ORACLE

Zero Trust Architektur für Voice

Ein kurzer Überblick

Stephan Dobratz

Director of Channels, EMEA
Communications Global Industry Unit

ORACLE

Perimeter Security Model

Das traditionelle „Perimeter“-basierte Sicherheitsmodell basiert auf einer starken Sicherheit an den Netzwerkgrenzen, um Schutz vor externen Bedrohungen zu bieten.

- **Interne Nutzer, Geräte und Anwendungen sind vertrauenswürdig**

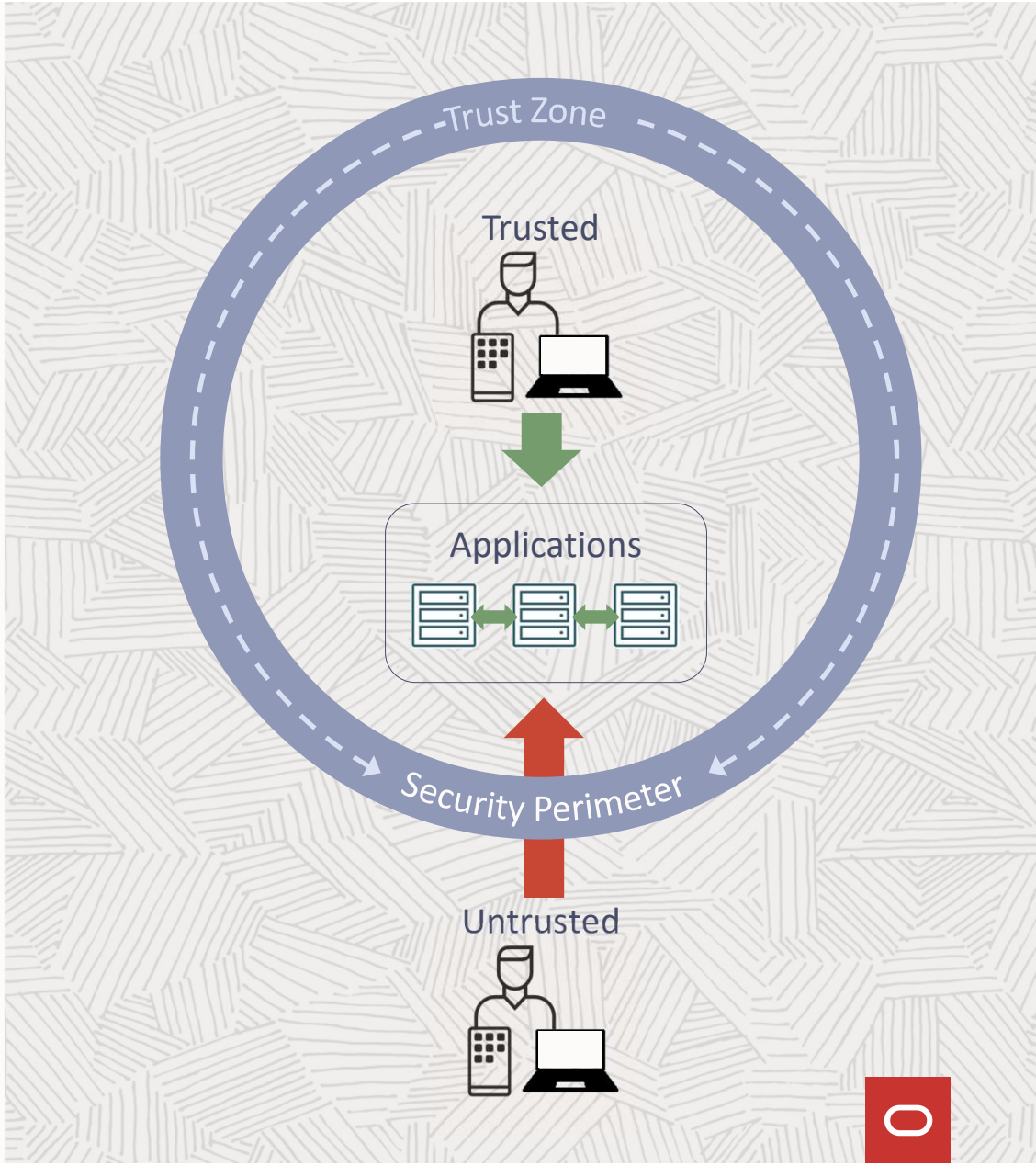
  Benutzer, Geräte und Anwendungen innerhalb des Sicherheits-bereichs sind „vertrauenswürdig“ und unterliegen einer geringeren Kontrolle als externe Einheiten

- **Externe Nuzer, Geräte und Anwendungen sind nicht vertrauenswürdig**

  Benutzer, Geräte und Anwendungen außerhalb des Sicherheits-bereichs gelten als „nicht vertrauenswürdig“ und müssen sich beim Netzwerk authentifizieren, um auf interne Ressourcen zugreifen zu können

- **Schützt vor direkten Attacken auf Netzwerkebene**

  Bietet Schutz vor direkten Angriffen, nur mit Schutz auf Netzwerkebene. Die Inspektion auf Anwendungsebene kann dies erweitern (z. B. Software Defined Networking, Deep-Packet Inspection), wird jedoch weiterhin nur auf Netzwerkebene angewendet.



ORACLE

Zero Trust Security Model

Das Zero-Trust-Sicherheitsmodell behandelt alle Benutzer, Geräte und Anwendungen als „nicht vertrauenswürdig“, unabhängig vom Standort im Netzwerk.

- **Vertraue nie, Verifiziere immer**

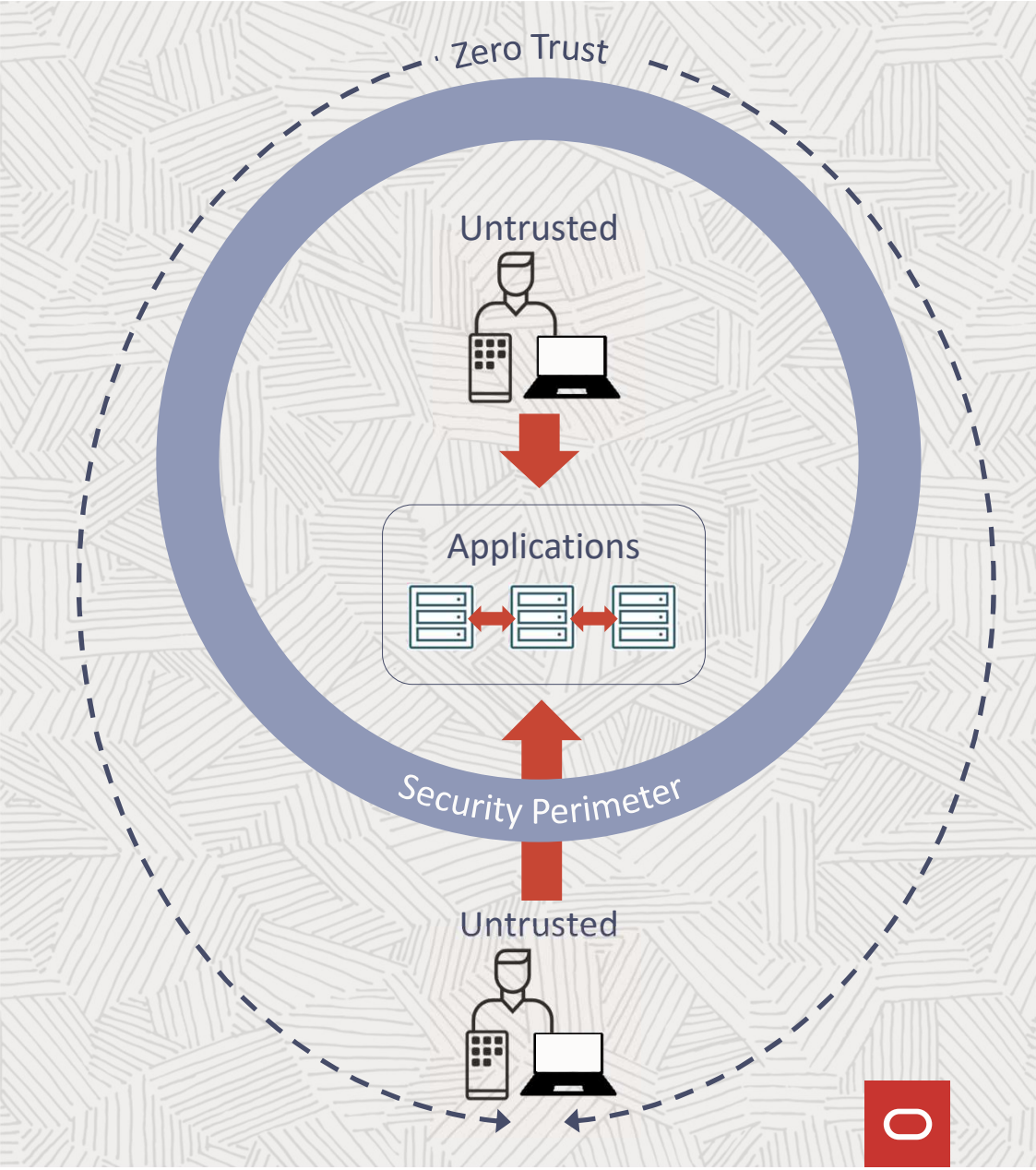
  Unabhängig davon, wo sie sich befinden, unterliegen alle Benutzer, Geräte und Anwendungen den gleichen strengen Sicherheits-maßnahmen.

- **Kontinuierliche Überwachung und erneute Authentifizierung**

  Alle Ressourcen werden kontinuierlich überwacht und müssen sich regelmäßig neu authentifizieren.

- **Es gibt keine einheitliche Lösung für die Zero-Trust-Architektur**

  Es gibt keine einzige Lösung, die eine Zero-Trust-Architektur bietet. Es handelt sich um eine Denkweise, die bei der Gestaltung der IT- und Service-Infrastruktur auf allen Ebenen innerhalb einer Organisation angewendet werden muss.



5 Säulen des Zero Trust

Jede dieser Säulen repräsentiert spezifische Schutzbereiche.

- **Identität**

  Bei der Verwaltung von Benutzern in einem Netzwerk wird die Identität zum ersten und wichtigsten zu schützenden Bereich. Schließlich wird hier der Zugriff auf ein Netzwerk, Daten oder eine Anwendung gewährt.

- **Gerät**

  Das Gerät, das versucht, auf Daten zuzugreifen, muss ebenfalls sorgfältig verwaltet werden. Mobile Geräteverwaltung, Patch-Verwaltung, Geräteerkennung und -konformität, Endpunkterkennung und -reaktion – allesamt Tools, die bei der Verwaltung von Geräten verwendet werden sollten, die auf Daten zugreifen

- **Netzwerk / Umgebung**

  Das Netzwerk (einschließlich verbundener Netzwerke) sollte als grenzenlos betrachtet werden. Gehen Sie davon aus, dass im Netzwerk keine Perimeter vorhanden sind. Wenden Sie dann Sicherheit im gesamten Netzwerk an, indem Sie Techniken wie Makro- und Mikrosegmentierung und softwaredefinierte Netzwerke verwenden.

- **Anwendung**

  Sichere Entwicklungsprozesse sind hier ein guter Ausgangspunkt. Kontinuierliche Überwachung, Software-Risikomanagement und sicheres Lieferkettenmanagement sind ebenfalls zu berücksichtigende Bereiche.

- **Daten**

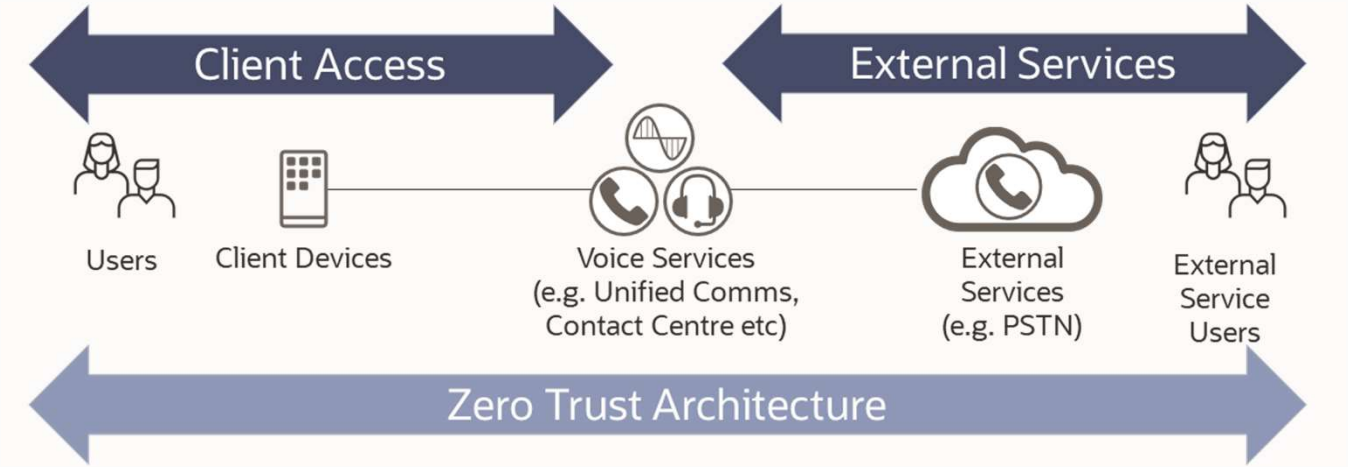
  Datenkennzeichnung und -markierung, Verschlüsselung, Zugriffskontrolle und ständige Überwachung sind Beispiele für Dinge, die zur Sicherung der Daten im Netzwerk beitragen können.

Source: InterSec

Zero Trust Architektur

Herausforderungen im Voice Umfeld

- Sprachlösungen müssen Dienste zwischen Nutzern bereitstellen, unabhängig davon, ob sie dieselbe oder eine andere Plattform nutzen.

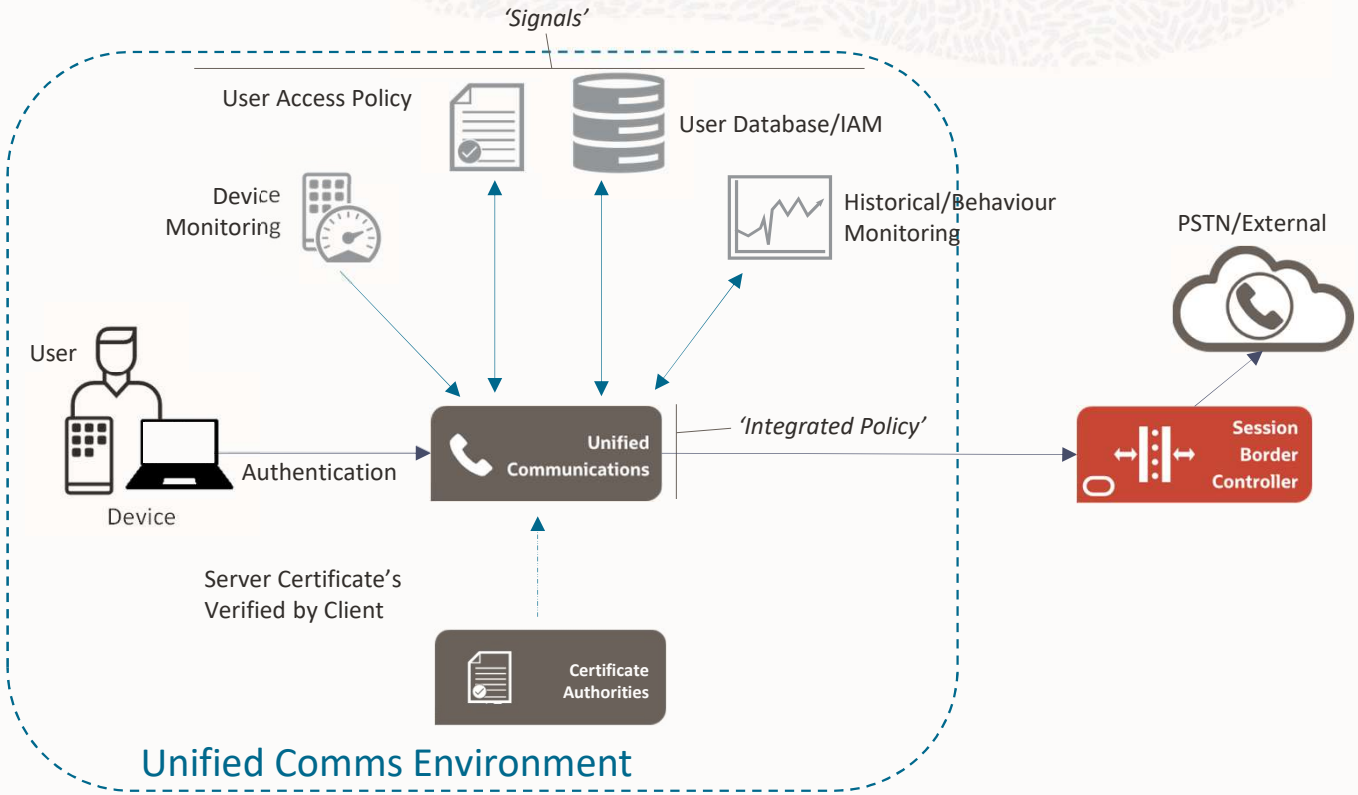


- Es reicht nicht aus, einfach nur den Client-Zugriff zu sichern. Wir müssen auch die mit externen Diensten und Benutzern eingerichteten Sitzungen berücksichtigen.

Aufbau einer Zero Trust SIP-Umgebung

Auswahl von Diensten mit Clientzugriffssicherheit

- Viele moderne Unified Communications- und Contact Center-Plattformen verfügen über starke Sicherheitslösungen.
- Dazu gehören Multi-Faktor-Authentifizierung, richtlinienbasierte Zugriffskontrolle auf Dienste, Geräte- und Benutzerüberwachung und Verschlüsselung.
- Wo möglich, sollten diese Lösungen genutzt werden.
- Die Lösung verfügt über begrenzte Funktionen, wenn Sitzungen aus der Unified Communications-Umgebung herausführen.

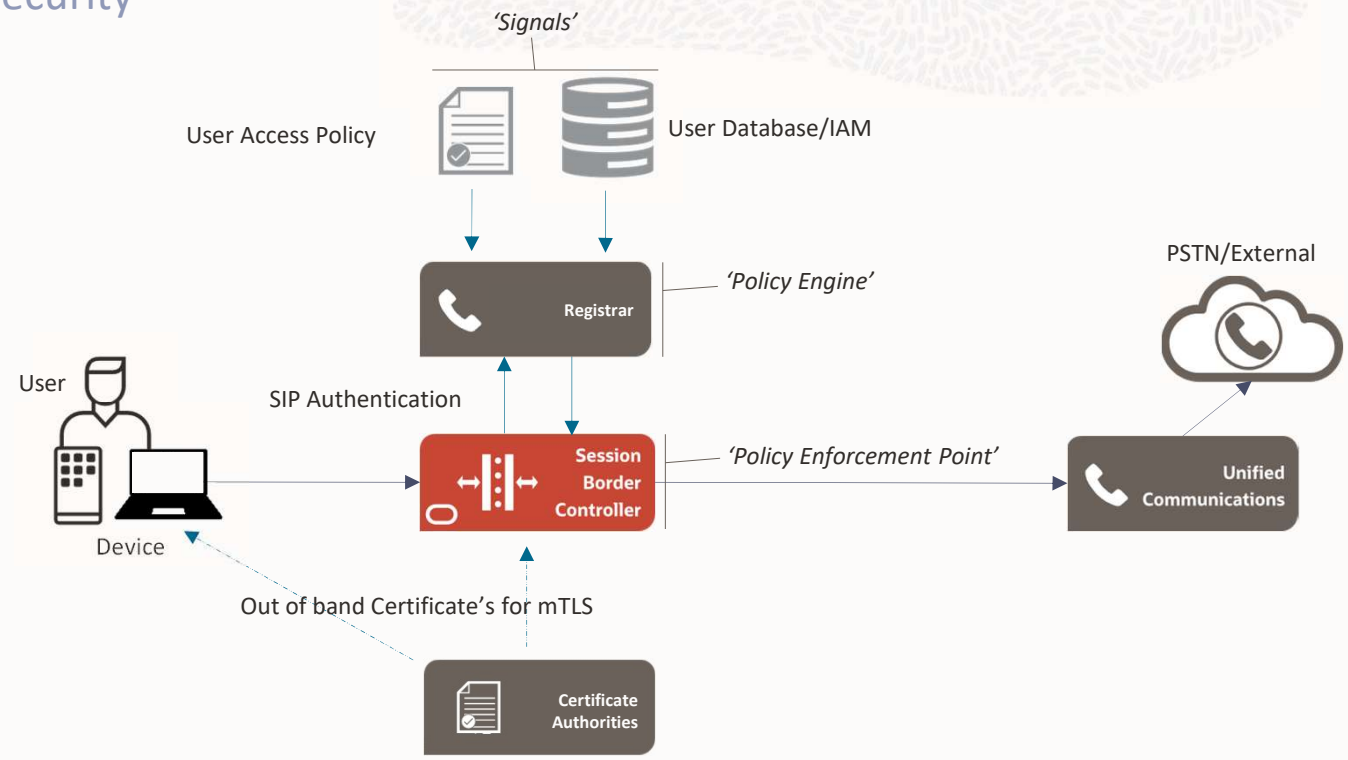


Beachte: In den meisten Fällen ist der Registrar eine Funktion der Unified Comms/PBX-Plattform

Aufbau einer Zero Trust SIP-Umgebung

Enhancing Generic SIP Client Access Security

- SBC (als Policy Enforcement Point) behandelt alle anfänglichen Anfragen als nicht vertrauenswürdig, bis sie beim Registrar (als Policy Engine) authentifiziert werden.
- Der Registrar konsumiert mehrere „Signale“. In diesem Beispiel;
  - User Access Policy definiert, auf welche Ressourcen ein Benutzer zugreifen kann
  - User Database/IAM stellt Authentifizierungsdaten bereit
- Gegenseitig authentifiziertes TLS bietet einen zweiten Authentifizierungsfaktor, um MFA-Kriterien zu erfüllen
- Kontinuierliche Neuauthentifizierung durch die SBC vorgeschrieben.
- Authentifiziert das Gerät und den Benutzer, jedoch nicht die Sitzung.

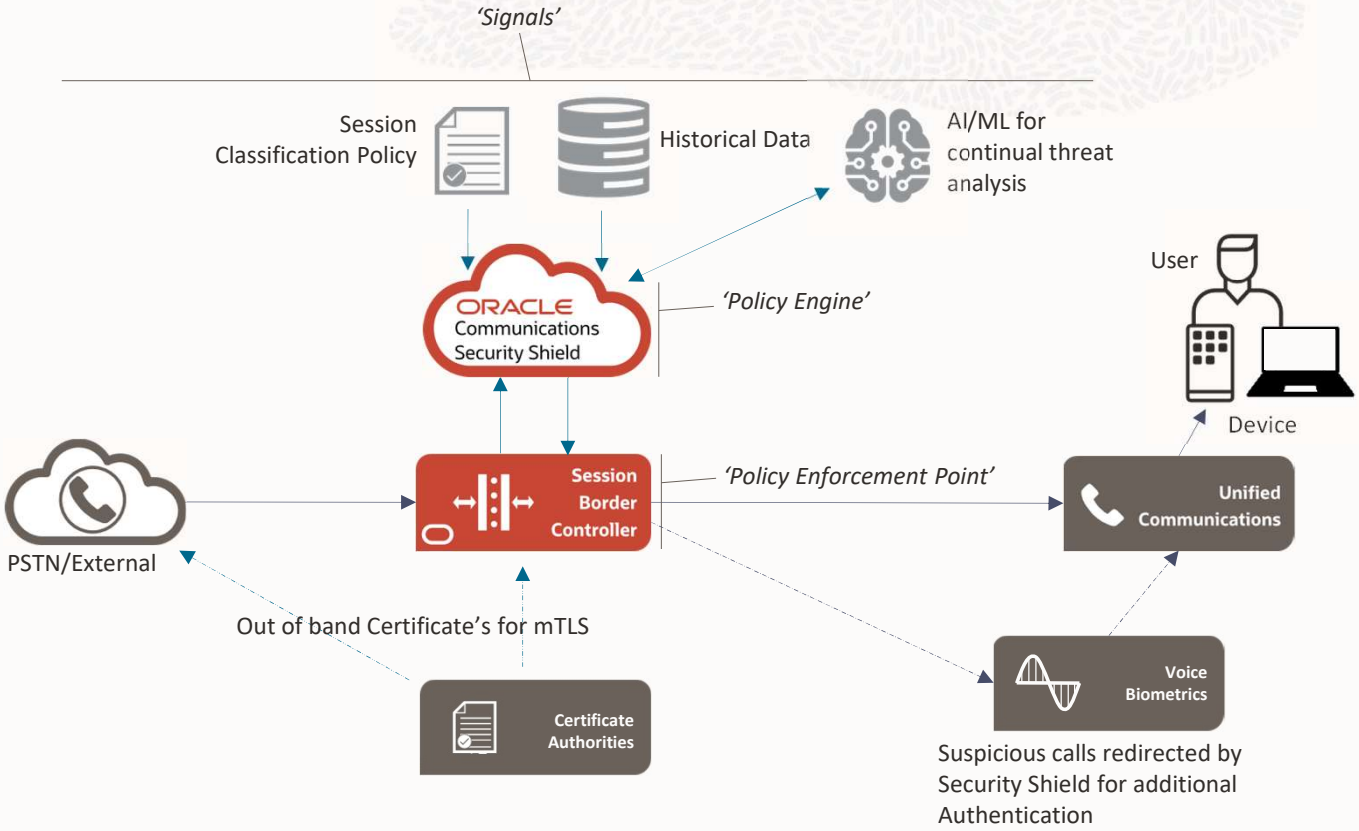


Beachte: In den meisten Fällen ist der Registrar eine Funktion der Unified Comms/PBX Plattform

Aufbau einer Zero Trust SIP Umgebung

Zero Trust PSTN Anrufe

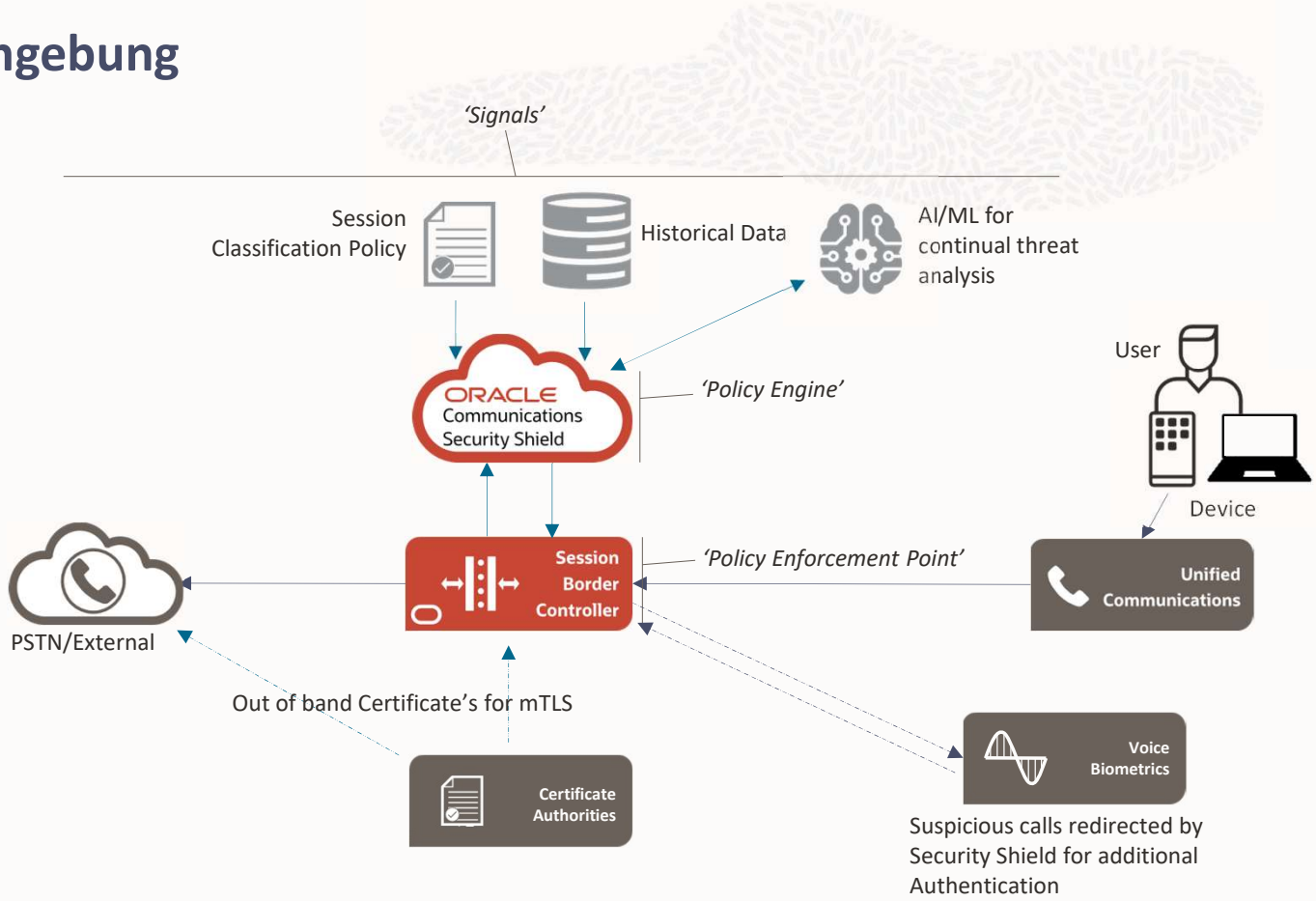
- SBC (der als Policy Enforcement Point fungiert) fragt Security Shield (der als Policy Engine fungiert) ab, um zu bestimmen, ob der Anruf zugelassen werden soll.
- Security Shield konsumiert mehrere ‘Signale’. In diesem Beispiel;
  - Internal and External DB’s of historical data that identifies known malicious callers
  - Die Session Classification Policy definiert, wann eine Sitzung zur zusätzlichen Authentifizierung abgelehnt oder umgeleitet werden soll.
  - AI/ML bietet eine kontinuierliche Sitzungsanalyse.
  - **Beachte:** TLS/mTLS mag unter Umständen nicht immer vom PSTN Provider unterstützt sein.



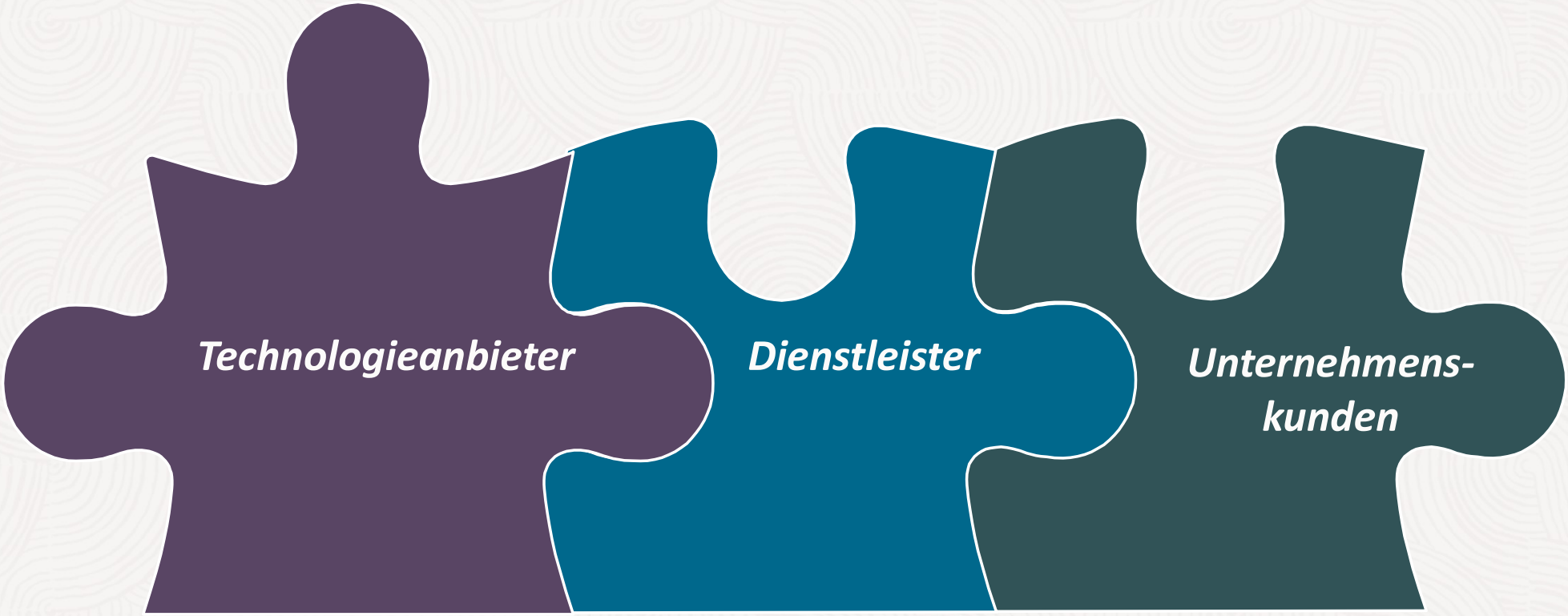
Aufbau einer Zero Trust SIP Umgebung

Zero Trust PSTN Anrufe

- SBC (der als Policy Enforcement Point fungiert) fragt Security Shield (der als Policy Engine fungiert) ab, um zu bestimmen, ob der Anruf zugelassen werden soll.
- Security Shield konsumiert mehrere ‘Signale’. In diesem Beispiel;
  - Internal and External DB’s of historical data that identifies known malicious callers
  - Die Session Classification Policy definiert, wann eine Sitzung zur zusätzlichen Authentifizierung abgelehnt oder umgeleitet werden soll.
  - AI/ML bietet eine kontinuierliche Sitzungsanalyse.
  - **Beachte:** TLS/mTLS mag unter Umständen nicht immer vom PSTN Provider unterstützt sein.



*Es gibt nicht die **eine** Lösung für Zero Trust …*



*…wir müssen **alle** zusammenarbeiten, um etwas zu erreichen*


ORACLE