzugrenzen

SASE Anwendungsfälle

- ✓ Neue Standorte schnell erschliessen
- ✓ Work from Home (WfH) absichern
- ✓ Traditionelles VPN ablösen
- ✓ Blitzschnell nach Bedarf Bandbreite und Sicherheit skalieren
- ✓ Visibilität schaffen

SASE umsetzen

Think big – start small.
Wir empfehlen, eine SASE Lösung zuerst auszutesten. Anschliessend einen einzelnen, einfachen Anwendungsfall abzubilden und danach weitere Komponenten zu aktivieren.

Mit unserer Lösung **«CATO in a Box»** können Sie die Umsetzung von SASE ganz einfach testen, ohne Änderungen an Ihrer Infrastruktur machen zu müssen. Sie sind damit sofort in der Lage, Konfigurationen durchzuführen und die Sicherheitskomponenten nach Ihren Bedürfnissen zu konfigurieren und zu testen.

Weitere Informationen

QR Codes mit Links zu spezifischen Themen unserer Website

Zero Trust Blog

Reifegrad Raster

Zero Trust Baukasten

Know-How Guide

CATO in a Box

Weitere Dienstleistungen

Inseya AG
Stauffacherstrasse 72
3014 Bern
031 914 18 18

www.inseya.ch