RISE with SAP S/4HANA Cloud, private edition

Security and Compliance

Jana Subramanian
CISPP, CCSP, CIPP/E/A, FIP, CISA, CRISC
IAPP Fellow of Information Privacy
APJ Principal Cyber Security Advisory Office
SAP Asia Pte Ltd

THE BEST RUN SAP

Disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. Except for your obligation to protect confidential information, this presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or any related document, or to develop or release any functionality mentioned therein.

This presentation, or any related document and SAP's strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information in this presentation is not a commitment, promise or legal obligation to deliver any material, code or functionality. This presentation is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This presentation is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this presentation, except if such damages were caused by SAP’s intentional or gross negligence.

All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

Agenda

RISE with SAP
S/4HANA Cloud, private edition

01 Deployment Model and Shared Security

02 Security Compliance

03 Security Architecture

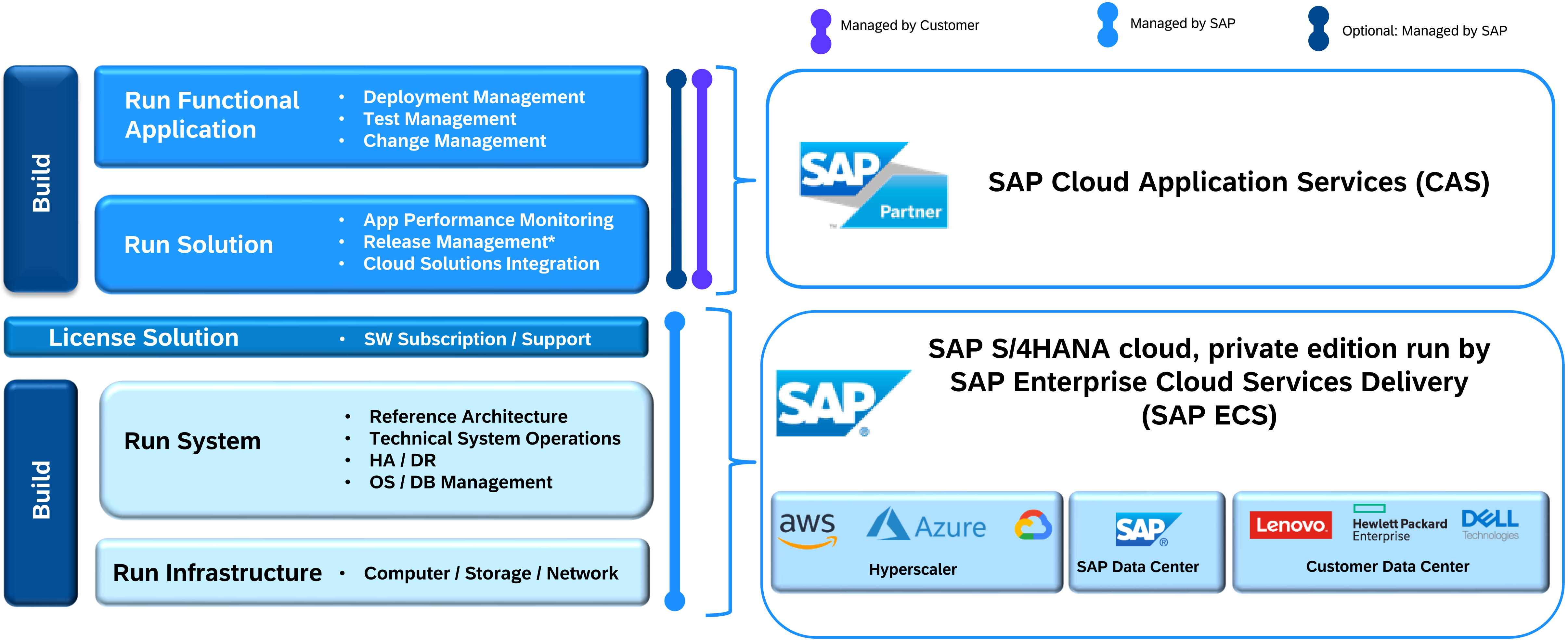
04 Logging and Monitoring

05 Security Operations

06 Q and A

Deployment Models

SAP S/4HANA Cloud, private edition: Deployment Models



● Managed by Customer

● Managed by SAP

● Optional: Managed by SAP

Build

Run Functional Application
- Deployment Management
- Test Management
- Change Management

Run Solution
- App Performance Monitoring
- Release Management*
- Cloud Solutions Integration

SAP Cloud Application Services (CAS)

License Solution
- SW Subscription / Support

Build

Run System
- Reference Architecture
- Technical System Operations
- HA / DR
- OS / DB Management

Run Infrastructure
- Computer / Storage / Network

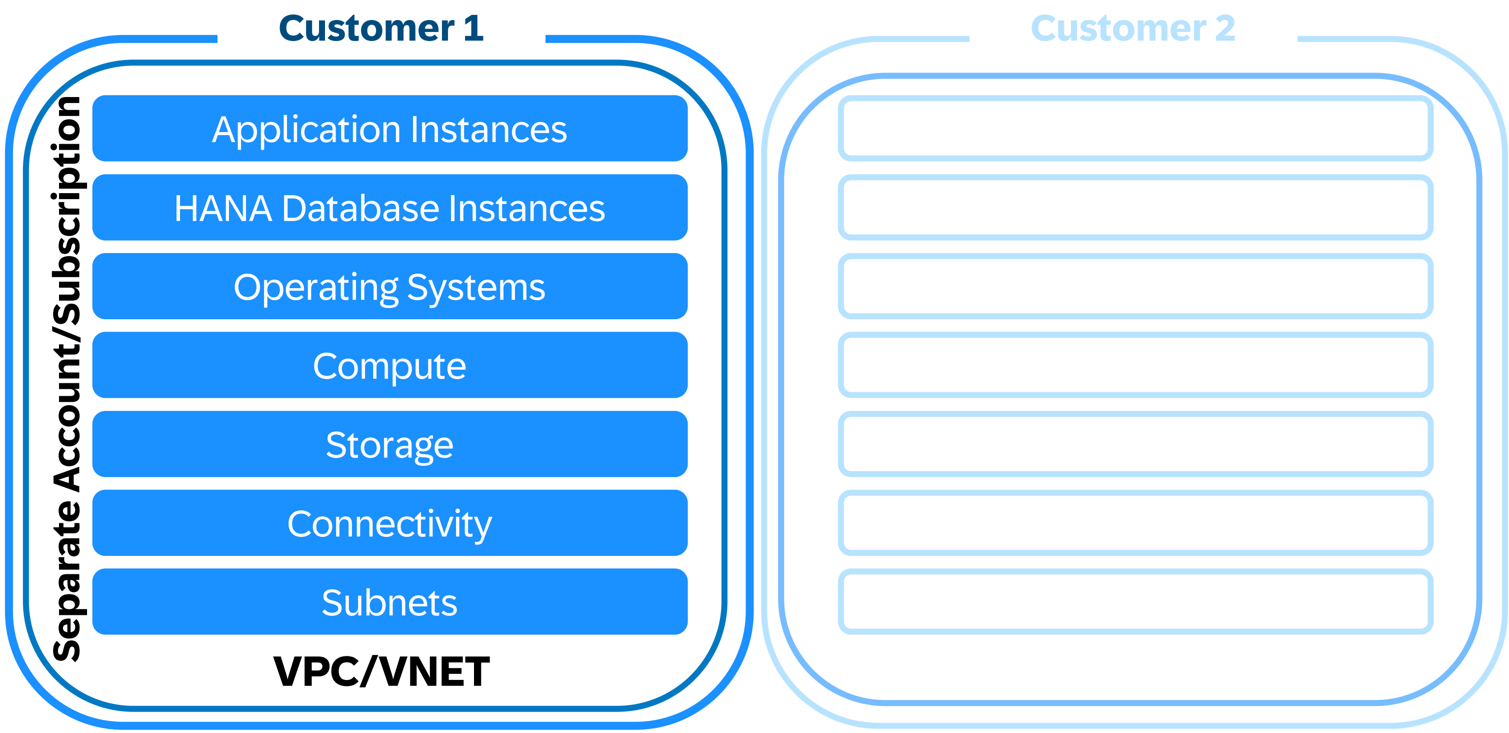
SAP S/4HANA cloud, private edition run by SAP Enterprise Cloud Services Delivery (SAP ECS)

Hyperscaler

SAP Data Center

Customer Data Center

SAP S/4HANA Cloud, Private Edition - Tenancy Model



Customer 1

Separate Account/Subscription

- Application Instances
- HANA Database Instances
- Operating Systems
- Compute
- Storage
- Connectivity
- Subnets

VPC/VNET

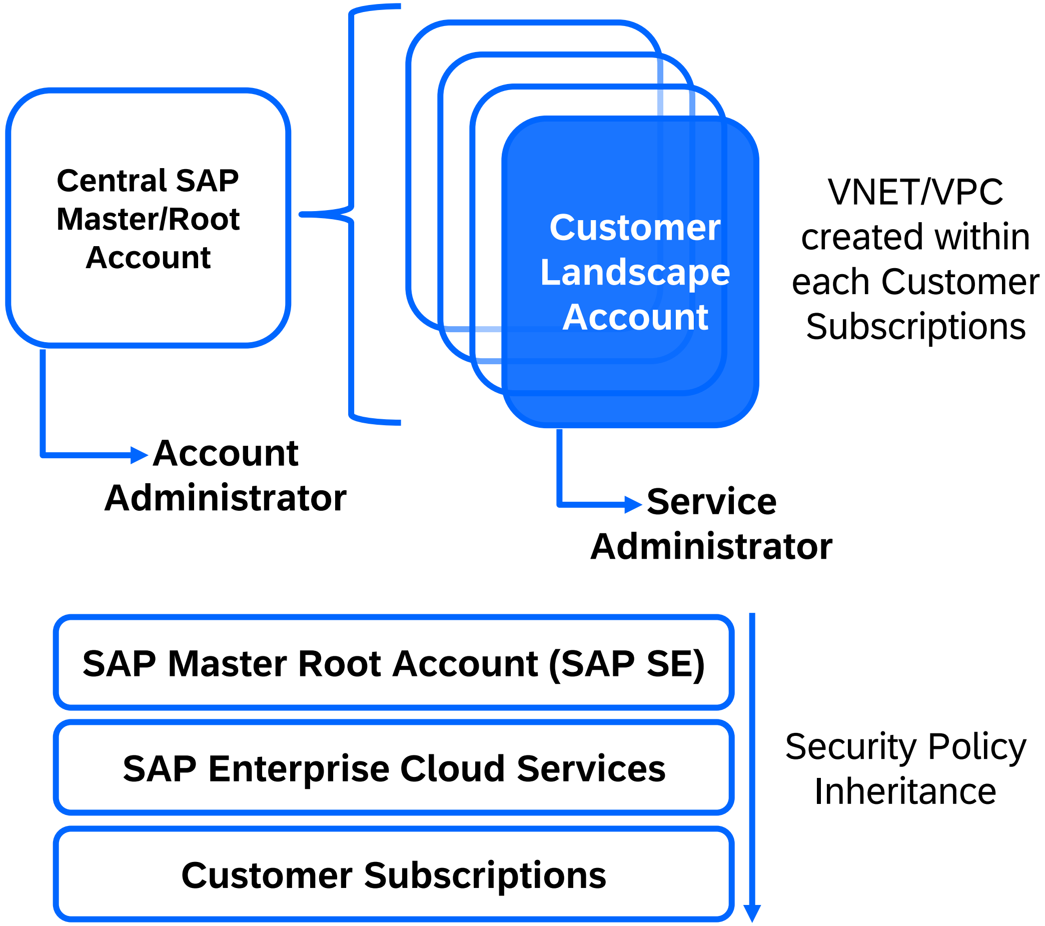
Customer 2

IaaS Provider — Customer's Choice – AWS, Azure or Google Cloud

Regional Admin VPC — Regional Admin | Infrastructure | Secure Admin Connectivity | Jump Hosts

SAP Global Security Operations — Monitoring & Alerting | Provisioning & Automation | SIEM | Asset & Lifecycle Management | VAPT & Security Patch Management | End Point Protection | Capacity Management | Admin Access

Customer Account Boundary



Central SAP Master/Root Account
Customer Landscape Account
VNET/VPC created within each Customer Subscriptions
Account Administrator
Service Administrator
SAP Master Root Account (SAP SE)
SAP Enterprise Cloud Services
Customer Subscriptions
Security Policy Inheritance

Customer Specific Subscription

- Hyperscaler Root Account is owned and managed by SAP
- Customer does not have access to the Hyperscaler Account/Subscription/Project
- SAP Global Security Policies and SAP Enterprise Cloud Services (ECS) Policies are applies through secure default deployment and compliance scans
- Customer chooses the Hyperscaler

aws

Shared Security Responsibility Model

RISE WITH SAP

S/4HANA Cloud, Private Edition

SAP Enterprise Cloud Services (ECS)

- ✓ Resilient platform architecture (HA and DR)
- ✓ Single Tenanted Landscape
- ✓ Managed Backup and Restore
- ✓ Building Secure Virtual Machines, Operating systems, networking, HANA Database
- ✓ HANA DB Management
- ✓ Technical Managed Services (R&R Link)
- ✓ Operational Security and Managing security incidents
- ✓ 24x7 Security Monitoring
- ✓ Personal Data Breach Notification
- ✓ SLA and Support Services
- ✓ Threat Management & Patch Management

Customer

- ✓ Dedicated Private Connectivity to Hyperscaler
- ✓ Application User Identity Management
- ✓ Application User Authentication and Authorisation Management
- ✓ Application User Roles, User Groups, Access Control
- ✓ Customer Data Ownership
- ✓ Compliance to Government & Industry Regulations
- ✓ Application Security Audit Logging (SAL)
- ✓ Integration and Extensions, Custom Applications Development
- ✓ Configuration of the Customer Business Processes
- ✓ Application Change Management

- ✓ 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

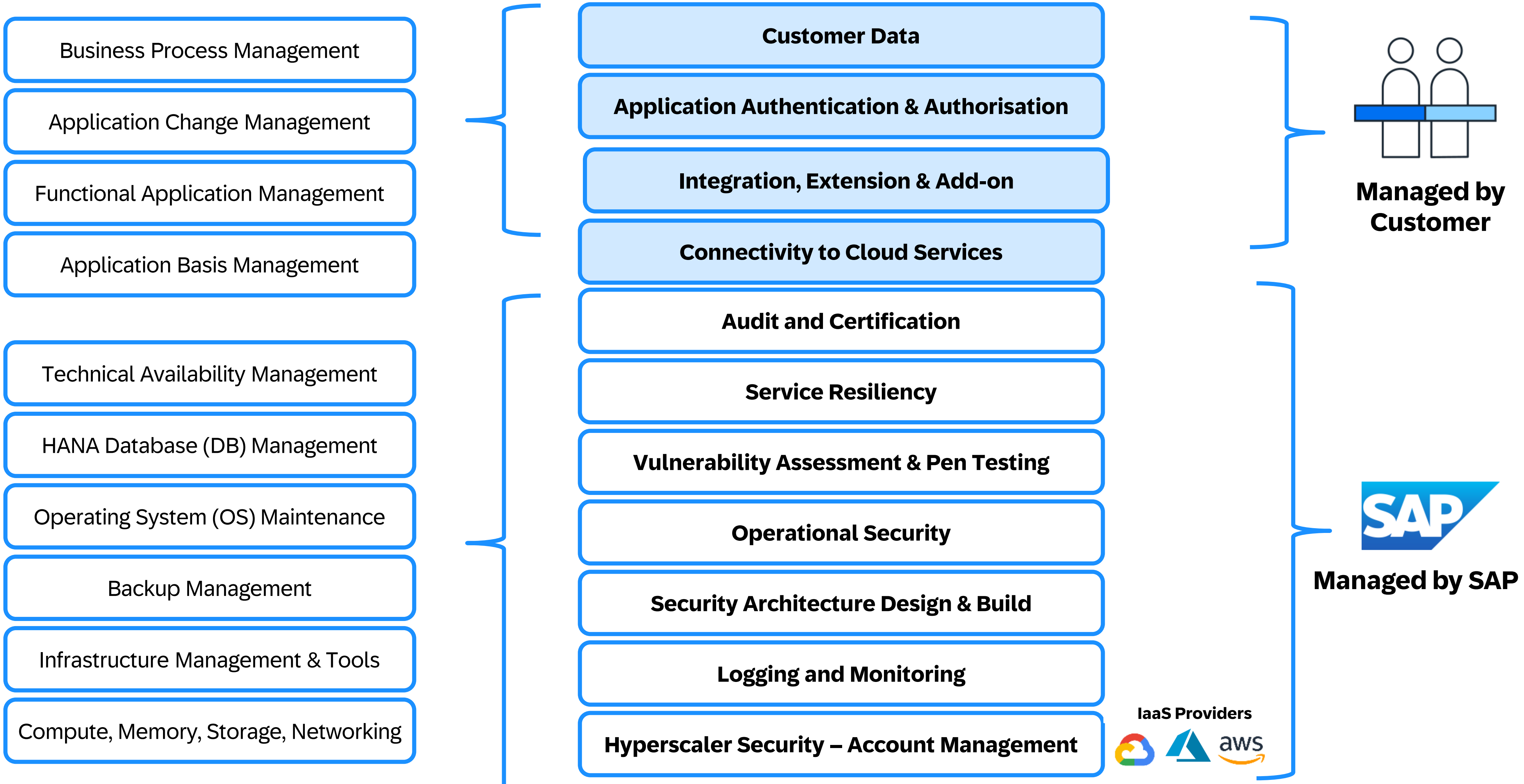
(Customer selected deployment Region)

Managed by SAP SE

Supported Hyperscalers

aws Azure Google Cloud

Shared Security Governance



- Business Process Management
- Application Change Management
- Functional Application Management
- Application Basis Management

- Customer Data
- Application Authentication & Authorisation
- Integration, Extension & Add-on
- Connectivity to Cloud Services

Managed by Customer

- Technical Availability Management
- HANA Database (DB) Management
- Operating System (OS) Maintenance
- Backup Management
- Infrastructure Management & Tools
- Compute, Memory, Storage, Networking

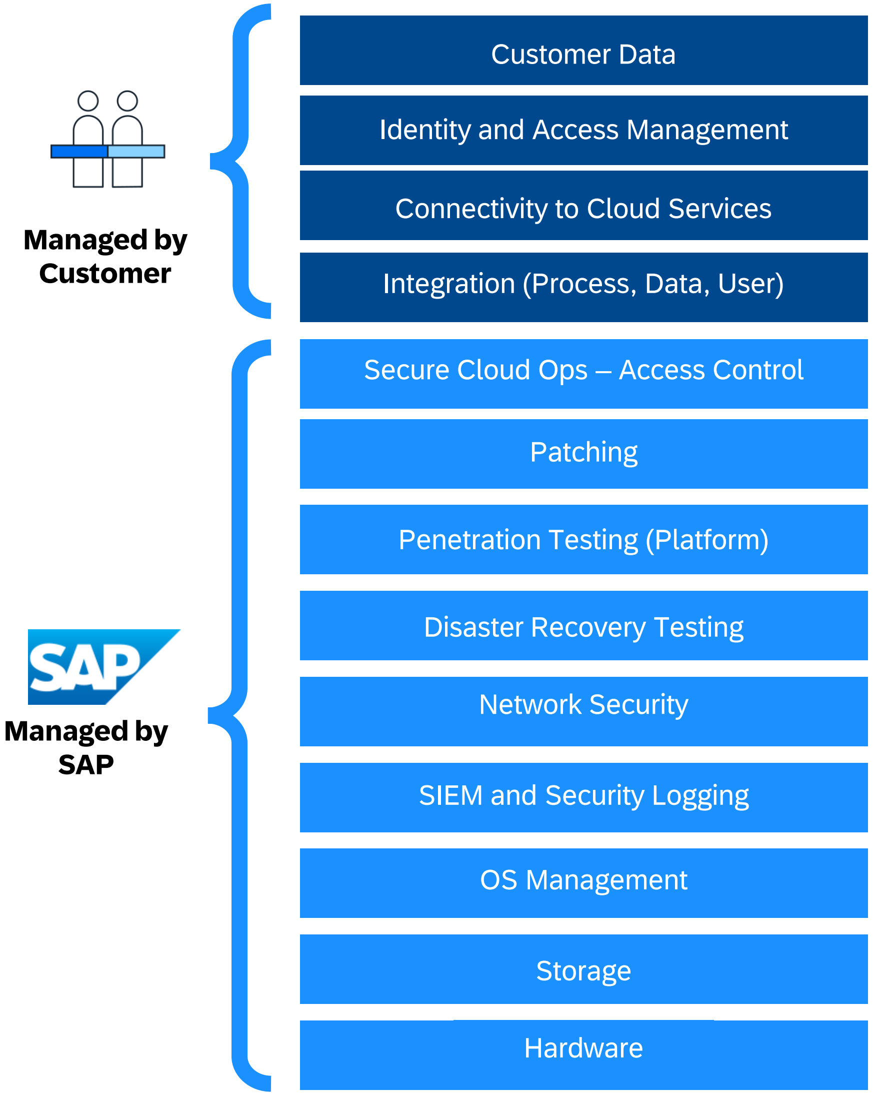
- Audit and Certification
- Service Resiliency
- Vulnerability Assessment & Pen Testing
- Operational Security
- Security Architecture Design & Build
- Logging and Monitoring
- Hyperscaler Security – Account Management

IaaS Providers

Managed by SAP

Security Compliance

Security Assurance



Managed by Customer

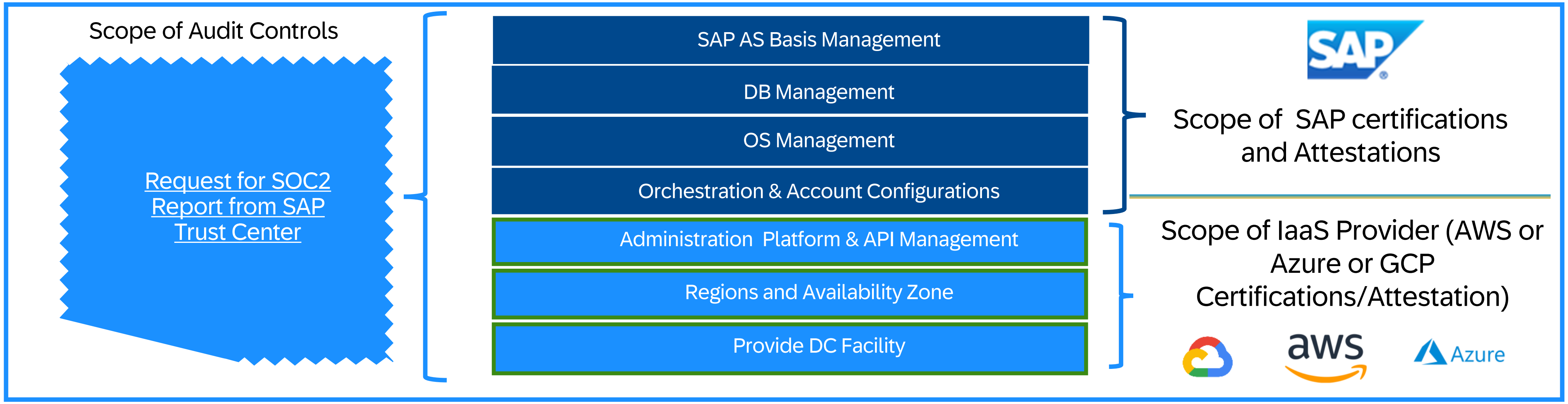
- Customer Data
- Identity and Access Management
- Connectivity to Cloud Services
- Integration (Process, Data, User)

Managed by SAP

- Secure Cloud Ops – Access Control
- Patching
- Penetration Testing (Platform)
- Disaster Recovery Testing
- Network Security
- SIEM and Security Logging
- OS Management
- Storage
- Hardware

SAP Audit Certification		
✓	ISO 27001	Certification for Information Security Management Systems
✓	ISO22301	Certification for Business Continuity Management Systems
✓	ISO 9000	Quality Management Systems
✓	SOC 1 Type 2	Statement of effectiveness of Type 1 examination
✓	BS10012	Personal Information Management
✓	SOC 2 Type 2	Service Organization Controls Report (Attestation report)

Scope of certification


Scope of Audit Controls
Request for SOC2 Report from SAP Trust Center
SAP AS Basis Management
DB Management
OS Management
Orchestration & Account Configurations
Administration Platform & API Management
Regions and Availability Zone
Provide DC Facility
Scope of SAP certifications and Attestations
Scope of IaaS Provider (AWS or Azure or GCP Certifications/Attestation)
aws
Azure

Cloud Service Group	Compliance / Certification
SAP Enterprise Cloud Services – operated by SAP on IaaS provider (AWS, Azure or GCP)	ISAE3402 SOC 1 Type II, ISAE 3000 SOC2 Type II, ISO 27001:2013, ISAE 3000 C5 Type II SOC2: 12 months ISO: 36 months with surveillance audits every 12 months.

SAP Cloud Services – Security Activity

Security Architecture Design and Build

- Creation of separate account/subscription
- Cloud Network Setup and configurations (VPC, Subnet, NSG, WAF, LB, DNS, Proxy etc)
- IP Addressing
- System build
- SAP Global Security Policy deployment

Continuous Logging and Monitoring

- Security Incident Management
- Monitoring, Alerting and Forensic Analysis
- Real Event Correlation and Security Event Management
- Personal Data Breach Notification
- Security Use Case Development
- External Cyber Threat Intelligence

Operational Security

- System Hardening
- Regular Scheduled Maintenance
- Access and Change Management
- Security Patch Management
- Administrative Access and User Management
- Backup and Restore

Threat Management

- Regular Vulnerability Management
- Regular Penetration Testing
- Perform Risk Assessment
- Remediation of identified vulnerabilities
- Approve and Review Customer Initiated Penetration Tests results (if any)

SAP Cloud Services – Security Activity

Service Resiliency

- Cloud Disaster Recovery and resiliency management
- IT Service Continuity Management
- Process Continuity
- Asset Management
- Business Continuity and Operational Resiliency

Hyperscale Account Security

- Preventive controls and Detective Monitoring of Cloud Accounts
- Cloud Account Life Cycle Management
- Golden Images
- Compliance Security Scanning

Audit and certifications

- Bi-Annual SOC 1 and SOC2 Audits and Report
- ISO 27001 Audits
- ISO22301 and BS10012 Audit
- ISO9001 Audits

Data Protection and Privacy

- Sub-processor and Sub-contractor Management
- Personal Data Breach Notifications
- Secure Data Deletion upon contract termination
- SAP DPA and Technical and Organisation Measures (TOM)

Secure Architecture

Secure Connectivity

1

IPSEC VPN

Site-to-site IPSEC VPN between an on-premise network and Hyperscale Network. The traffic between the environment supports network layer encryption.

2

Dedicated Private Connection

Using dedicated connectivity options such as AWS Direct Connect, Azure Express Route and Google Cloud Interconnect, customer can establish dedicated connectivity from customer on-premise network to RISE with SAP S/4HANA Cloud, Private Edition landscape.

3

VPC Peering

Secure Connectivity between SAP managed customer landscape and customer owned landscape on Hyperscaler

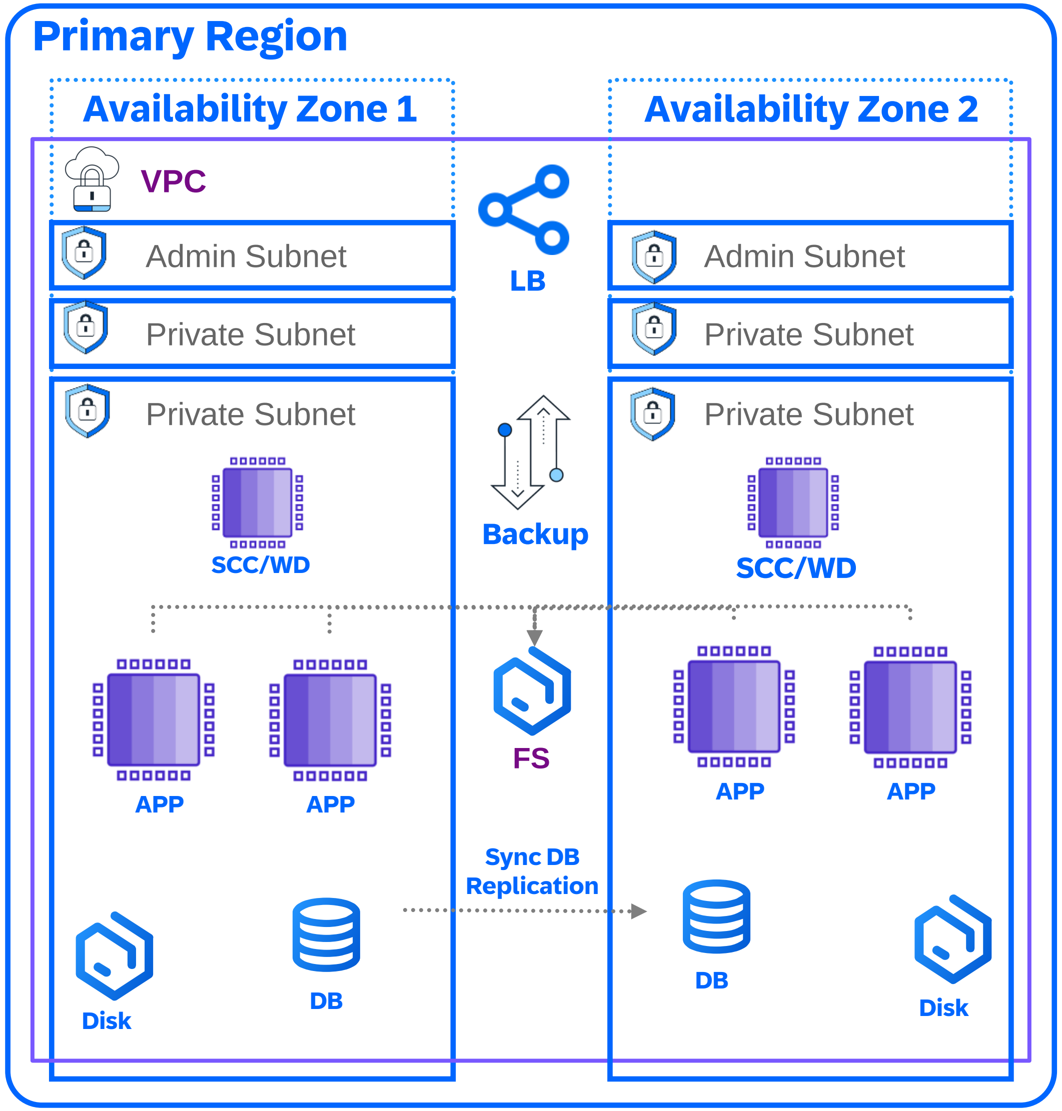
Virtual network peering creates network connectivity between two virtual networks (VPC for AWS or VNet for Azure), which are owned by different account holders.

4

Inbound Internet

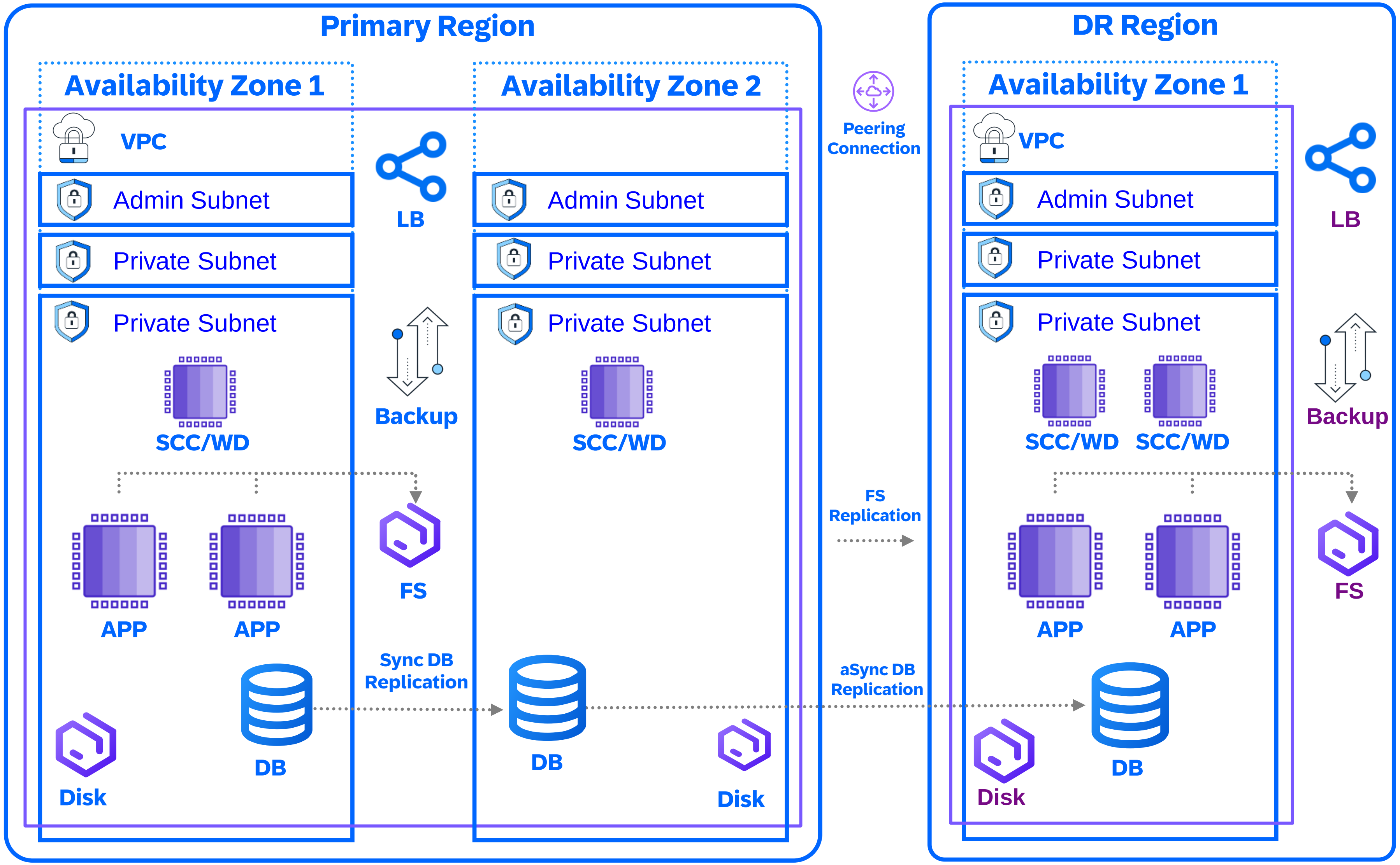
Inbound traffic from Internet can be allowed and will be screened via WAF. Application Load Balancer will be able to route traffic to the Web Dispatcher in the production subnet. Traffic is encrypted with TLS1.2 encryption.

SAP S/4HANA Cloud, private edition – Short Distance DR



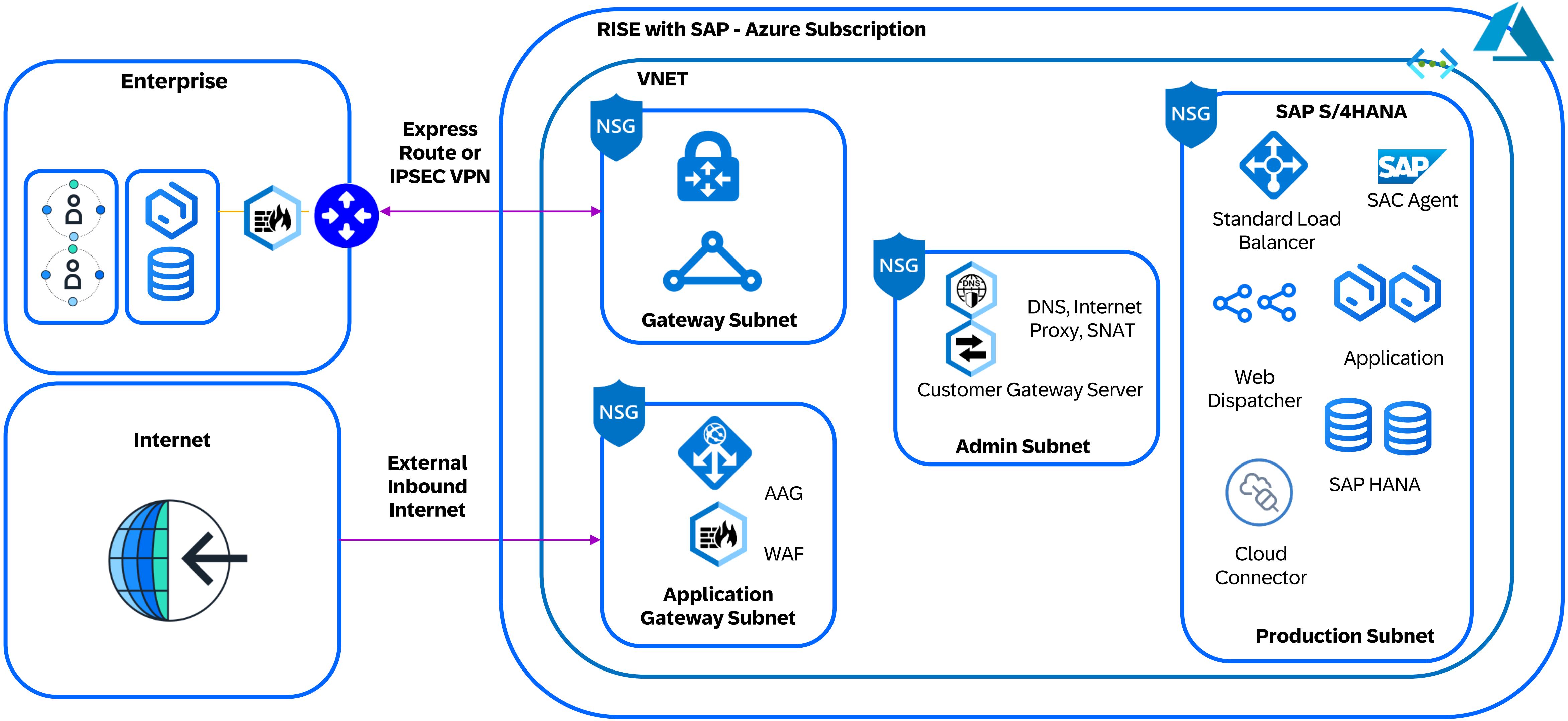
- ✓ SAP Solution is deployed across two Availability Zones (AZ) in a single region for HA/DR. The components deployed in each of the AZ's are symmetrical
- ✓ Application components such as Application Servers and Web Dispatchers are running Active-Active across the two Availability Zones (AZ) with Application Load Balancer (ALB) in front distributing traffic.
- ✓ Database is running in Active-Passive mode. Synchronous Database Replication via native replication mechanisms is enabled.
- ✓ Block storage for DB file systems like data and log volumes. Zone resilient NFS is used for shares and application file system. BLOB storage is primarily used for backups.
- ✓ Instance Auto Recovery with scripts.
- ✓ Protect against Availability Zone failure
- ✓ No Regional outage Protection

SAP S/4HANA Cloud, private edition – Long Distance DR



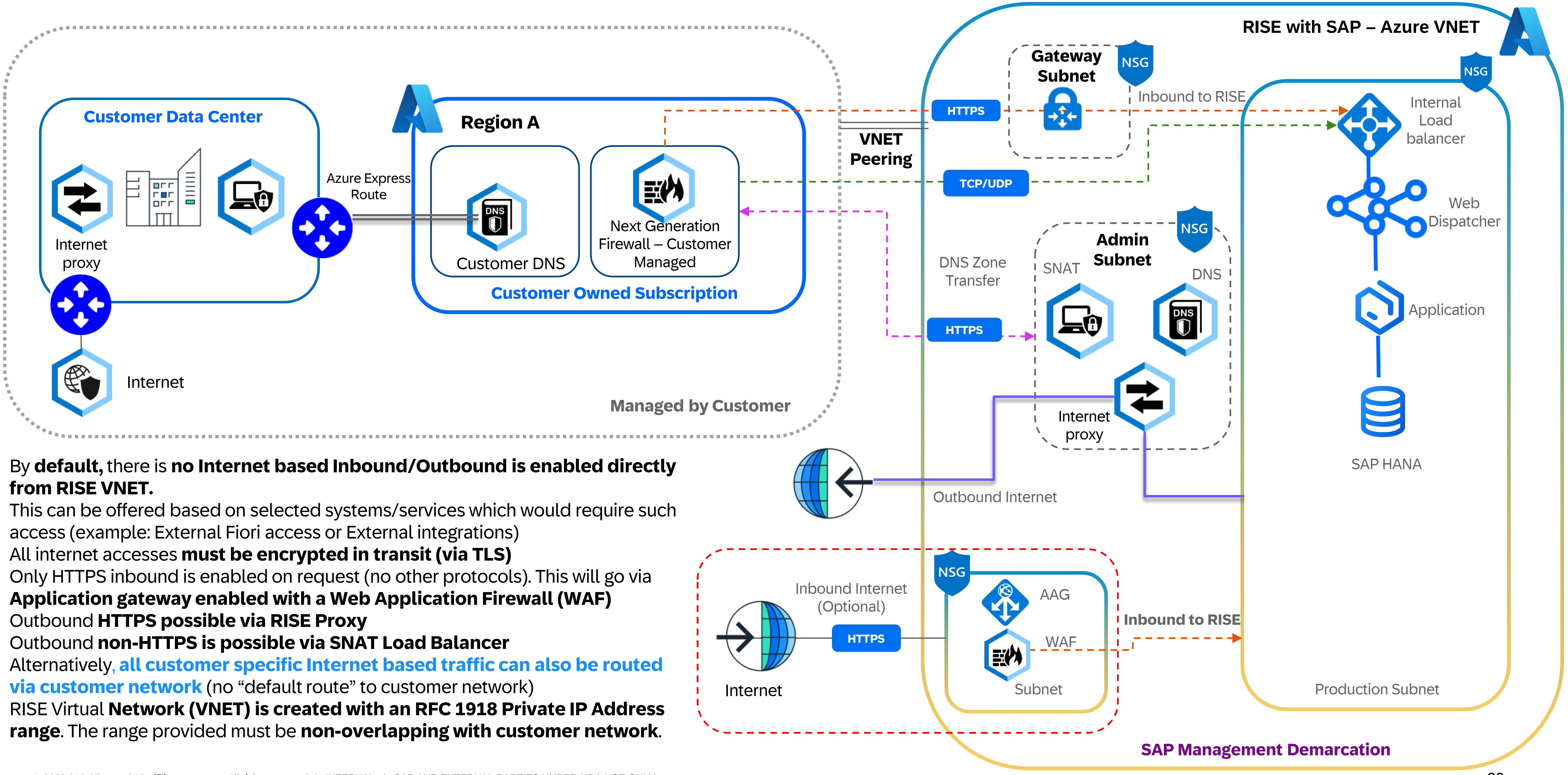
- Protect against region outages
- SAP Solution is deployed across two regions for regional DR
- SAP Application and Database is deployed in single AZ of primary and DR region. Additionally DB HA node mandatory for VM is greater then 8TB for HANA.
- Web Dispatchers and Cloud Connectors are deployed across two AZ's in primary Region and single AZ in DR region.
- VPC Peering is used to connect Primary with DR Region
- Asynchronous Database Replication via native replication mechanisms to DR region.
- Filesystems are synchronization
- Usage of Auto Recovery with scripts.

RISE with SAP – Landscape



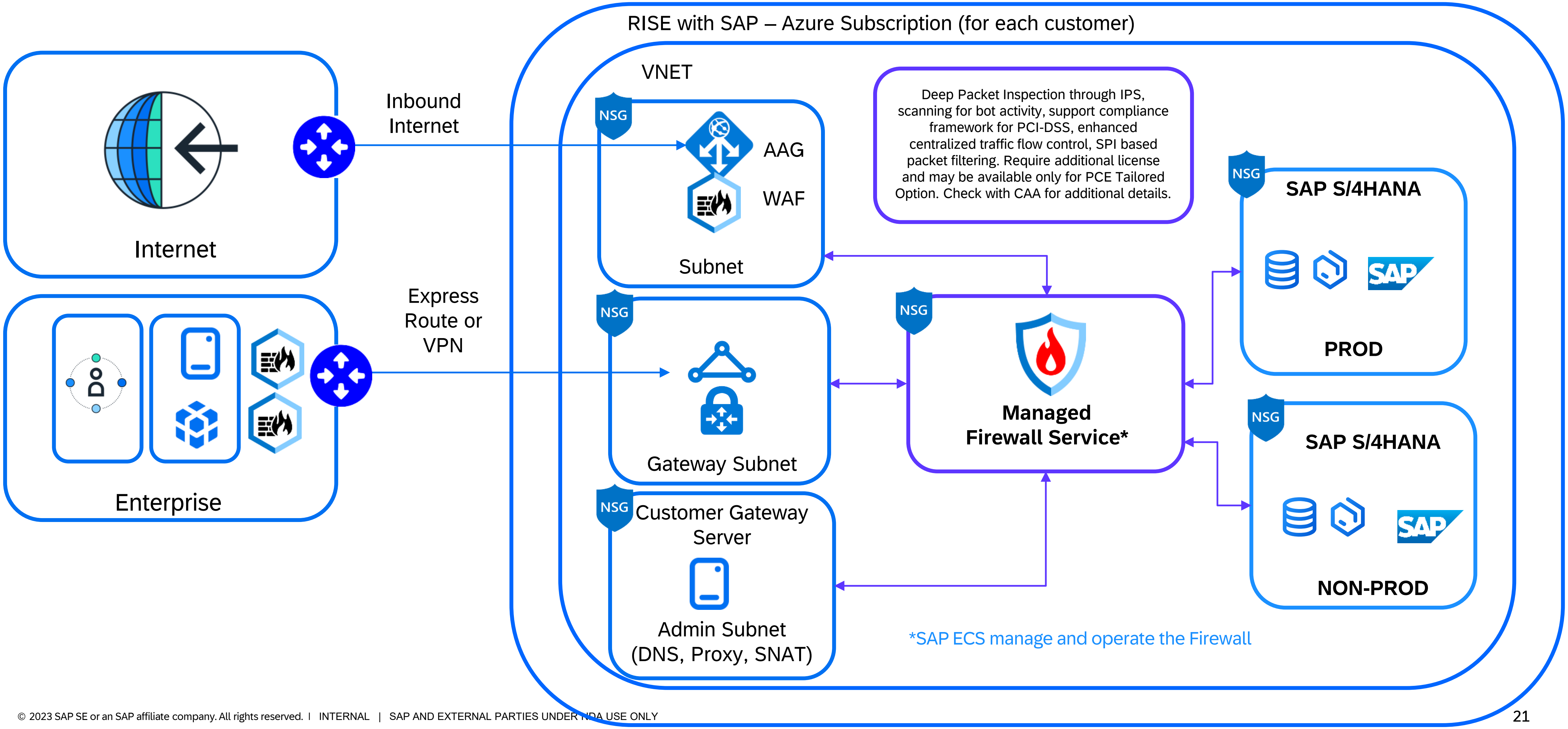
Source : https://blogs.sap.com/2023/09/20/secure-data-flow-and-connectivity-with-sap-cloud-services/

Secure Data Flow



- By **default,** there is **no Internet based Inbound/Outbound is enabled directly from RISE VNET.**
- This can be offered based on selected systems/services which would require such access (example: External Fiori access or External integrations)
- All internet accesses **must be encrypted in transit (via TLS)**
- Only HTTPS inbound is enabled on request (no other protocols). This will go via
- **Application gateway enabled with a Web Application Firewall (WAF)**
- Outbound **HTTPS possible via RISE Proxy**
- Outbound **non-HTTPS is possible via SNAT Load Balancer**
- Alternatively**, all customer specific Internet based traffic can also be routed via customer network** (no "default route" to customer network)
- RISE Virtual **Network (VNET) is created with an RFC 1918 Private IP Address range**. The range provided must be **non-overlapping with customer network.**

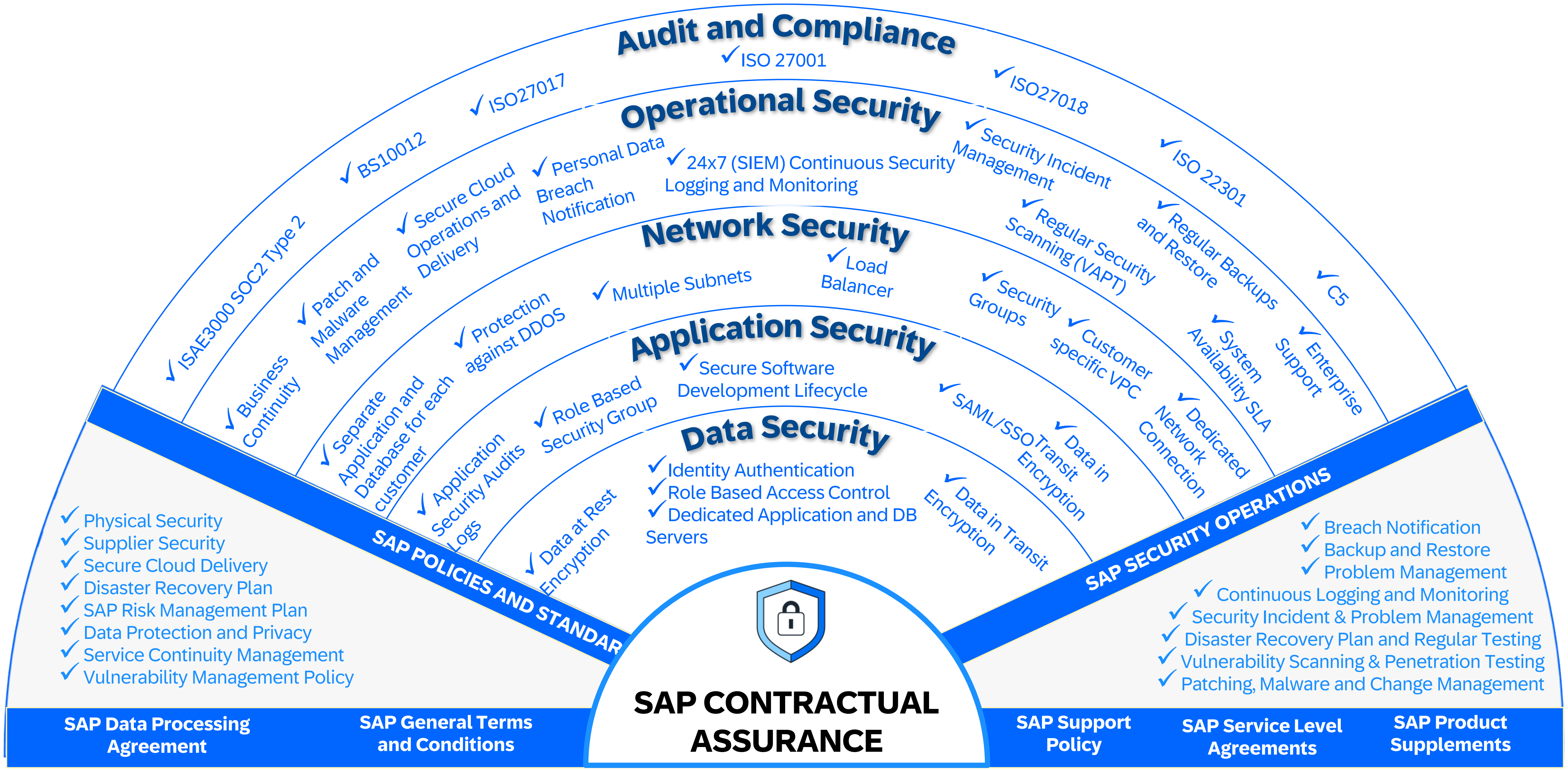
SAP ECS Managed Firewall Service (Optional Service)



Deep Packet Inspection through IPS, scanning for bot activity, support compliance framework for PCI-DSS, enhanced centralized traffic flow control, SPI based packet filtering. Require additional license and may be available only for PCE Tailored Option. Check with CAA for additional details.

*SAP ECS manage and operate the Firewall

Defense in Depth Security



Audit and Compliance

- ✓ ISAE3000 SOC2 Type 2
- ✓ BS10012
- ✓ ISO27017
- ✓ ISO 27001
- ✓ ISO27018
- ✓ ISO 22301
- ✓ C5
- ✓ Enterprise Support

Operational Security

- ✓ Business Continuity
- ✓ Patch and Malware Management
- ✓ Secure Cloud Operations and Delivery
- ✓ Personal Data Breach Notification
- ✓ 24x7 (SIEM) Continuous Security Logging and Monitoring
- ✓ Security Incident Management
- ✓ Regular Security Scanning (VAPT)
- ✓ Regular Backups and Restore
- ✓ System Availability SLA

Network Security

- ✓ Separate Application and Database for each customer
- ✓ Protection against DDOS
- ✓ Multiple Subnets
- ✓ Load Balancer
- ✓ Security Groups
- ✓ Customer specific VPC
- ✓ Dedicated Network Connection

Application Security

- ✓ Application Security Audits Logs
- ✓ Role Based Security Group
- ✓ Secure Software Development Lifecycle
- ✓ SAML/SSO
- ✓ Data in Transit Encryption

Data Security

- ✓ Data at Rest Encryption
- ✓ Identity Authentication
- ✓ Role Based Access Control
- ✓ Dedicated Application and DB Servers
- ✓ Data in Transit Encryption

SAP POLICIES AND STANDAR

- ✓ Physical Security
- ✓ Supplier Security
- ✓ Secure Cloud Delivery
- ✓ Disaster Recovery Plan
- ✓ SAP Risk Management Plan
- ✓ Data Protection and Privacy
- ✓ Service Continuity Management
- ✓ Vulnerability Management Policy

SAP SECURITY OPERATIONS

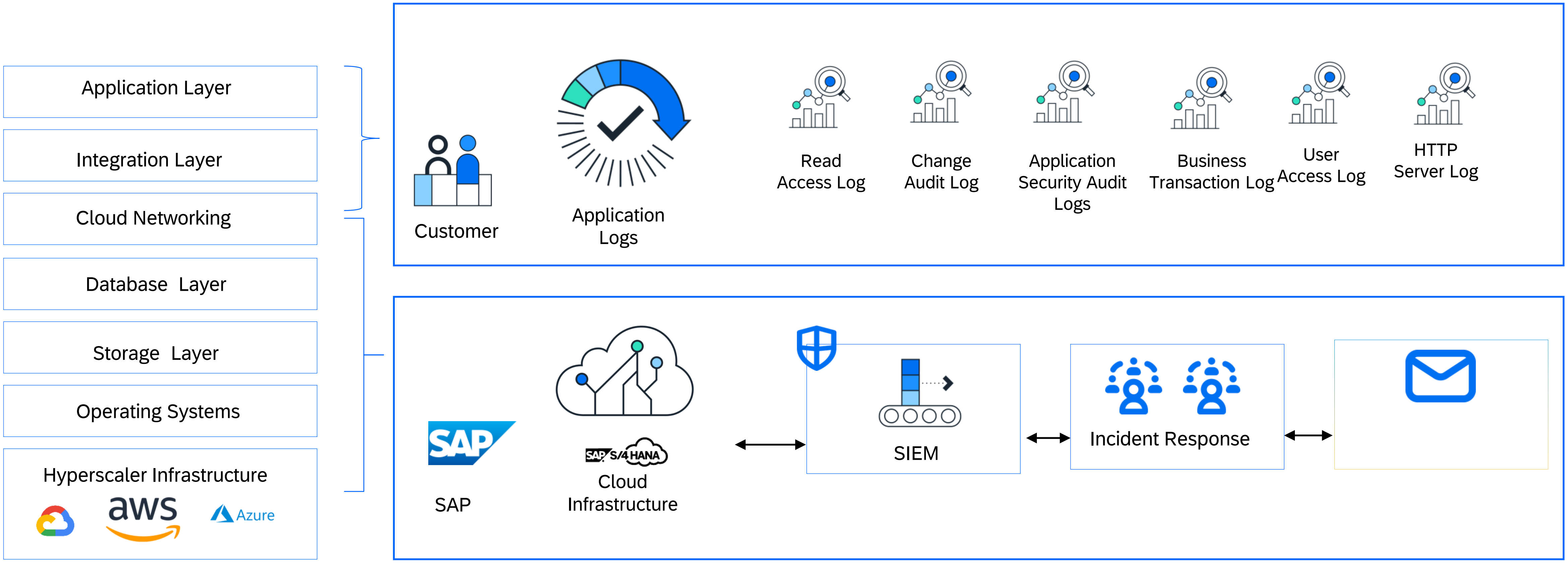
- ✓ Breach Notification
- ✓ Backup and Restore
- ✓ Problem Management
- ✓ Continuous Logging and Monitoring
- ✓ Security Incident & Problem Management
- ✓ Disaster Recovery Plan and Regular Testing
- ✓ Vulnerability Scanning & Penetration Testing
- ✓ Patching, Malware and Change Management

SAP CONTRACTUAL ASSURANCE

SAP Data Processing Agreement | **SAP General Terms and Conditions** | **SAP Support Policy** | **SAP Service Level Agreements** | **SAP Product Supplements**

Logging and Monitoring

Application and Infrastructure Logs



Application Layer

Integration Layer

Cloud Networking

Database Layer

Storage Layer

Operating Systems

Hyperscaler Infrastructure

Customer

Application Logs

Read Access Log

Change Audit Log

Application Security Audit Logs

Business Transaction Log

User Access Log

HTTP Server Log

SAP

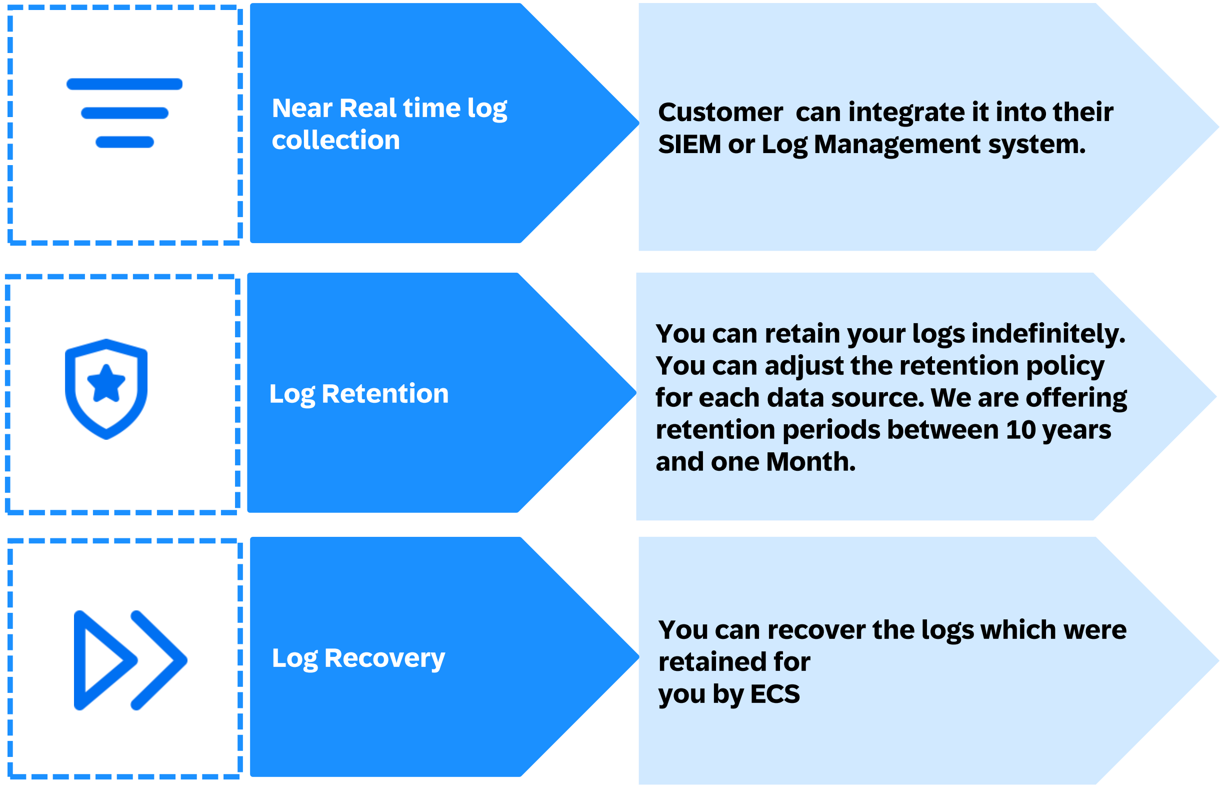
Cloud Infrastructure

SIEM

Incident Response

LOGSERV Services

LOGSERV



Near Real time log collection

Customer can integrate it into their SIEM or Log Management system.

Log Retention

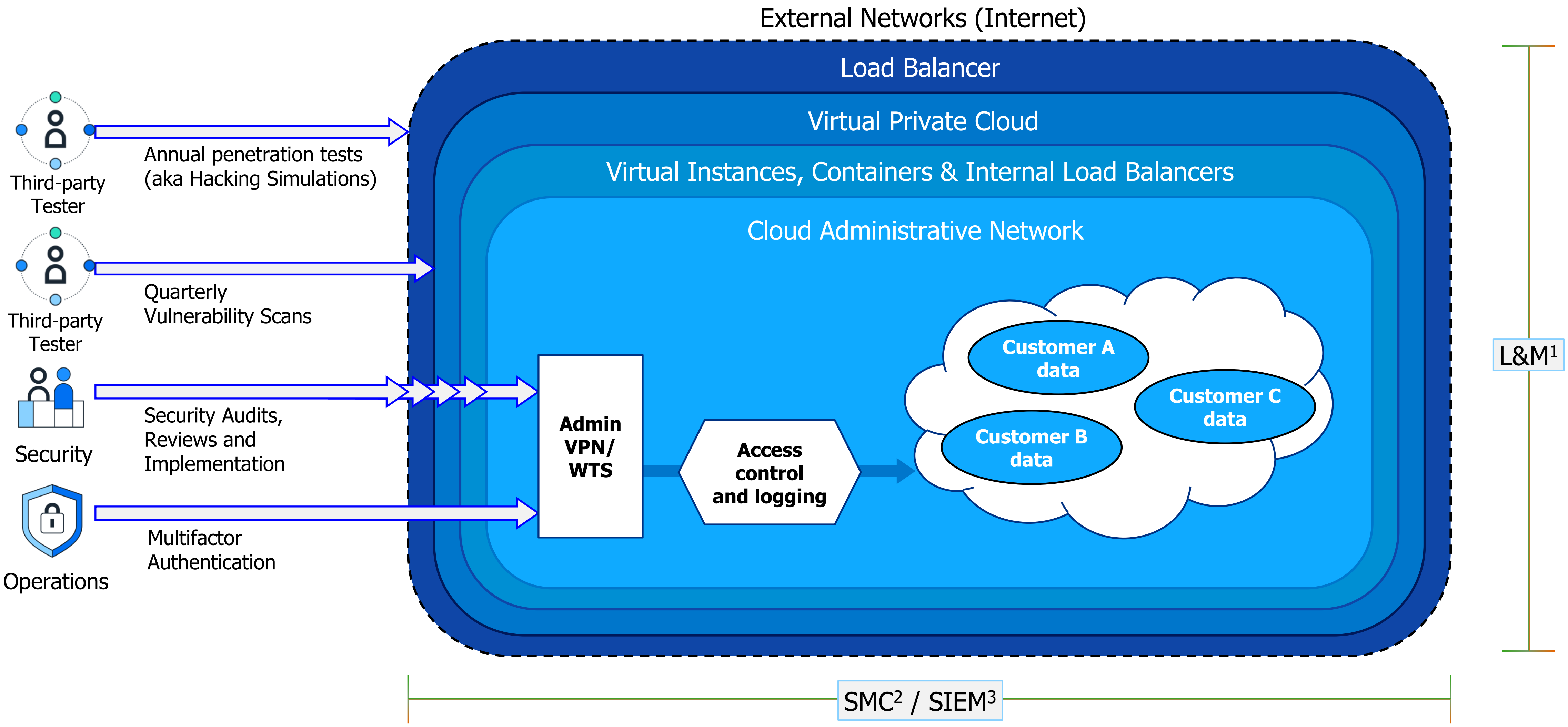
You can retain your logs indefinitely. You can adjust the retention policy for each data source. We are offering retention periods between 10 years and one Month.

Log Recovery

You can recover the logs which were retained for you by ECS

Security Operations

Vulnerability Advisory Services


External Networks (Internet)
Load Balancer
Virtual Private Cloud
Virtual Instances, Containers & Internal Load Balancers
Cloud Administrative Network
Third-party Tester
Annual penetration tests (aka Hacking Simulations)
Third-party Tester
Quarterly Vulnerability Scans
Security
Security Audits, Reviews and Implementation
Operations
Multifactor Authentication
Admin VPN/ WTS
Access control and logging
Customer A data
Customer B data
Customer C data
L&M1
SMC2 / SIEM3

1. L&M = API Logging and Monitoring

2.SMC = Security Monitoring Center (7*24)

3. SIEM = Security Information and Event Management

NIST Framework Alignment

Identify

- Security Patch Management
- Vulnerability Scanning
- Vulnerability Advisory
- Customer Penetration Testing
- Hacking Simulations
- Cloud Security Compliance Scanning
- Security Awareness
- Asset & Change Mgmt.

Protect

- Malware Management
- Identity & Access Management
- Privileged Identity Management
- Backup and Restore
- Single Tenant Data Segregation
- Security Hardened System
- DDoS Protection
- Web Dispatcher (Proxy)
- Cloud Connector
- Golden Image (Hyperscaler)

Detect

- 24x7 Security Monitoring
- Cloud Security & Compliance
- Application Security Audit Logs (SAL)
- Cloud Security Configuration Checks
- Baseline Configuration Checks

Application Security Updates

Respond

24x7 Incident Response

- Root Cause Analysis
- PII Data Breach Notification

Recover

- Advanced Forensics
- Lesson Learned

Follow us

www.sap.com/contactsap

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.