European Journal of Computer Science and Information Technology, 14(1),1-11, 2026

Print ISSN: 2054-0957 (Print)

Online ISSN: 2054-0965 (Online)

Website: https://www.eajournals.org/

Publication of the European Centre for Research Training and Development -UK

Security Architecture and Zero-Trust Models for SAP BTP (Business Technology Platform)

Vishnu Kiran Bollu
Senior SAP Security & Governance Specialist

doi: https://doi.org/10.37745/ejcsit.2013/vol14n1111 Published January 11, 2026

Citation: Vishnu Kiran Bollu (2026) Security Architecture and Zero-Trust Models for SAP BTP (Business Technology Platform), *European Journal of Computer Science and Information Technology*, 14(1),1-11

Abstract: *The acceleration of cloud transformation has brought SAP Business Technology Platform (SAP BTP) to the center of intelligent enterprise architectures. As organizations expand hybrid landscapes integrating SAP S/4HANA, cloud extensions, APIs, and third-party systems, traditional perimeter-based security models have become insufficient [3]. This paper presents comprehensive security architecture grounded in Zero-Trust principles, continuous verification, identity centric security, least privilege design, and micro segmentation, aligned with industry standards defined by NIST and adapted for SAP BTP's multi-tenant environment. The study evaluates identity governance using SAP Cloud Identity Services, secure integration patterns for SAP CPI, and AI-driven threat detection mechanisms. Through comparative assessments and real-world architectural patterns, this work demonstrates that Zero-Trust adoption significantly enhances confidentiality, integrity, audit readiness, and resilience across SAP BTP ecosystems [5], [10].*

Keywords: SAP Business Technology Platform (SAP BTP), SAP Cloud Identity Services, Zero-Trust Architecture (ZTA), Identity and Access Governance (IAG)

INTRODUCTION

Cloud security challenges have intensified due to API-driven integrations, distributed workloads, and the rise of multi-tenant cloud environments. SAP BTP now serves as a foundational layer for application extensions, analytics, automation, and enterprise integration. As a result, security cannot rely on legacy network boundaries or periodic audits but must shift toward identity-centric, continuously validated access models as recommended in Zero-Trust architecture frameworks [3].

SAP BTP operates across diverse cloud infrastructures (AWS, Azure, GCP), hosting services such as Cloud Foundry, Kyma, SAP CPI/Integration Suite, and SAP HANA Cloud. Each of these components introduces unique security risks, including misconfigurations, broad entitlements, unsecured destinations, and token exposure, issues frequently highlighted in cloud security assessments [5], [9]. Zero-Trust provides a modern framework combining continuous verification, least-privilege enforcement, and micro-segmentation to mitigate these risks in multi-layered cloud environments [3], [6].

Given SAP BTP's role in enterprise transformation, security must be governed through structured identity services such as IAS/IPS [2], automated policy enforcement, strong runtime isolation, and AI-assisted threat analytics [8]. These practices align with emerging research that identifies Zero-Trust as a core strategy for future cloud security resilience [10]. Therefore, this paper establishes the architectural principles and deployment blueprint needed to implement Zero-Trust security effectively within SAP BTP ecosystems.

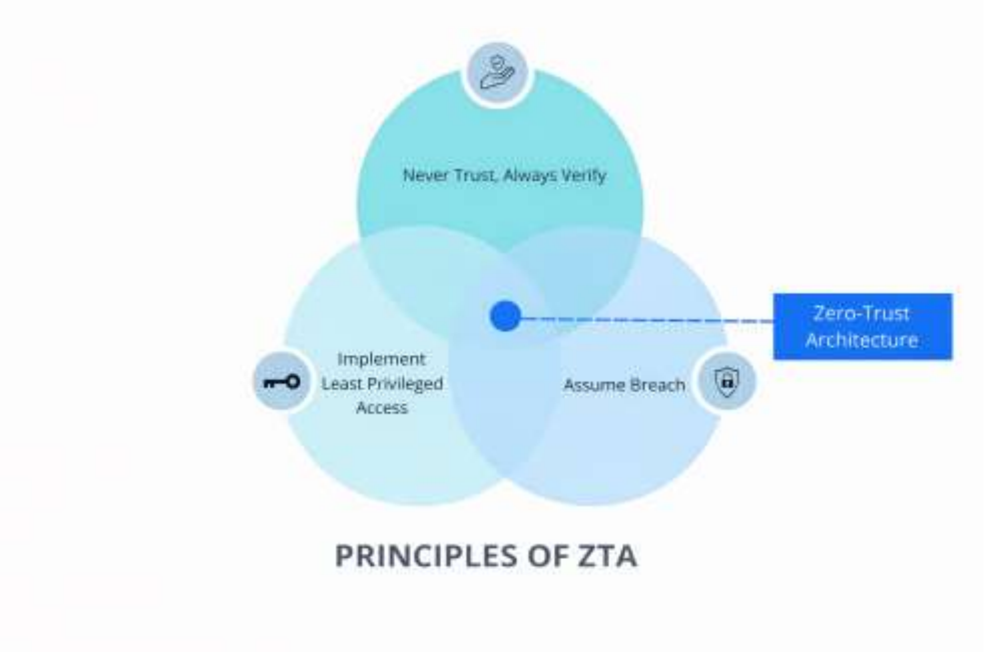
Evolution of SAP Security Toward Zero-Trust

The security model for SAP landscapes has evolved significantly as enterprises transition from monolithic, on-premise ERP systems to distributed, cloud-native architectures powered by SAP Business Technology Platform (SAP BTP). Traditional SAP security relied heavily on perimeter defenses, network segmentation, role-based access control, and implicit trust within corporate boundaries. While effective in tightly controlled environments, these approaches are inadequate for modern SAP ecosystems characterized by multi-cloud deployments, API-driven integrations, and continuous external connectivity [5], [9].

SAP BTP introduces new security challenges through its multi-tenant architecture, decentralized runtimes (Cloud Foundry, Kyma, ABAP Environment), and extensive use of OAuth-based service communication and APIs [1], [4]. These capabilities significantly expand the attack surface, increasing exposure to identity misuse, token replay attacks, misconfigured entitlements, and lateral movement across subaccounts. Legacy perimeter-based controls lack the granularity, visibility, and adaptability required to address these risks effectively [3], [5].

Several factors have accelerated Zero-Trust adoption within SAP landscapes. First, hybrid and multi-cloud deployments demand consistent security controls independent of infrastructure boundaries [6]. Second, API centric integration via SAP CPI and API Management necessitates strong service to service authentication and fine-grained authorization [4]. Third, increased regulatory scrutiny requires continuous monitoring, traceability, and audit ready security controls rather than periodic assessments [7], [10]. Finally, the growing sophistication of cloud native attacks such as credential theft, OAuth abuse, and supply-chain compromise exposes fundamental weaknesses in static security models [5], [8].

As a result, SAP security is transitioning toward the first identity architecture anchored by SAP Cloud Identity Services, granular entitlement governance, subaccount level segmentation, and centralized observability [2], [7]. Automation and policy driven controls further reduce configuration drift and enforce least privilege access consistently across development and production environments [9], [10]. This evolution establishes Zero Trust not as an optional enhancement, but as a foundational requirement for securing SAP BTP and supporting resilient, compliant enterprise cloud transformation.



SAP BTP Security Architecture: Core Components

SAP Business Technology Platform (SAP BTP), delivered by **SAP SE**, provides a cloud-native foundation for enterprise application development, integration, and analytics across hybrid and multi cloud environments. While SAP BTP embeds native security controls, effective protection in distributed landscapes requires an explicit alignment with Zero-Trust architecture principles rather than reliance on implicit platform trust [1], [3].

At the core of SAP BTP security lies an **identity centric control plane**, where all human and non-human access is mediated through centralized identity services. Identity federation, multi-factor authentication, and conditional access policies ensure continuous verification and eliminate network based trust assumptions [2], [6]. Trust relationships between directories and subaccounts are carefully managed to prevent unauthorized privilege propagation across tenants.

Account, directory, and entitlement governance form the second critical layer. SAP BTP's hierarchical structure enables scalability but introduces risks of over entitlement and lateral access if not governed properly. Zero Trust adoption enforces subaccount isolation, environment-based segmentation, least-privilege service enablement, and separation of duties between platform administration, security governance, and development teams [1], [9].

Unlike traditional SAP environments, **network and connectivity security** in SAP BTP is explicitly authenticated and encrypted. All communication relies on secure destinations, OAuth2-based authorization, certificate driven trust, and mTLS for service-to-service interactions. Backend connectivity through SAP Cloud Connector follows Zero-Trust tunneling principles, ensuring internal systems are never directly exposed to the cloud [3], [4], [5].

Application runtime and integration security further reinforce Zero Trust by isolating workloads across Cloud Foundry, Kyma, and the ABAP environment. Dedicated service instances scoped and short-lived tokens, secure CI/CD pipelines, and runtime monitoring reduce the risk of credential misuse and integration compromise [4], [7]. Integration services such as SAP Cloud Integration require strict credential separation and message-level security controls to protect data flows.

Finally, **data protection and observability** provide continuous assurance across the platform. SAP BTP enforces encryption at rest and in transit with tenant specific key management, while centralized logging and alerting enable real time monitoring and AI assisted anomaly detection [1], [7], [8]. Together, these capabilities ensure visibility, audit readiness, and rapid response to emerging threats.

In summary, SAP BTP security architecture, when designed around Zero-Trust principles, establishes a resilient, identity first security foundation. By integrating identity governance, entitlement control, secure connectivity, runtime isolation, and continuous observability, organizations can significantly reduce attack surfaces and support secure, compliant enterprise cloud transformation.

Zero-Trust Framework for SAP BTP

Zero-Trust Architecture (ZTA) provides a modern security paradigm that eliminates implicit trust and enforces continuous verification across cloud platforms. In SAP Business Technology Platform (SAP BTP), Zero-Trust functions as an integrated framework rather than a single control, spanning identity, policy enforcement, connectivity, and continuous monitoring in alignment with NIST SP 800-207 guidelines [3].

At the foundation of the framework is an **identity centric control plane**, where all user and service interactions are governed through centralized identity services provided by **SAP SE**. Identity federation, multi-factor authentication, conditional access, and token-based authentication ensure that access decisions are evaluated dynamically rather than relying on static network trust [2], [6].

A core principle of Zero-Trust in SAP BTP is **least privilege access**, enforced through fine-grained role collections, scoped service entitlements, and strict environment segregation. Broad administrative access and shared technical users are avoided to reduce privilege sprawl and lateral movement risks [1], [9]. Access policies are centrally governed and continuously reviewed to maintain compliance and audit readiness [10].

Secure connectivity and micro segmentation further strengthen the Zero-Trust model. All communication within SAP BTP relies on explicit authentication and encryption using OAuth2, mTLS, and secure destination configurations. Integration with on-premises systems via SAP Cloud Connector follows Zero-Trust tunneling principles, ensuring backend systems are never directly exposed [4], [5]. Subaccount-level isolation limits the impact of potential compromises.

Continuous monitoring and adaptive trust decisions complete the framework. Centralized logging, integration telemetry, and identity activity are analyzed in real time, often augmented by AI-driven behavioral analytics to detect anomalies such as token misuse or abnormal access patterns [7], [8]. Trust levels are dynamically adjusted based on observed behavior, enabling proactive threat containment rather than reactive incident response.

In summary, the Zero-Trust framework for SAP BTP establishes a resilient, identity-first security foundation that supports secure cloud extensibility, reduces attack surfaces, and enhances compliance assurance. By combining continuous verification, least-privilege enforcement, micro-segmentation, and real-time observability, organizations can securely scale SAP BTP while aligning with modern enterprise security and regulatory requirements.

Identity & Access Governance in SAP BTP

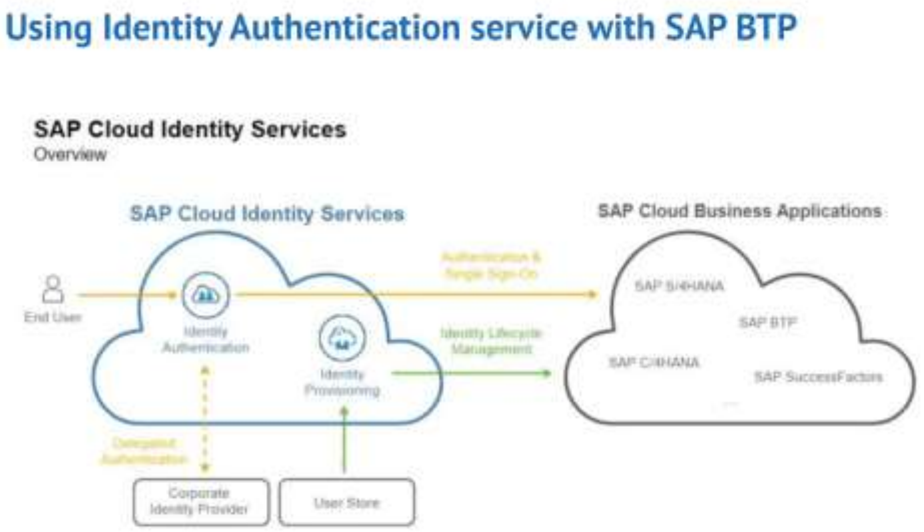
Identity and Access Governance (IAG) is the cornerstone of Zero-Trust security in SAP Business Technology Platform (SAP BTP). As SAP BTP operates in a distributed, multi-tenant cloud environment, identity replaces network location serves as the primary security boundary. Effective governance ensures that only authenticated and authorized users, services, and integrations can access platform resources with permissions continuously evaluated and constrained by policy [1], [3].

At the core of BTP identity governance is centralized identity management provided by **SAP SE**, enabling federation with enterprise identity providers and consistent enforcement of authentication policies across applications and services. Single sign-on, multi-factor authentication, and conditional access controls reduce reliance on static credentials and significantly lower the risk of identity compromise [2], [6]. In a Zero-Trust model, authentication is treated as a continuous process, not a one-time validation.

Access governance in SAP BTP is enforced through **role collections, entitlements, and trust configurations** across global accounts, directories, and subaccounts. Zero-Trust principles require that access be provisioned using least-privilege design, avoiding broad default roles and unrestricted administrative access. Environment-based segregation (development, quality, and production) and business-domain isolation further reduce blast radius and prevent unauthorized lateral movement [1], [9].

A critical aspect of identity governance is the separation of **human and non-human identities**. Technical users, service instances, and integration flows rely on OAuth2 tokens, certificates, and scoped authorizations instead of shared credentials. This approach minimizes credential leakage, supports short-lived access tokens, and enables precise traceability for audit and incident response [4], [7].

Continuous governance is achieved through **automated access reviews, entitlement monitoring, and audit logging**. Identity events, role changes, and privileged access activities are logged centrally and integrated with SIEM platforms for real-time visibility and anomaly detection [7], [8]. Automation reduces configuration drift and ensures that access policies remain aligned with compliance requirements such as SOX, GDPR, and industry regulations [10].


Using Identity Authentication service with SAP BTP
SAP Cloud Identity Services
Overview
SAP Cloud Identity Services
SAP Cloud Business Applications
End User
Identity Authentication
Authentication & Single Sign-On
Identity Provisioning
Identity Lifecycle Management
Delegated Authentication
Corporate Identity Provider
User Store
SAP S/4HANA
SAP BTP
SAP C/4HANA
SAP SuccessFactors

Network, Integration, Application Runtime, and Data Security in SAP BTP

Network, integration, and application runtime security in SAP Business Technology Platform (SAP BTP) are fundamentally designed around Zero-Trust principles, where no network, workload, or integration path is implicitly trusted. Unlike traditional SAP landscapes that relied on trusted internal networks, SAP BTP enforces **explicit authentication, encryption, and authorization for every connection and execution context**, regardless of origin [3], [5].

All network communication within SAP BTP is secured using OAuth2, JSON Web Tokens (JWT), certificates, and mutual TLS (mTLS). Backend connectivity is governed through secure destination services and policy-controlled credential handling rather than static secrets. Integration with on-premises SAP and non-SAP systems is enabled through SAP Cloud Connector using Zero-Trust tunneling, ensuring that internal systems are never directly exposed to the public cloud [4]. These controls significantly reduce risks associated with credential leakage, unsecured endpoints, and unauthorized system access.

Integration services such as SAP Cloud Integration and API Management are critical attack surfaces in BTP environments. Zero-Trust integration security mandates **dedicated credentials per integration flow**, short-lived and scoped tokens, enforced HTTPS communication, and strict separation of development and production interfaces. API traffic is continuously monitored to detect abnormal patterns, excessive calls, or token misuse, enabling early identification of integration-centric threats [7], [8].

At the application runtime layer, SAP BTP supports multiple execution environments including Cloud Foundry, Kyma (Kubernetes), and the ABAP Environment each providing tenants and workload isolation.

Zero-Trust principles extend runtime security by enforcing container isolation, namespace-level segmentation, secure CI/CD pipelines, and runtime authorization checks. Applications and services are granted only the minimum permissions required, preventing privilege escalation and lateral movement even in the event of compromise [1], [9].

Data security is enforced through encryption by default across all layers. SAP BTP applies strong encryption for data at rest and in transit, combined with tenant-specific key management to maintain cryptographic isolation in multi-tenant environments. Sensitive data processed by applications and integrations is further protected through masking, tokenization, and controlled access policies aligned with regulatory requirements such as SOX and GDPR [7], [10].

Continuous observability ties together network, integration, runtime, and data security. Centralized logging, audit trails, and telemetry from APIs, runtimes, and integration flows are forwarded to enterprise SIEM platforms, where AI assisted analytics identify anomalous behavior, suspicious access patterns, and potential breaches in near real time [8]. This continuous feedback loop enables adaptive trust decisions and rapid containment of threats.

Threat Detection, Monitoring, and AI-Driven Security in SAP BTP

Effective Zero-Trust security in SAP Business Technology Platform (SAP BTP) depends on continuous visibility and adaptive threat detection rather than static preventive controls alone. Given the dynamic nature of cloud-native workloads, API-driven integrations, and distributed identities, traditional rule-based monitoring is insufficient to detect advanced and stealthy attacks. SAP BTP therefore relies on centralized observability combined with AI-driven analytics to identify threats in near real time [7], [8].

At the foundation of threat detection is **comprehensive telemetry collection** across identity, network, application runtime, and integration layers. SAP BTP generates detailed audit logs for authentication events, role and entitlement changes, API access, integration message flows, and runtime activities. These logs are centrally aggregated and forwarded to enterprise SIEM platforms, enabling correlation across multiple services and environments delivered by **SAP SE** [1], [7].

Zero-Trust monitoring emphasizes **continuous verification and behavioral analysis** rather than reliance on static signatures. Identity activity is monitored for anomalies such as abnormal login patterns, excessive token usage, privilege escalation attempts, and unusual access timing. API and integration telemetry is analyzed for deviations in call frequency, payload characteristics, and token scope usage, which may indicate misuse or compromise [5], [8].

AI-driven security analytics play a critical role in scaling threat detection across large SAP BTP landscapes. Machine learning models analyze historical baselines to detect subtle deviations that traditional threshold-based alerts may miss. These capabilities enable early identification of threats such as OAuth token abuse, credential stuffing, integration manipulation, and lateral movement attempts across subaccounts or runtimes [8].

Continuous monitoring also supports **adaptive trust decisions**, a core principle of Zero-Trust. When elevated risk is detected, access can be dynamically restricted, tokens invalidated, sessions terminated, or additional authentication challenges enforced. This shift from reactive incident response to proactive containment significantly reduces dwell time and potential impact of security incidents [3], [6].

Typical Risk Scenarios & Attack Vectors in SAP BTP

As SAP Business Technology Platform (SAP BTP) enables cloud-native extensibility, integration, and multi-tenant operations, it introduces a distinct set of security risks that differ from traditional SAP landscapes. These risks primarily arise from identity misuse, misconfigurations, API exposure, and integration complexity rather than direct infrastructure compromise. Understanding these attack vectors is critical for designing effective Zero-Trust controls within environments operated by **SAP SE** [1], [3].

One of the most common risk scenarios in SAP BTP is **identity and token misuse**. OAuth tokens, JWTs, and service credentials used for application and integration access can be exploited if they are long-lived, overly scoped, or improperly stored. Token replay attacks and unauthorized API access are particularly impactful in API-driven BTP architectures [4], [8]. Zero-Trust mitigates this risk through short-lived tokens, continuous verification, and strict scope enforcement.

Misconfigured entitlements and role collections represent another significant attack vector. Broad role assignments, directory-level entitlement inheritance, and insufficient separation of duties can lead to privilege escalation and unauthorized access across subaccounts. Such misconfigurations are a leading cause of security findings in cloud environments and often enable lateral movement between applications and services [1], [9].

Integration-layer vulnerabilities are especially critical in SAP BTP due to heavy reliance on SAP Cloud Integration and API Management. Shared credentials, unsecured destinations, lack of mTLS, or exposed endpoints can allow attackers to manipulate business processes, exfiltrate data, or inject malicious payloads into integration flows [4], [5]. Zero-Trust integration design emphasizes dedicated credentials, encrypted connectivity, and continuous monitoring of message flows.

Another prevalent risk involves **lateral movement across tenants or environments**. Weak isolation between development, quality, and production subaccounts—or excessive trust between directories—can allow attackers to pivot from low-risk environments to sensitive production workloads. Micro-segmentation and explicit trust boundaries are essential to contain such threats [3], [9].

Finally, **insufficient logging and monitoring** significantly increases dwell time for attackers. Without centralized audit trails and real-time analytics, malicious activity such as abnormal API usage, unauthorized role changes, or integration abuse may go undetected for extended periods. This risk underscores the importance of continuous observability and AI-driven threat detection in SAP BTP security architectures [7], [8].

Automation, Policy Enforcement, and Continuous Compliance in SAP BTP

As SAP Business Technology Platform (SAP BTP) environments scale across multiple subaccounts, regions, and services, manual security controls become unsustainable and error prone. Automation and policy driven enforcement are therefore essential to operationalizing Zero Trust at scale and maintaining continuous compliance. In SAP BTP, automation ensures that security controls are applied consistently, deviations are detected early, and compliance evidence is generated continuously rather than retrospectively [3], [7].

Policy enforcement in SAP BTP is centered on codifying security requirements as machine enforceable rules. Identity policies define authentication strength, conditional access, and role assignment constraints, while entitlement policies restrict service enablement and prevent unauthorized inheritance across directories and subaccounts. By embedding these policies into provisioning workflows, organizations prevent misconfigurations that commonly lead to privilege escalation and audit findings [1], [9].

Infrastructure as Code (IaC) and CI/CD integration play a critical role in Zero Trust automation. BTP subaccounts, entitlements, destinations, and runtime configurations are deployed through version-controlled pipelines with embedded security checks. Automated validation ensures that only compliant configurations such as encrypted connectivity, scoped credentials, and environmental isolation are promoted to production. This approach significantly reduces configuration drift and enforces consistent security baselines across landscapes managed by **SAP SE** [4], [10].

Continuous compliance monitoring replaces periodic audit preparation with real-time assurance. Identity changes, role assignments, entitlement updates, integration modifications, and runtime events are logged centrally and correlated against defined compliance policies. Deviations from approved baselines trigger alerts or automated remediation actions, enabling rapid correction before risks materialize [7], [8]. This model aligns strongly with regulatory frameworks such as SOX, GDPR, and industry-specific controls that require traceability and timely response.

Automation also enables **continuous evidence generation** for audits. Security logs, access reviews, policy attestations, and configuration snapshots are captured automatically and retained in audit-ready formats. This reduces manual effort, improves audit accuracy, and shortens compliance cycles while increasing confidence in control effectiveness [9], [10].

Implementation Roadmap, Challenges, and Limitations for Zero-Trust Adoption in SAP BTP

Adopting Zero-Trust security in SAP Business Technology Platform (SAP BTP) requires a **phased, governance-driven approach** to balance risk reduction with operational continuity across multi-tenant, multi-cloud environments delivered by **SAP SE**. A structured roadmap enables organizations to incrementally embed Zero-Trust controls while addressing practical constraints related to identity complexity, entitlement governance, and operational maturity.

The **implementation roadmap** typically progresses through four stages. First, organizations establish a **foundation** by assessing current identity posture, rationalizing roles and entitlements, enforcing identity federation and MFA, and enabling centralized logging. Second, **identity and access hardening** embeds least-privilege role design, separation of duties, conditional access, and strict segregation of human and service identities. Third, **secure connectivity and micro-segmentation** are implemented using OAuth2, mTLS, secure destinations, Zero-Trust tunneling via Cloud Connector, and environment isolation across subaccounts. Finally, **automation and continuous compliance** integrate policy enforcement into CI/CD pipelines and Infrastructure-as-Code, supported by real-time monitoring, AI-assisted analytics, and automated audit evidence generation.

Despite its benefits, Zero-Trust adoption in SAP BTP presents **notable challenges and limitations**. **Identity complexity** including hybrid users, multiple identity providers, and large volumes of service identities demand mature IAM processes and strong operational discipline. **Entitlement governance** across directories and subaccounts can inadvertently propagate privileges if automation and clear design standards are lacking. Additionally, **operational overhead** from continuous authentication, token rotation, and extensive logging must be carefully tuned to avoid performance or usability impacts.

Organizations may also encounter **visibility gaps** across hybrid and multi-cloud deployments, complicating centralized monitoring and AI-driven threat detection. Finally, Zero-Trust requires a **cultural shift**: development, security, and operations teams must align policy-as-code, automation, and shared accountability. Without executive sponsorship and governance alignment, implementations risk remaining partial or inconsistent.

In summary, a phased roadmap enables practical Zero-Trust adoption in SAP BTP, progressing from foundational identity controls to automated, intelligence-driven security operations. While challenges related to identity scale, entitlement management, operational overhead, and organizational change exist, they can be mitigated through automation, clear governance models, and continuous monitoring. When executed holistically, Zero-Trust becomes a sustainable, audit-ready security foundation for SAP BTP rather than a one-time transformation effort.

Future Research Directions

Future research on Zero-Trust security for SAP Business Technology Platform (SAP BTP) should focus on advancing **AI-native and autonomous security capabilities** that move beyond static policy enforcement. One key direction is the development of **AI-driven identity risk scoring models** that dynamically evaluate user and service behavior, device posture, and workload context to enable adaptive, real-time access decisions in complex BTP landscapes delivered by **SAP SE**.

Emerging technologies also present important research opportunities. The applicability of **quantum-resistant cryptography**, **confidential computing**, and **secure multi-party computation** to SAP BTP environments remain largely unexplored and will be critical as cloud platforms evolve. Additionally, empirical studies evaluating the operational, security, and audit impacts of Zero-Trust adoption in large scale SAP BTP deployments can provide quantitative benchmarks and validate long-term effectiveness.

CONCLUSION

The growing reliance on cloud-native services, APIs, and multi-tenant architecture has made SAP Business Technology Platform (SAP BTP) a critical component of modern enterprise systems. These shifts expose limitations in traditional perimeter-based security models, necessitating a transition to **Zero-Trust Architecture (ZTA)**. This study demonstrates that Zero-Trust—centered on continuous verification, identity-centric access control, least-privilege enforcement, micro-segmentation, and continuous monitoring—is essential for securing SAP BTP environments delivered by **SAP SE**.

By examining SAP BTP security architecture, identity governance, secure integration patterns, automation, and AI-driven monitoring, the paper establishes a practical Zero-Trust framework tailored to SAP BTP. When implemented holistically, this approach reduces attack surfaces, limits lateral movement, and improves audit readiness across hybrid and multi-cloud SAP landscapes.

In conclusion, Zero-Trust represents a strategic and continuous security model for SAP BTP rather than a one-time implementation. Organizations that embed Zero-Trust principles into their SAP BTP strategy are better positioned to securely scale innovation, maintain regulatory compliance, and strengthen long-term resilience in cloud-enabled SAP ecosystems.

REFERENCES

[1] **SAP SE**, *SAP Business Technology Platform – Security Whitepaper*, SAP Documentation, 2023.

[2] **SAP SE**, *SAP Cloud Identity Services: Identity Authentication and Identity Provisioning*, SAP Help Portal, 2023.

[3] **National Institute of Standards and Technology**, *Zero Trust Architecture (NIST SP 800-207)*, U.S. Department of Commerce, 2020.

[4] **SAP SE**, *SAP Integration Suite and Cloud Integration – Security Guide*, SAP Help Portal, 2024.

[5] **Gartner**, *Zero Trust Security: A Strategic Approach for Cloud and Hybrid Environments*, Gartner Research, 2023.

[6] **Microsoft**, *Zero Trust Adoption Framework*, Microsoft Security Documentation, 2022.

[7] **SAP SE**, *SAP BTP Audit Logging, Monitoring, and Alert Notification Services*, SAP Security Documentation, 2024.

[8] L. Newman, "Enterprise Cloud Security and AI-Driven Threat Detection," *IEEE Cloud Computing*, vol. 10, no. 4, pp. 45–53, 2023.

[9] **Deloitte**, *Zero-Trust Security Architecture for SAP Landscapes*, Deloitte Insights, 2023.

[10] **IBM**, *Hybrid Cloud Security and Continuous Compliance*, IBM Redbooks, 2022.