



SAP Security Group Deutschland

Innovation gemeinsam erleben

3./4. Juni 2025

Cloud Security im Fokus SAP BTP

Yannick Voß & Udo Hofmann
NTT Data Business Solutions AG

Moin und Hallo

Yannick Voß

SAP Security Consultant
Seit 2016 bei NTT
Fokus auf Authentifizierung

Udo Hofmann

SAP Security Consultant
Seit 2025 bei NTT
Fokus auf Benutzer- und Berechtigungsverwaltung



Agenda

- 1. Grundsätzlicher Aufbau der BTP**
- 2. Die 5 Säulen der BTP Security**
- 3. Security-Herausforderungen**
- 4. Empfehlungen**
- 5. Take-Aways**





**Wer von Ihnen hat schon heute
die SAP BTP im Einsatz?**

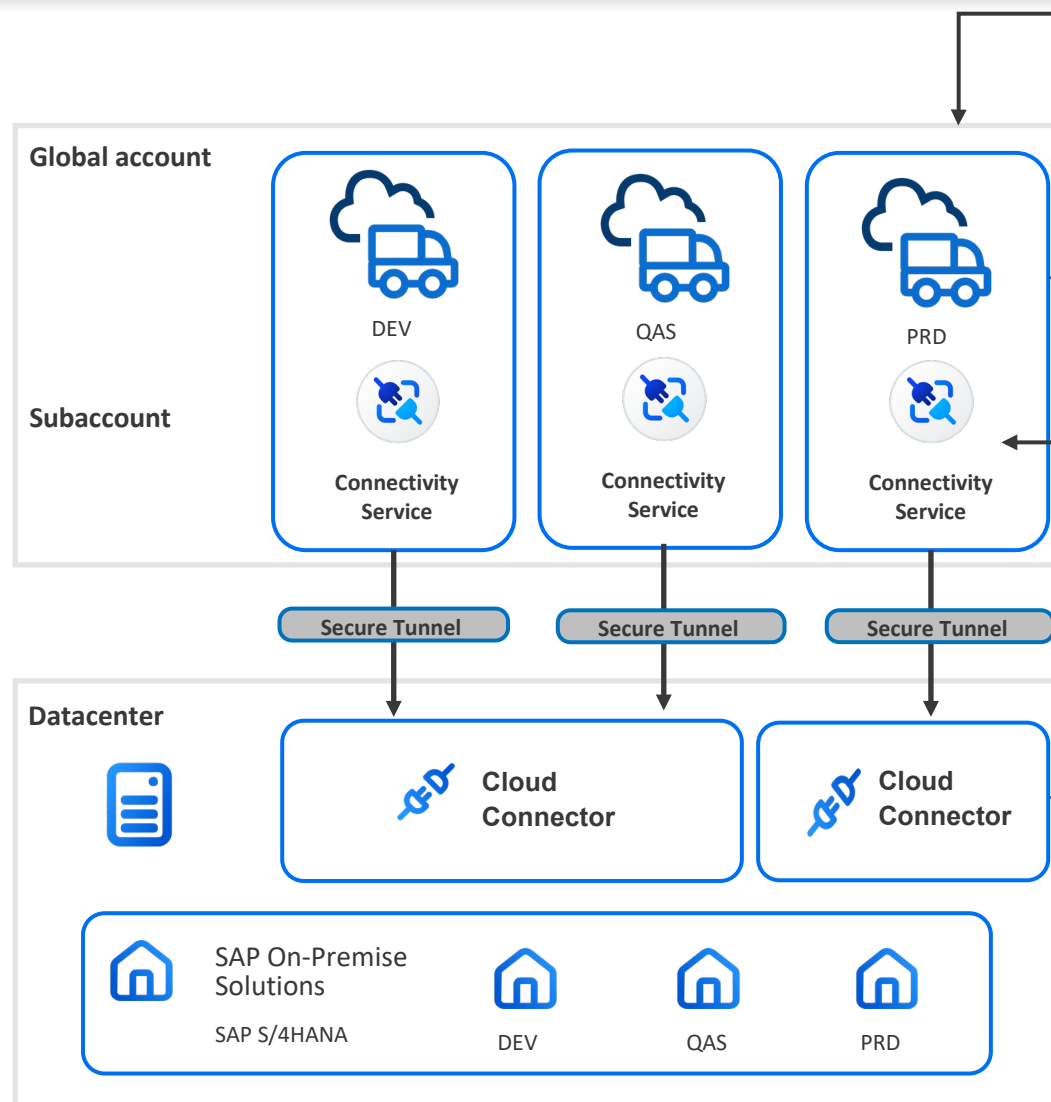


**Wer von Ihnen hat bereits eine
SAP BTP Security Strategie?**

1. Grundsätzlicher Aufbau der BTP

The background features a gradient from red on the left to dark blue on the right. It is decorated with various geometric elements: numerous small triangles of different sizes and orientations, some solid and some outlined; a series of vertical lines of varying heights, each topped with a small circle; and a prominent, wavy line composed of many small dots that spans the width of the image.

Grundsätzlicher Aufbau SAP BTP



Global Account

- Der Global Account ist die 1:1 Beziehung zu einem SAP Cloud Vertrag.
- Ermöglicht es die Kosten pro SAP BTP Instanz zu monitoren.

Sub Account

- Der SAP BTP Subaccount wird verwendet um Anwendungen zu deployen, Services zu nutzen und Abonnements zu verwalten. Er ermöglicht es, die Anforderungen einer Organisation zu strukturieren, einschließlich Benutzern und deren Berechtigungen.
- Üblicherweise entspricht die Architektur einer SAP On-Premise Landschaft (Skizziert am Beispiel des SAP BTP Transportation Managements)

SAP BTP Services

- Die SAP BTP Services sind Instanz basiert und zeichnen sich durch ihre Flexibilität, Integration und umfassenden Funktionen aus. Sie bieten eine zentrale Plattform für Anwendungsentwicklung und Datenmanagement.
- **Achtung!** Jeder Service, welcher abonniert wird, hat ggf. eine eigene Kostenstruktur.

SAP Cloud Connector

Der SAP Cloud Connector ist eine kritische Komponente für die Integration von Cloud- und On-Premise-Systemen.

- Er bietet eine sichere Verbindung zwischen Cloud-Anwendungen und On-Premise-Systemen.
- Cloud-Diensten kann Zugriff auf lokale Daten und Services ermöglicht werden.
- Darüber hinaus ermöglicht er eine unkomplizierte Einrichtung und Konfiguration für die Integration.



2. Die 5 Säulen der BTP Security

The background is a gradient from red on the left to dark blue on the right. It features several abstract elements: a series of overlapping triangles in various shades of red and purple, and a prominent wavy line composed of small dots that spans the width of the image near the bottom. Vertical lines of varying heights, some ending in small dots, are scattered across the lower half of the image.

Die fünf Säulen der BTP Security

Die SAP BTP hat Auswirkungen auf Ihre gesamte Sicherheitsstrategie!

Externe Zugriffe:



Über das Internet erfolgende Zugriffe können potenzielle Einfallstore für externe Bedrohungen darstellen.

Hohe Konnektivität:

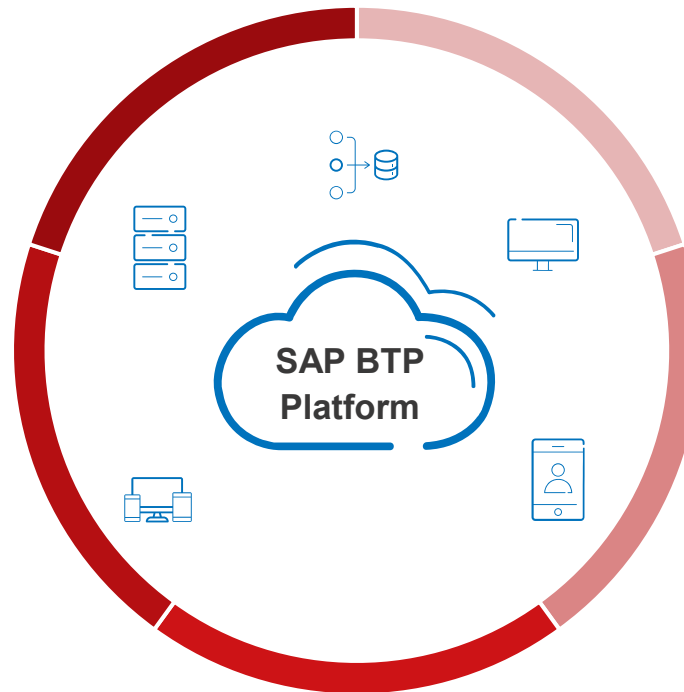


Die Bereitstellung von Daten über mehrere Input-/Output-Kanäle und die Anbindung an den SAP-Kern können die Angriffsfläche vergrößern.

Diverse Anwendungsfälle:



Die Nutzung der SAP BTP für verschiedene Geschäfts- und IT-Prozesse erhöht die Komplexität und stellt höhere Anforderungen an die Sicherheit.



1

Richtlinien & Verantwortung

Klare Security-Richtlinien und definierte Rollen steuern Verantwortlichkeiten und setzen Prioritäten in der SAP BTP Security.

2

Risikomanagement

Potenzielle Sicherheitsrisiken werden frühzeitig identifiziert und bewertet, um geeignete Schutzmaßnahmen zu implementieren.

3

Schutzmaßnahmen für Anwendungen

Sicherheitsprozesse und -kontrollen werden gezielt an verschiedene Anwendungsszenarien angepasst, um Schwachstellen zu minimieren.

4

Identitäts- & Zugriffsmanagement

Ein sicheres Identitäts- und Zugriffsmanagement ermöglicht die effektive Verwaltung von Benutzern, Rollen und Berechtigungen und verhindert unbefugten Zugriff.

5

Sicheres IT-Ökosystem

Eine robuste IT-Infrastruktur wird durch eine sichere Architektur, geschützte Schnittstellen und kontinuierliche Sicherheitskontrollen gewährleistet.

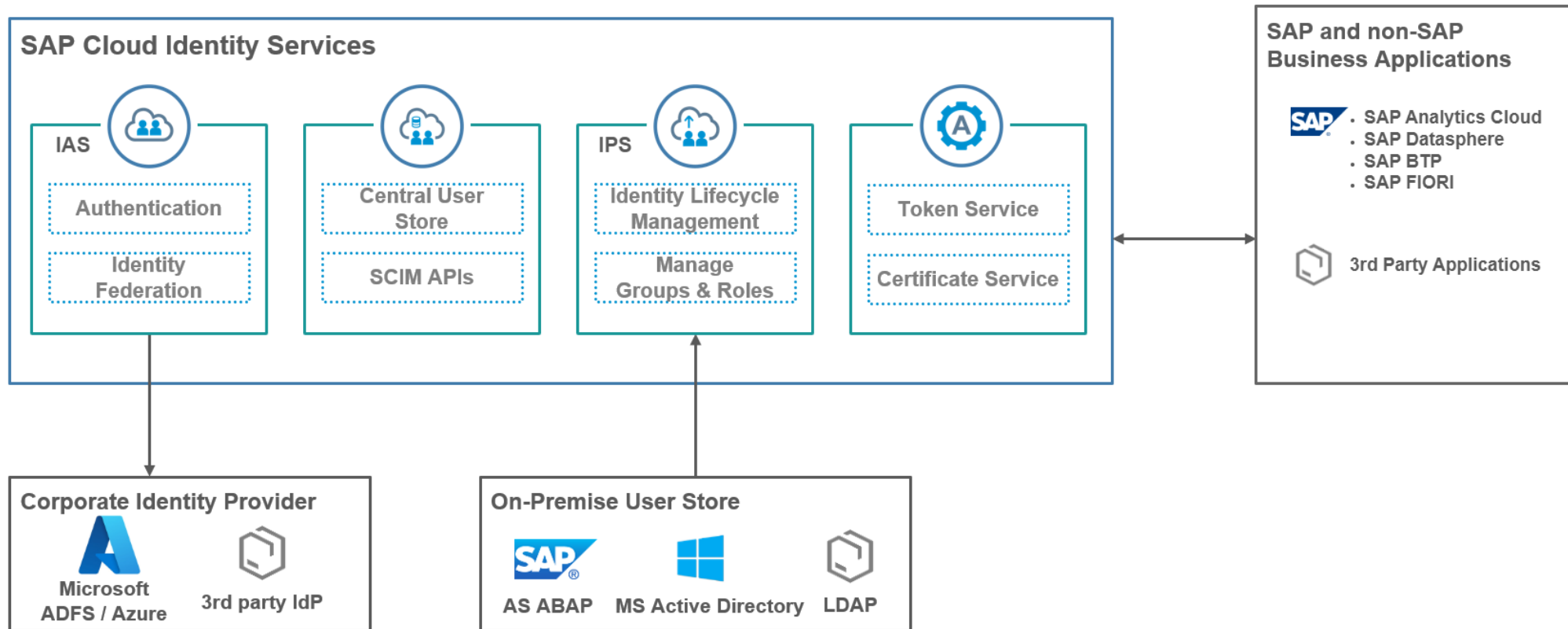


3. Security Herausforderungen

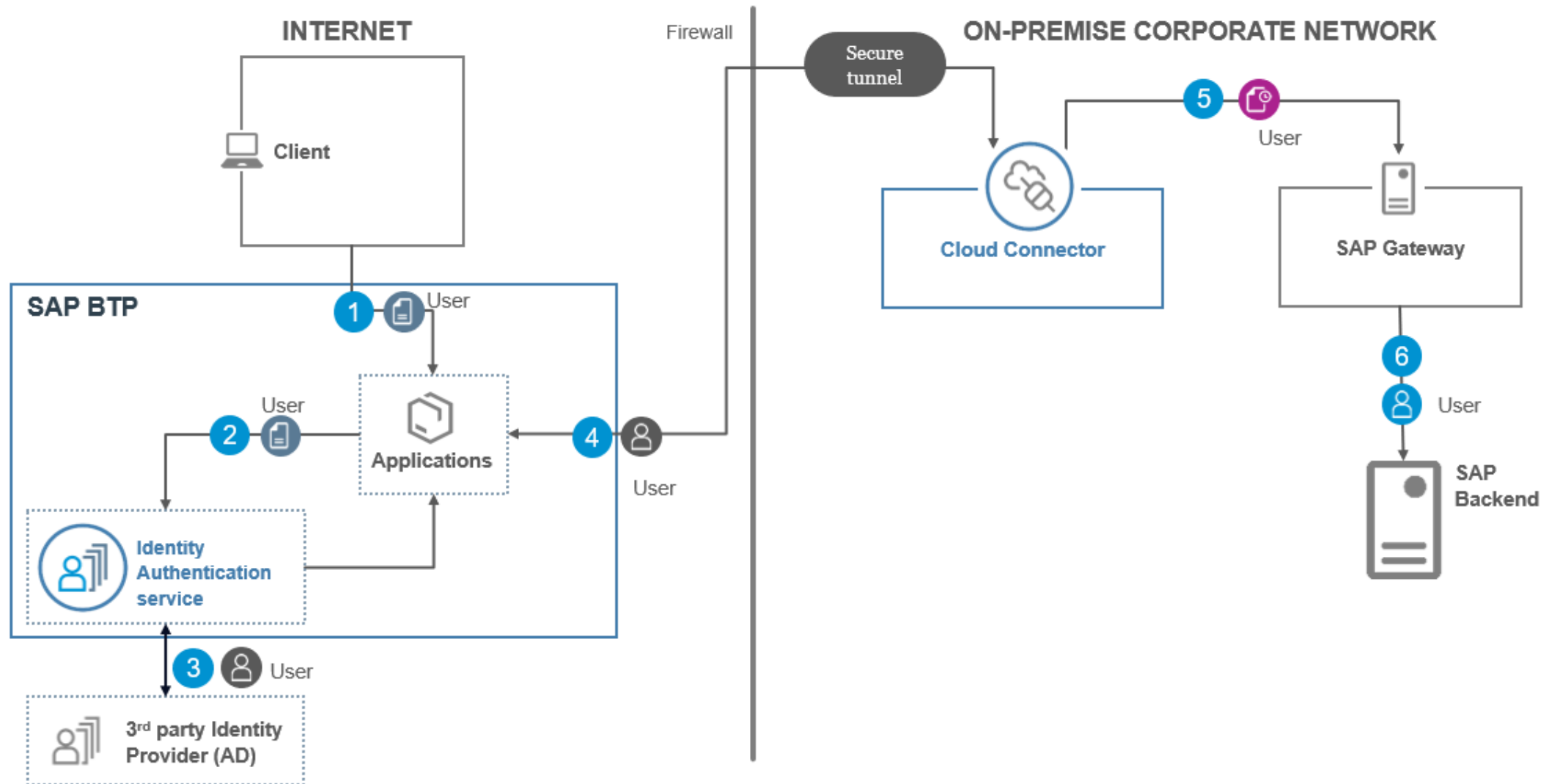
The background features a gradient from red on the left to blue on the right. It is decorated with various geometric elements: translucent triangles of different sizes and orientations, thin vertical lines with small circular dots at their bases, and a prominent wavy line composed of a dense grid of small dots that spans the width of the image.

Security Herausforderungen: Trusted Identity Provider

Trusted Identity Provider (IDP) stellen Authentifizierung und Autorisierung außerhalb des BTP-Subaccounts sicher!



Security Herausforderungen: Principal Propagation

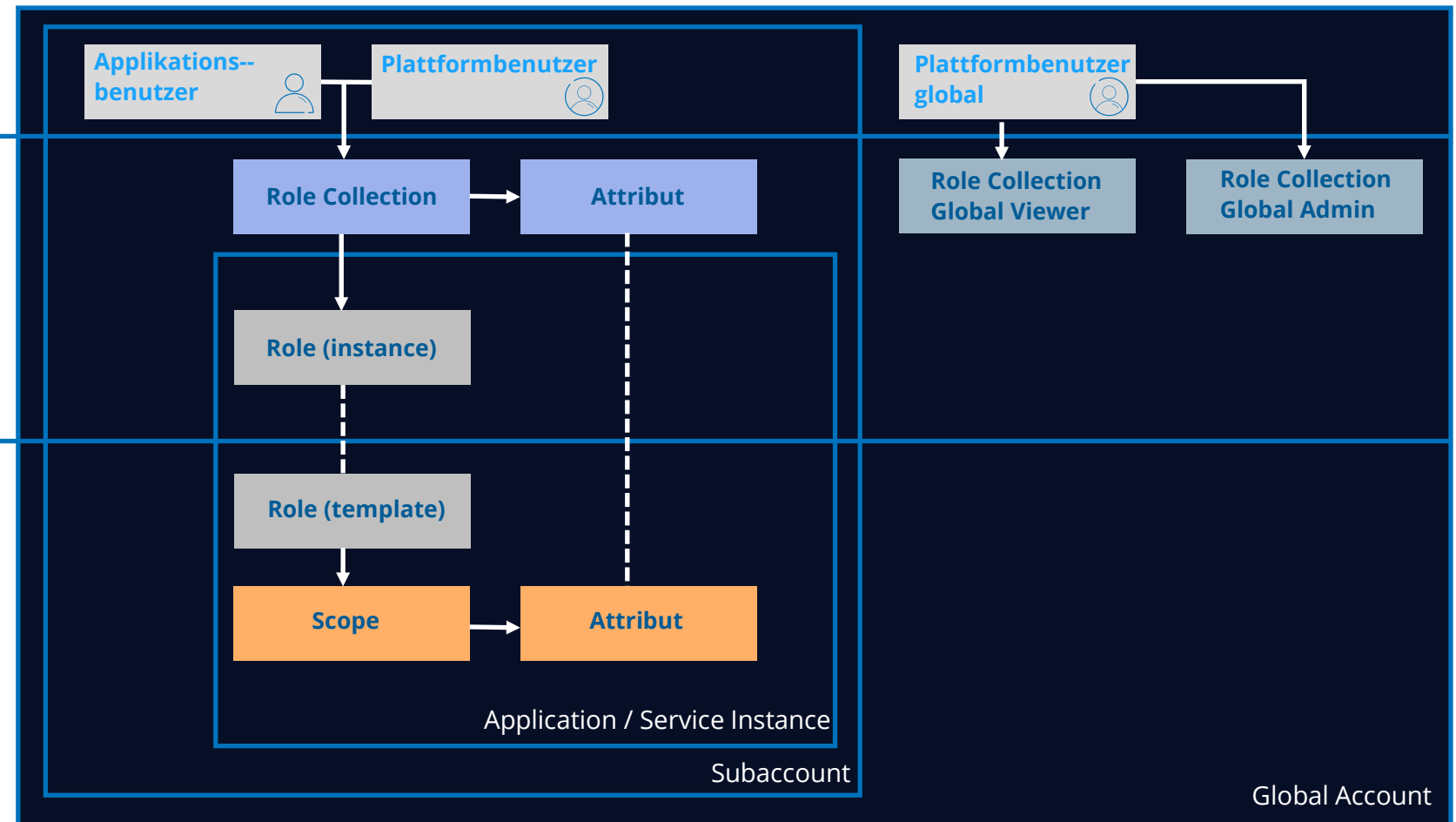


Rollenkonzept in der BTP

Benutzer Level

Rollen Level

Technische Autorisierung



Berechtigungsmanagement

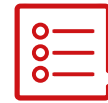
Modellierung

Ein durchdachtes Rollenkonzept bildet die Grundlage für eine sichere und effiziente Berechtigungssteuerung. Entscheidend ist die konsistente Anwendung für alle relevanten BTP-Dienste und -Applikationen.



Compliance

SoD-Checks sind auch in der BTP wichtig – interne Kontrollen sollten effizient und regelmäßig überprüft werden.



Governance

Klare Verantwortlichkeiten, nachvollziehbare Zuweisungen und dokumentierte Prozesse sind essenziell.



Automatisierung

Zentralisieren Sie die Berechtigungsverwaltung mit SAP Cloud Identity Services oder passenden IAM-Lösungen.



4. Empfehlungen

The background features a gradient from red on the left to dark blue on the right. It is decorated with various geometric elements: several triangles of different sizes and orientations, some with internal line patterns; a series of vertical lines of varying heights, each topped with a small dot; and a prominent, wavy line composed of many small dots that spans the width of the image near the bottom.

Empfehlungen: Security Assessments

Mithilfe von Security Assessments werden detailliert die Schwachstellen in der Konfiguration aufgezeigt.



- ✓ Regelmäßige Security Assessments & Penetration Tests durchführen
- ✓ Sicherheitsrisiken aus der Perspektive von Angreifern bewerten
- ✓ Automatisierte Security Assessments nutzen, um Konfigurationsschwachstellen zu identifizieren
- ✓ Drittanbieter-Tools einbinden, um kontinuierliche Sicherheitsprüfungen zu gewährleisten



Ziel: Proaktive Erkennung & Schließen von Sicherheitslücken in der BTP

▼ 5.1.1 Cloud Connector

- ▶ 5.1.1.1 [2895_2] Cloud Connector Subaccounts
- ▶ 5.1.1.2 [2900] Cloud Connector Hochverfügbarkeit
- ▶ 5.1.1.3 [2901] Cloud Connector Authentifizierung
- ▶ 5.1.1.4 [2906] Cloud Connector Zertifikate
- ▶ 5.1.1.5 [3311_2] Security State ciphers
- ▶ 5.1.1.6 [3311_3] Security State ldapAuth
- ▶ 5.1.1.7 [3311_4] Security State trustStore
- ▶ 5.1.1.8 [3311_1] Security State uiCert
- ▶ 5.1.1.9 [2896] Cloud Connector Version
- ▶ ⓘ 5.1.1.10 [3312] Cloud Connector Alert Einstellungen
- ▶ ⓘ 5.1.1.11 [3313] Cloud Connector Alerts anzeigen
- ▶ ⓘ 5.1.1.12 [3309] Cloud Connector Auditlog Einstellungen
- ▶ ⓘ 5.1.1.13 [2902] Cloud Connector Solution Manager Konfiguration
- ▶ ⓘ 5.1.1.14 [2895_1] Cloud Connector Subaccounts
- ▶ ⓘ 5.1.1.15 [3310] Cloud Connector Auditlog anzeigen



Empfehlungen: Security Monitoring

Ein umfassendes Security Monitoring sollte ein elementarer Bestandteil einer Security Strategie sein.



Ohne verlässliche Informationen in Bezug auf Ihre Security können Sie **nur reagieren** und **nicht proaktiv** agieren.

Bei Cyberangriffen sind Sie dann nur der „zweite Sieger“!



Nutzen Sie spezielle „Datensensoren“, um beispielsweise das Security Audit Log der BTP / Cloud Foundry auszuwerten.



Legen Sie Zuständigkeiten fest: Wer analysiert Findings? Wer setzt Maßnahmen um? Haben Sie genug Kapazitäten?



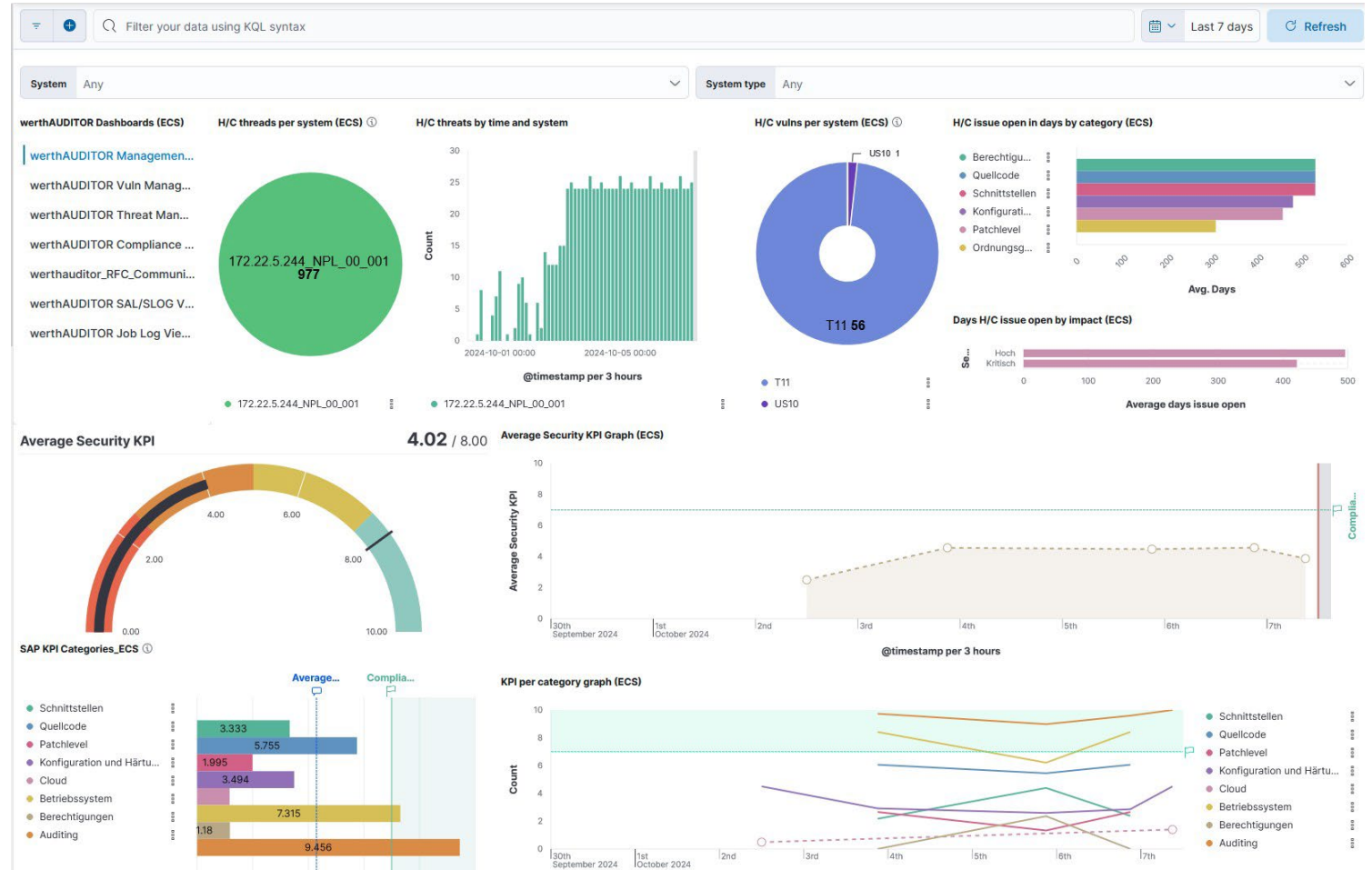
Entwickeln Sie eine Strategie, um in angemessener Zeit auf Security Vorfälle reagieren zu können. Haben Sie ein SOC im Zugriff oder betreiben Sie „externe Security“?



Empfehlung: Unterschiedliche Welten

Betrachten Sie Sicherheitsaspekte ganzheitlich und fördern Sie die Zusammenarbeit über Abteilungsgrenzen hinweg.

Die Anforderungen an SAP und Cloud wachsen zunehmend zusammen. Integrieren Sie deshalb auch das ‚Microsoft Infrastruktur-Team‘ in die Sicherheitsstrategien.

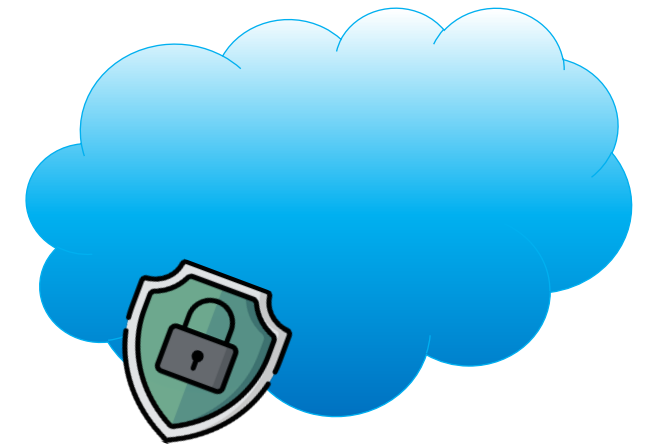


5. Take Aways

The background is a gradient from red on the left to dark blue on the right. It features several geometric elements: a series of thin, vertical lines of varying heights, each topped with a small dot; a wavy line composed of many small dots that spans the width of the image; and various translucent triangles and polygons scattered throughout the upper half.

Take Aways

- ✓ Bewerten Sie die SAP BTP Security nicht isoliert – sie sollte integraler Bestandteil Ihrer übergeordneten Security Strategie sein.
- ✓ Entwickeln Sie robuste Konzepte für Authentifizierung und Autorisierung, die den Sicherheitsanforderungen Ihres Unternehmens gerecht werden.
- ✓ Gestalten Sie ein User-Provisioning-Konzept, welches die spezifischen Prozesse und Anforderungen Ihres Unternehmens abbildet.
- ✓ Security Assessments und kontinuierliches Monitoring sind wesentliche Bestandteile einer erfolgreichen BTP Security Strategie.
- ✓ Gehen Sie mit Vertrauen und offenen Armen auf die SAP BTP zu – jedes Unternehmen fängt irgendwann einmal an...



Wir freuen uns über Ihre Kontaktaufnahme!

Yannick Voß

SAP Security Consultant
Platforms & Integration

www.nttdata-solutions.com
yannick.voss@nttdata.com

Udo Hofmann

SAP Security Consultant
Platforms & Integration

www.nttdata-solutions.com
udo.hofmann@nttdata.com

