THE BEST RUN SAP

Rise with SAP
SAP S/4HANA Cloud, Private Edition
Cyber Security & Data Privacy
User Group Session

Jana Subramanian
CISSP, CCSP, CIPP/A, CIPP/E, CRISC, CISA, FIP, TOGAF 9
Fellow of Information Privacy (IAPP)
Head of Cybersecurity
Strategic Customer Engagements

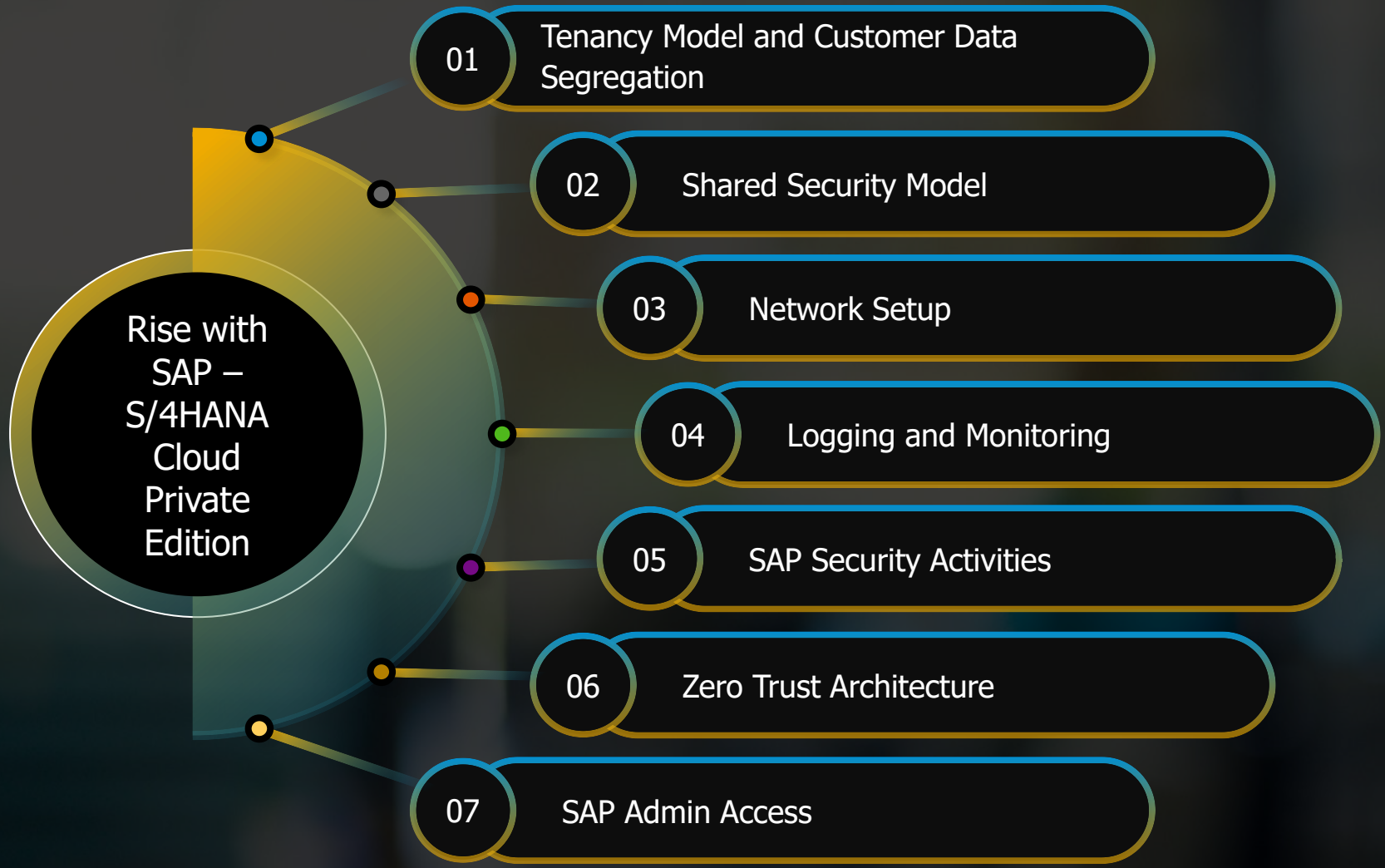
Disclaimer

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.

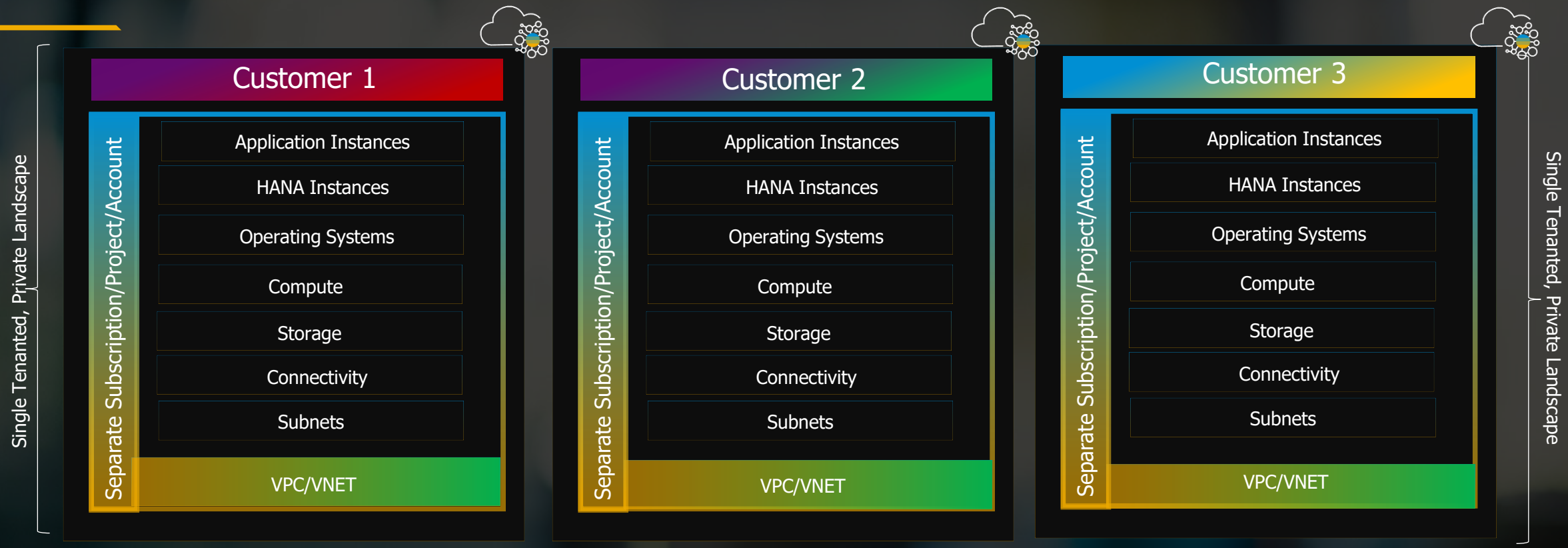
All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied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

Agenda


Rise with SAP – S/4HANA Cloud Private Edition
01
Tenancy Model and Customer Data Segregation
02
Shared Security Model
03
Network Setup
04
Logging and Monitoring
05
SAP Security Activities
06
Zero Trust Architecture
07
SAP Admin Access

Tenancy Model

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



Azure aws IaaS Provider – AWS, Azure and 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 & Response | Capacity Management | Admin Access Management**

Shared Security Model

Key Activities in Shared Security Governance

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

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

- Customer Data
- Application Authentication and Authorization
- Connectivity to Cloud Services
- Integration. Extensions and Add-on
- Audit and Certification
- Service Resiliency
- Vulnerability Assessment & Penetration Testing
- Operational Security
- Security Architecture Design and Build
- Logging and Monitoring
- Hyperscale (Azure) - IaaS

Managed by Customer

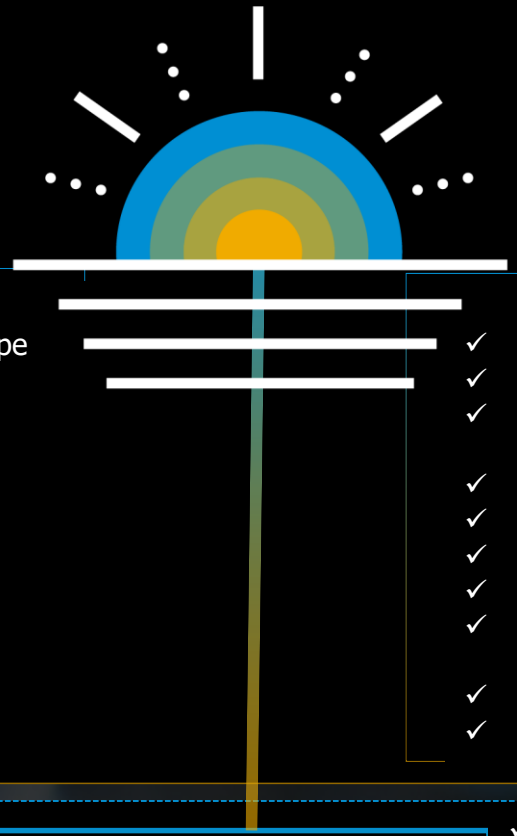
Managed by SAP

Azure

aws

Shared Security Responsibility Model

RISE WITH SAP
S/4HANA Cloud, Private Edition
Shared Security



SAP

- ✓ Resilient platform architecture (HA and DR)
- ✓ Hyperscaler Subscription and 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
- ✓ Security Audits and Compliance of the Cloud Services

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
- ✓ Integration and Extensions, Custom Applications Development
- ✓ Configuration of the Customer Business Processes
- ✓ Application Change Management

IaaS Provider
(Managed under SAP SE)

aws Azure

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

Shared Security Governance

https://assets.cdn.sap.com/agreements/product-policy/hec/roles-responsibilities/sap-hana-enterprise-cloud-roles-and-responsibilities-for-project-also-known-as-cloud-start-v402-english-v2-2021.pdf

Application Change Management

Functional Application Support

Technical Availability Management

HANA DB Management (HANA DB)

OS Maintenance (OS)

Backup Management

Infrastructure Management & Tools

Compute, Memory, Storage, Networking

Availability Zones

Regions

aws

Azure

SAP S/4HANA Cloud, Private Cloud Edition (PCE) - Hyperscaler

Azure or AWS or GCP as IaaS Provider

Hyperscaler Account Management

Central SAP Master Account

SAP SE Multi-Cloud

Account Administrator

Azure

Customer Landscape Account

SAP-hec-cust-001

Service Administrator

VNET/VPC Created within each Customer Subscriptions

SAP Master Root Account (SAP SE)

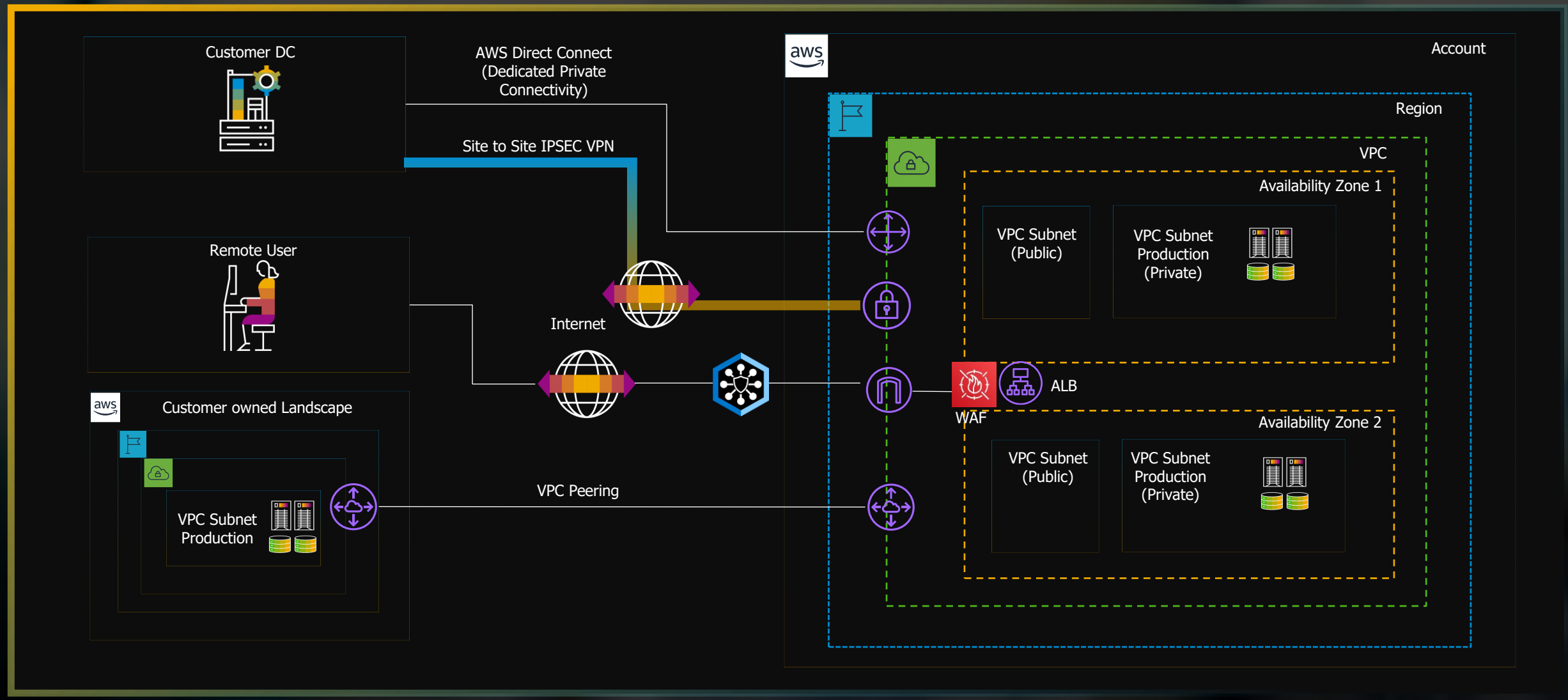
SAP ECS - Rise with SAP – SAP S/4HANA Cloud, PCE

Customer Subscriptions

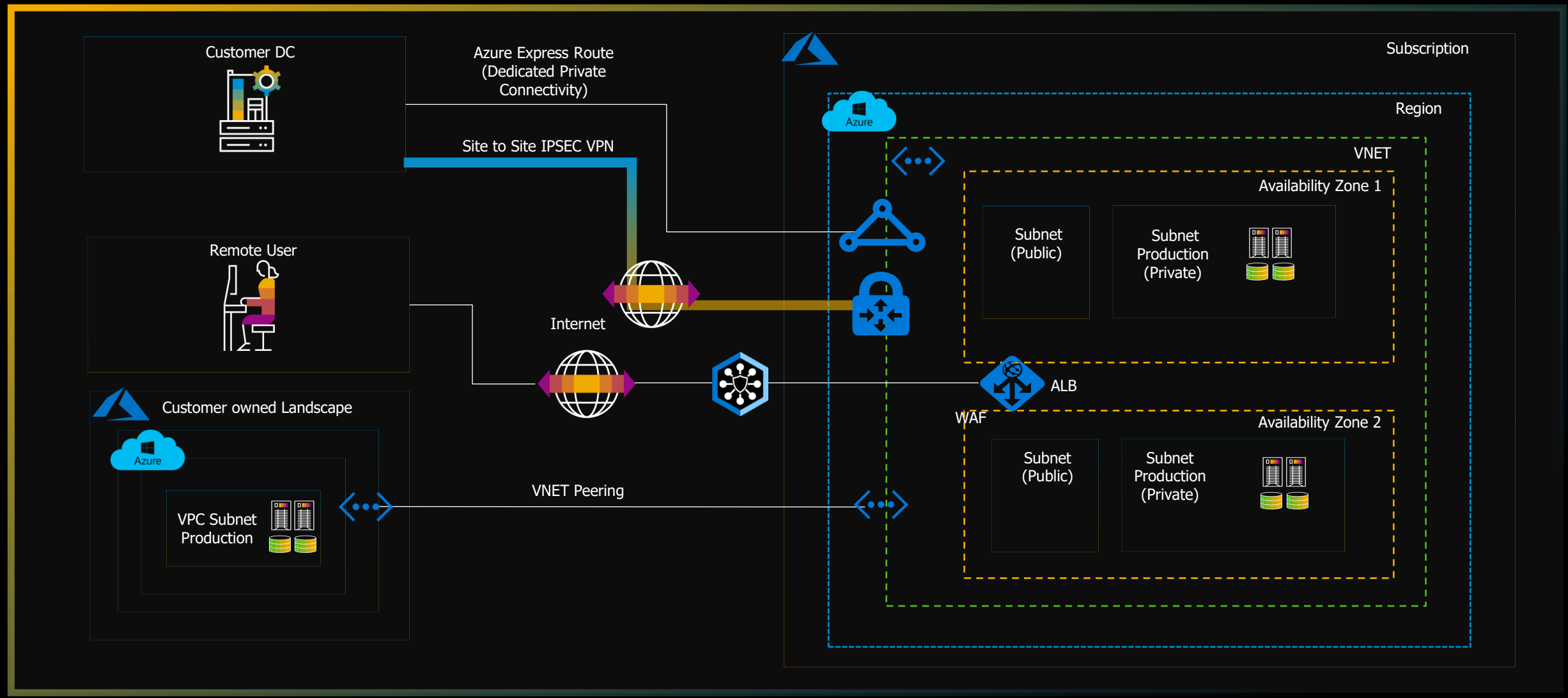
Security Policy Inheritance

3 Network setup for SAP S/4HANA Cloud, Private Edition

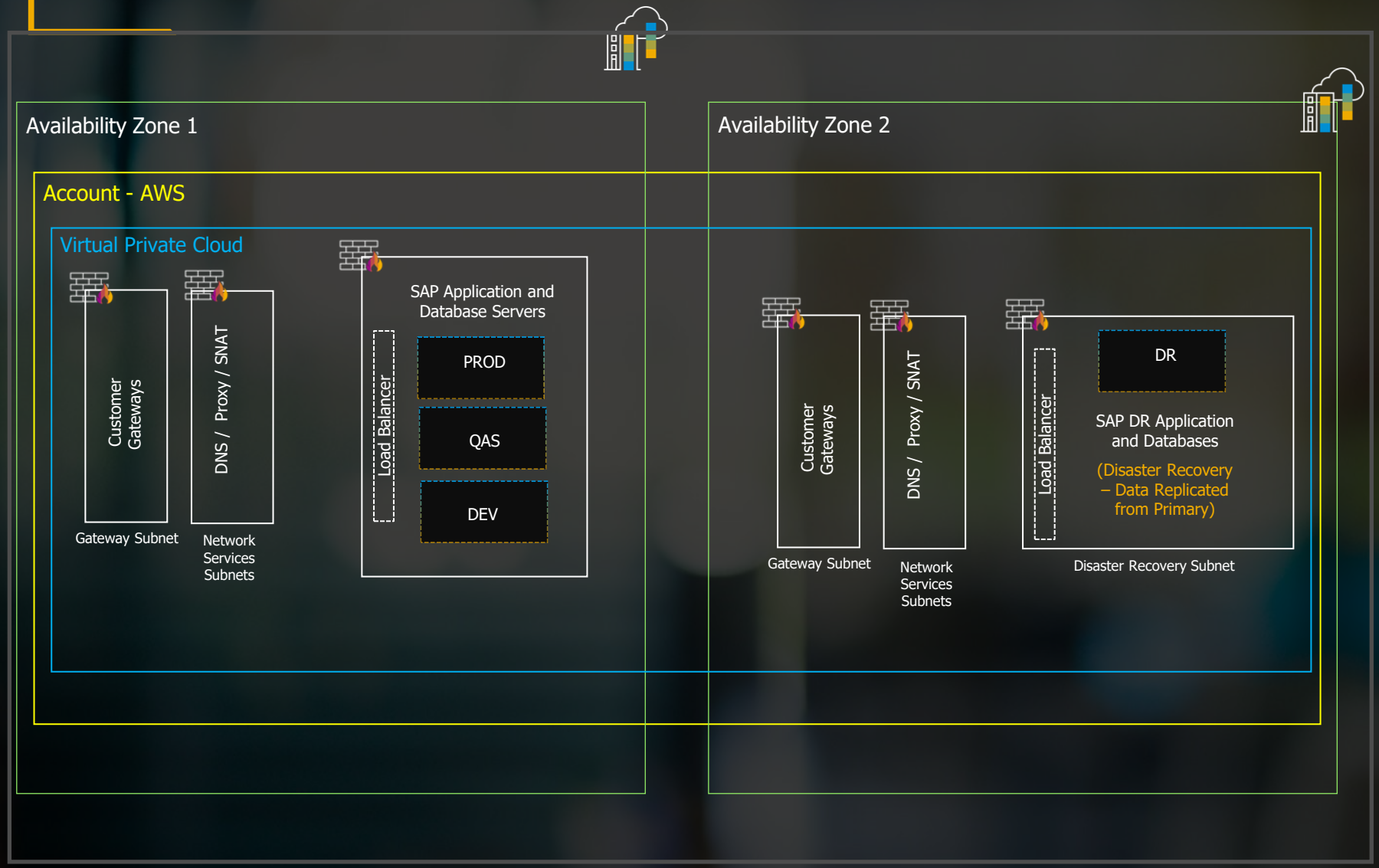
AWS Connectivity Options



Azure Network Connectivity Options – SAP S/4HANA Cloud - PCE



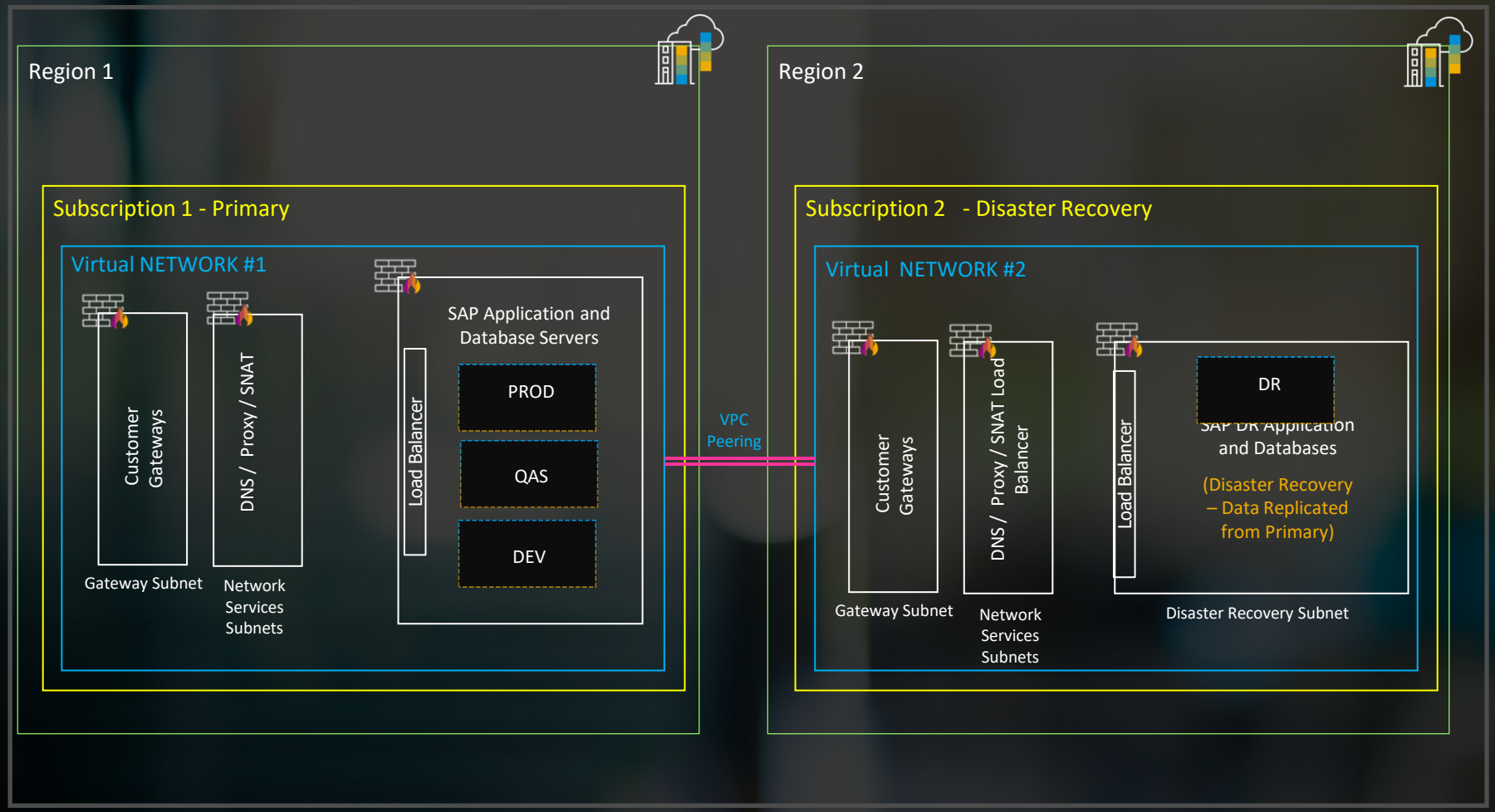
Network Segregation - AWS



1. There will be a dedicated AWS account for each customer. A separate SAP instances (virtual) exclusive for each customer
2. Virtual Private Cloud are created within each AWS account to address specific system/data isolation requirements. Within each Virtual Network, there will be multiple subnets (using private CIDR block IP addresses) created to segregate the environments
3. Each subnet is configured with Security Group with specific set of rules to control the network traffic.
4. Security policies that are defined at the higher level hierarchy are pushed to each subscription/ project/ account. Data replication traffic from primary to DR site will always go via private connectivity (peering)
5. Customer access to VNET will only be via a private dedicated connectivity. No user network access will be allowed to the managed environment from Internet.
6. Backup services are integrated with native and 3rd party services.

Refers to IaaS provider security services Security Groups (AWS)

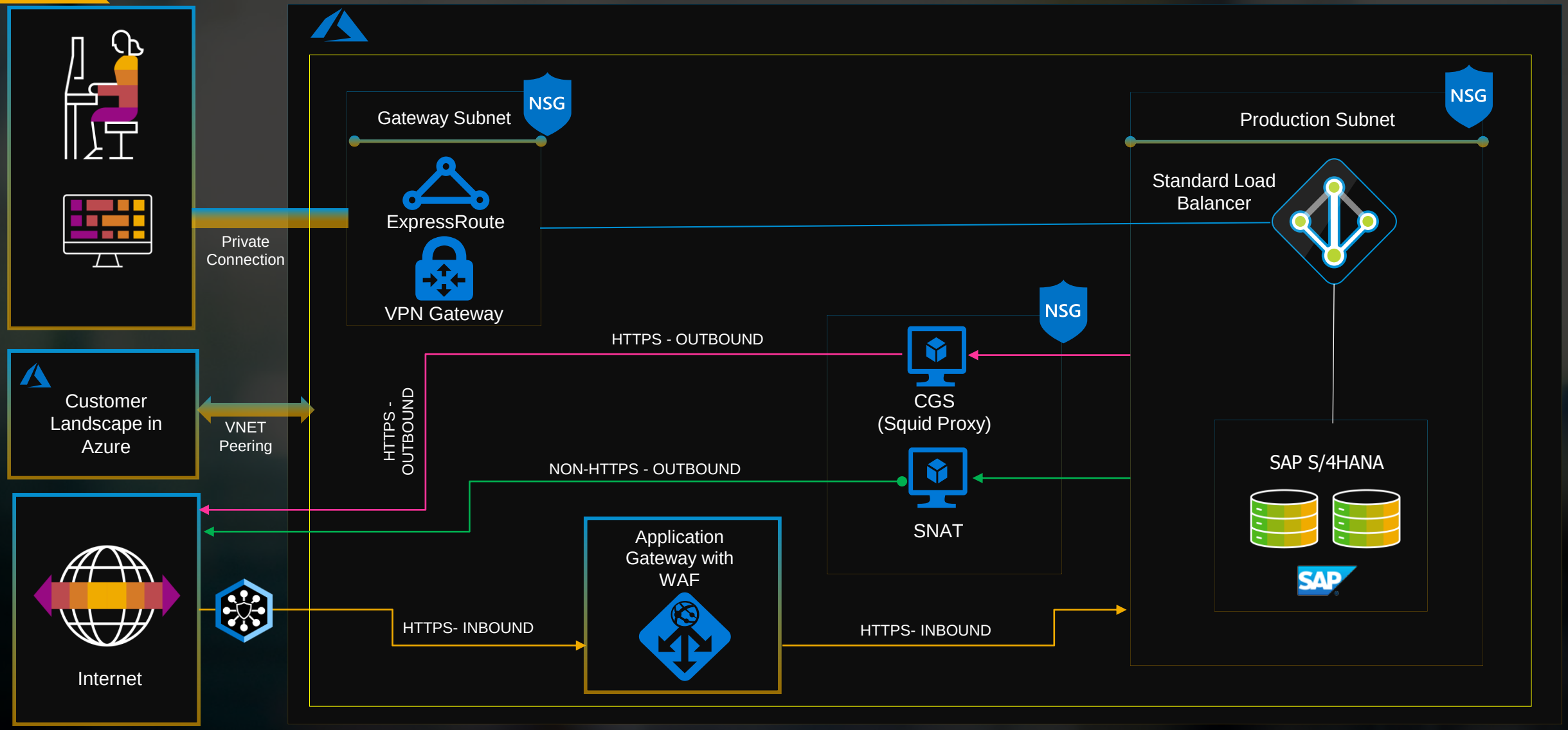
Network Segregation - Azure



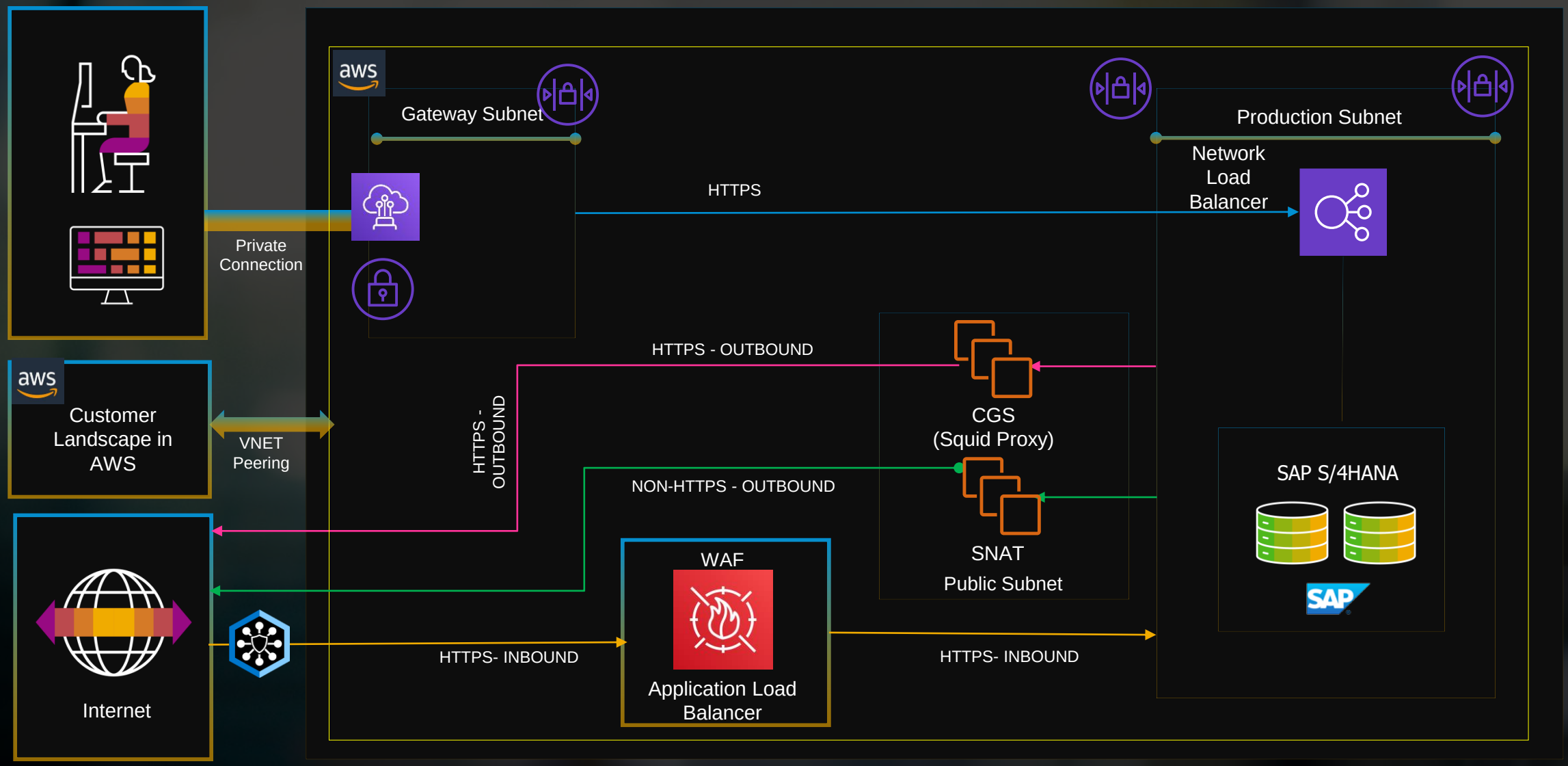
1. There will be a set of subscriptions in Azure created for Customer to deploy dedicated SAP instances (virtual)
2. Virtual Network (VNET) are created within each subscription/account to address specific system/data isolation requirements. Within each Virtual Network, there will be multiple subnets (using private CIDR block IP addresses) created to segregate the environments
3. Each subnet is configured with Network Security Group with specific set of rules to control the network traffic.
4. Security policies that are defined at the higher level hierarchy are pushed to each subscription/ project/ account. Data replication traffic from primary to DR site will always go via private connectivity (peering)
5. Customer access to VNET will only be via a private dedicated connectivity. No user network access will be allowed to the managed environment from Internet.

Refers to IaaS provider security services such as Network Security Groups (Azure), Security Groups (AWS) and GCP (Firewall) .

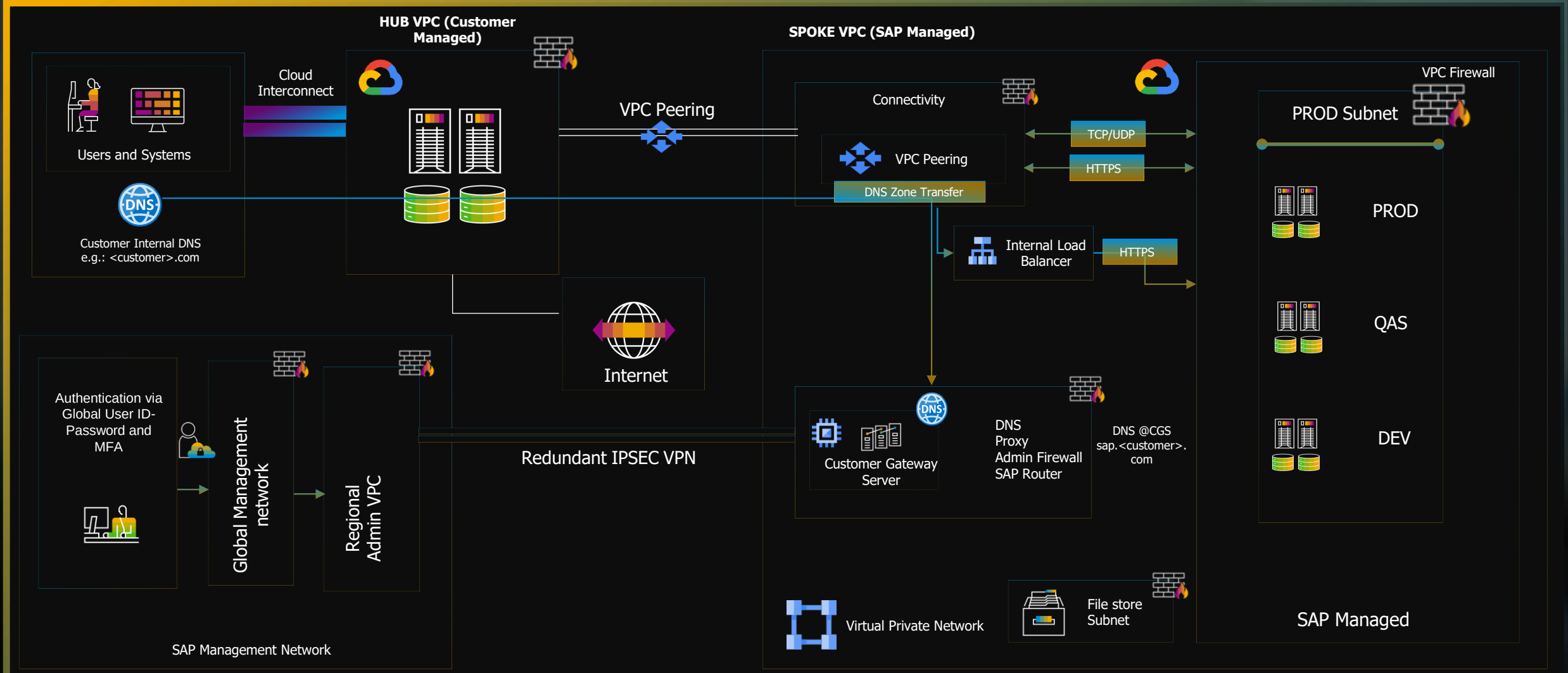
SAP S/4HANA Cloud, Private Edition – Azure Network Setup



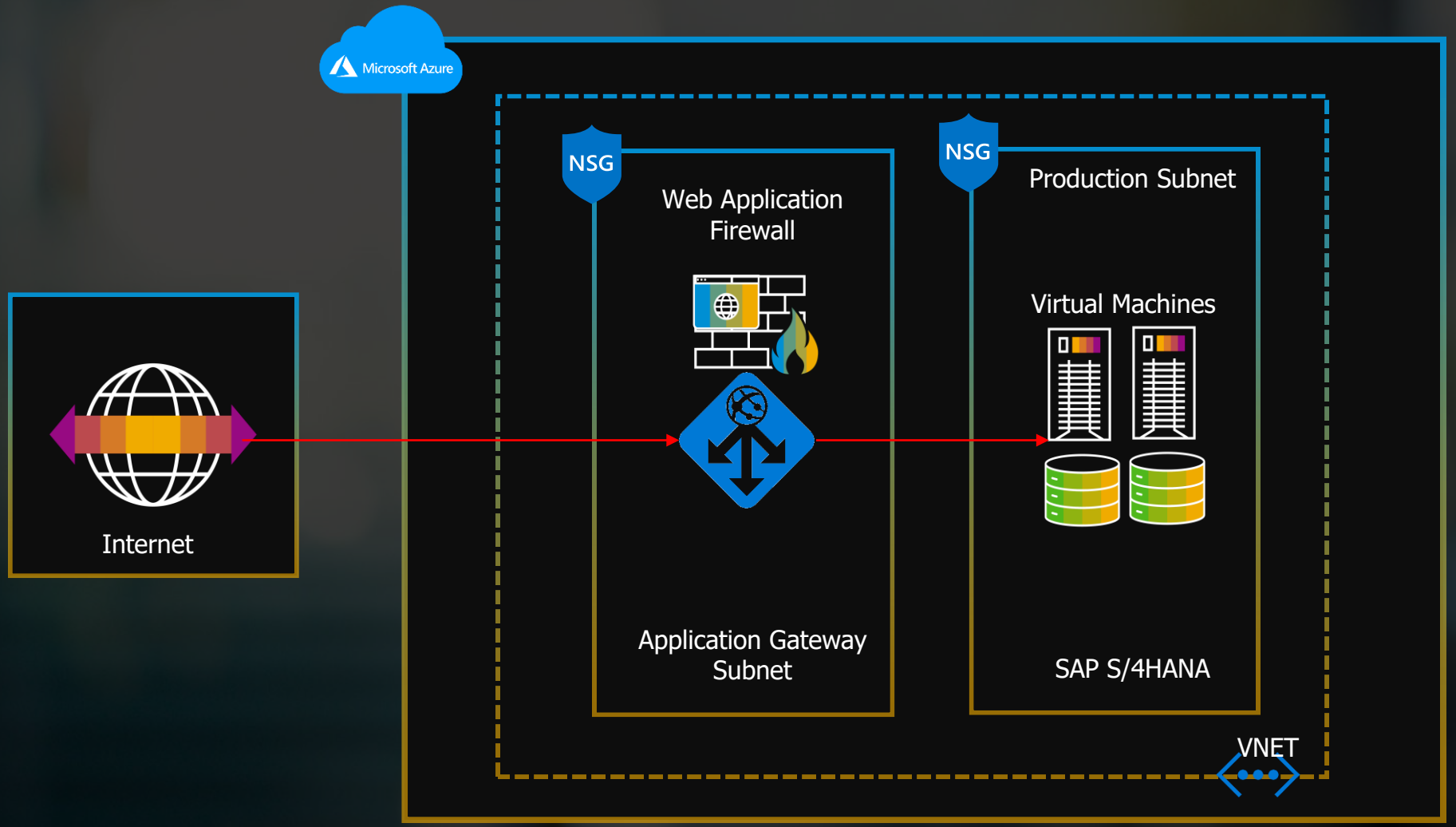
SAP S/4HANA Cloud, Private Edition – AWS Network Setup



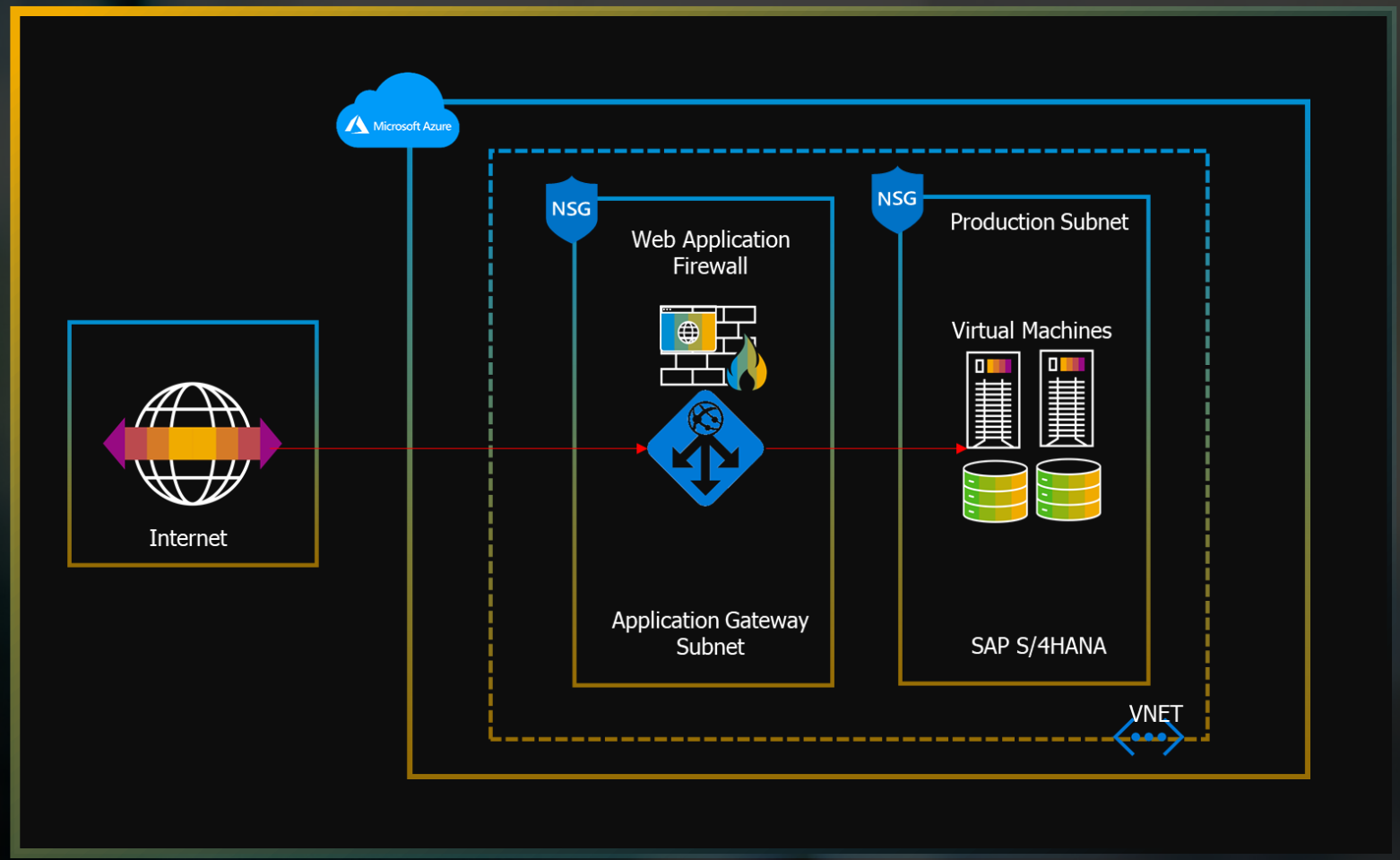
SAP S/4HANA Cloud, Private Edition – GCP Network Setup



Securing Inbound Traffic from Internet



Securing Inbound Traffic from Internet

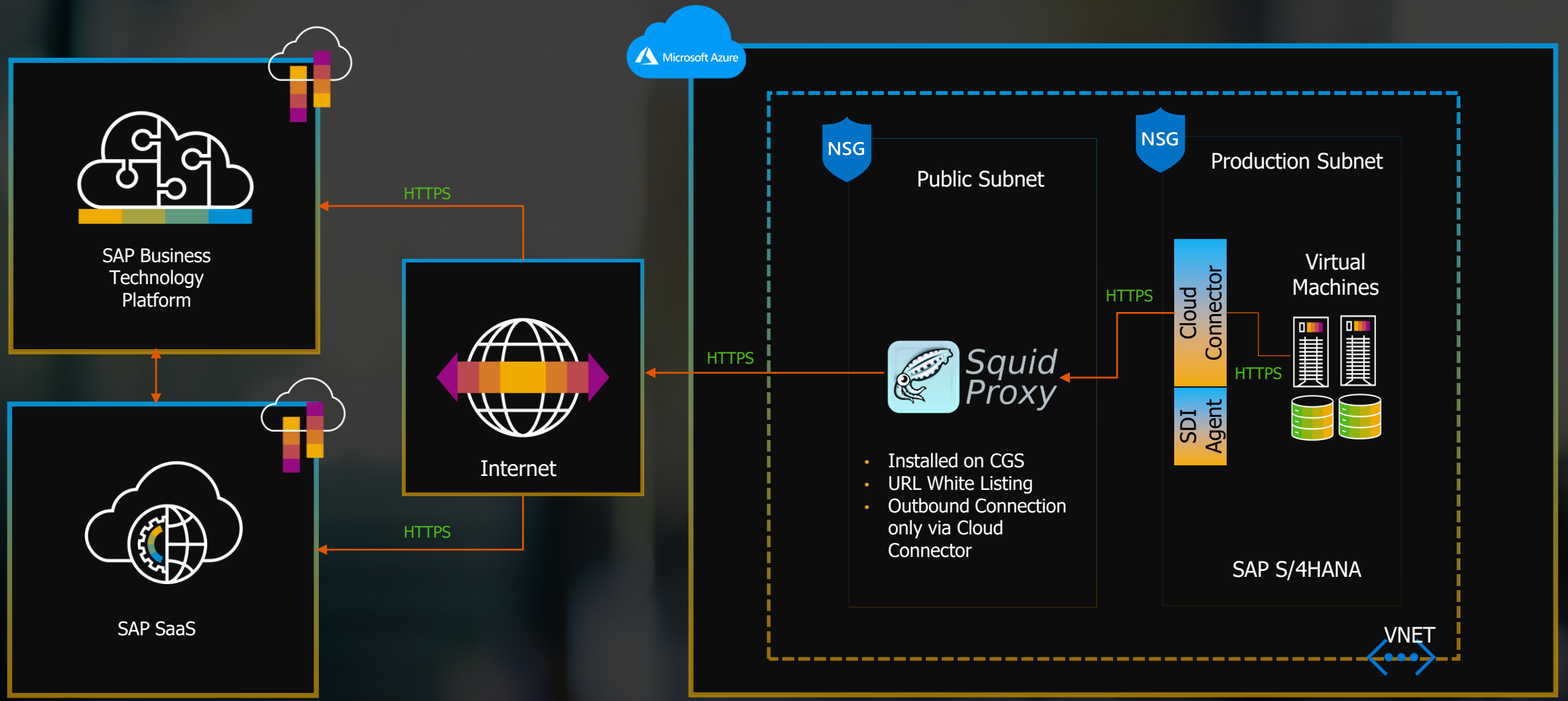


Azure Application Gateway (AAG) is a web traffic load balancer that is used to manage https traffic to the respective SAP solutions. It contains features of a Layer 7 load balancer and a Web Application Firewall (WAF).

Web application firewall (WAF) is a feature of Application Gateway that provides centralized protection of the web applications from common exploits and vulnerabilities based on OWASP 3.0. Preconfigured Rule Sets to protect against:

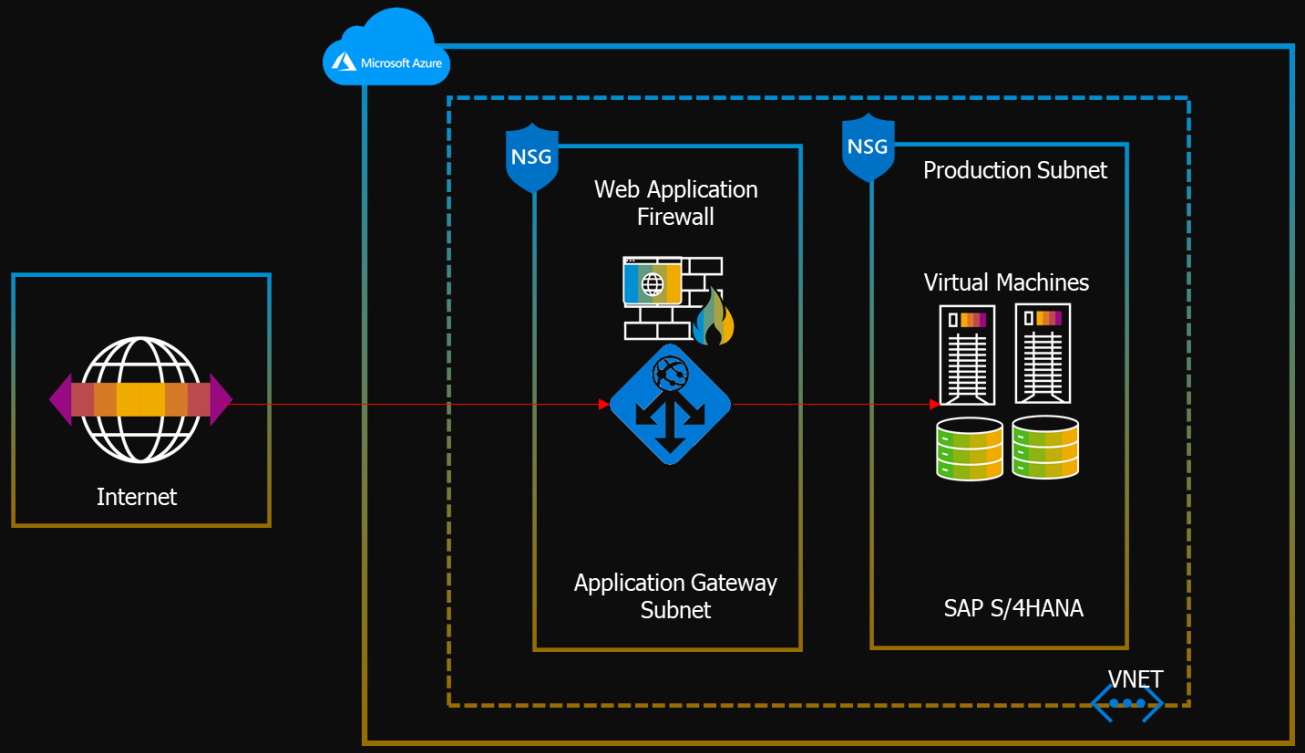
SQL injection protection
Cross site scripting protection
Common Web Attacks Protection such as command injection, HTTP request smuggling, HTTP response splitting, and remote file inclusion attack
Protection against HTTP protocol violations
Protection against HTTP protocol anomalies such as missing host user-agent and accept headers
Prevention against bots, crawlers, and scanners
Detection of common application misconfigurations (i.e. Apache, IIS, etc.)

Securing Outbound Traffic to Internet



External (Internet) Inbound – Application Gateway and WAF

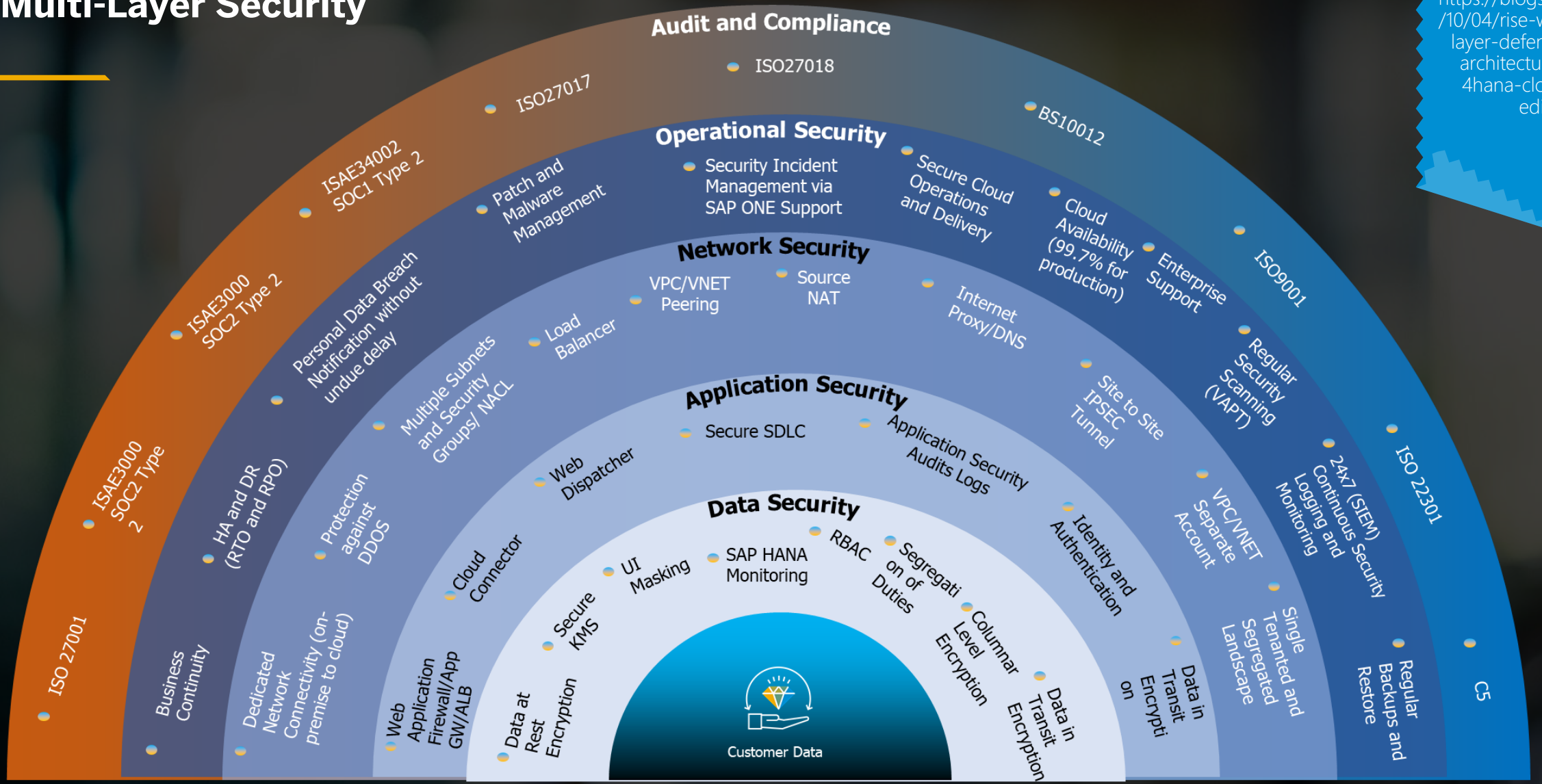
Application Gateway and WAF



- Application Gateway/WAF is deployed on a dedicated VNET Subnet
- For inbound connection (internet facing) only https is allowed (Only TLS version 1.2 or above is allowed). AAG supports SSL offload and end-to-end SSL, which re-encrypts the traffic to the backend.
- WAF is configured for internet inbound connections (WAF does not provide additional DDoS prevention)
- WAF & DDOS features are provided natively by Azure (standard features)
- Application Gateway can also be deployed for Internal inbound use cases without WAF
- Web application firewall (WAF) is a feature of Application Gateway that provides centralized protection of the web applications from common exploits and vulnerabilities based on OWASP_3.0. Examples of WAF Rule Set:
  - SQL injection protection and Cross site scripting protection
  - Common Web Attacks Protection such as command injection, HTTP request smuggling, HTTP response splitting, and remote file inclusion attack
  - Protection against HTTP protocol violations
  - Protection against HTTP protocol anomalies such as missing host user-agent and accept headers
  - Prevention against bots, crawlers, and scanners
  - Detection of common application misconfigurations (i.e. Apache, IIS, etc.)

Zero Trust Architecture is supported with SAP S/4HANA Cloud, Private Edition

Multi-Layer Security



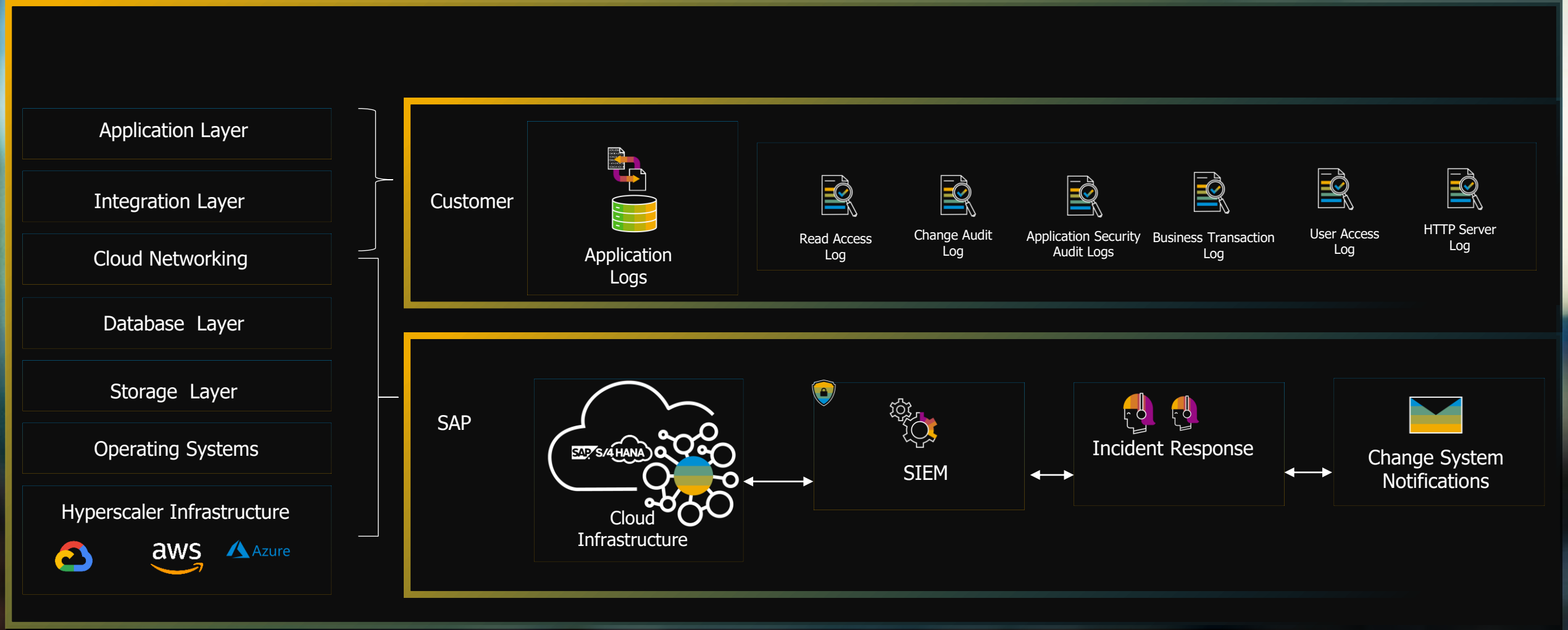
Source: https://blogs.sap.com/2021/10/04/rise-with-sap-multi-layer-defense-in-depth-architecture-of-sap-s-4hana-cloud-private-edition/

Zero Trust Architecture Principles

Logging and Monitoring

Detection, Protection and Response

Application and Infrastructure Logs



RISE with SAP – Security Activities

Security Value Proposition

RISE with SAP
Customer Managed

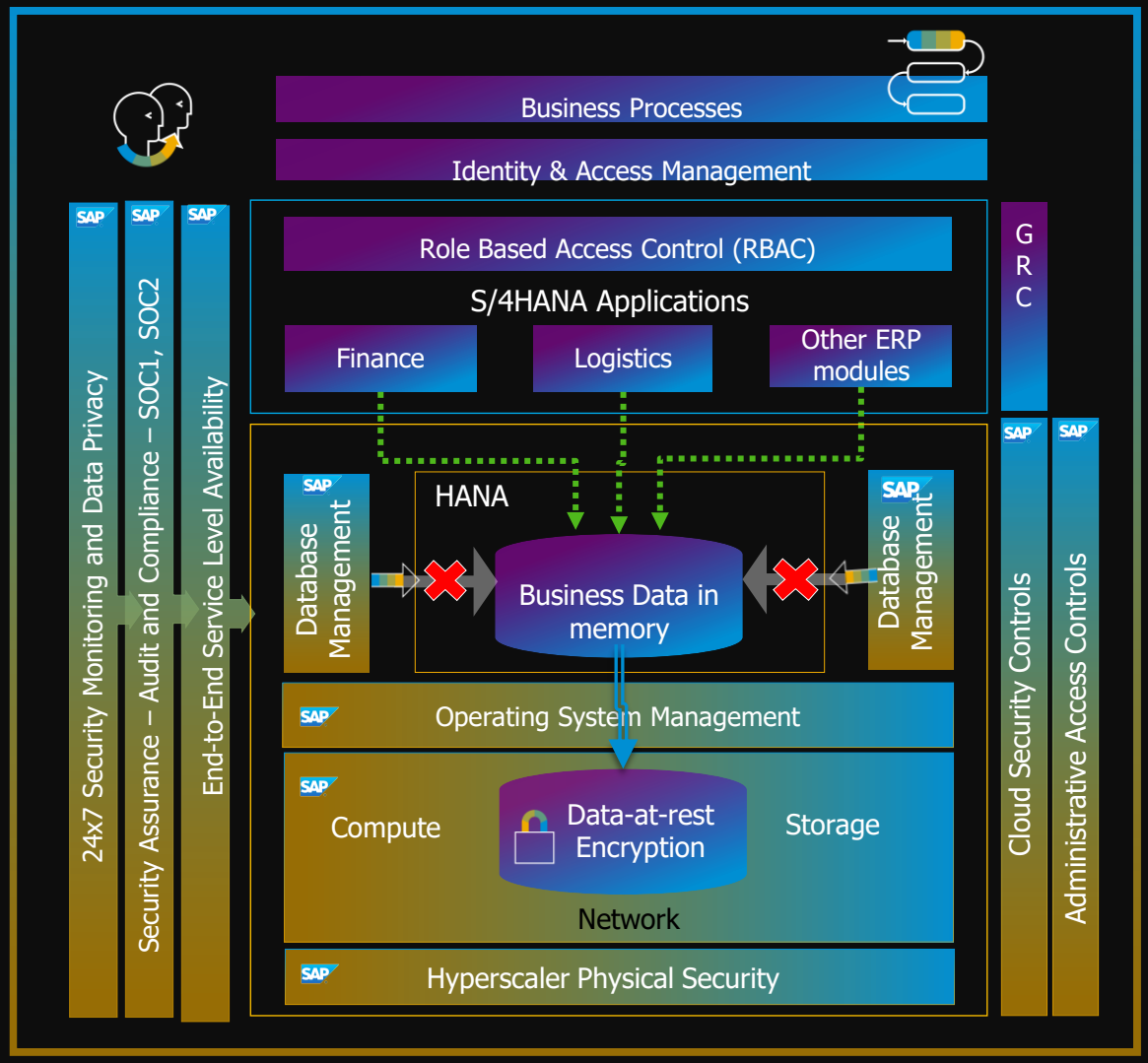
For Security Assurance, Bi-Annual SOC1/SOC2 audits available to customers under NDA.

Forensic Security Experts to perform Root Cause Analysis

Extensive automated scanning of VMs based on ISO, NIST and SANS controls

Personal Data Breach Notification Process with support of Cyber Legal, SAP DPO, Forensic Expert

Secure Admin Access to the environment – logged and monitored



State of Art Tools – Splunk, Security Automation, Splunk Phantom, End-Point Detection and Response, DLP, Enterprise Threat Detections - Cyber SOC operating 24x7

Certified SAP Security Analyst – People, Technology and Process based on SAP Global Security Framework

Global Partnership with External Cyber Threat Intelligent Sources on the emerging Threats. Internal SEM Research developing Security Use Cases

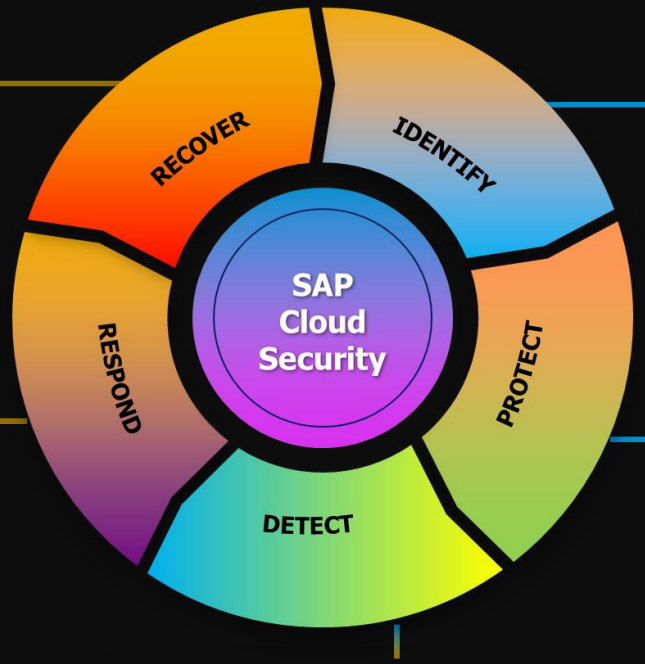
Weekly Scanning of External IPs, Quarterly VA scans and Bi-Annual Penetration Testing and remediation performed in timely manner

SAP Patches, Emergency Patch Updates and application patches in consultation with customers

SAP Secure Cloud Operations

RECOVER

- Remediation
- Disaster Recovery Planning/Testing
- Lesson Learned
- Communications



IDENTIFY

- Asset Management
- Risk Management
- Security Governance
- Configuration Management
- Supply Chain Risk Management (Sub processor/Subcontractor)

RESPOND

- Response Planning
- Communications
- Root Cause Forensic Analysis
- Security Breach Notifications

DETECT

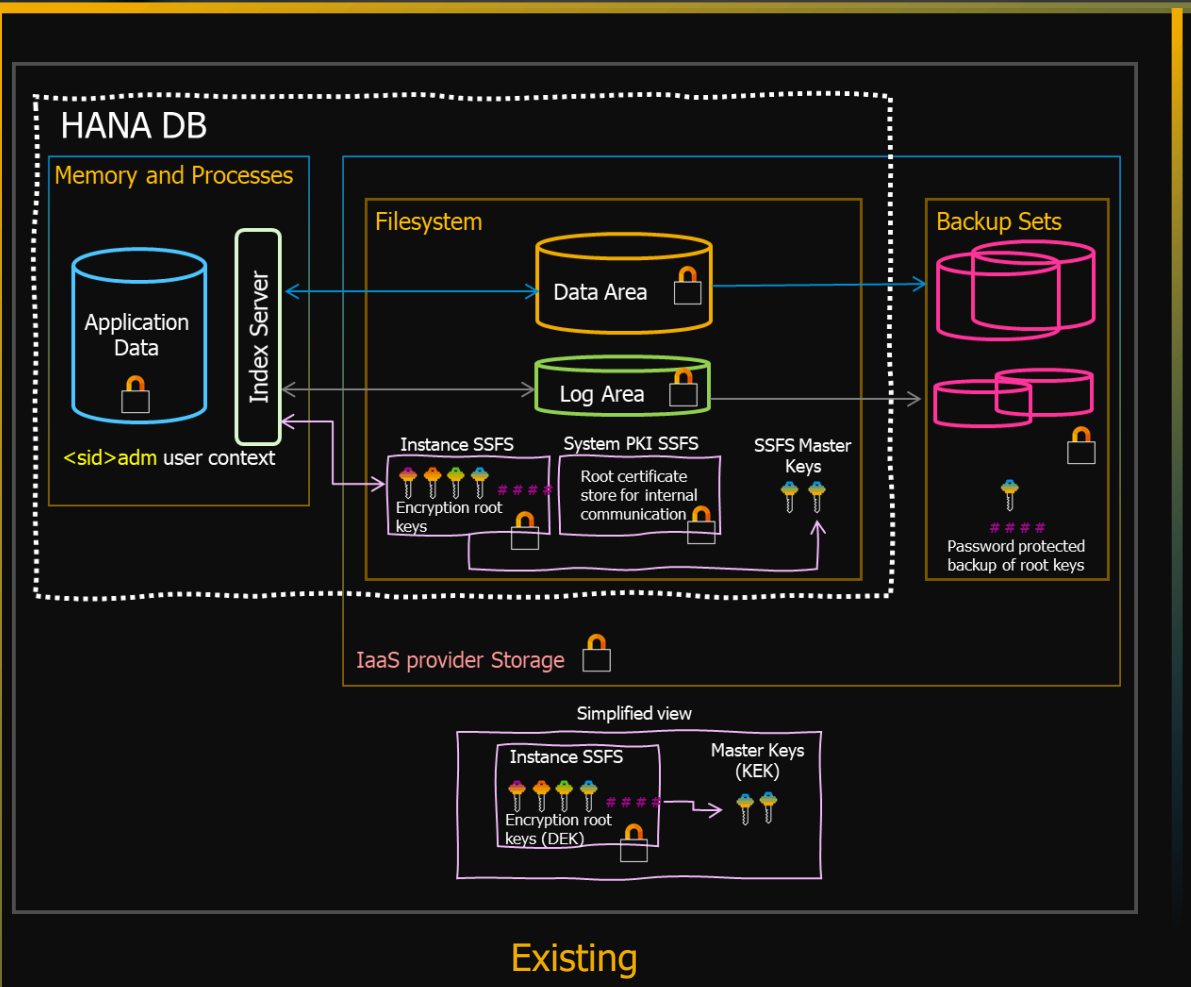
- Continuous Monitoring and Logging
- Event Correlations
- Security Incident Management
- VAPT
- EDR
- SOAR

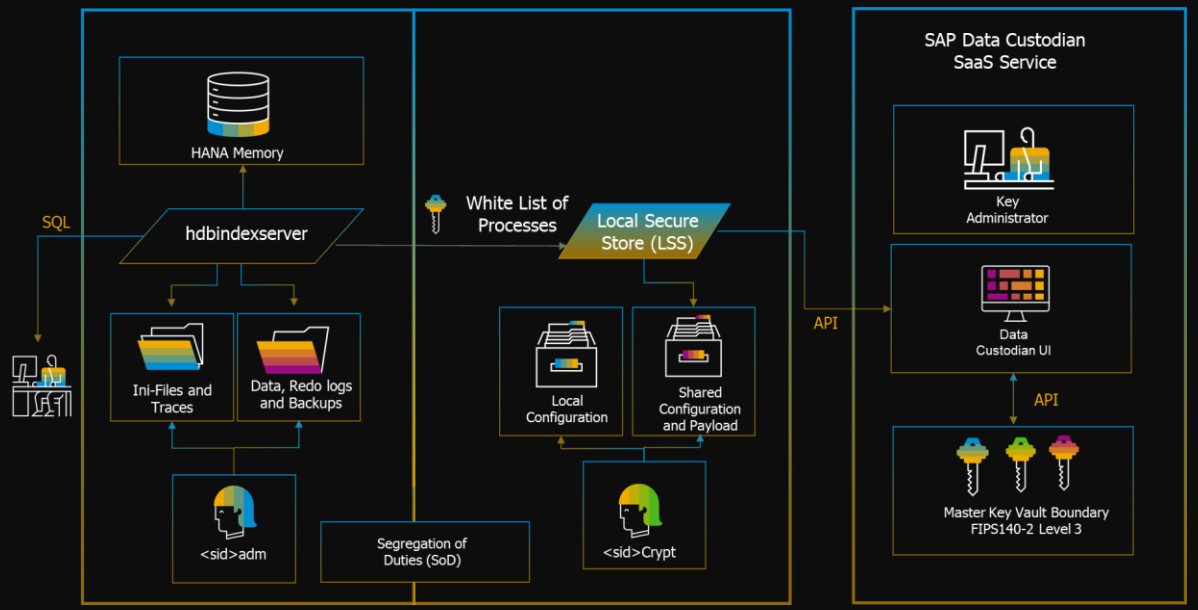
PROTECT

- Network Security – Segmentation, WAF, NSG
- Data Security
- Secure Cloud Admin Access
- RBAC – CAM
- Security Patch Management
- Security Controls at various layers

7 Key Management

Customer Controlled Key Management Service





Future State: Data Custodian with Customer owned KMS

THE BEST RUN SAP

[redacted]

Jana Subramanian
APJ Principal Cyber Security Advisor
Industries and Customer Advisory
T +65 81238535
jana.subramanian@sap.com

[redacted]

SAP Asia Pte Ltd
30 Pasir Panjang Rd, Singapore 117440