



Amazon Web Services: Security Overview





Hello

Thank you.



360° *Overview*



amazon
web services™

Infrastructure services

Data centre abstraction



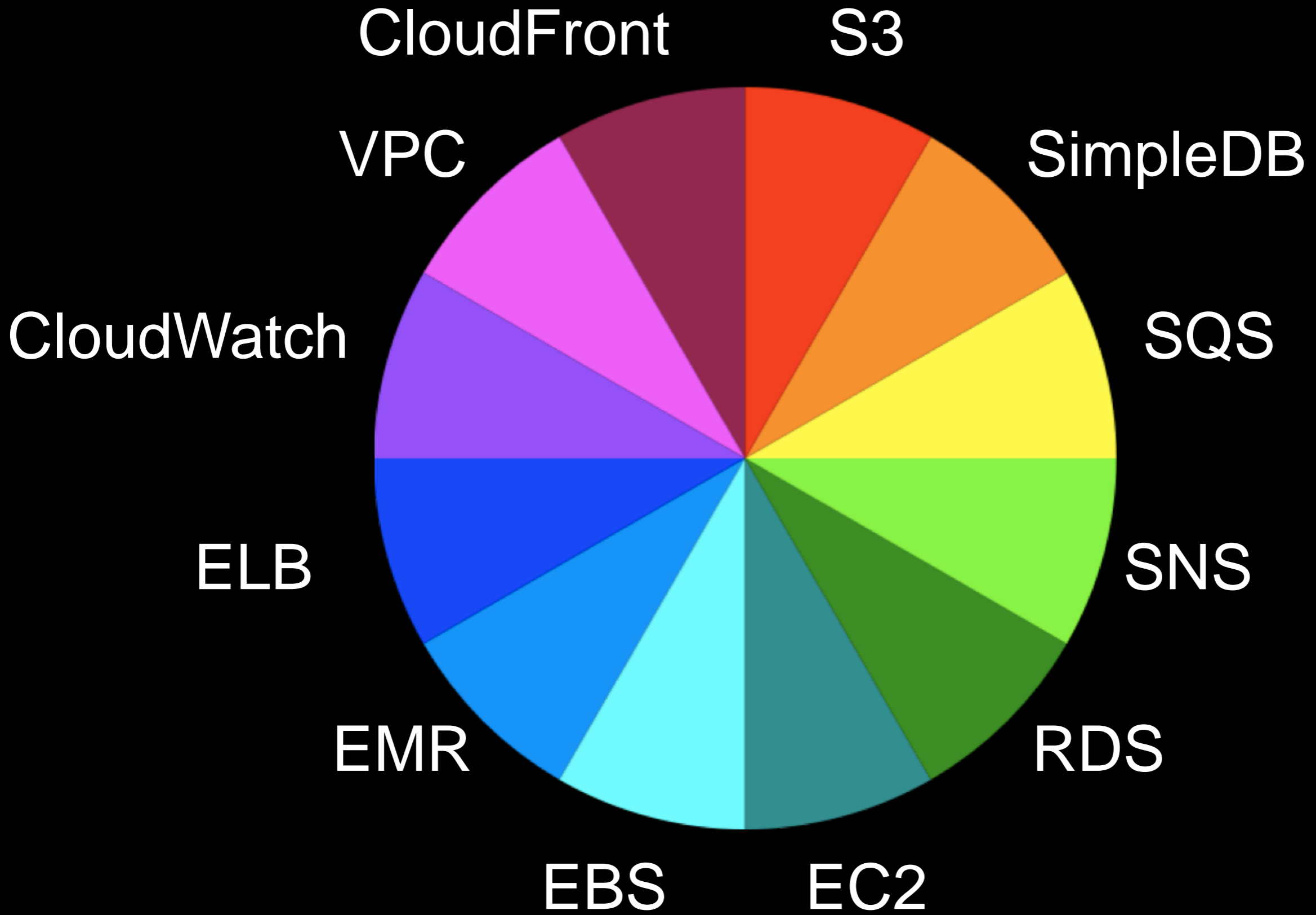
“Undifferentiated
heavy lifting”

On demand

Pay as you go

Pay for what
you use

Highly available



Security at every level



Security best practice

Security White Paper

aws.amazon.com/security

Updated twice a year - Feedback welcome

2

*Security in
the Cloud*

Shared
responsibility

Shared responsibility environment



APPLICATION and DATA

PHYSICAL INFRASTRUCTURE and
VIRTUALISATION

Certified:

Sarbanes-Oxley (SOX)

SAS70 Type II Audit

Pursuing:

FISMA (NIST) C&A

ISO 27001

SAS70 Type II Control Objectives

Security organisation	Employee lifecycle
Logical security	Secure data handling
Physical security	Environmental safeguards
Change management	Incident handling
Data integrity	Availability and redundancy

Deployed:

HIPAA (health care)

DSS (credit card)

Many years of experience in building
large-scale, secure facilities.

Non-descript buildings

Robust perimeter controls

Strictly controlled physical access

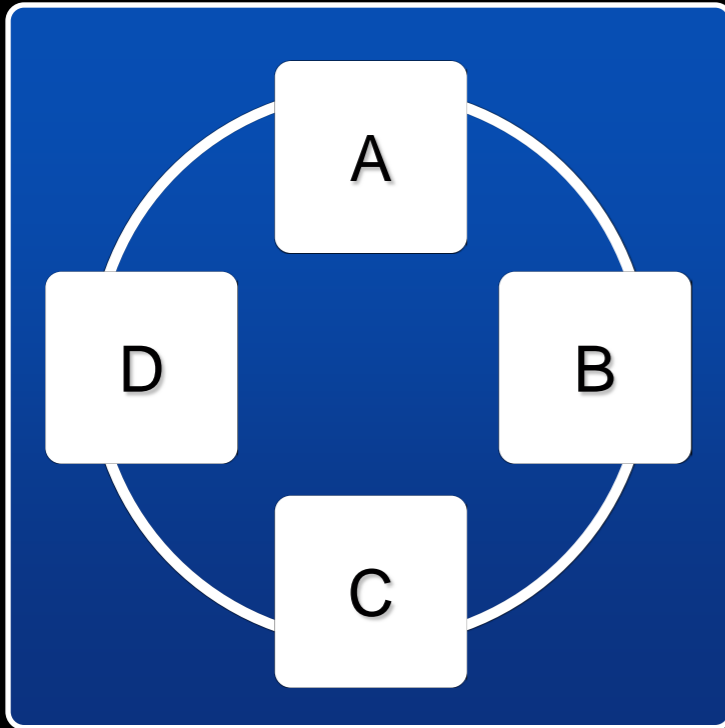
2 or more levels of two-factor authentication

Controlled, need-based access

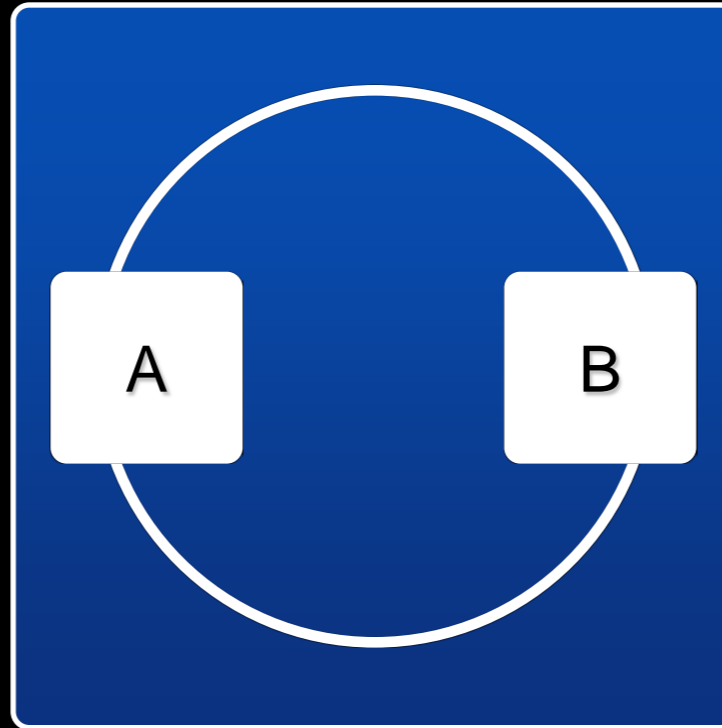
All access is logged and reviewed

FAULT SEPARATION

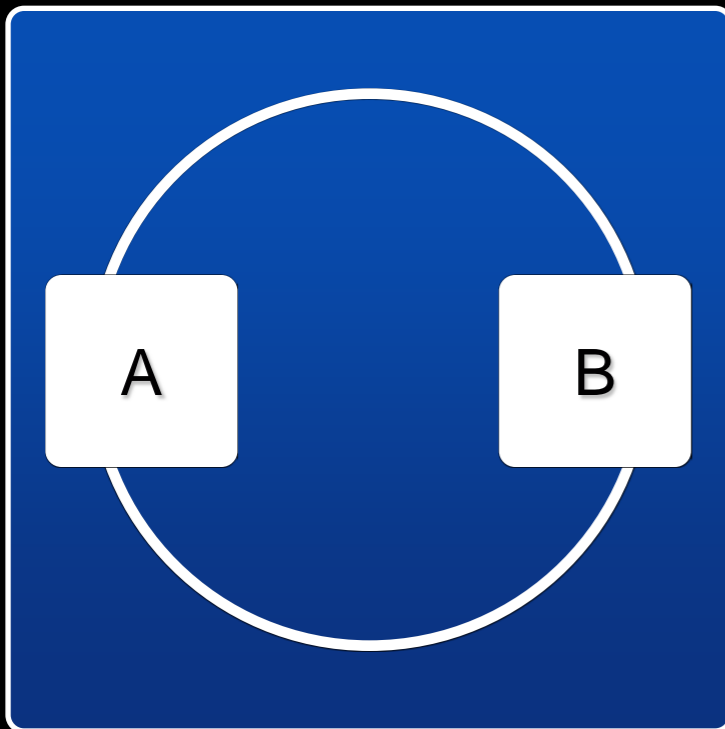
US East



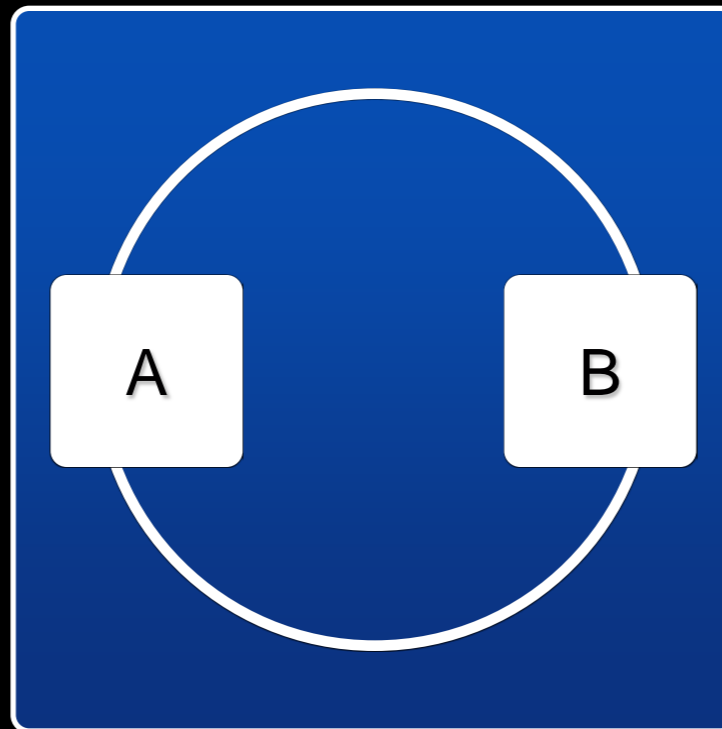
US West



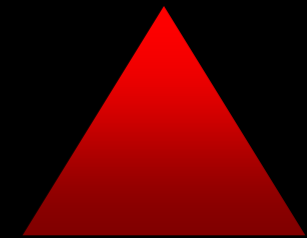
EU West



APAC



CloudWatch



Autoscaling
Monitoring
Load balancing

Redundant storage

Multiple physical locations

EBS redundancy remains in single
Availability Zone

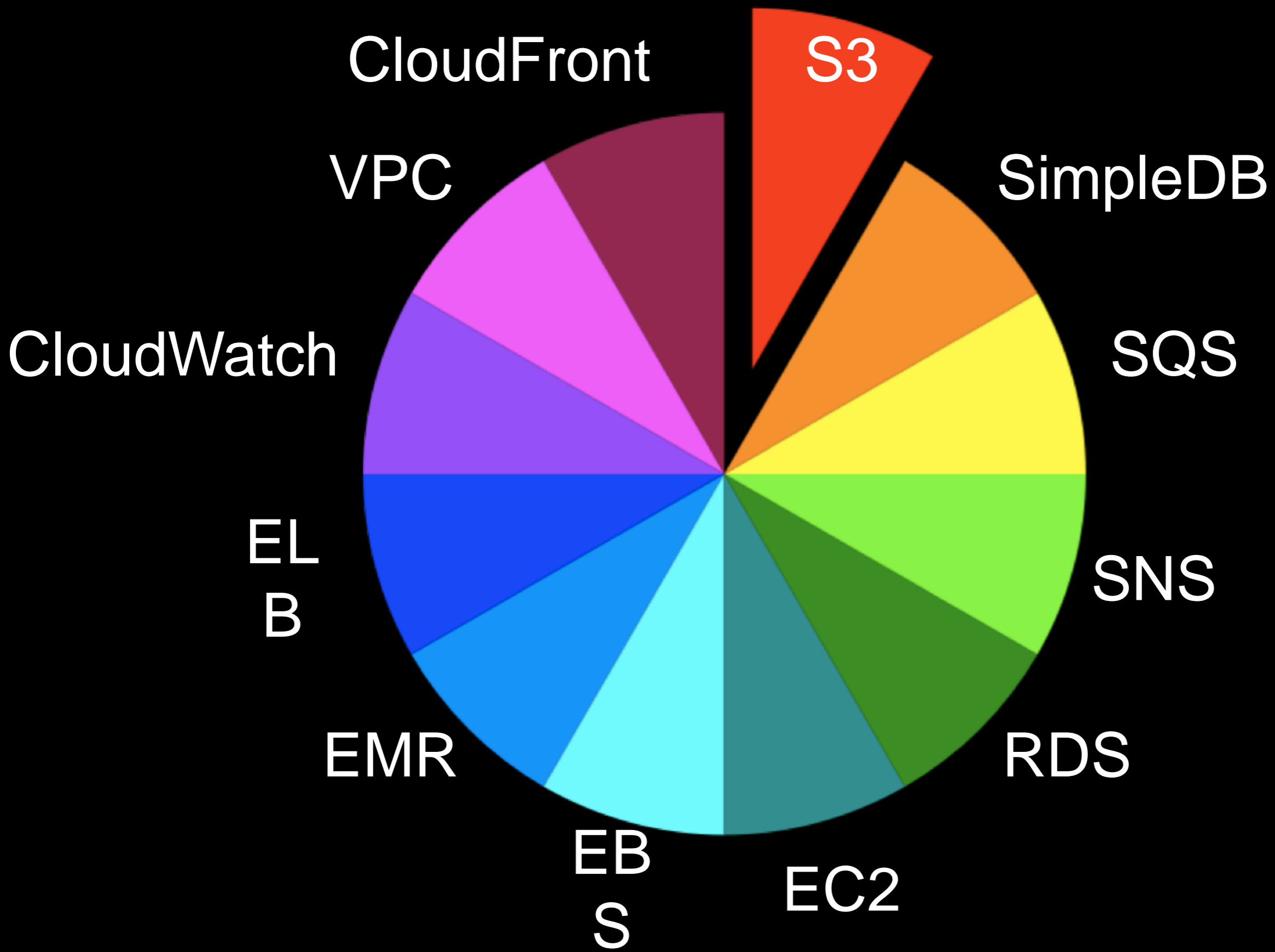
S3 and SimpleDB objects replicated
across multiple Availability Zones

EC2 local data must be copied to EBS
or S3 for redundancy



**Multifactor authentication
to protect credentials**

Recommended. Opt in.



Access controls for buckets and objects

Read, write, full

Owner has full control

Owner should encrypt when stored

Time limited URLs

Versioning (with MFA delete)

Detailed access logging

Data management

Data in transit: SSL end points

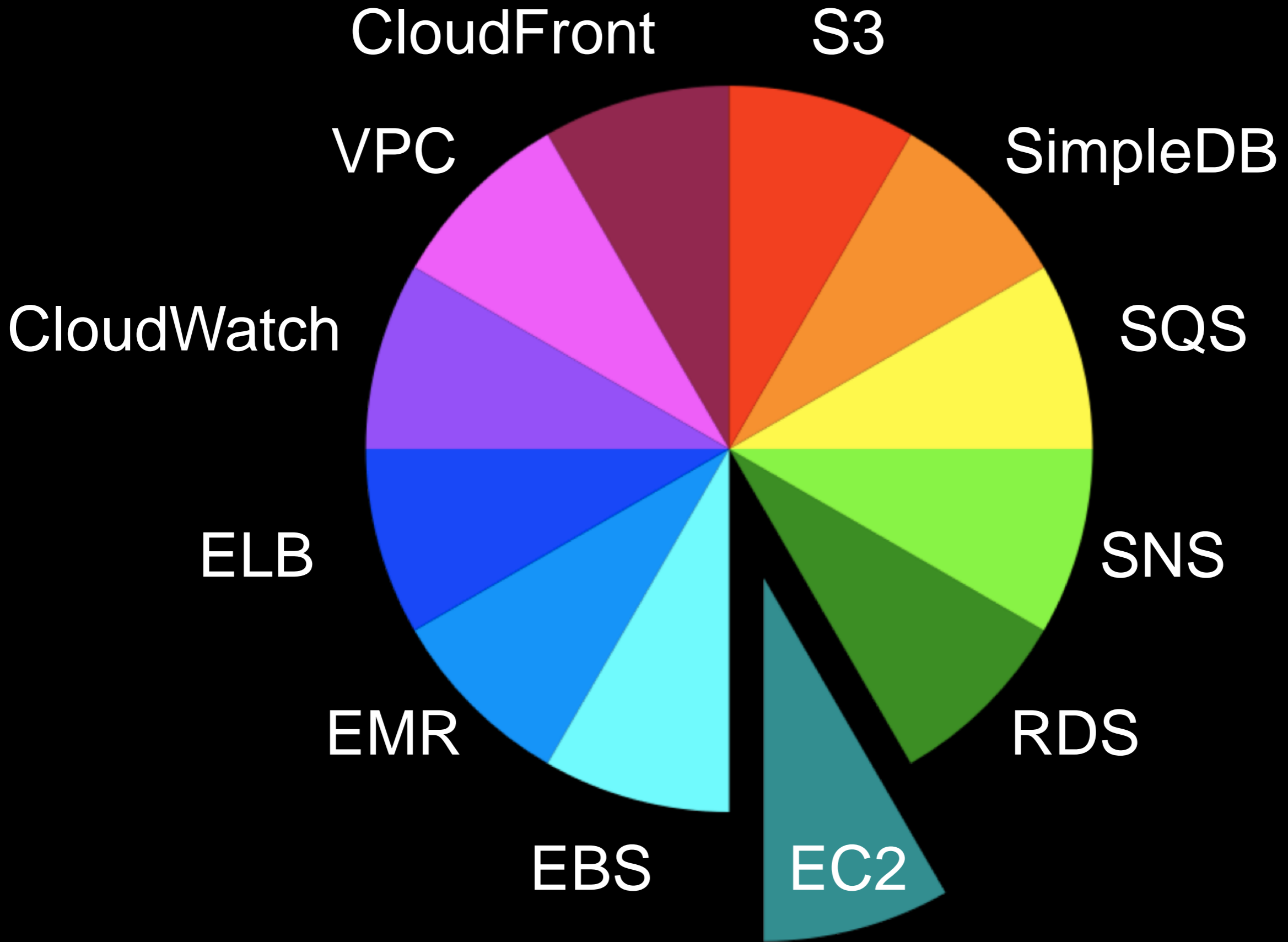
Data at rest: physical security & encryption

Redundant devices, redundant locations

Storage Drive Decommissioning

Military grade data destruction

DoD 5220.22-M/NIST 800-88



Security at every level

APPLICATION and DATA

GUEST OS

HYPERVERSOR

HOST OS and VIRTUAL INTERFACES

FIREWALL AND SECURITY GROUPS

PHYSICAL INFRASTRUCTURE

Guest OS - Customer controlled

Certificate based root login

Customer generated keypairs

No access for AWS admins

Host OS - AWS controlled

SSH keyed logins via Bastion host

All access logged and reviewed

Security groups

Customer controlled

Fine grained access control

Stateful firewall

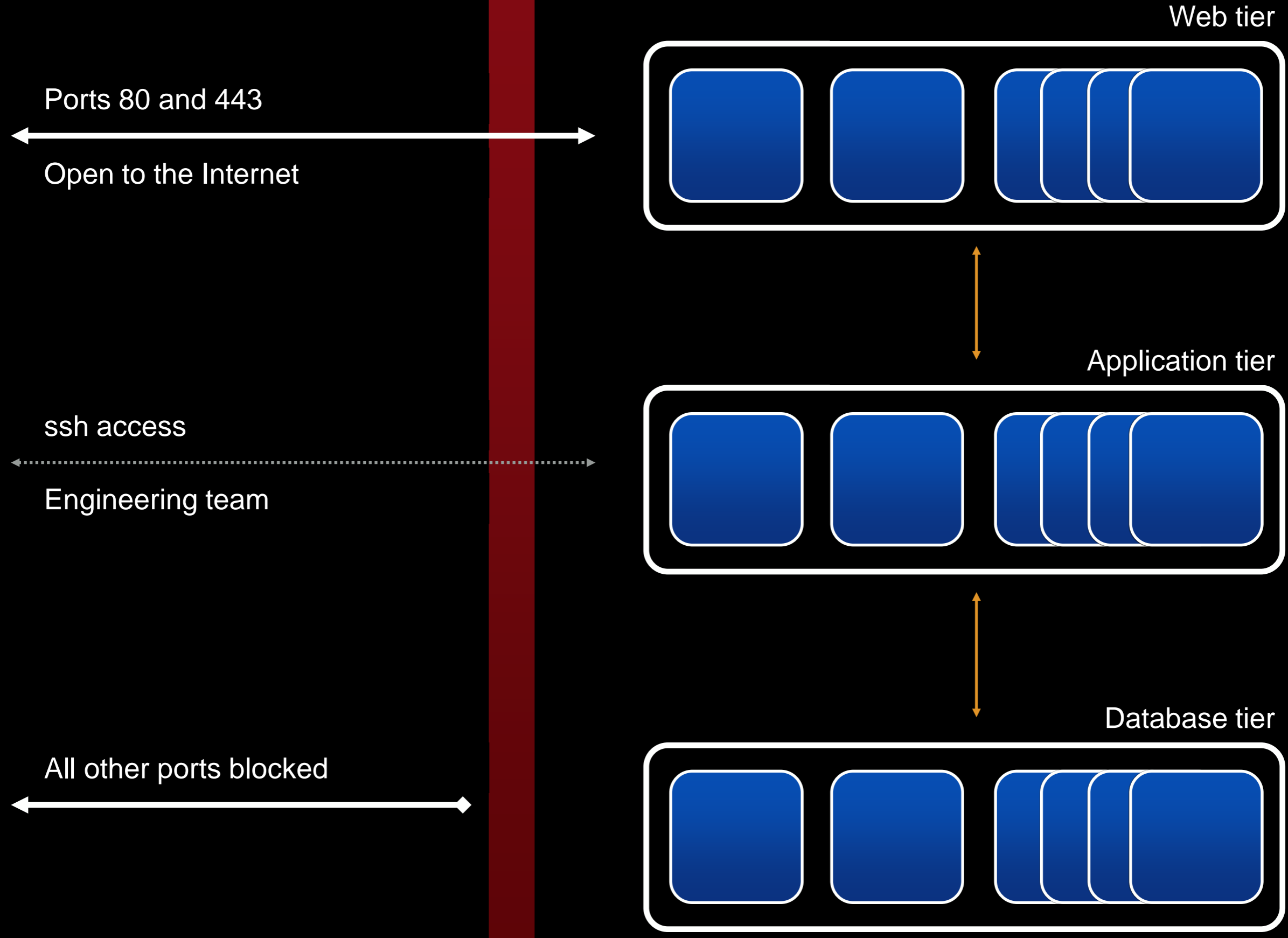
Mandatory inbound firewall

Default deny

Signed API calls

Requires X.509 certificate or secret key

EC2 SECURITY



Web tier

Ports 80 and 443

Open to the Internet

ssh access

Engineering team

All other ports blocked

Application tier

Database tier

Distributed Denial of Service

Mitigation techniques in effect
Multi-homed connections

Man in the Middle

All endpoints protected by SSL
Fresh EC2 host keys generated at boot

IP spoofing

Prohibited at Host OS level

Unauthorised port scanning

Terms of Service violation

Actively monitored

Detected, stopped and blocked

Ineffective since inbound ports blocked by default

Packet sniffing

Promiscuous mode is ineffective

Protection at hypervisor level

Configuration management

Configuration changes are:
authorised, logged, tested approved and
documented

Most updates are done without affecting
customers

Communication via email and
Service Health Dashboard

3

*Identity and
access*

Create users within a single AWS account

Individuals, systems or applications

Manage by user group

Assign and manage credentials per account

Assign, rotate and revoke access keys

Limit access to specific AWS services

Restrict access to specific API calls

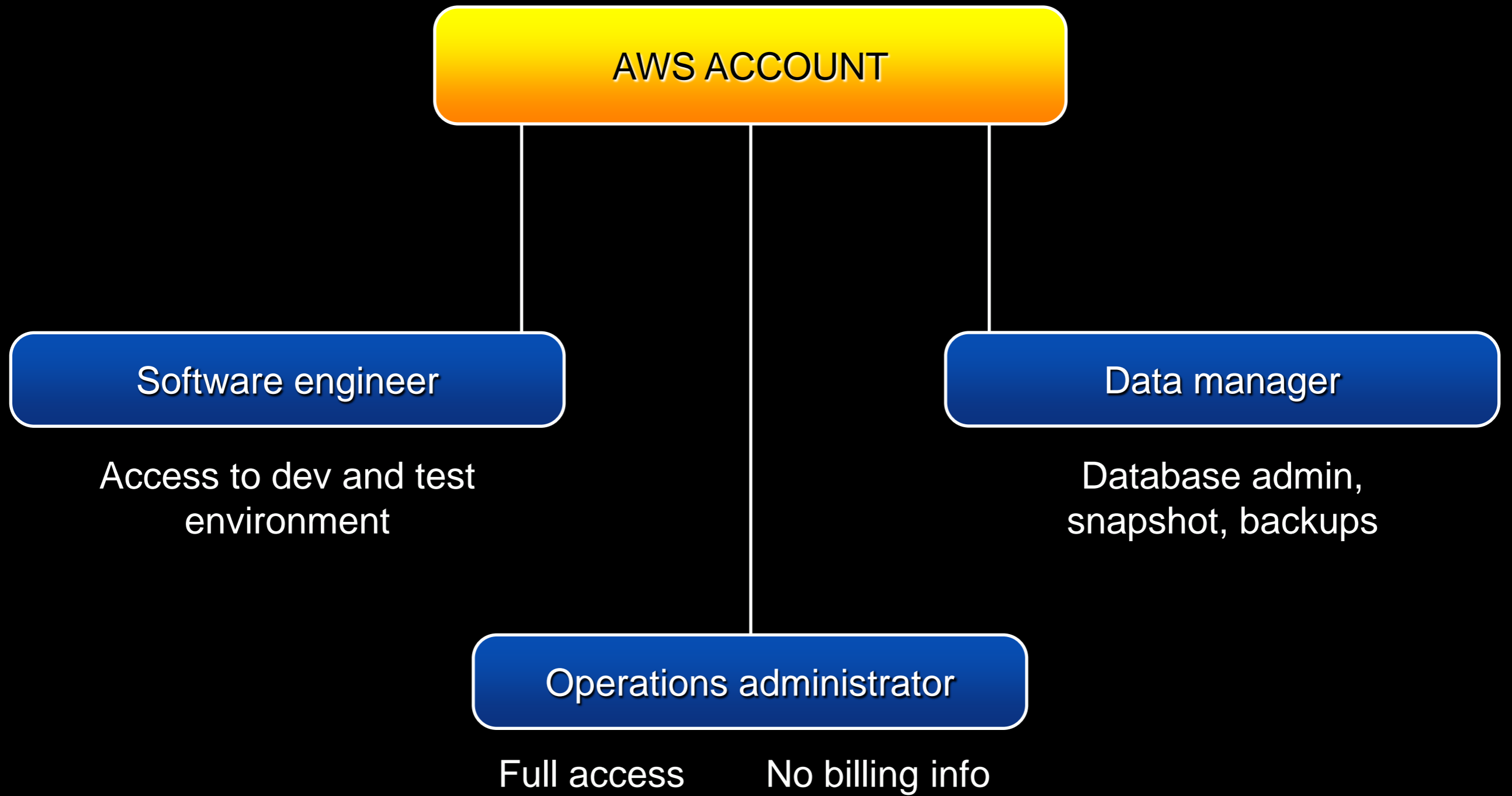
Complete restriction by default

Assign and manage credentials

Conditional access: time based, IP based,
SSL requirement

One single, consolidated bill

IDENTITY AND ACCESS



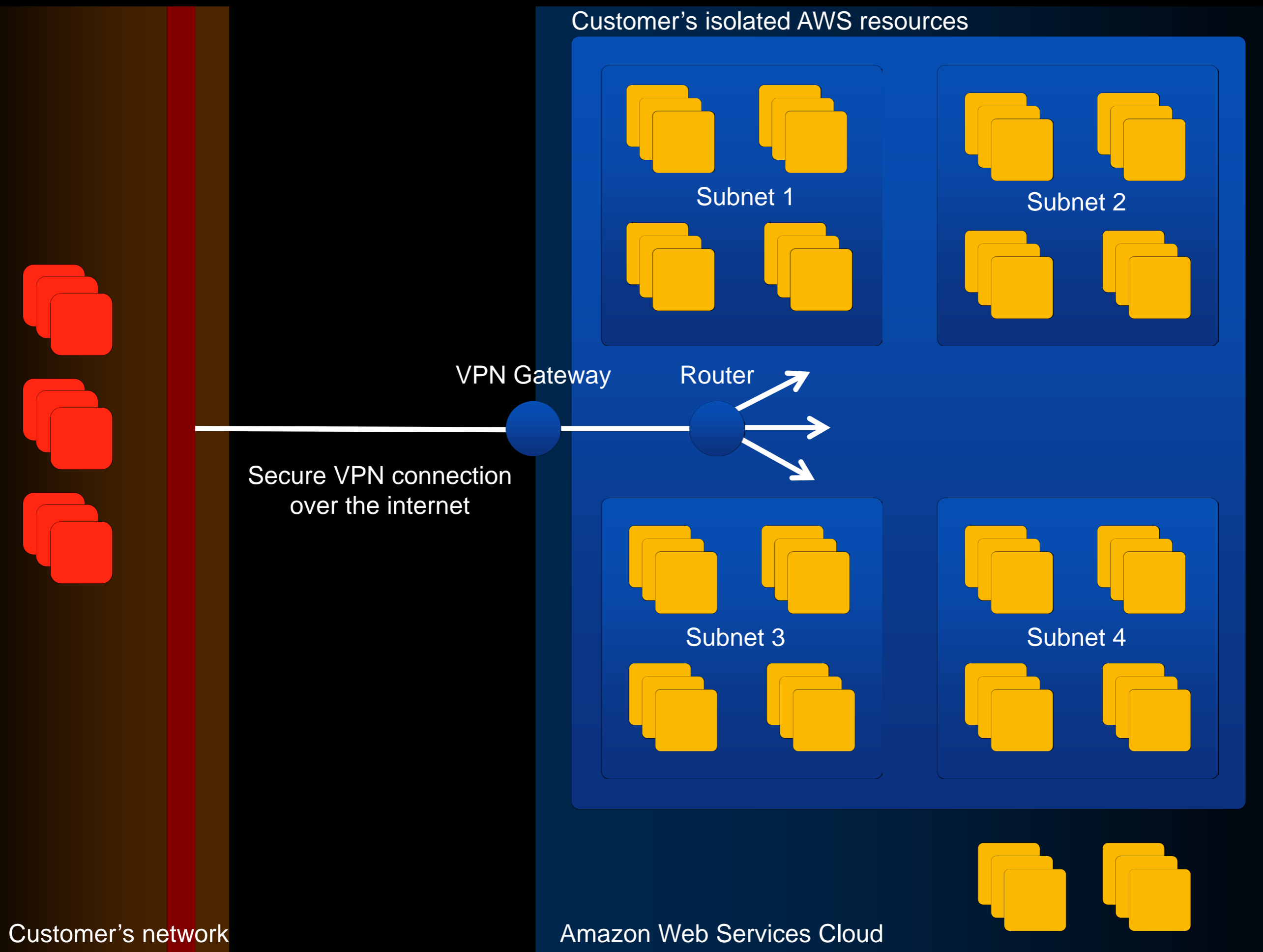
Available now:
preview beta

4

Isolating resources

Extend your VPN

VIRTUAL PRIVATE CLOUD



Create isolated environment within AWS

Establish subnets for access control

Connect your isolated AWS resources and
IT infrastructure via a VPN

Launch AWS resources within the isolated network

Extend existing security and networking technologies to examine traffic to and from your isolated resources

Extend existing security and management policies within your IT infrastructure to your isolated AWS resources as if they were running within your own infrastructure

Thank you

Questions, feedback:
mawood@amazon.com
