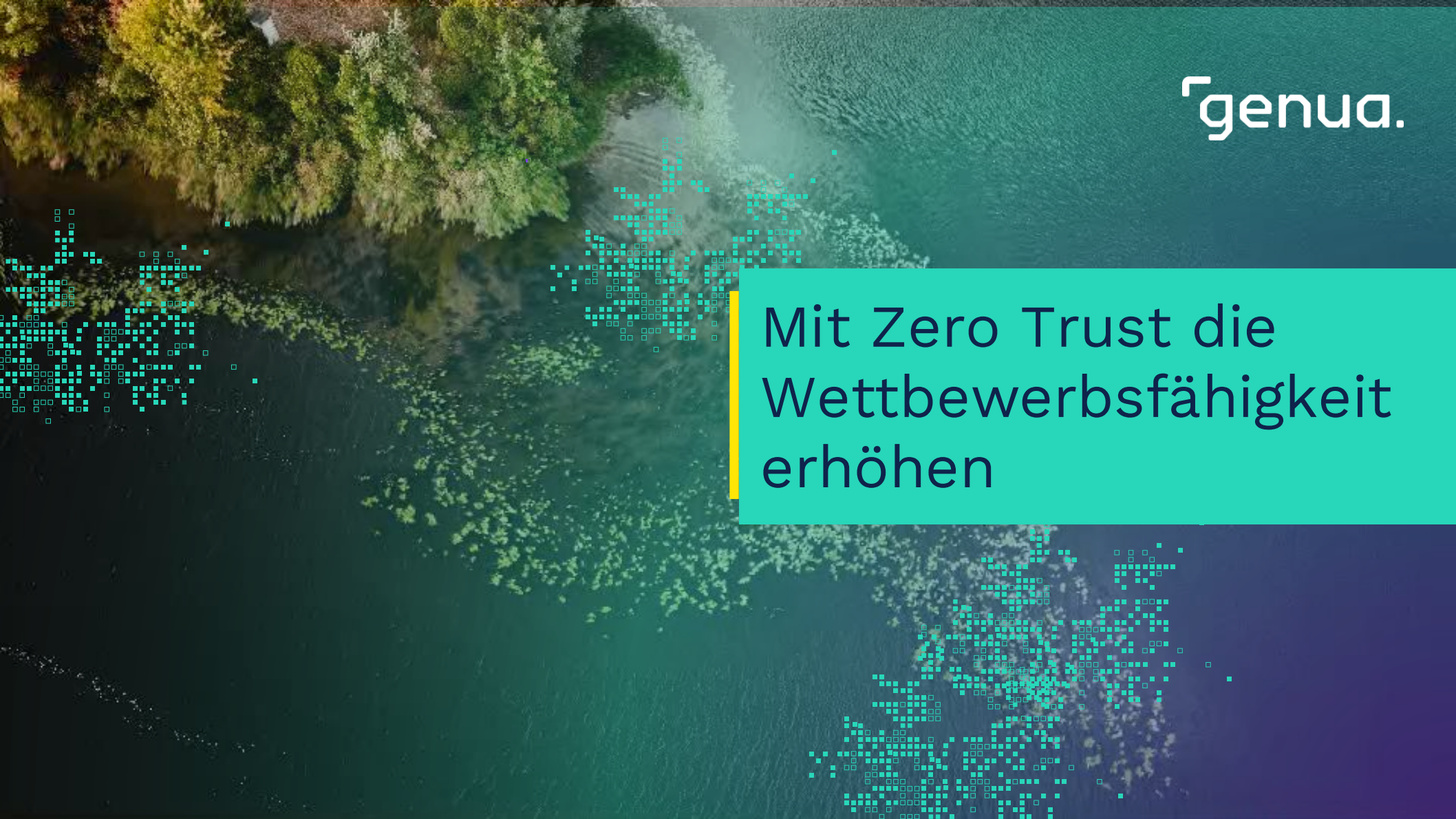


Mit Zero Trust die Wettbewerbsfähigkeit erhöhen

genua.

VIKTOR ULRICH

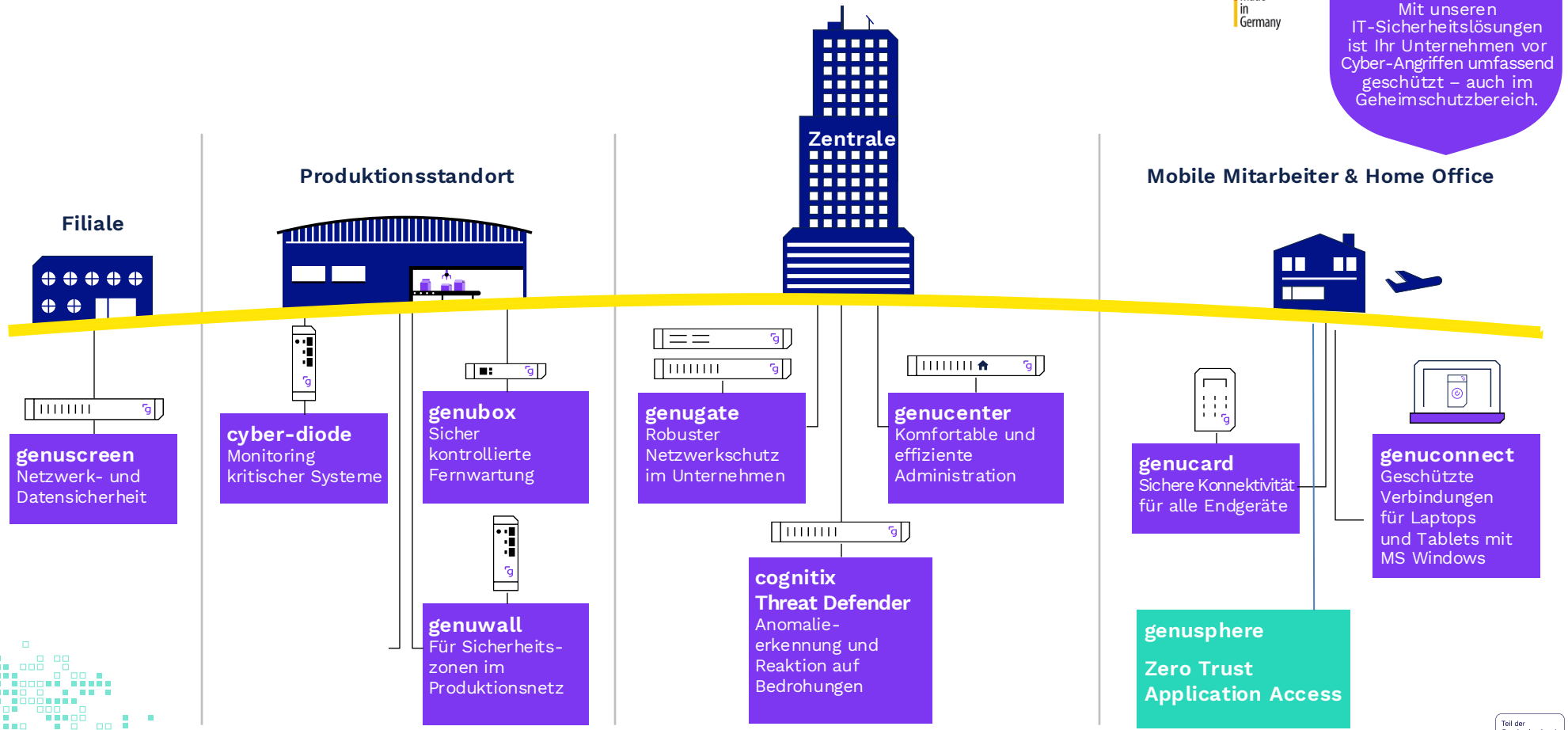
RESEARCH & INNOVATIONS

Sicherheit ist unsere Welt

SecurITy made in Germany

genua.

Mit unseren IT-Sicherheitslösungen ist Ihr Unternehmen vor Cyber-Angriffen umfassend geschützt – auch im Geheimschutzbereich.



Teil der Bundesdruckerei-Gruppe

bdr

Ausgangslage

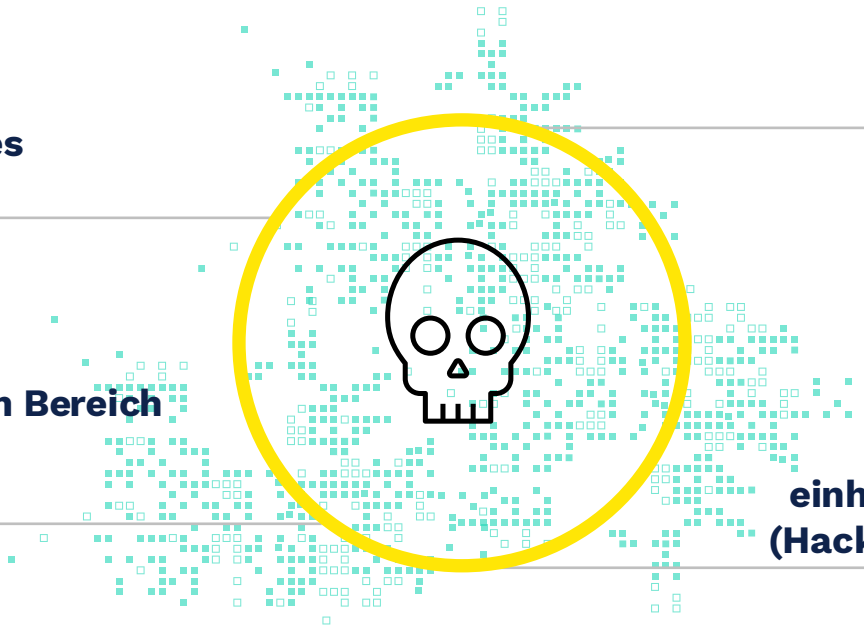
Die Herausforderung

genua.

Bedrohungslage

Nationalstaatliche Akteure

Lukratives und florierendes Geschäftsmodell



Technische Fortschritte im Bereich Angriffs-Baukästen, Automatisierung

Niedrige Einstiegshürde und einhergehende breite Verfügbarkeit (Hacking as a Service, Black Market)

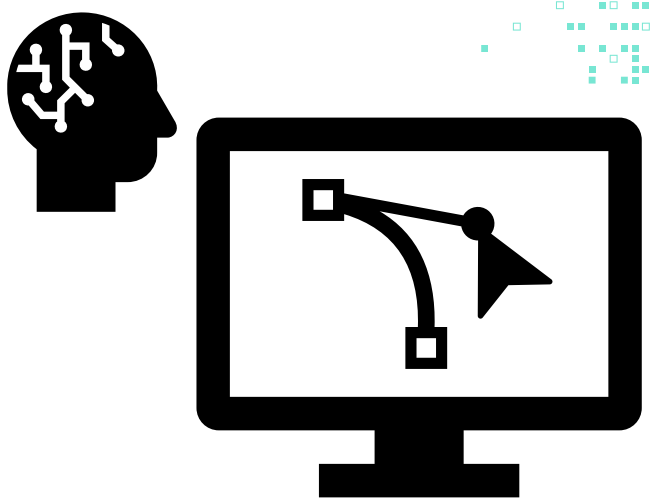
Die neue Realität

KI bleibt kontrovers.

Aber KI geht nicht wieder weg.

Fortschritt

Adaption



TOP 1: Das Ende der "Wahrheit"

Trend: Generierung und Manipulation von Bild und Ton werden Mainstream

Wettbewerbsvorteil

- Hyper-Personalisierung im Marketing durch maßgeschneiderte Werbung
- Produktvisualisierungen
- Trainings

Bedrohung

- Deepfakes
- Identitäts-Diebstahl
- CEO-Fraud
- Desinformationskampagnen
- Umgehung biometrischer Sicherheitssysteme

Vertrauen ist gut.
Aber auf welcher Basis?

→ Genauer identifizieren und verifizieren

TOP 2: Software generieren

genua.

Trend: Es wird immer leichter, komplexe und qualitativ hochwertige Software zu erzeugen

Wettbewerbsvorteil

- Viel schneller neue Ideen umsetzen
- Auf Marktanforderungen in "Echtzeit" reagieren
- Refactoring von Legacy Code

Bedrohung

- Black Box Software: Wer übernimmt Verantwortung?
- Shadow IT: Jeder Mitarbeiter kann aufwändige Software entstehen lassen
- Sicherheitsrisiken: Die Angriffsfläche wird größer

→ Isolieren und stärker kontrollieren

TOP 3: Agentische Systeme

genua.

Trend: Aufwändige Aufgaben werden automatisiert geplant und umgesetzt

Wettbewerbsvorteil

Open Source Projekte und proprietäre Angebote zeigen die Richtung:

- Service-as-a-Software: Skalierung ≠ Linear Personal
- Agilität durch autonome Zielverfolgung: Planen & reagieren
- Komplexität beherrschen: Multi-Agenten Systeme

→ Dynamische Rechtevergabe und Kontrolle

Bedrohung

- Verlust der Steuerbarkeit: Alignment Problem – Macht die KI tatsächlich was ich möchte?
- Kaskadierende Systemfehler: In der Agenten-Interaktion
- Autonome Sicherheitsverletzungen:
  - personalisiertes Spear-Phishing
  - Zero-Day Exploits

Der klassische Ansatz

Es gibt keine Burg mehr

- Der Einsatz der Cloud, die Nutzung von SaaS Anwendungen und Remote Work erschweren einen Perimeterschutz

Zu viel Vertrauen ist unangebracht

- Unterschiedlichste Endgeräte und BYOD
- Laterale Bewegung von Angreifern
- Autonome Agenten

User Experience leidet

- Opportunitätskosten
- Uneinheitliche Benutzererfahrung

genua.

Große Angriffsfläche

Hohe Betriebskosten

Schlechte User Experience

Mit dem Sicherheitsparadigma **Zero Trust** reagieren

Zero Trust

genua.

Zero Trust ist ein Sicherheits-Ansatz der Anwender explizit identifiziert und nur die notwendigen Zugriffsrechte gewährt. Damit werden reibungslose Geschäftsprozesse ermöglicht und die Risiken reduziert.

Zero Trust – Die Bausteine

Identitäten

- Digitale Identitäten stehen im Mittelpunkt
- Prüfung bei jedem Zugriff
- Egal ob Mensch, Service oder KI

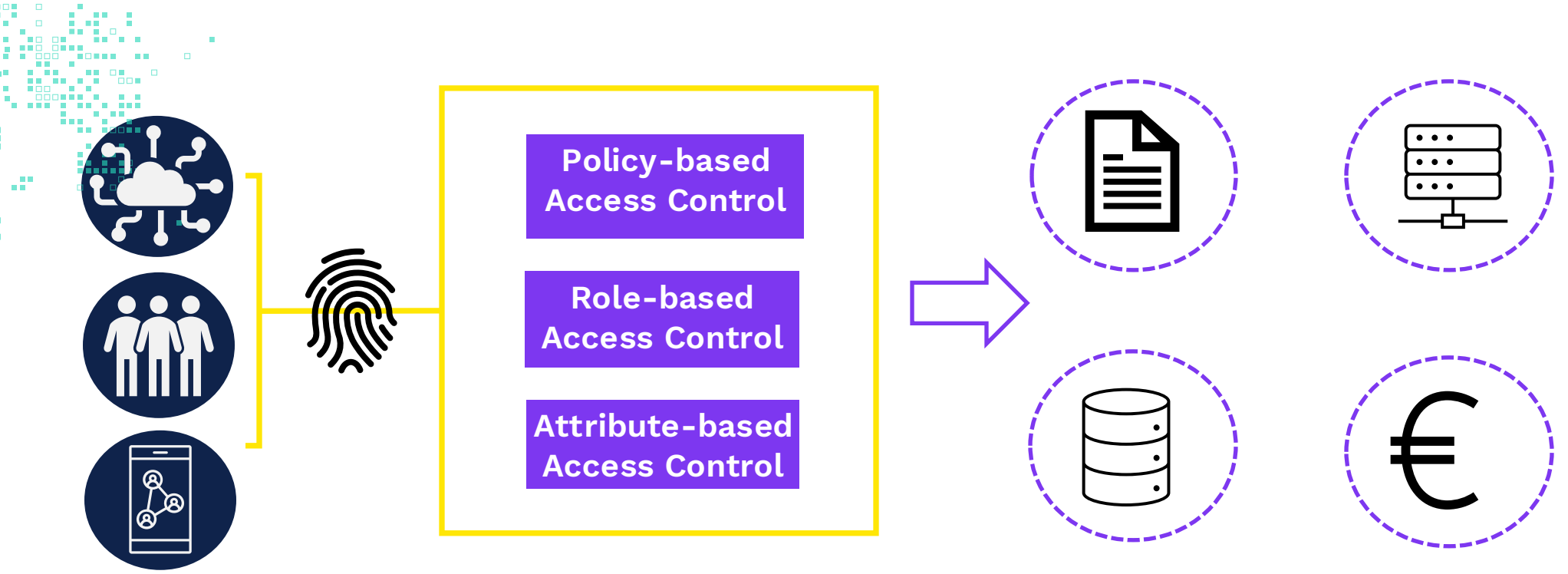
Assume Breach

- 100% Schutz nicht möglich
- Schadensrisiko durch Beschränkung auf notwendige Zugriffsrechte reduzieren

Kontext

- Verschiedene Kriterien für den Zugriff berücksichtigen
- Prüfung der Kriterien bei jedem Zugriff und kontinuierlich
- Wer, Wann, Wo, Wie, Was, Warum

Zero Trust



Anfrage Identität Prüfung Zugriff

Das Zero Trust Versprechen - Wettbewerbsvorteile

genua.

Agil agieren – Resilient und flexibel

Komplexität reduzieren

Das Risiko drastisch senken

Fundament für eine erfolgreiche **digitale Transformation**. In einer modernen und dynamischen Arbeitswelt

KI Möglichkeiten wahrnehmen – aber sicher!

Zwischenfazit

Ausgangslage und Problematik wurden erkannt

Die moderne Arbeitswelt ist dynamisch. Zu viel Vertrauen ist hier nicht mehr zeitgemäß

Die Notwendigkeit für Veränderung ebenfalls

Das Bedürfnis nach Wettbewerbsfähigkeit und die Gefahren durch die neue Bedrohungslage erfordern eine angepasste Strategie

Eine Lösung für diese Herausforderung existiert

Der Zero Trust Ansatz adressiert die relevanten Themen

Die Zero Trust - Wahrheit

Es gibt nicht das EINE Zero Trust Produkt, mit dem all meine Wünsche erfüllt werden.

Es ist vielmehr eine Strategie, die Schritt für Schritt umgesetzt wird

Zero Trust: Der Start

genua.

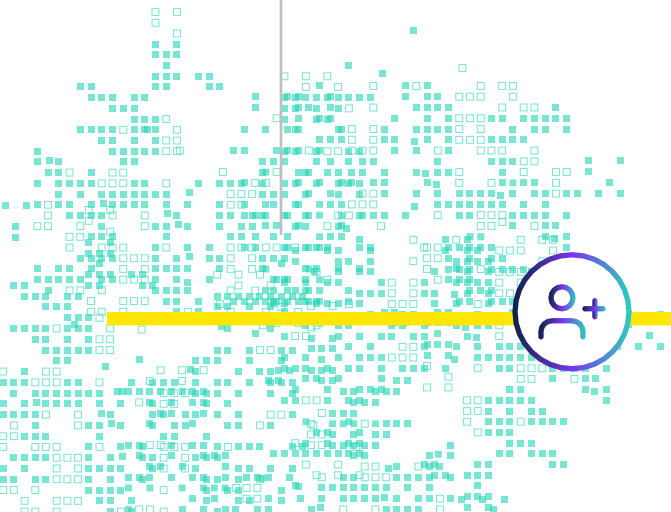
Verständnis und Commitment

Strategie

- Zu schützende Daten und Anwendungen definieren
- Interaktionen abbilden
- Architektur festlegen
- Richtlinien ableiten
- Prüfung und Wartung

Umsetzung

- Priorisierung nach Risiko und Aufwand
- Auswahl einer Lösung nach geeigneten Kriterien



Zero Trust - Verständnis und Commitment

Herausforderungen aufgreifen

Kultur

Jeder will überall Zugriff

Investitionen

Notwendigkeit und Vorteile müssen vermittelt werden

Zero Trust: Die Empfehlung

genua.

Priorität

- Menschen im Fokus
- Browser ist der neue Arbeitsplatz
- Zugriff auf Web-Applikationen

Zero Trust Application Access

Auswahl

- Integration in bestehende Strukturen
- Skalierende Lösung
- Flexibilität und Austauschbarkeit

Einführung

- Klein starten und erste Erfolge zeigen
- Auf den Mehrwert Aufmerksam machen
- Langsam aber kontinuierlich ausbauen und die Strategie verfolgen

Vielen Dank für Ihre Aufmerksamkeit!