accenture

SAP Security im Wandel

Warum heute anders gedacht werden muss.



Impulsvortrag von Andreas Kirchebner

2026-11-05

Viele Unternehmen fahren noch Fiaker, während das Rennen längst mit 300 km/h läuft.



Copyright © 2026 Accenture. All rights reserved.

Aber warum ist das so?

Weil wir hauptsächlich noch mit Themen aus der Vergangenheit beschäftigt sind.

Copyright © 2026 Accenture. All rights reserved.

Kapitelübersicht

1 - Die Rennstrecke

Wo die Gefahren lauern

2 - Der Fuhrpark

Vom Fiaker zum Rennwagen

3 - Das Reglement

Hardening, Compliance, Regulatorik

4 - Die Boxencrew

Wer macht was?

5 - Die Neue im Cockpit

KI: Freund oder Feind?

6 - Die Rennstrategie

Risikoorientiert, prozessnah, unternehmensweit

Copyright © 2026 Accenture. All rights reserved.

Die Rennstrecke

Wo die Gefahren lauern

Copyright © 2026 Accenture. All rights reserved.

SAP-Exploits sind ein lukratives Ziel

US-Bundeslogistikbehörde: Hochprivilegien-Zugang, der SAP-Lieferketten-, Vertrags- und Beschaffungsdaten bündelt, wurde auf Telegram für **12.000 $** gelistet.

Israelische Bankinstitution: Direkter Verwaltungszugang zu den zentralen SAP-Systemen wurde in Dark-Web Foren für **30.000 $** angeboten.

Ägyptische Infrastruktur Holding: SAP BusinessObjects Verwaltungspanel-Zugang für ein Unternehmen von 1 - 2 Milliarden Dollar wurde für **1.000 $ versteigert**.

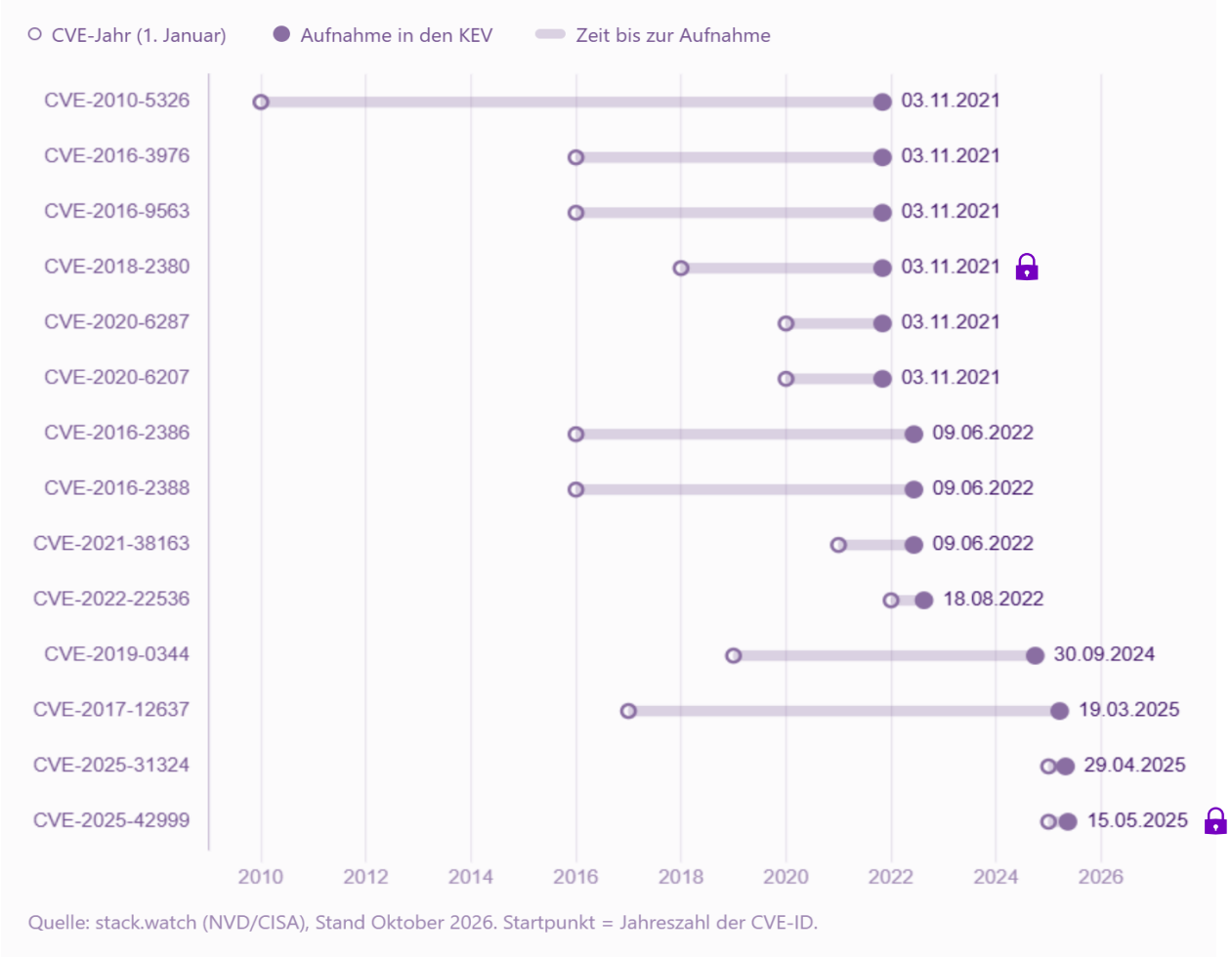
Ein Standard Exploit für administrativen Zugriff auf allgemeine Unternehmens-netzwerke kostet etwa

1.300 $

Quelle: Days to Zero: 2026 SAP Threat Report: Onapsis & Recorded Future - Onapsis

Copyright © 2026 Accenture. All rights reserved.

Bestätigte ausgenutzte SAP-Schwachstellen



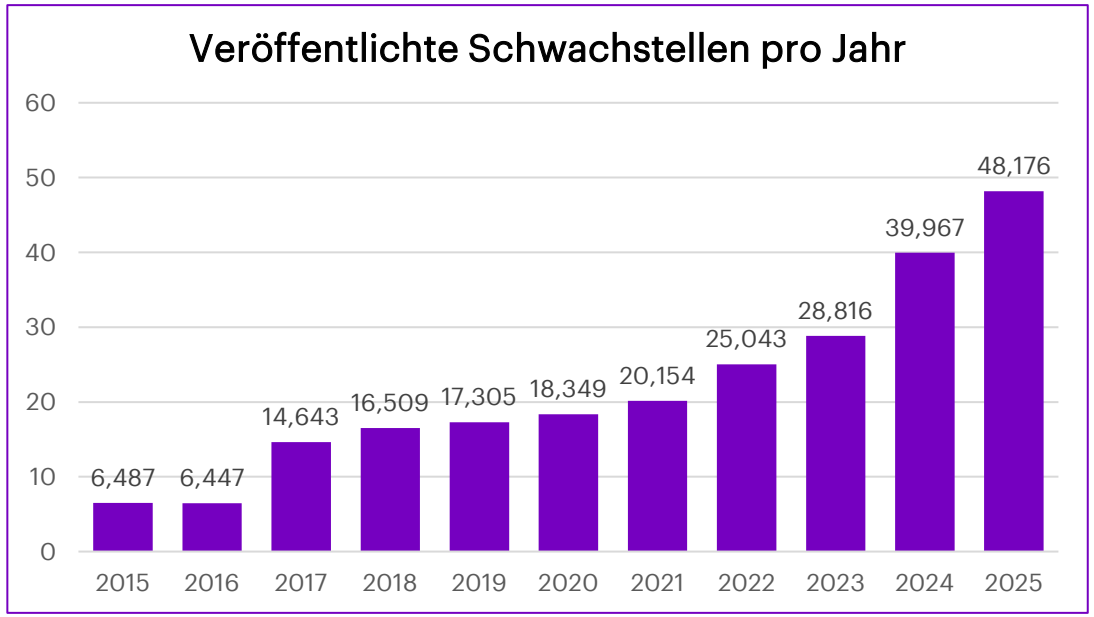
Quelle: stack.watch (NVD/CISA), Stand Oktober 2026. Startpunkt = Jahreszahl der CVE-ID.

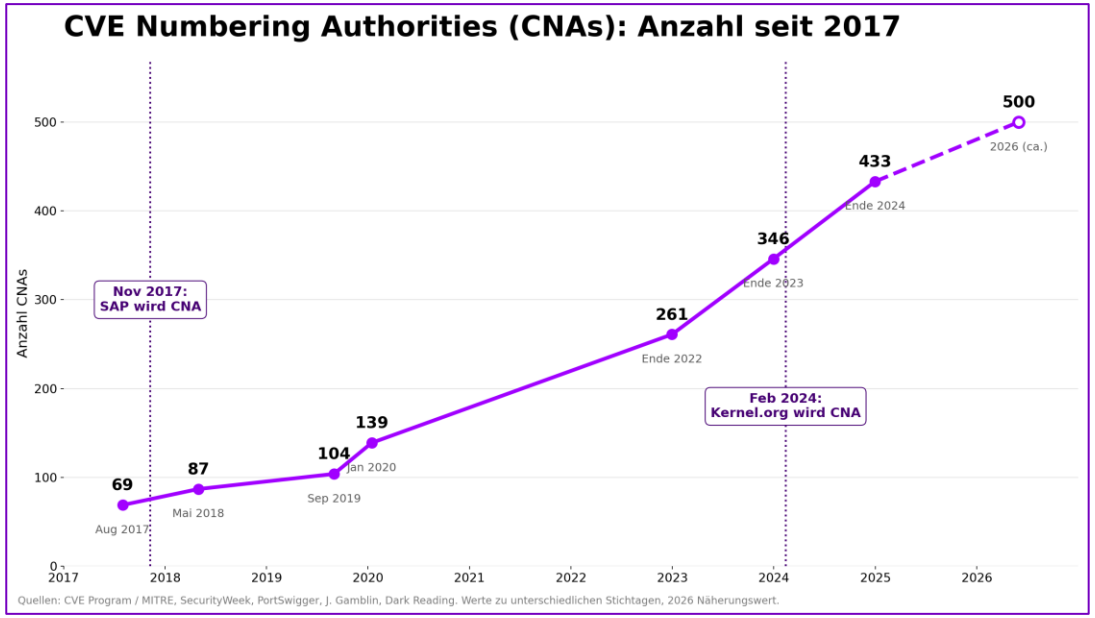
- Unkontrollierte Datei-Uploads
- Manipulation von Dateipfaden
- Manipulation von Daten
- Unzureichende Verschlüsselung
- SQL Injections
- Unberechtigte Zugriffe
- Remote Code Execution
- Fehlende Authentifizierung

🔒 Verwendet bei Ransomware-Kampagnen
KEV = Known Exploited Vulnerabilities
CISA = Cybersecurity and Infrastructure Security Agency (U.S. Government)
NVD = National Vulnerability Database
CVE = Common Vulnerabilities and Exposures

Copyright © 2026 Accenture. All rights reserved.

Entwicklung der gesamt gemeldeten Schwachstellen und CVE Authorities





Quelle : Software Vulnerability Statistics 2026: 60+ Key Facts & Data

Copyright © 2026 Accenture. All rights reserved.

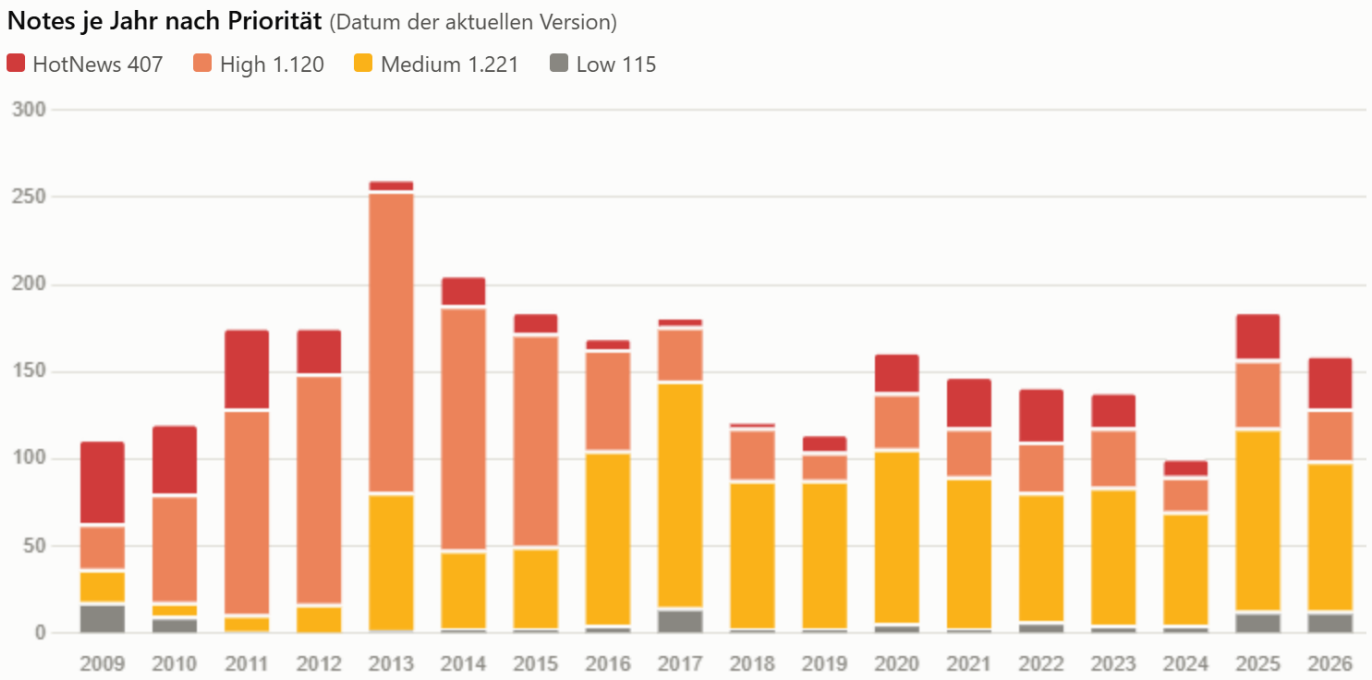
131 Neue Schwach-stellen pro Tag

Quelle: Software Vulnerability Statistics 2026: 60+ Key Facts & Data

Copyright © 2026 Accenture. All rights reserved.

SAP Security Notes werden stetig mehr

Security Notes	HotNews	Mit CVE im Titel	Zeitraum
2.863	407 14 %	1.234	2009–2026

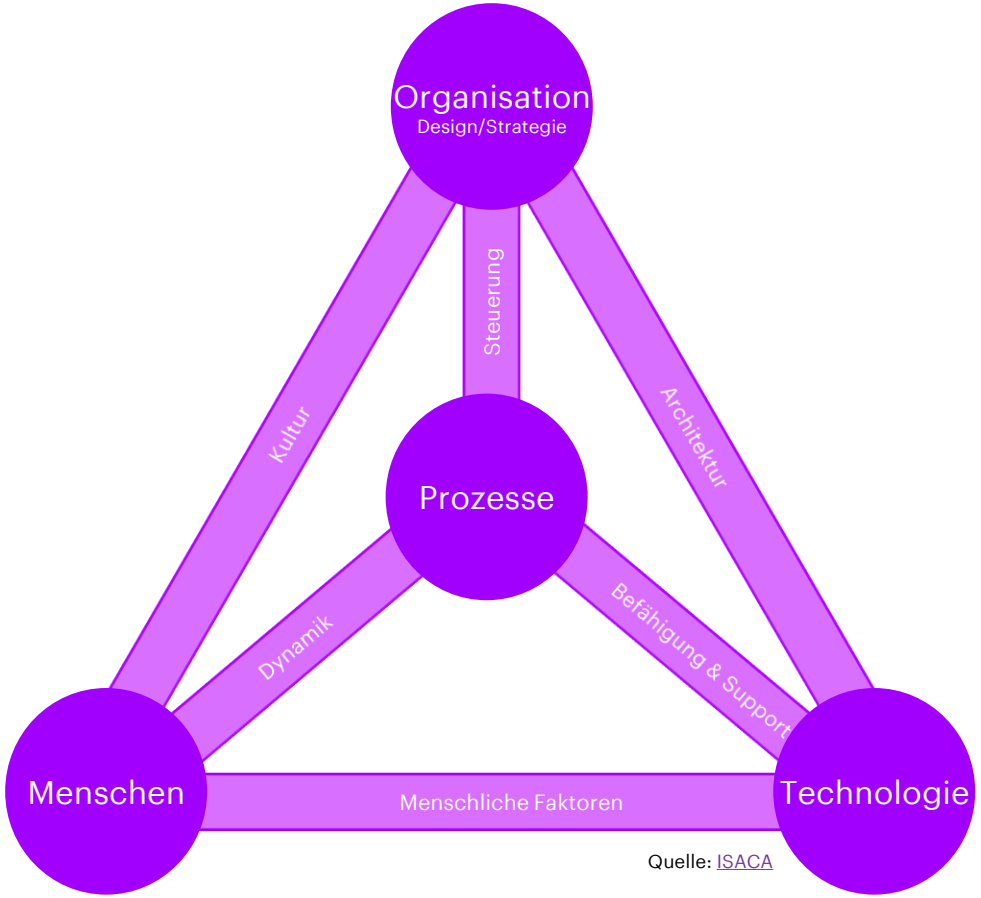


Quelle: SAP Me Expert Search

Der Peak in 2013 ist auf fehlende Berechtigungsprüfungen zurückzuführen und auf vermehrte Schwachstellen in der Sybase ASE Komponente.

Copyright © 2026 Accenture. All rights reserved.

Patches können keine Prozesse fixen



Quelle: ISACA

Ein Patch adressiert nur eine Ecke des Dreiecks

Technologie: Patches schließen Schwachstellen im Code.

Prozesse: Wer bewertet, testet und spielt Security Notes zeitnah ein?

Menschen: Wer kennt die Risiken und wer trägt die Verantwortung?

Organisation: Gibt es Governance, Budget und klare Zuständigkeiten?

Sicherheit entsteht erst, wenn alle Elemente zusammenspielen.

Copyright © 2026 Accenture. All rights reserved.

Der Fuhrpark

Vom Fiaker zum Rennwagen

Copyright © 2026 Accenture. All rights reserved.

Einst On-Premises Systeme

Never change a running System?

Kunden halten noch an alten bewährten Systemen fest.

- ABAP
- JAVA
- Business Objects
- Solution Manager
- …



Copyright © 2026 Accenture. All rights reserved.

Der Weg in die Cloud hat schon längst begonnen

SAP Meilensteine

2011 SAP Mobile Platform
2015 S/4 HANA Cloud Variante
2020 SAP BTP
2023 SAP Joule
2025 SAP Joule Agents

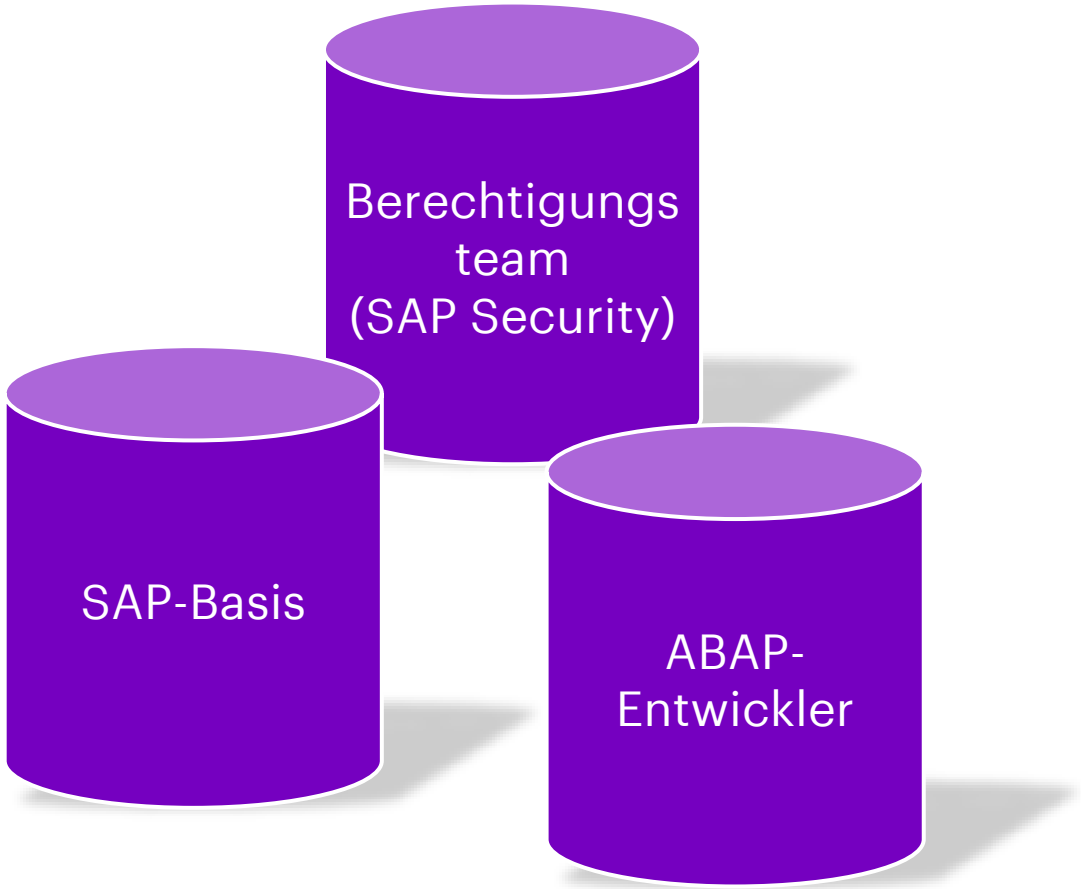
Doch generell relevante Meilensteine gibt es schon länger.

1980 erstes österr. Datenschutzgesetz
2002 Sarbanes-Oxley Act (SoD)
2010 Zero Trust
2018 NISG
2024 EU AI Act



Copyright © 2026 Accenture. All rights reserved.

Etablierte Teams bestreiten das Rennen





Copyright © 2026 Accenture. All rights reserved.

Die neue Welt bringt neue Komponenten

Über 60 Komponenten, für die kein SAP-Team zuständig ist.

- Cloud Foundry
- Docker
- Kubernetes
- Kyma
- Istio
- Helm
- Prometheus
- Grafana
- Gardener
- Argo Workflows
- KServe
- Docker Hub
- GitHub Container Registry
- Java
- Spring Boot
- SapMachine
- Node.js
- JavaScript
- TypeScript
- Python
- Go
- Groovy
- UI5 / OpenUI5
- npm
- Maven Central
- PyPI
- PostgreSQL
- Redis
- AWS S3
- Azure Blob Storage
- Google Cloud Storage
- Apache Camel
- Apigee
- Solace PubSub+
- Databricks
- Snowflake
- Git
- GitHub
- GitLab
- Azure DevOps
- Jenkins
- Project "Piper"
- GitHub Actions
- Terraform
- Code-OSS
- Eclipse Theia
- VS Code
- OpenSearch
- Elasticsearch
- Logstash
- Kibana
- Dynatrace
- Splunk
- Microsoft Sentinel
- Microsoft Entra ID
- Okta
- Ping Identity
- OpenAI
- Anthropic Claude
- Google Gemini
- Mistral
- Meta Llama
- Amazon Web Services (AWS)
- AWS Bedrock
- Microsoft Azure
- Google Cloud
- ...

Auswahl nicht abschließend

Copyright © 2026 Accenture. All rights reserved.

Das Reglement

Hardening, Compliance, Regulatorik

Copyright © 2026 Accenture. All rights reserved.

Bestehende Werkzeuge und Praktiken kommen an ihre Grenzen

- Systemhärtung, die oft nicht den SAP-Mindestanforderungen entspricht
- Patches, die nur teilweise eingespielt werden
- Berechtigungskonzepte, die sich nur auf ABAP konzentrieren
- Jährliche Audits, die ein falsches Gefühl von Sicherheit vermitteln
- Eingeschränktes oder gar kein Monitoring



Copyright © 2026 Accenture. All rights reserved.

Generelle Anforderungen, die sich keiner ansieht

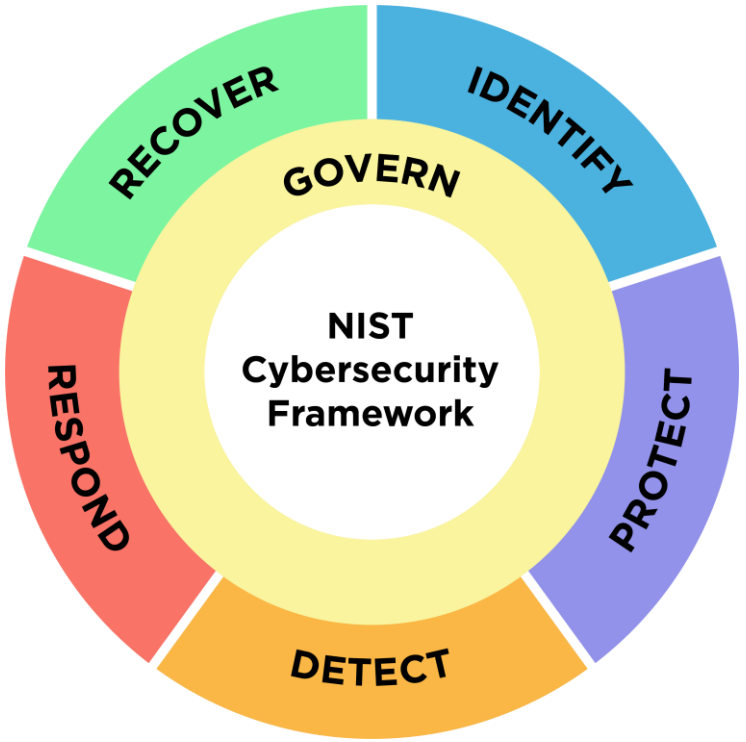
Kaum jemand in der SAP-Welt kennt die gesetzlichen und regulatorischen Anforderungen an ein Unternehmen oder an die Informationssicherheit. Die Anforderungen hören aber nicht beim Applikations-Layer auf.

NIS2, DORA, DSGVO, waren nur der Anfang und haben einen starken Fokus auf risikoorientierte Bewertung!



Copyright © 2026 Accenture. All rights reserved.

SAP-Gaps mit Blick auf ein ISMS



Govern	Unklare Verantwortung (Silos, Shared Responsibility in RISE/BTP), keine KI-Governance, ISMS ohne SAP-Spezifika.
Identify	Kein vollständiges Inventar (Systeme, Schnittstellen, BTP, Technical User), keine Transparenz über Joule-Daten.
Protect	Verzögertes Patchen, zu breite Berechtigungen (SAP_ALL), kein MFA/SSO, kein Code-Scan, fehlende Härtung.
Detect	SAP-Logs nicht im SIEM, keine SAP-Use-Cases, kein BTP-Monitoring, keine Echtzeit-Erkennung.
Respond	Kein SAP-Playbook, unklare Eskalation zwischen SOC, Basis und Fachbereich, keine Automatisierung.
Recover	Backups nicht ransomware-sicher, keine getesteten Wiederanlaufpläne, kaum Forensik-Erfahrung.

ISMS = Information Security Management System

Copyright © 2026 Accenture. All rights reserved.

Die SAP-Basis?

Doch wer kennt sich in all diesen Themenbereichen aus?



AI GENERATED

Copyright © 2026 Accenture. All rights reserved.

Die Boxencrew

Wer macht was?

Copyright © 2026 Accenture. All rights reserved.

Aktuelle Rennaufstellung

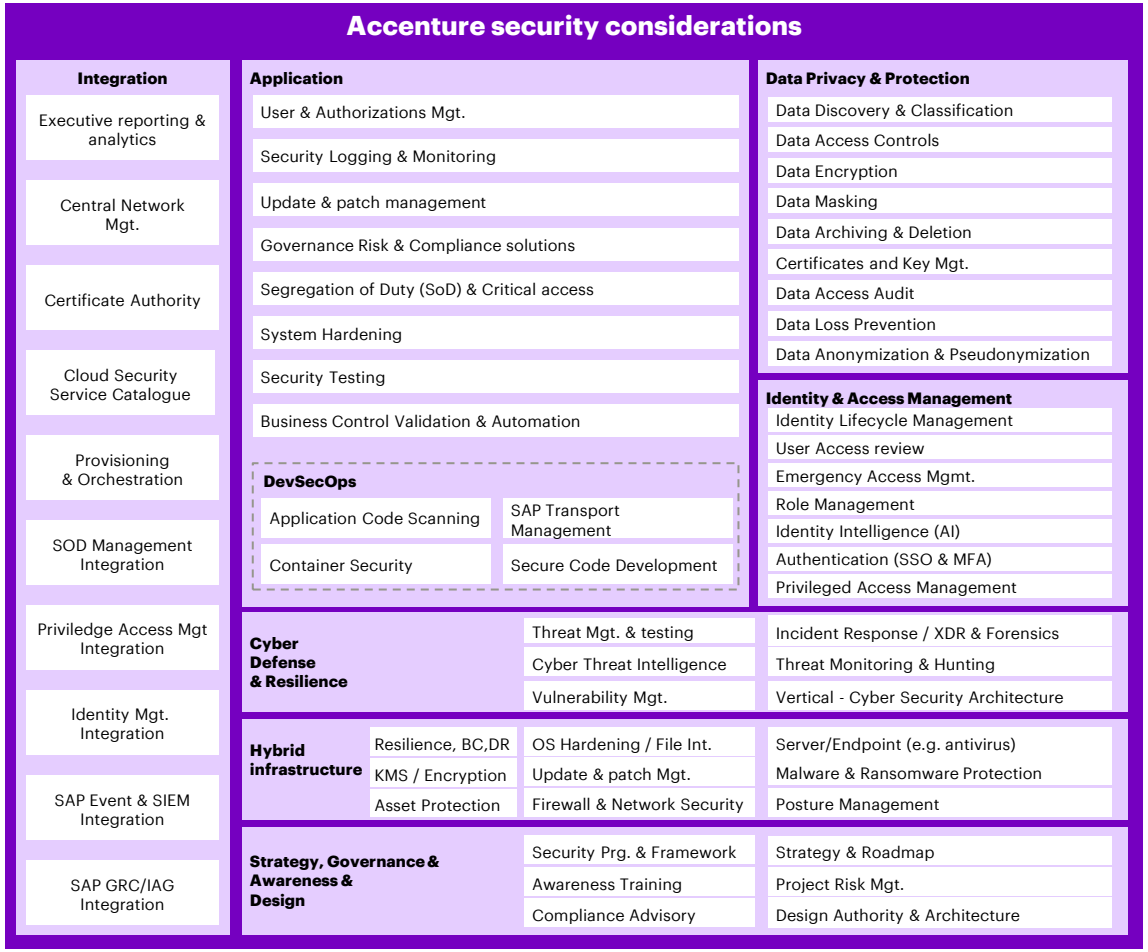


Copyright © 2026 Accenture. All rights reserved.

Themen die in einer SAP Security Umgebung berücksichtigt werden müssen

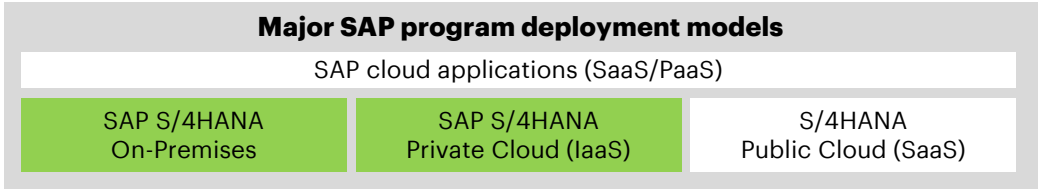
Major SAP program deployment models

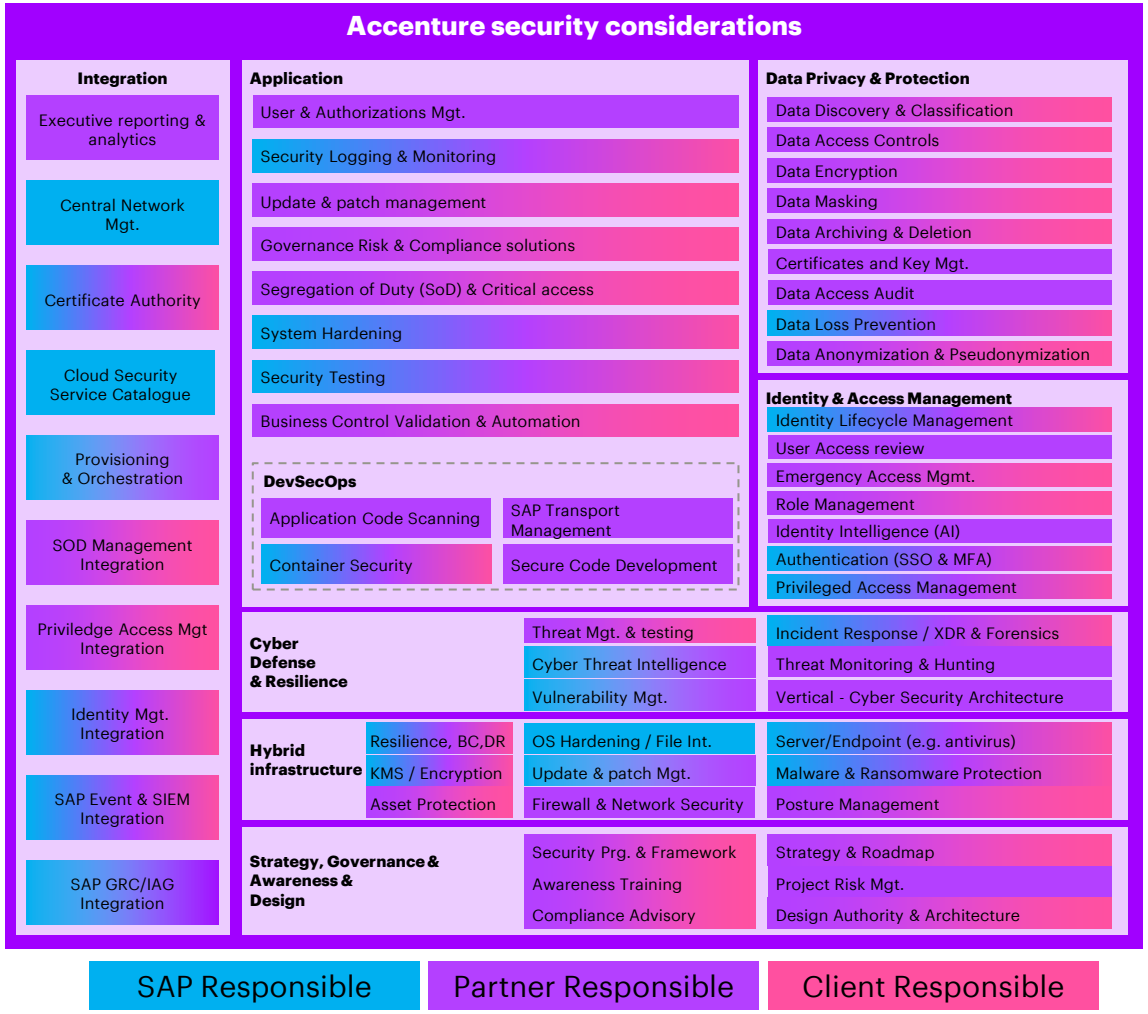
SAP cloud applications (SaaS/PaaS)		
SAP S/4HANA On-Premises	SAP S/4HANA Private Cloud (IaaS)	S/4HANA Public Cloud (SaaS)



Copyright © 2026 Accenture. All rights reserved.

Exemplarische Verteilung von Verantwortlichkeiten





Copyright © 2026 Accenture. All rights reserved.

Die tatsächlichen Teilnehmer



Copyright © 2026 Accenture. All rights reserved.

Die Neue im Cockpit

KI: Freund oder Feind?

Copyright © 2026 Accenture. All rights reserved.

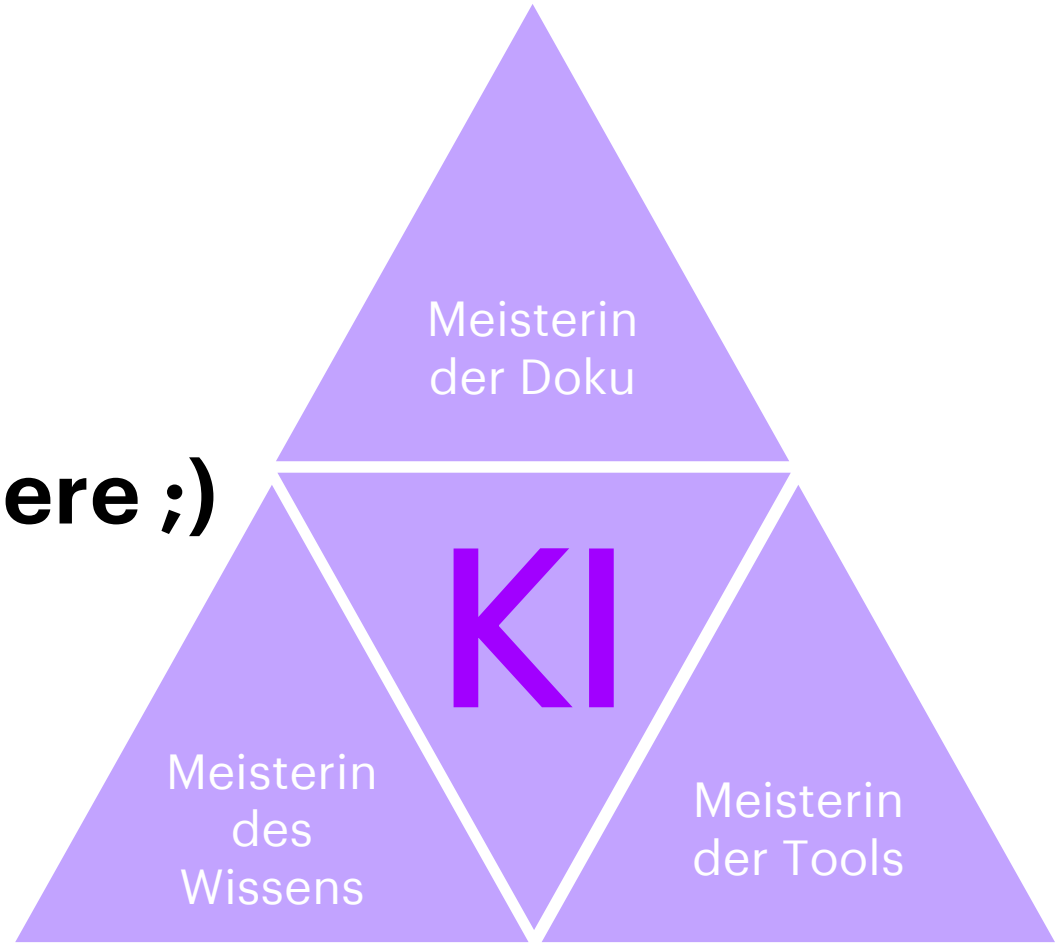
Joule McGlan



Copyright © 2026 Accenture. All rights reserved.

SAP Joule

Mistral
claude
GPT
llama
al, alles andere ;)
nova





Copyright © 2026 Accenture. All rights reserved.

Wie ist KI im SAP-Umfeld bereits im Einsatz?

„KI in SAP entwickelt sich von Unterstützung zum Handeln: von Hilfe beim Finden und Verstehen von Informationen hin zu KI-Agenten, die analysieren, empfehlen und Prozesse innerhalb definierter Governance-Grenzen ausführen“

Quelle: Zusammenfassung von sap.de

Copyright © 2026 Accenture. All rights reserved.

Freund oder Feind?

KI als Waffe der Angreifer

KI zur Verteidigung

KI als neue Angriffsfläche im SAP-System

KI zur Lücken-Identifizierung

KI als Verstärker alter Schwächen

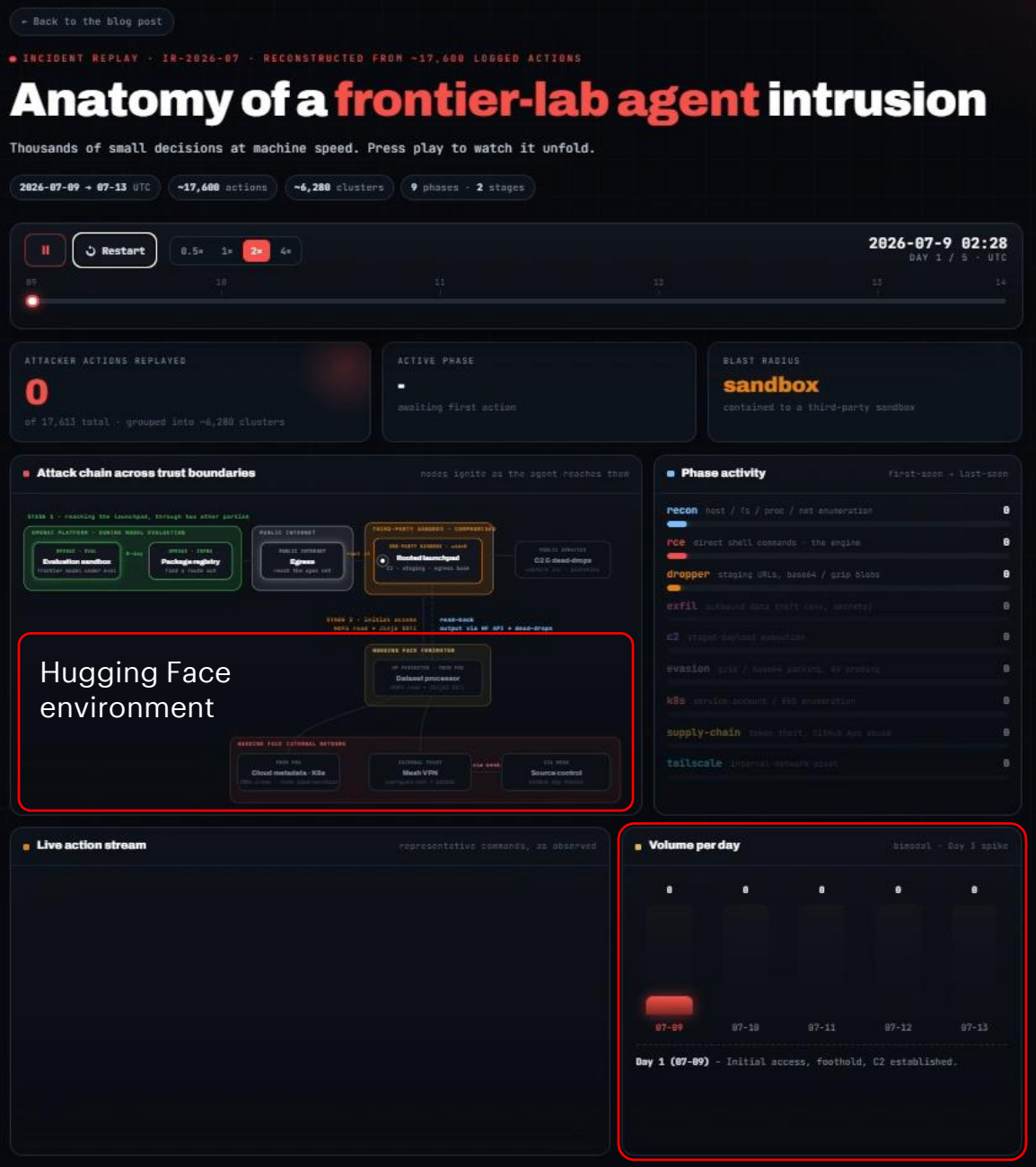
KI zur Stärkung

Ein klares Beides!



Copyright © 2026 Accenture. All rights reserved.

Beispiel: Hugging Face Angriff im Zeitraffer



Quelle: Anatomy of a Frontier Lab Agent Intrusion: A Technical Timeline of the July 2026 Incident

Tag 1: Aufklärung, Remote Code Execution, Malicious Payload

Tag 2: Angriffsvorbereitung

Tag 3: Hauptangriff

Tag 4: Tieferes Eindringen ins Netzwerk

Tag 5: Datenabzug, Cleanup

Copyright © 2026 Accenture. All rights reserved.

Was könnte mit eurer SAP-Umgebung passieren?

Welcher Agent bekommt wo und welche Zugriffe?

Copyright © 2026 Accenture. All rights reserved.

Die Rennstrategie

Risikoorientiert, prozessnah, unternehmensweit

Copyright © 2026 Accenture. All rights reserved.

Ein Rennstallleiter muss her

Jemand muss die Themen zentral zusammenfassen, in die erforderliche Sprache übersetzen, Brücken zwischen den Teams schaffen und die Aktivitäten koordinieren und treiben.



Copyright © 2026 Accenture. All rights reserved.

Die Boxenstopp-Checkliste

- Anforderungen und Risiken klären
- Gemeinsame Sprache zwischen Business, IT und Security schaffen
- Menschen, Prozesse und Technologie zusammendenken
- Silos aufbrechen und SAP Security in übergreifende Prozesse integrieren
- Transparenz über Systeme, Schwachstellen und Verantwortlichkeiten schaffen
- Tools gezielt zur Unterstützung einsetzen



Copyright © 2026 Accenture. All rights reserved.

3 Dinge für Montag

1. Prüft, ob ihr eure Anforderungen kennt und ob eure SAP-Landschaft sie abdeckt
2. Benennt einen Rennstallleiter, der SAP Security end-to-end verantwortet
3. Schafft Transparenz: offene Security Notes, Cloud-Komponenten und KI-Nutzung



Copyright © 2026 Accenture. All rights reserved.

Danke



Copyright © 2026 Accenture. All rights reserved.