ZERO TRUST

ENDPOINT & DATA

Zero Trust Endpoint

Fokus: Sicherung aller Endpunkte (PCs, Smartphones, IoT)

- Ähnlich wie Zero Trust Device, aber speziell für alle Arten von Endgeräten, nicht nur Firmengeräte.

Kernmaßnahmen:

✅Endpoint Detection & Response (EDR) zur Erkennung von Angriffen
✅Zero Trust Network Access (ZTNA) für mobile Geräte
✅Sicherheitskontrollen für IoT & OT-Geräte

Beispiel: Ein Smart-Device (IoT) muss sich authentifizieren und Sicherheitsrichtlinien erfüllen, bevor es mit dem Netzwerk kommunizieren darf.

Zero Trust Data

Fokus: Schutz von Daten – egal, wo sie sich befinden

- Daten sind oft das wertvollste Ziel für Cyberangriffe. Zero Trust Data sorgt dafür, dass Daten selbst dann geschützt bleiben, wenn Angreifer bereits Zugriff auf ein System haben.
- Datenverschlüsselung, Zugriffsbeschränkungen und Monitoring verhindern unbefugten Zugriff und Datenlecks.

Zero Trust Data

Kernmaßnahmen:

- ✅ Datenverschlüsselung (at rest & in transit) – Daten sind immer geschützt, egal ob gespeichert oder übertragen.
- ✅ Data Loss Prevention (DLP) – Verhindert, dass sensible Daten unerlaubt weitergegeben oder gestohlen werden.
- ✅ Zugriffssteuerung basierend auf Sensibilitätsstufen – Nicht jeder sollte Zugriff auf alle Daten haben!
- ✅ Digitale Rechteverwaltung (DRM) – Schutz von Dokumenten & Dateien, selbst wenn sie das Unternehmen verlassen.

Beispiel: Ein Mitarbeiter sendet versehentlich eine E-Mail mit sensiblen Daten an die falsche Person. Dank Zero Trust Data bleibt die Datei unzugänglich, da sie verschlüsselt ist und nur autorisierte Nutzer Zugriff haben. Selbst wenn die Datei in falsche Hände gerät, kann sie nicht geöffnet oder weitergeleitet werden.

Zero Trust Network

Zero Trust Identity

Zero Trust Application

ZERO TRUST

SECURITY

Zero Trust Workload

Zero Trust Endpoint

Zero Trust Data