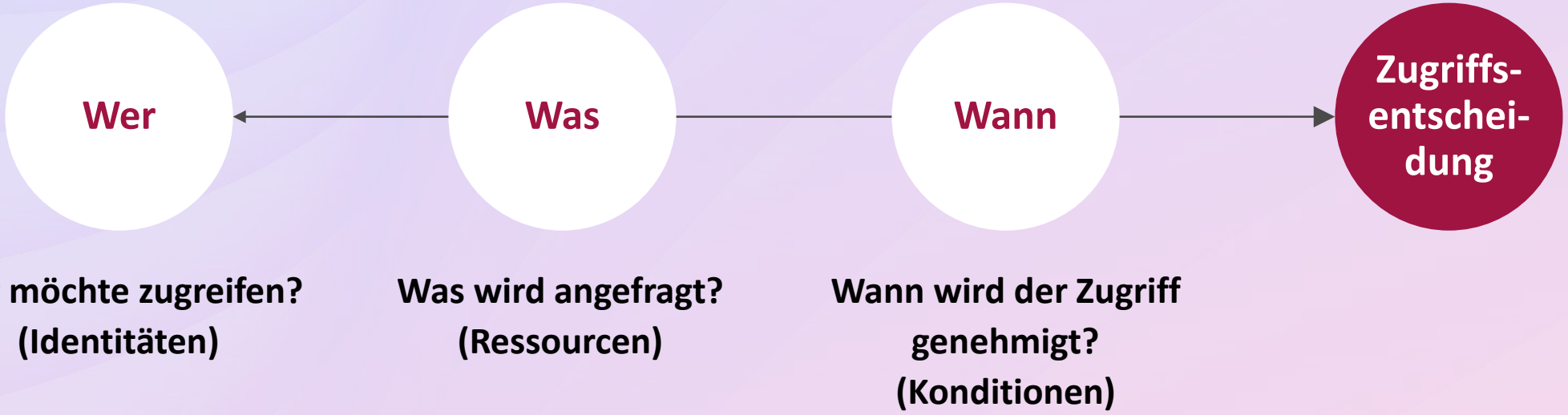
ZERO TRUST:
DECRYPTING THE MYTH

Zero Trust prägt die Cyber Security. Der Vortrag betrachtet Zero Trust aus unterschiedlichen Perspektiven und liefert praktische Ansätze.

Beispiel Zero Trust Zugriffsanfrage

Ein Nutzer möchte auf Dateien in einem Cloud Service zugreifen.
Identität | Gerät | Zeit | Ort | Kritikalität | Zugriffsmuster

---

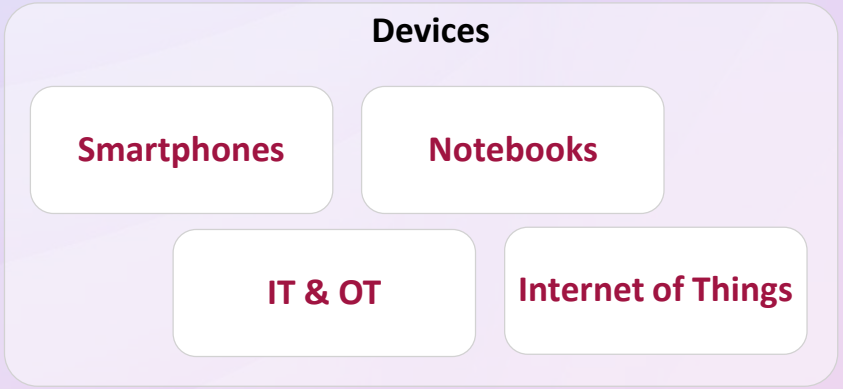


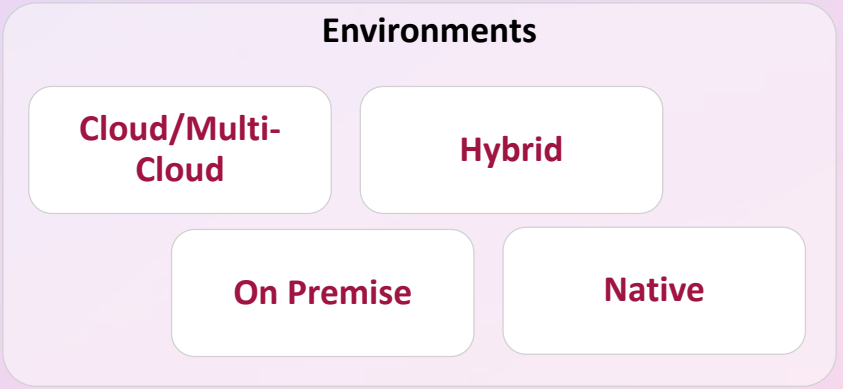
Traditionelles Sicherheitsmodell

- Schutz des Netzwerks im Fokus
- Implizites Vertrauen innerhalb des Unternehmensnetzwerks
- Perimeter-zentrierter Ansatz
- Einsatz bewährter Lösungen wie z. B. VPN (Virtual Private Network) und NAC (Network Access Control)

Neue Anforderungen durch steigende Komplexität

- Zugriffe von unterschiedlichen Geräten und Standorten
- Zugriffe auf unterschiedliche Umgebungen
- Vergrößerung der Angriffsfläche
- Schutz der Daten im Fokus
- Mikrosegmentierung
- Dynamischer, flexibler und einfacher Ansatz zur Absicherung



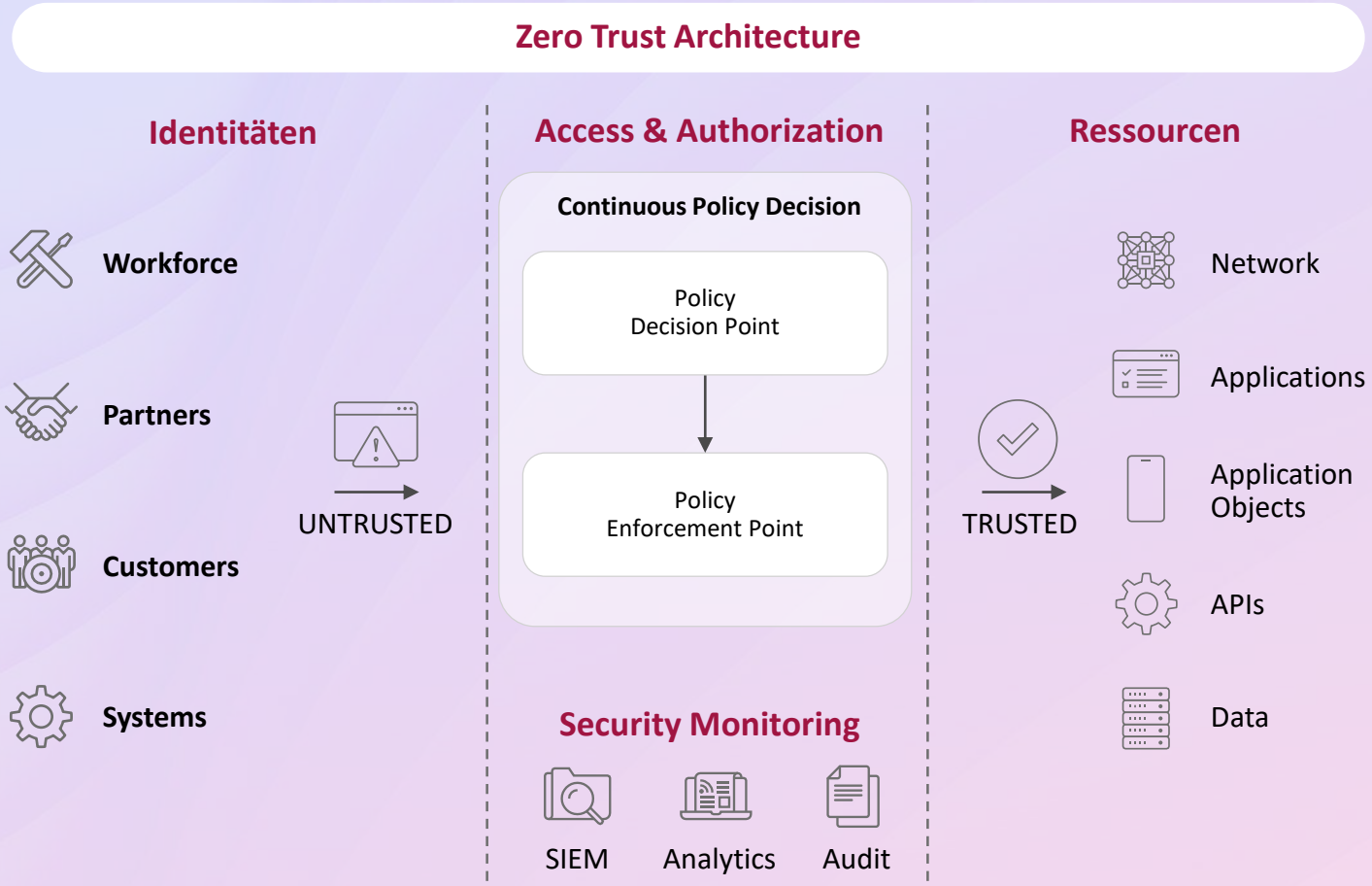


Zero Trust Kernprinzipien nach Forrester und NIST

- **Secure Access**: Zugriffe auf alle Ressourcen erfolgen authentifiziert und gesichert.
- **Least Privilege**: Zugriffe werden konsequent ausschließlich mit den geringsten Rechten durchgesetzt.
- **Security Monitoring**: Umfassende Sicherheitsüberwachung mit Identitäts- und Gerätekontexten

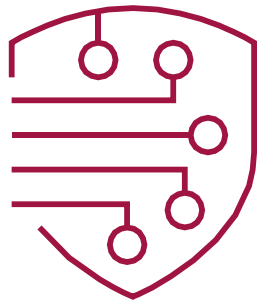
Default Deny	**Access by Policy only**	**Least Privilege Access**	**Security Monitoring**	**Risk based verification**	**Data, Workloads, User, Devices**

Zero Trust Architektur



Integration in bestehende Infrastrukturen & Prozesse

- Identity und Access Management (IAM)
- Privileged Access Management (PAM)
- VPN
- Netzwerk (u.a. Firewalls, DNS)
- Next Generation Firewalls
- Intrusion Detection Systems (IDS)
- SIEM
- Endpoint Security
- Data Loss Prevention (DLP)



Unsere Perspektive

- **Zero Trust** als **ganzheitliches Sicherheitsmodell** für den Schutz von Netzwerk-, Anwendungs- und Datenressourcen
- Schwerpunkt auf **Zugriffssteuerung** durch ein **identitätszentriertes Richtlinienmodell**.
- **Aufbau** von „Trust“ in **Komponenten** und **Prozesse**
- Gateway und Endpoint Security als „First Line of Defense“
- Defense in Depth: „It's all about layers, vectors and levels of risk.“

Praktische Ansätze für die Zero Trust Journey

1. Festlegung einer ganzheitlichen Zero Trust Strategie
2. Identifikation der zu schützenden Objekte und Schichten
3. Analyse bestehender Security Technologien und Prozesse
4. Erfassung von Benutzer-, Dienste- und Geräteidentitäten (Identitätsmanagement)
5. Ermittlung des Benutzerverhaltens und Zuständen von Geräten und Diensten
6. Auswahl geeigneter technischer Lösungen
7. Ableitung einer Zero Trust Konzeption
8. Erstellung von dynamischen Richtlinien zur Berechtigungsprüfung
9. Umsetzung eines umfassenden Security Monitoring für Benutzer, Geräte und Dienste
10. Kontinuierliche Verbesserung und Messung der Wirksamkeit

Get Started Today!

Contact us at:

Deniz Wetz
Lead Consultant Information Security & Compliance msg

msg systems ag
Robert-Bürkle-Straße 1
85737 Ismaning

+49 89 96101-0
+49 89 96101-1113

info@msg.group