

Security, Compliance nel SAP Cloud ERP

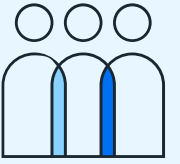
Samuele Scarpa, SAP
June, 2026

PUBLIC



Rising cybersecurity challenges

Complexity and skills shortages dominate



\$
4-10m. Average cost
of a data
breach¹

Only
1/3 of data breaches are detected
by a company's own security
teams and tools²

Over
71% of companies are expect to
adopt cloud sovereignty to
ensure regulatory compliance³

How Chronic Staff Shortages Amplify Cyber Risk

Which cybersecurity challenges do you believe could have been addressed effectively with adequate staffing?

- 1 — Insufficient Time for Comprehensive Risk Assessment and Management 
- 2 — Process and Procedural Oversights 
- 3 — Delays in Patching Critical Systems 
- 4 — Inadequate Training Opportunities for Cybersecurity Team Members 
- 5 — System Misconfigurations 

3 key factors for security and resilience

Designing an effective strategy



Defending against cyberattacks

Threats are appearing in a **greater variety of forms**, including ransomware, social engineering, and DDoS attacks.

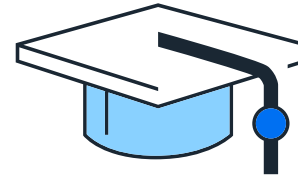
Cyberattacks are **evolving rapidly**, leveraging AI and other technologies, making traditional defense methods less effective.



Manage regulatory compliance

Constantly changing directives, laws, and regulations vary widely across regions.

Organizations face challenges in assessing compliance and risk **fines or penalties** for non-compliance.

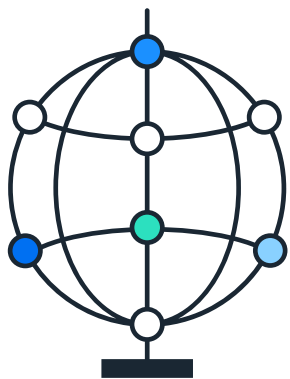


Tackling skills and technology gaps

Repetitive and time-consuming tasks prevent security teams from focusing on broader strategies, increasing vulnerability.

More investment is needed in technologies to promptly identify threats, manage vulnerabilities, and ensure compliance.

SAP supports security and compliance for more than



One-third

of the total global economy



Shared security responsibility model

Working together to become a secure-by-default company

RISE with SAP

SAP S/4HANA Cloud Private Edition

We (SAP Global Cloud Operation)

- Resilient platform architecture (HA and DR)
- Single-tenant landscape
- Managed backup and restore
- Building secure virtual machines, operating systems, networking, SAP HANA database
- SAP HANA database management
- Technical managed services ([R&R Link](#))
- Operational security and security incident management
- 24x7 security monitoring
- Personal data breach notification
- SLA and support services
- Threat management and patch management



You (Customer)

- Customer data ownership
- Compliance to government and industry regulations
- Application user identity management
- Application user authentication and authorisation management
- Application user roles, user groups, access control
- Application users behaviour analysis and monitoring
- Dedicated private connectivity to hyperscalers
- Vulnerability and patch management for applications
- Application security audit logging (SAL)
- Monitoring of security logs at application layer
- Security hardening and penetration testing of applications

IaaS provider

(Customer-selected deployment region) Managed by SAP

- Physical data centre security in multiple regions
- Resilient network connectivity and availability zones
- Underlying physical, virtual infrastructure and hypervisor
- Network availability with built-in basic DDoS protection
- Audit, security, and compliance on IaaS

Supported hyperscalers



Shared Security Responsibility Model

SAP S/4HANA Cloud, Public Edition



SAP S/4HANA Cloud, Public Edition

- Resilient SaaS architecture
- Advanced Multi-Tenant Logical Separation
- Backup and restoration and Disaster Recovery
- Securing the infrastructure, operating systems, and networking, and applications
- Operational security monitoring & incident management
- Personal Data Breach Notification
- Hardening and Patching Operating Systems and solution support
- Adherence SLA and Contractual Assurance via SLA, SAP DPA, Support Policy

Customer

- Configuration of the Business Processes
- Tenant Administration and Management
- Identity Management
- Authentication and Authorization
- Business Roles, User Groups, Access Control
- Customer Data Ownership and Protective Handling
- Compliance to Regulations
- Analysis of Application Logs
- API Extension, Integration and 3rd party connectivity

- Physical Data Center Security in multiple Regions
- Resilient Network Connectivity and Availability Zones
- Underlying Physical, Virtual Infrastructure & Hypervisor
- Network Availability with built-in basic DDoS protection
- Audit, Security and Compliance on IaaS

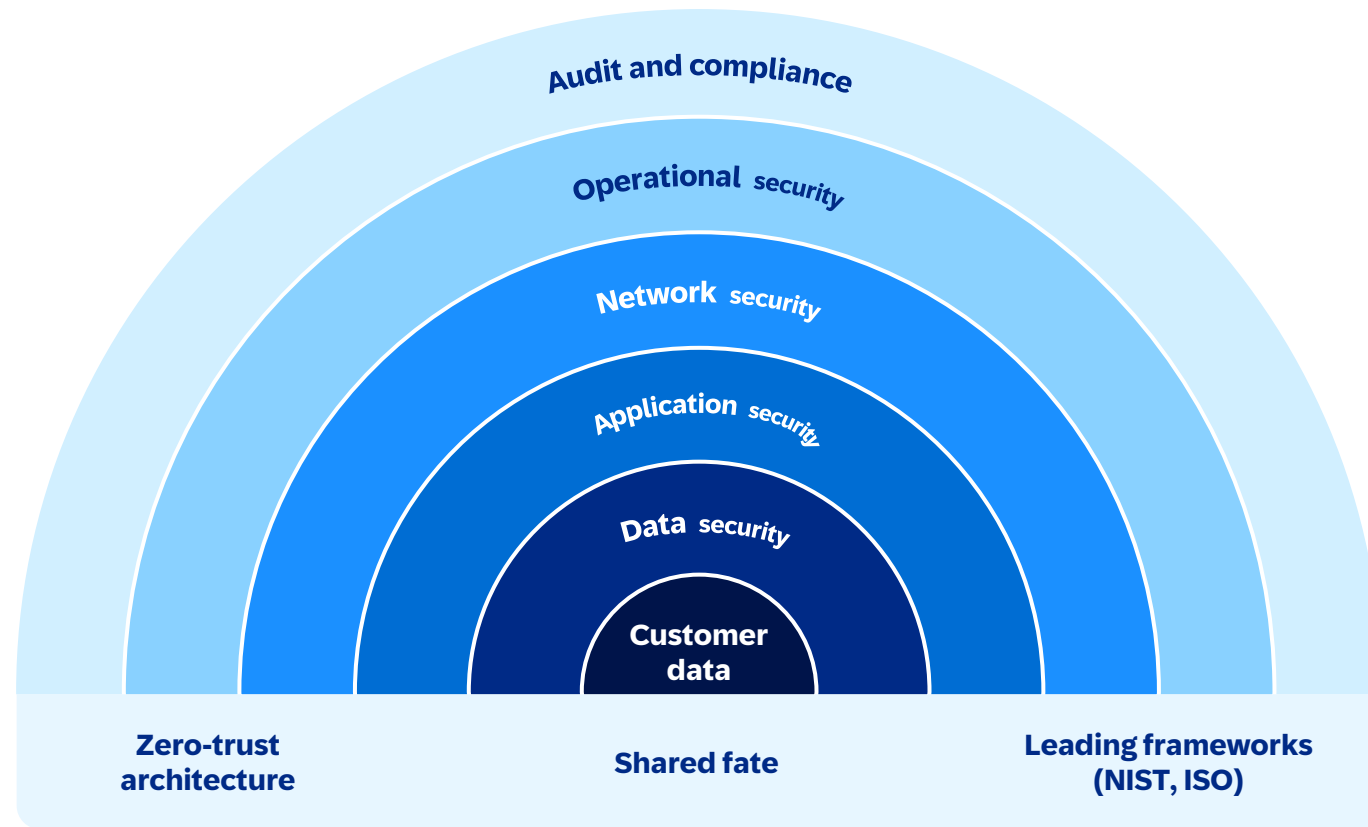
**IaaS Provider
Managed by SAP SE**

Supported IaaS Providers



SAP cloud ERP: Defense in depth

A multi-layered approach to help protect your data



- ISO 27001
- ISO 27017
- ISO 27018
- ISO 22301

- Business continuity
- Disaster recovery
- Patch and malware management

- Customer environment isolation with security groups
- Customer tenant isolation
- DDoS protection

- Secure software development lifecycle
- Web application firewall
- Cloud connector

- Dedicated application and database servers
- Data-at-rest encryption
- Data-in-transit encryption

- BS 10012
- ISAE 3402 SOC1 Type 2
- ISAE 3000 SOC Type 2
- C5

- Security incident management
- Regular security scanning (VAPT)
- Continuous security logging and monitoring

- Separate application & database for each customer
- Network micro-segmentation
- No default internet exposure

- Identity and authentication
- Application security audit logs
- Data-in-transit encryption

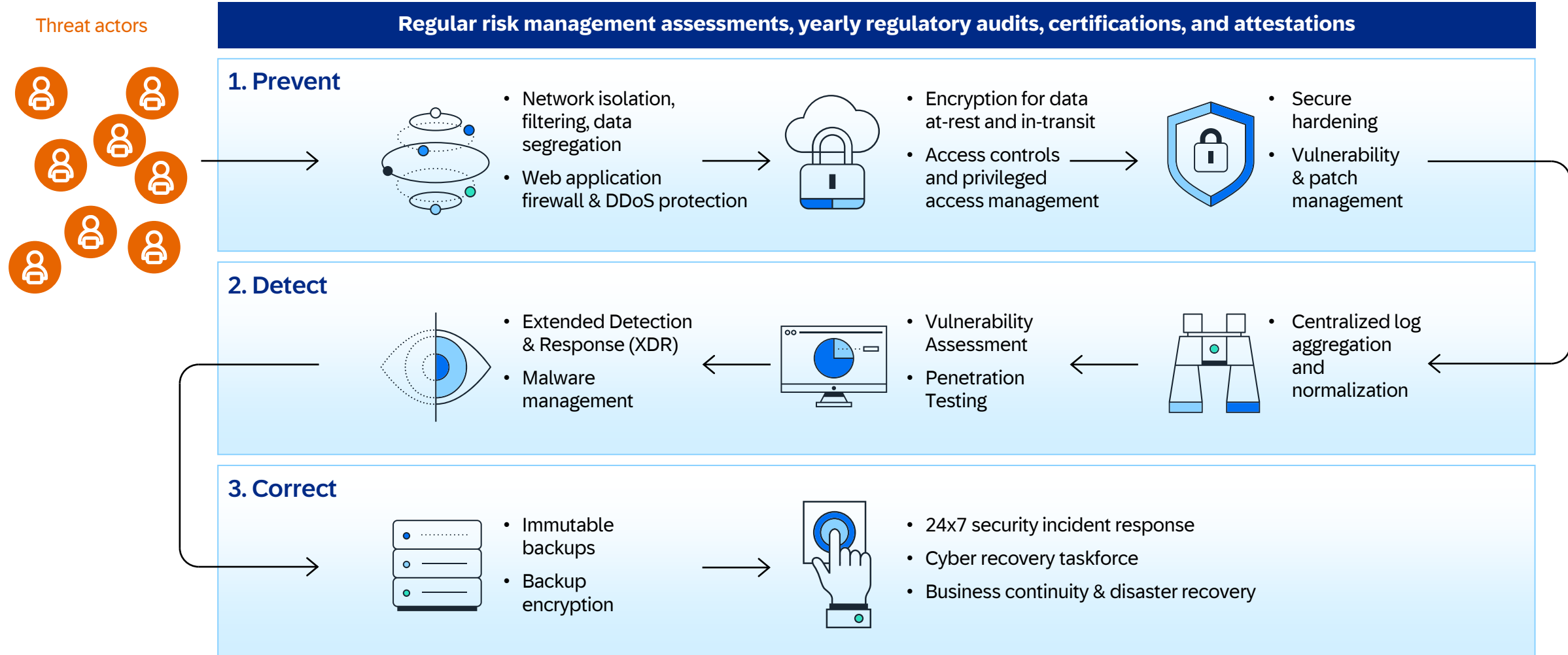
- Role-based access control
- Database monitoring
- Secure key management service

The background of the slide is a solid light blue color. Overlaid on this are several large, three-dimensional, translucent blue geometric shapes. These shapes are rectangular prisms of varying sizes and orientations, creating a sense of depth and movement. They are arranged in a way that they appear to be floating or stacked, with some overlapping others. The lighting is soft, creating subtle gradients and shadows on the surfaces of the prisms.

Security and compliance solutions and services

A multi-layered security and compliance model

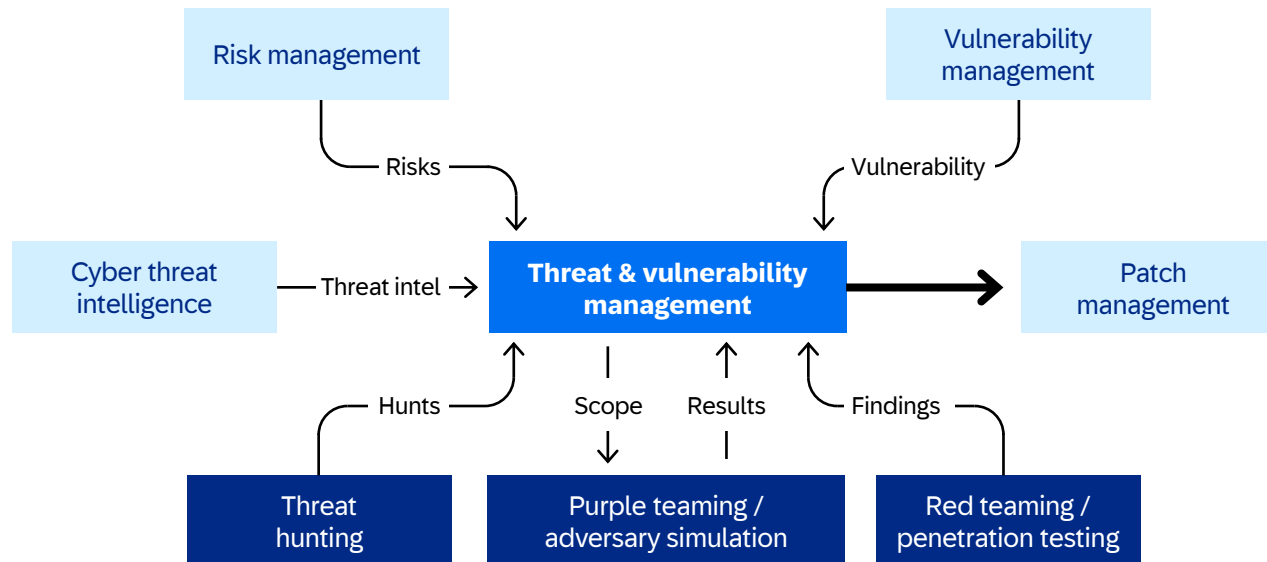
Defend against cyberattacks at every stage



Threat and vulnerability management

Identify, assess, and mitigate security risks to protect the system from cyberattacks and help ensure business continuity.

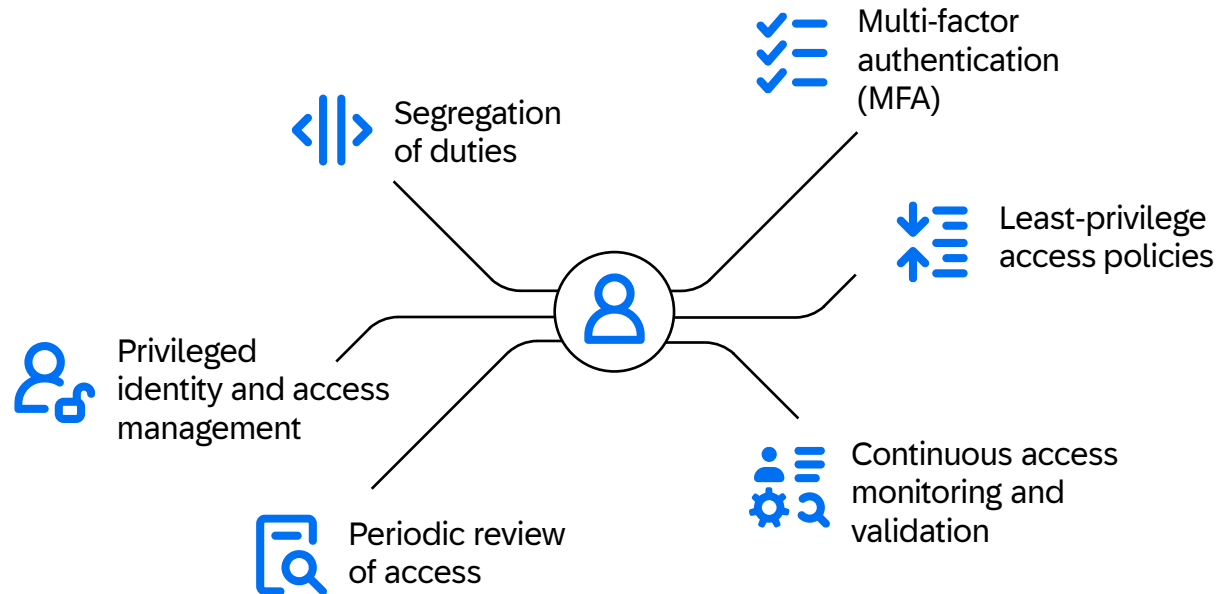
Key objectives: Regular vulnerability scanning and patching, incorporating threat intelligence from multiple sources and enabling early detection and response.



Identity and access management

Manage users and identities, implement dynamic access controls for SAP cloud operations, and support compliance with security policies, and data protection laws.

Key objectives: Managing user identities, implementing strict access control policies, and restricting access to data.



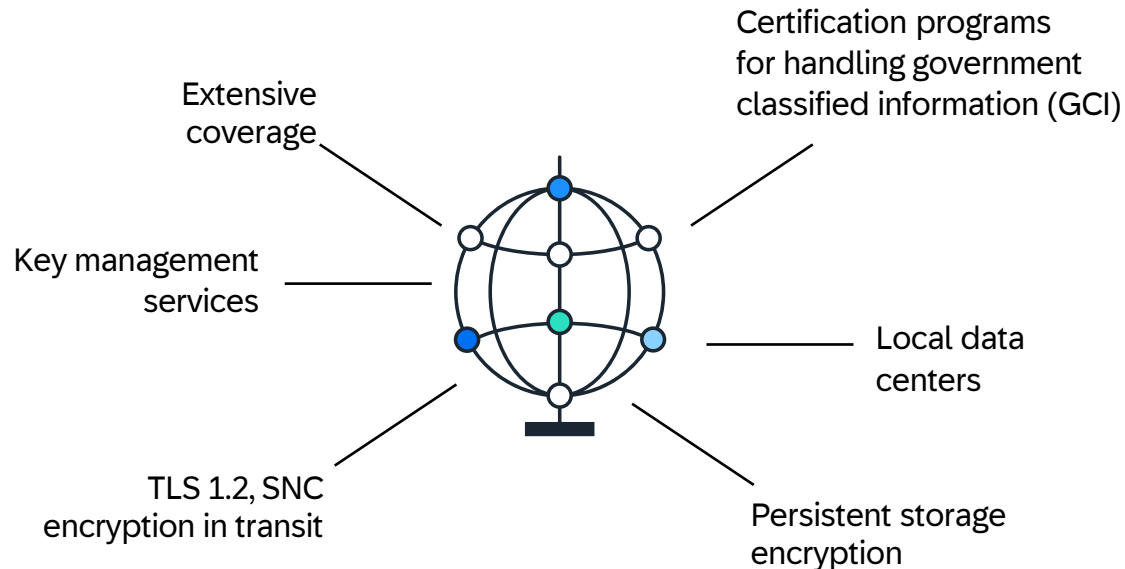
Username:

Password:

Data protection and sovereign cloud

Protect the confidentiality, integrity and availability of sensitive data stored and managed in the cloud, including customers' business and operational data.

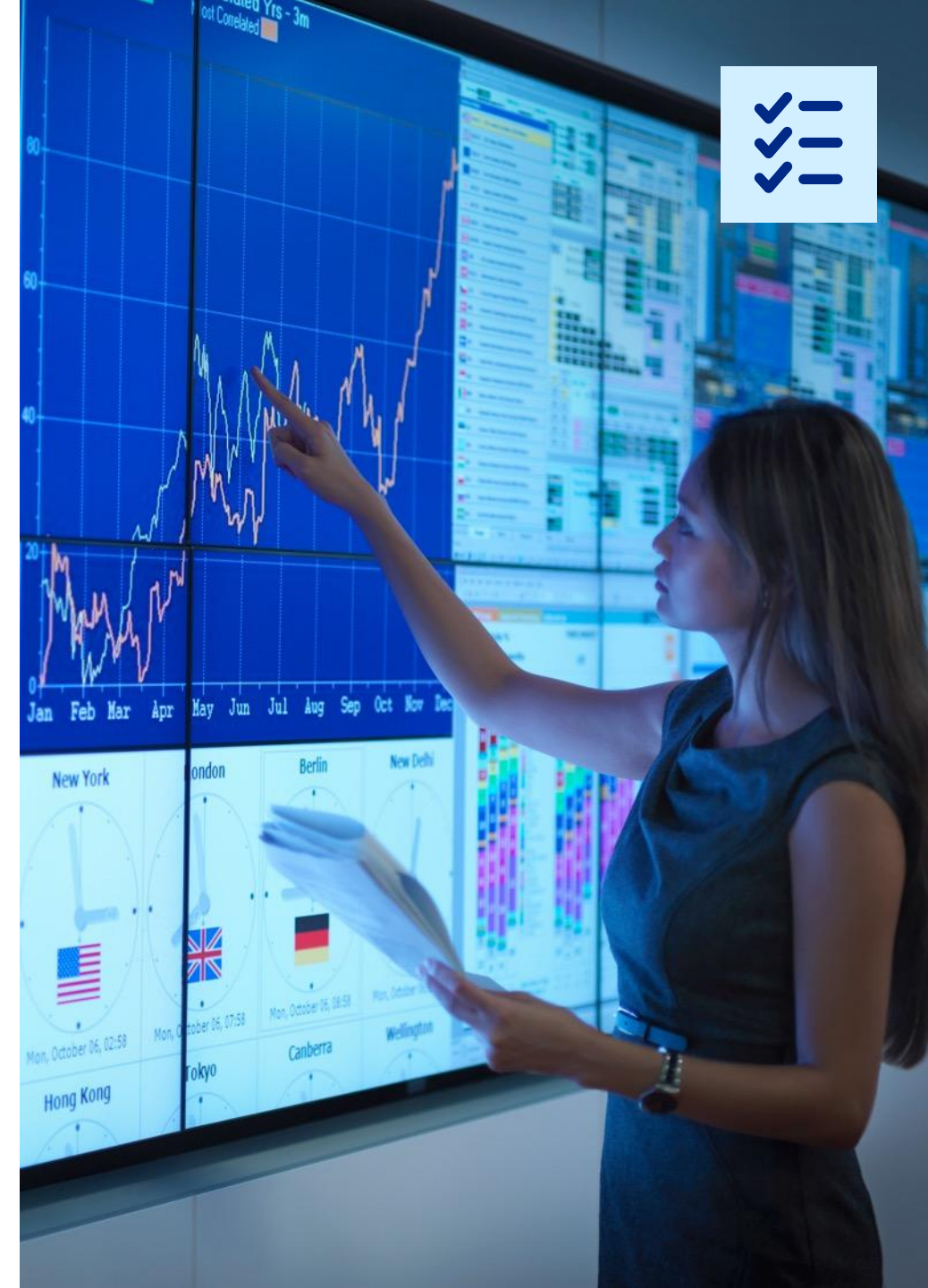
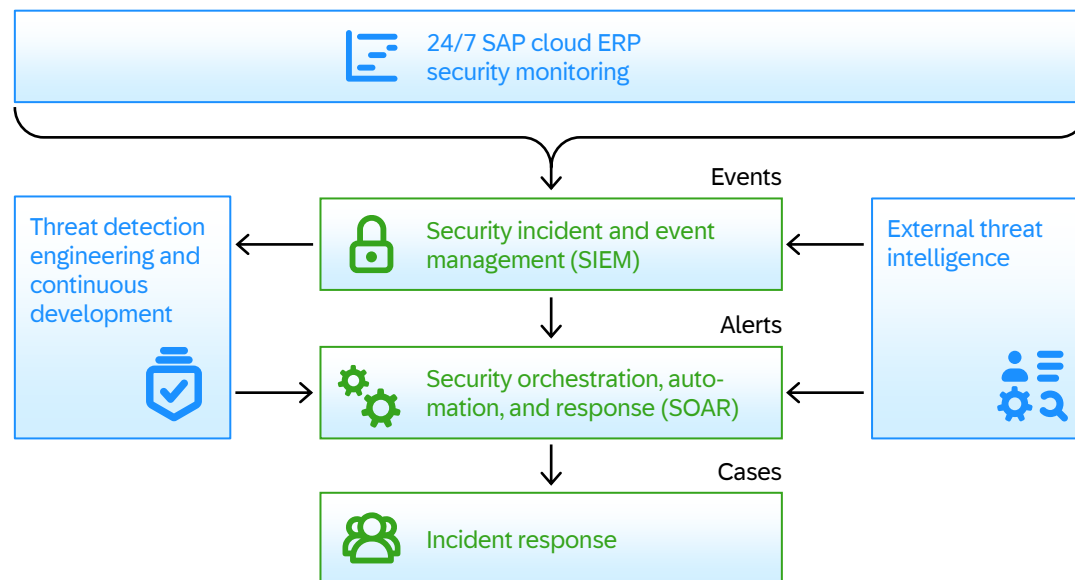
Key objectives: Encrypting data at rest and in transit, secure key management, backup immutability, preventing data leaks or unauthorized access, and enforcing access control policies.



Security logging and monitoring

Provide real-time visibility of events within the ERP landscape, enabling the detection of suspicious activity and potential security incidents.

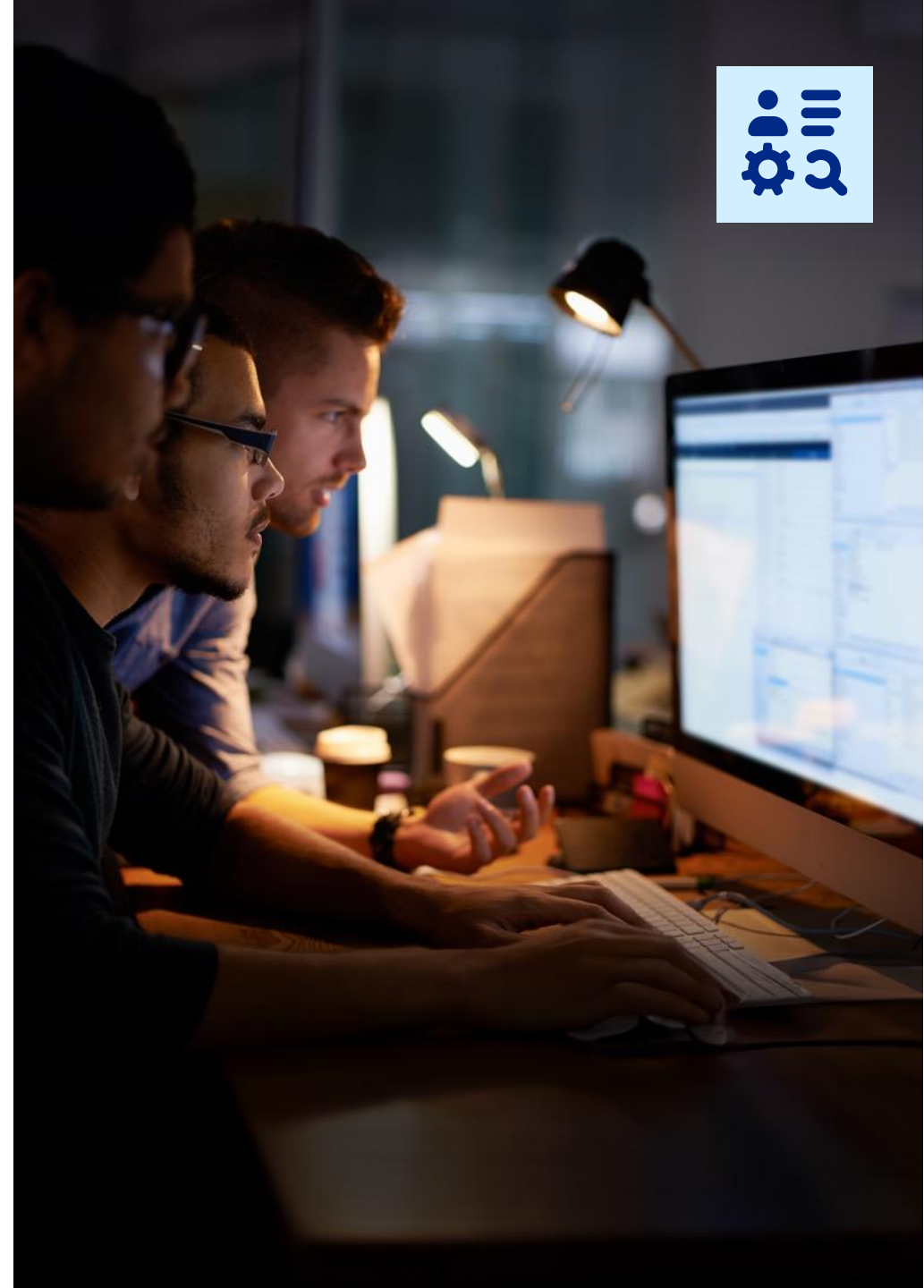
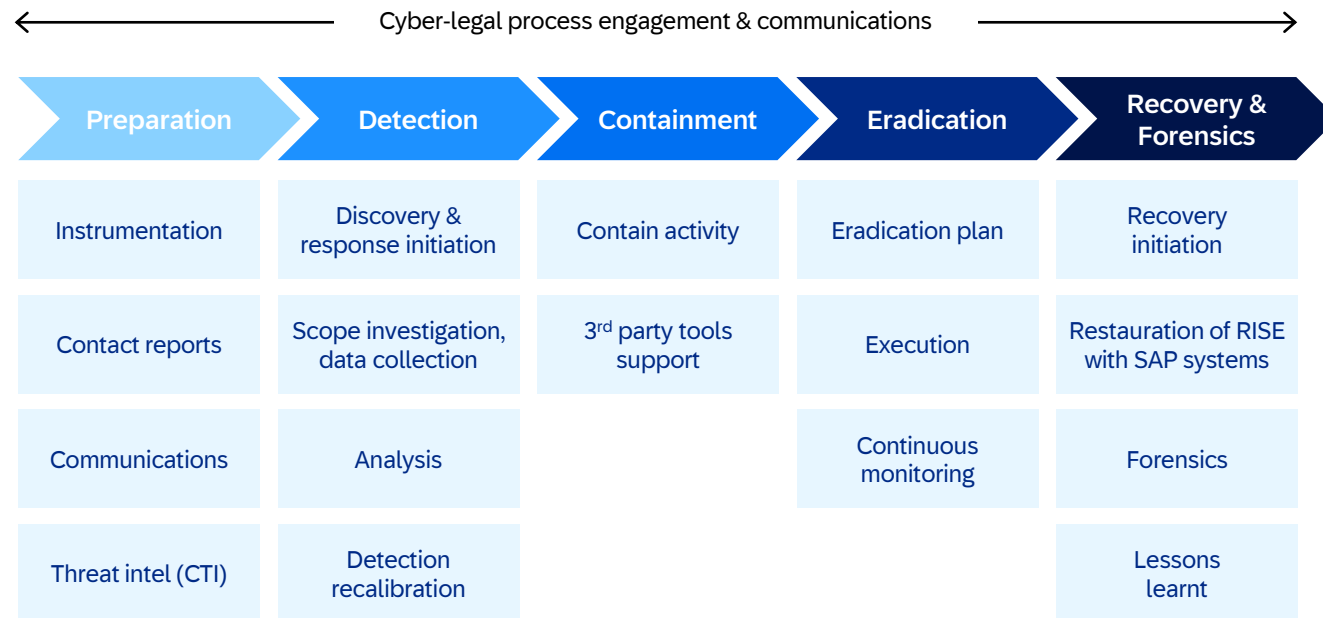
Key objectives: Implementing centralized log aggregation and normalization to detect suspicious activity in real time, along with ongoing development of new threat detection use cases.



Incident response

Manage and resolve security incidents to minimize damage and quickly restore normal operations.

Key objectives: Ensuring swift response to security incidents while facilitating rapid containment, eradication and recovery.

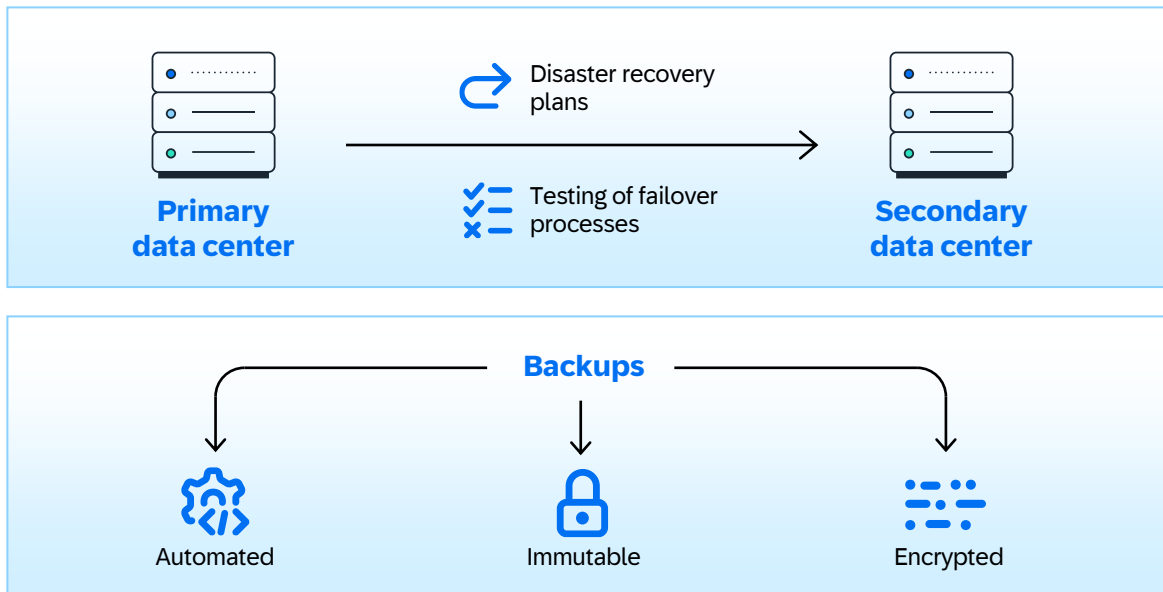


Business continuity and disaster recovery

Prepare systems and processes to help ensure operational resilience and rapid recovery after disruptions.

Key objectives: Regular data backups, replication of critical systems, and the ability to restore operations quickly after an outage.

High availability*



Governance and regulatory compliance

Manage cybersecurity standards, frameworks, and adherence to relevant industry regulations, such as NIST CSF, GDPR, HIPAA, PCI-DSS, and more.

Key objectives: Meeting data privacy, sovereignty and residency requirements, ensuring compliance to global and regional cybersecurity regulations required to operate the cloud service.

- Assessing cybersecurity regulations
- Conducting compliance audits throughout the financial year
- Maintaining security certifications
- Enforcing data governance policies
- Supporting compliance with data sovereignty regulations

Current certifications include:

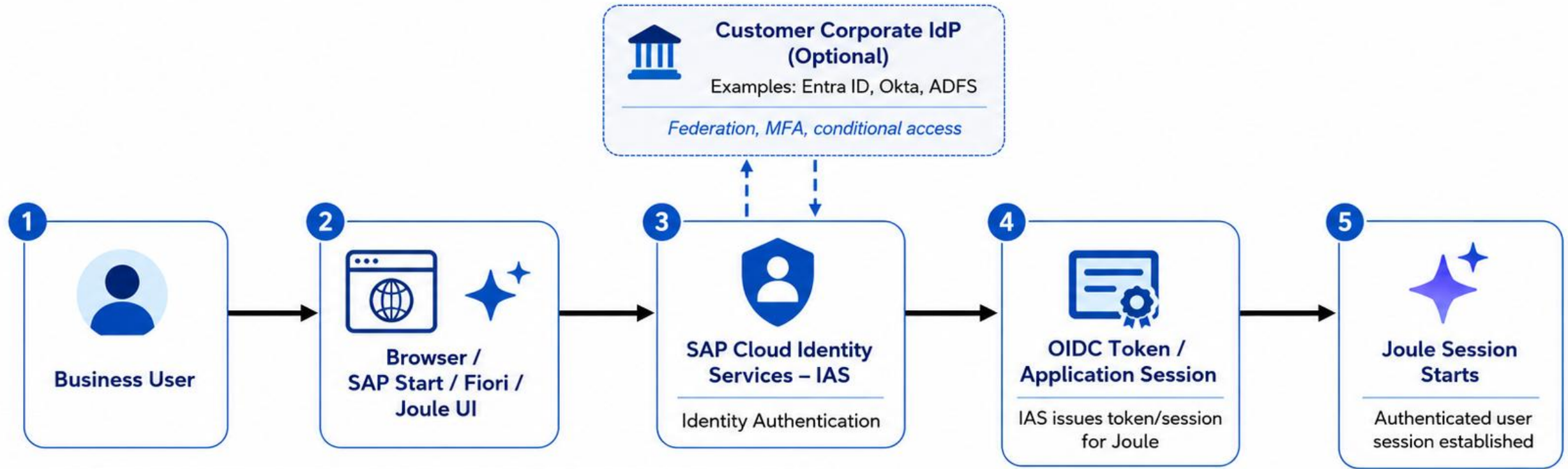
ISO 27001, ISO 27017, ISO 27018, ISO 22301, ISO 9001, BS 10012, ISAE 3402 SOC1 Type 2, ISAE 3000 SOC2 Type 2, BSI-C5, GDPR-readiness, NIST CSF, PCI-DSS, HIPAA, CCPS, ENS, ISMAP



Joule Integration with Cloud ERP

How Joule Authenticates to Start With

The starting point is the business user authenticating to Joule — not Joule logging directly into S/4HANA.



Runtime login behavior

1. User opens Joule.
2. If no active session exists, Joule redirects to IAS.
3. IAS may redirect to the corporate IdP for authentication.
4. After successful login, IAS returns an OIDC token/session to Joule.

→ = authentication flow
↔ = redirect / return flow

i This step authenticates the user to Joule, not directly to S/4HANA.



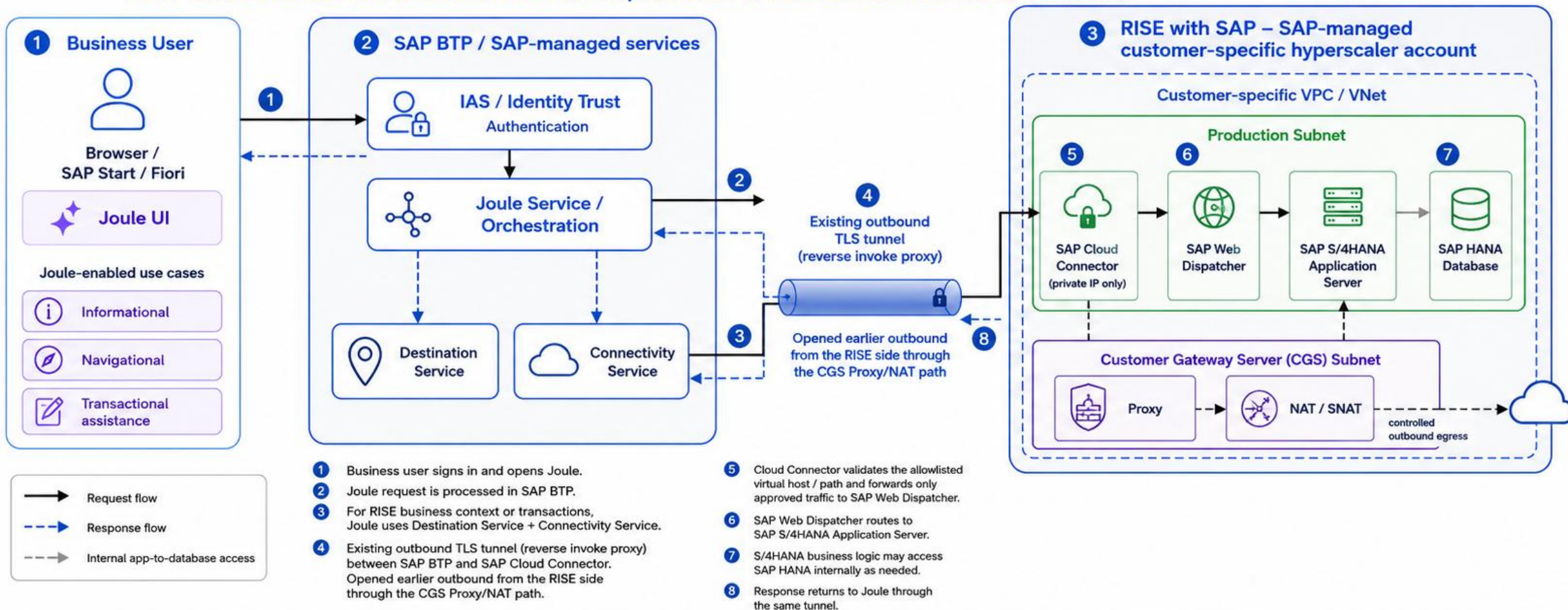
Slide-safe statement

Joule authenticates the user through SAP Cloud Identity Services – Identity Authentication. IAS may federate to the customer corporate IdP for MFA and conditional access. After successful authentication, IAS issues the token/session used by Joule.



RISE with SAP + Joule: secure integration architecture

How Joule-enabled use cases interact with a private RISE environment with secure data flow



Security controls



Identity & session trust:

- IAS / OAuth / authenticated user access



Outbound-only connectivity:

- private IP Cloud Connector, no inbound internet opening



Allowlisted backend access:

- Cloud Connector exposes only approved virtual endpoints



Application-layer control:

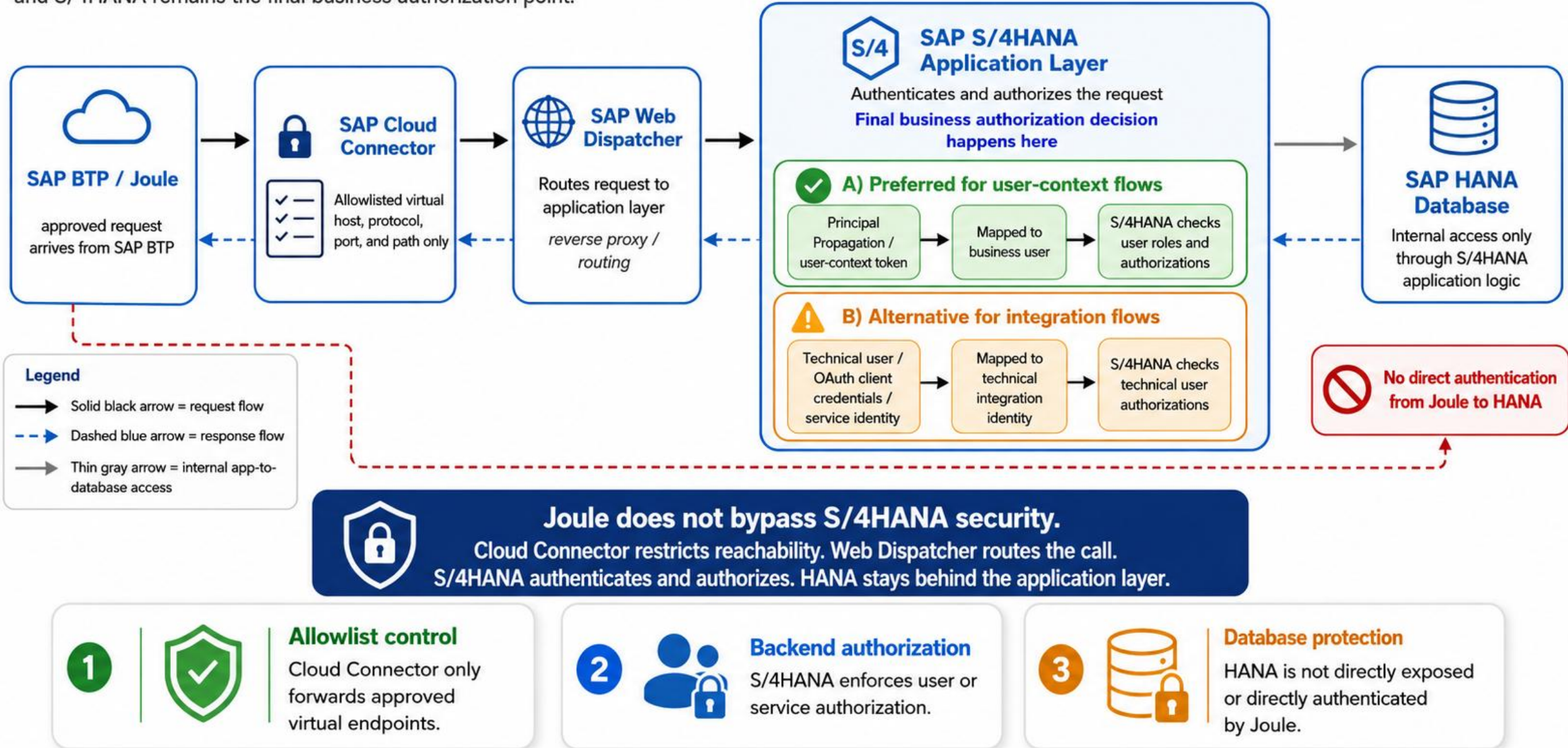
- Web Dispatcher and S/4HANA enforce business logic and authorization; HANA remains behind the app layer



Joule uses SAP BTP services and the existing Cloud Connector reverse-invoke tunnel to securely reach approved S/4HANA business functions in the private RISE environment.

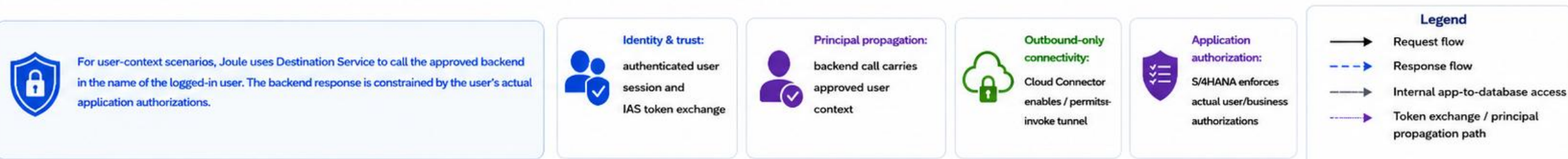
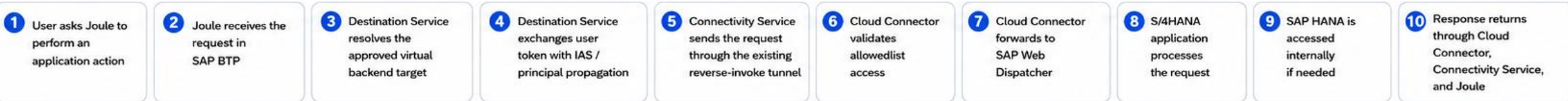
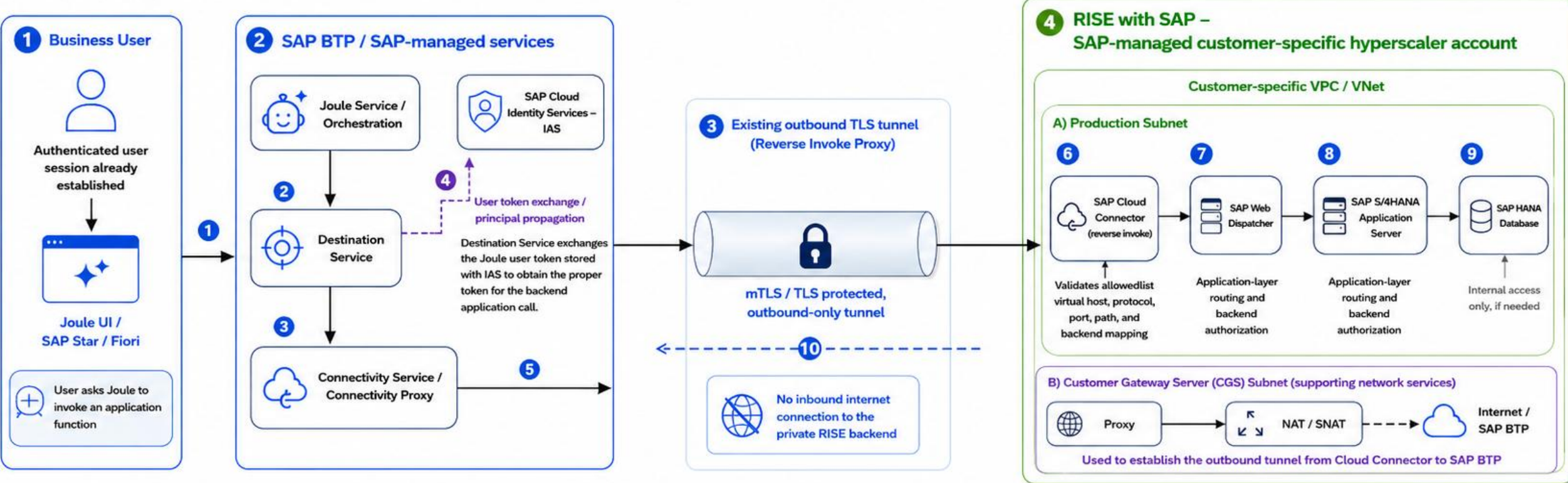
What S/4HANA Does at the Backend

Cloud Connector forwards only allowlisted access, Web Dispatcher routes the request, and S/4HANA remains the final business authorization point.



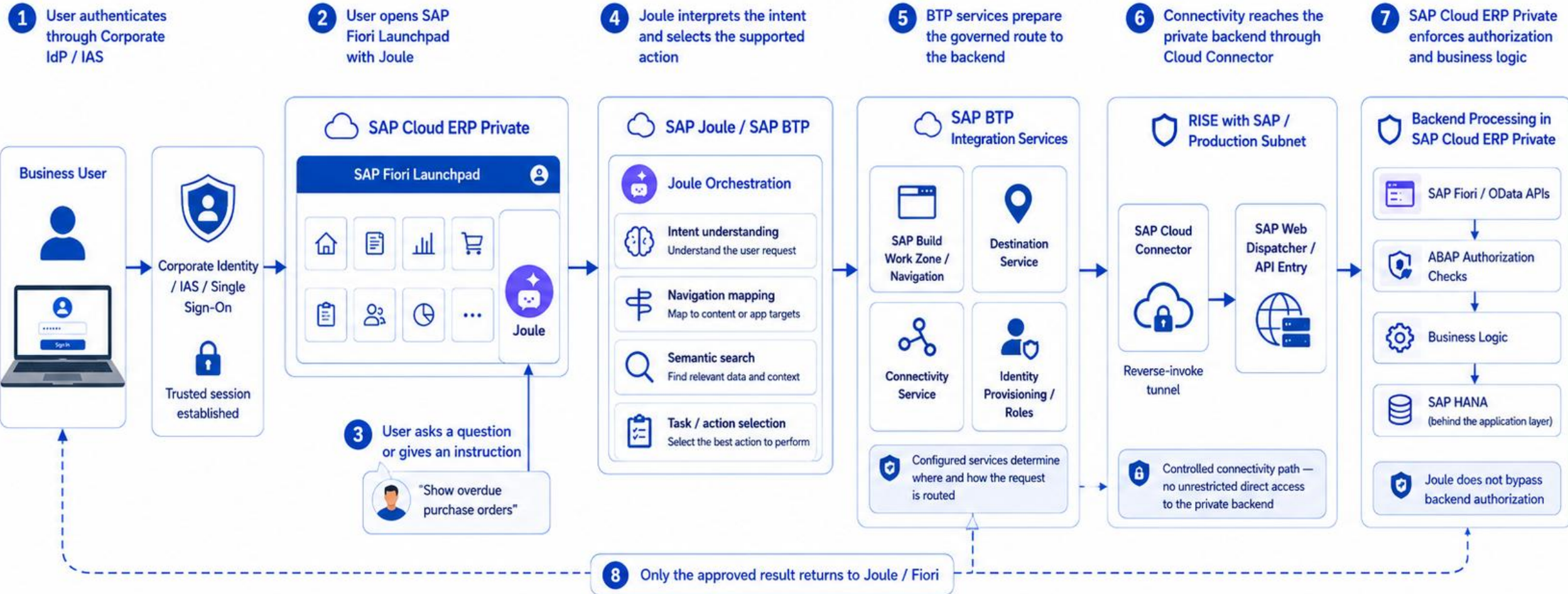
When Joule Needs to call RISE with SAP Cloud ERP Private

User-context business API flow from Joule to a private RISE backend using Destination Service, principal propagation, and Cloud Connector reverse-invoke connectivity.



Secure Data Flow Architecture — SAP Joule with SAP Cloud ERP Private

End-to-end user, identity, orchestration, connectivity, and backend authorization flow



Thank you

Samuele Scarpa

HEAD of SAP Cloud Architect & Advisor Italy
Global Cloud Operations

 Global Cloud Operations



CLOSED CAPTION: Avoid content in this area for your presentation. This bar will not show up when presenting in slideshow mode.