Building a data perimeter in AWS

Tatyana Yatskevich

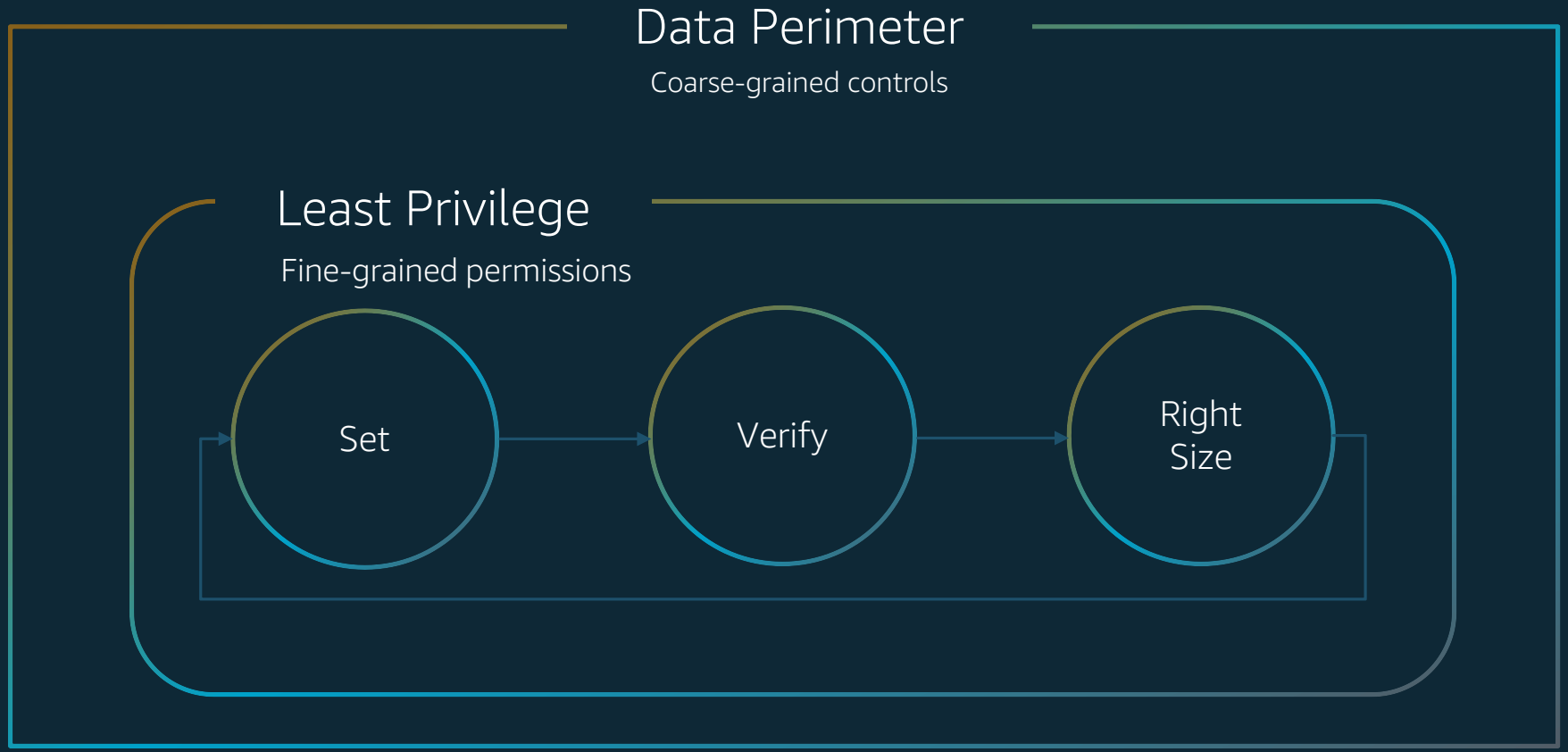
05/18/2022

Agenda

- Data perimeter concept
- Establishing a data perimeter
- Implementing a data perimeter (demo)

Data perimeter concept

Access Management



What is a data perimeter?

A set of preventive guardrails that ensures that access to *trusted resources* is restricted to *trusted identities* from *expected networks*

Trusted resources: *resources owned by your AWS accounts or by AWS services acting on your behalf*

Trusted identities: *principals (IAM roles or users) within your AWS accounts, or AWS services acting on your behalf*

Expected networks: *Your on-premises data centers and virtual private clouds (VPCs), or networks of AWS services acting on your behalf*

Data is stored in *trusted resources*

aws

Data perimeter controls

Perimeter	Intent / Control Objective
Identity	Only trusted identities can access my resources
	Only trusted identities are allowed from my network
Resource	My identities can access only trusted resources
	Only trusted resources can be accessed from my network
Network	My identities can access resources only from expected networks
	My resources can only be accessed from expected networks

aws

Benefits

Build Corporate Boundary

Restrict access to sensitive data based on expected access patterns

Provide Developer Freedom

Allow developers to innovate and move fast

Meet Compliance Requirements

Implement guardrails to meet compliance requirements at scale

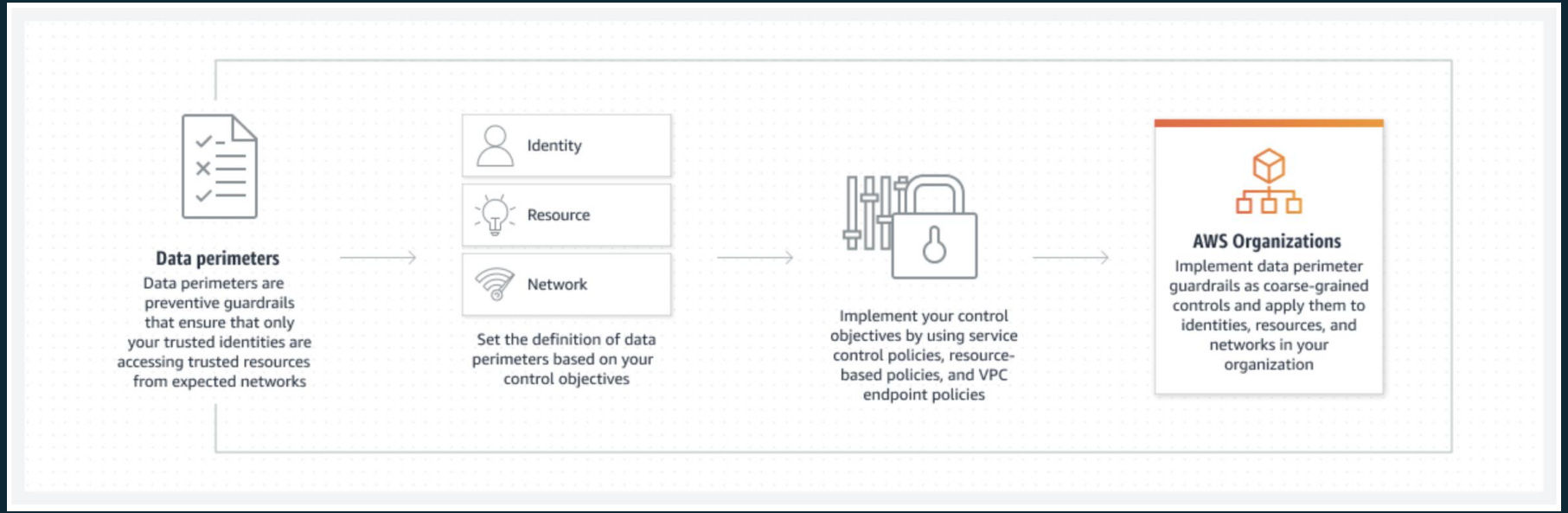
Defense in Depth

Central control over security invariants

aws

Establishing a data perimeter

Establishing a data perimeter



Primary Tools for your Data Perimeter

Service control policies

Permissions guardrails for identities

VPC endpoint policies

Ensure network access only from trusted identities

Resource-based policies

Ensure access only by trusted identities and AWS services

aws

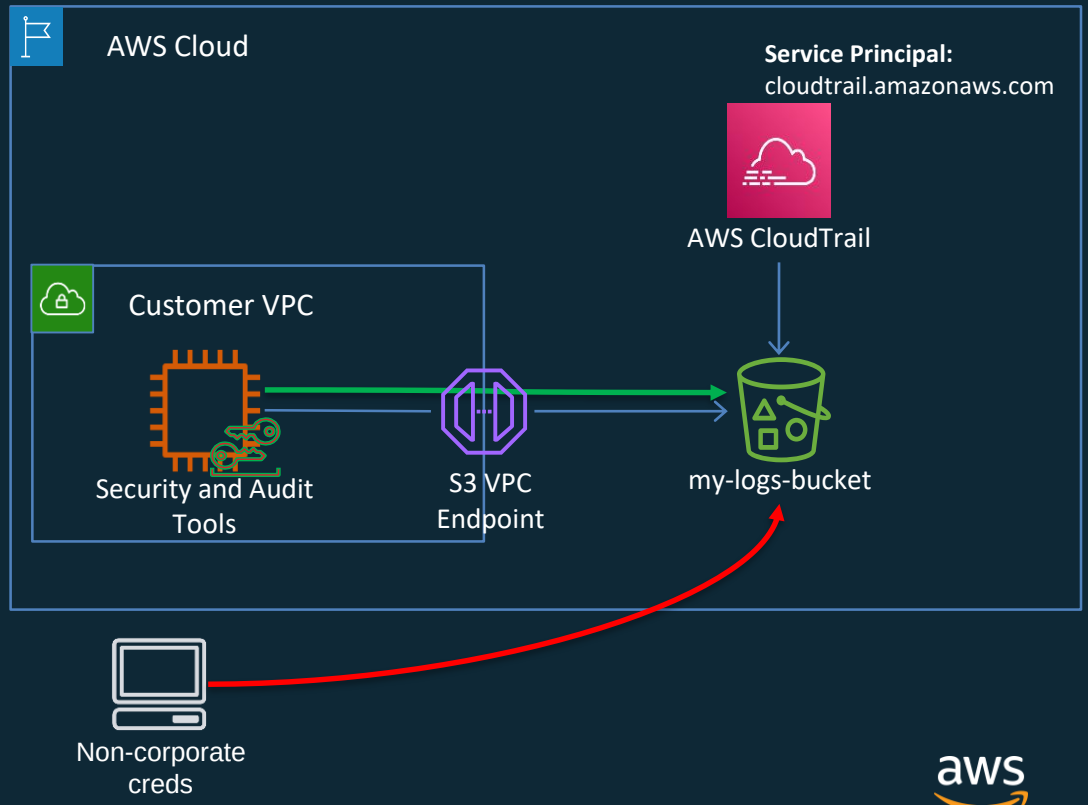
Data perimeter controls

Perimeter	Intent / Control Objective	Applied on	Using
Identity	Only trusted identities can access my resources	**Resources**	Resource-based policy
	Only trusted identities are allowed from my network	**Network**	VPC endpoint policy
Resource	My identities can access only trusted resources	**Identities**	SCP policy
	Only trusted resources can be accessed from my network	**Network**	VPC endpoint policy
Network	My identities can access resources only from expected networks	**Identities**	SCP policy
	My resources can only be accessed from expected networks	**Resources**	Resource-based policy

Identity Perimeter on Resources

Only trusted identities can access my resources

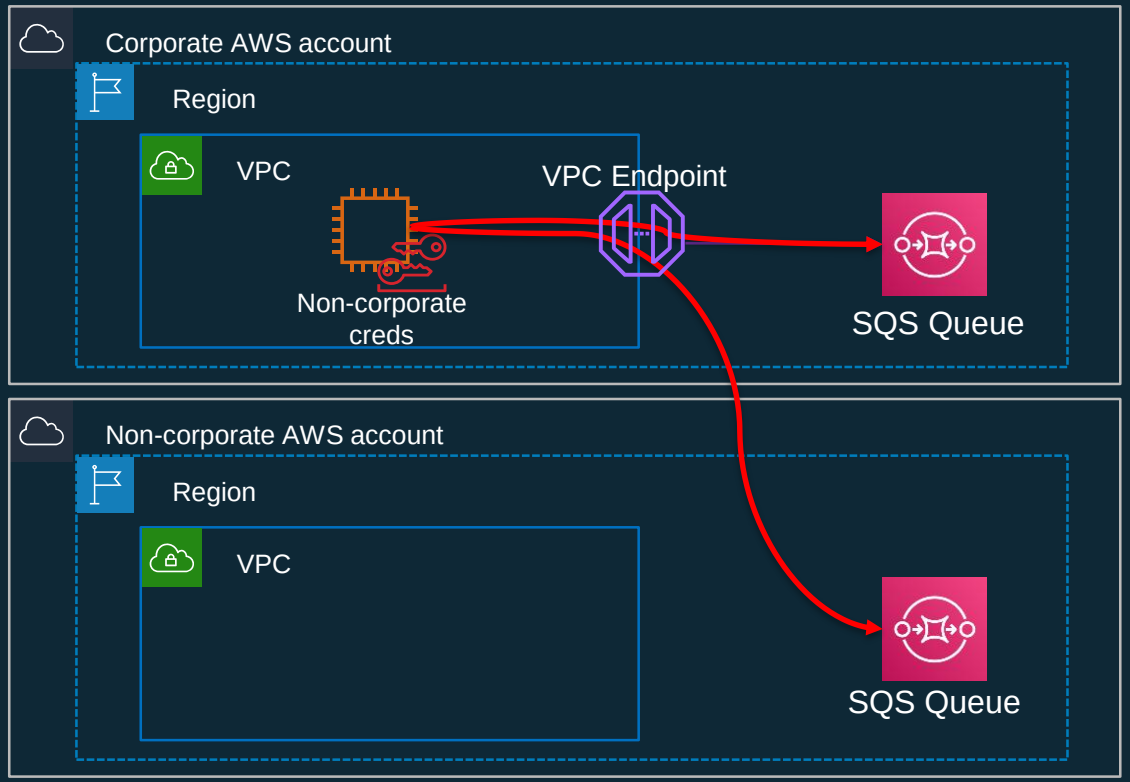
```
……
{
  "Effect": "Deny",
  "Principal": "*",
  "Action": [
    "s3:ListBucket",
    "s3:PutObject*",
    "s3:GetObject*"
  ],
  "Resource": [
    "arn:aws:s3:::<my-data-bucket>",
    "arn:aws:s3:::<my-data-bucket>/*"
  ],
  "Condition": {
    "StringNotEquals": {
      "aws:PrincipalOrgID": "<o-xxxxxxxx>"
    },
    "Bool": {
      "aws:PrincipalIsAWSService": "false"
    }
  }
}
……
```



Identity Perimeter on Network

Only trusted identities are allowed from my network

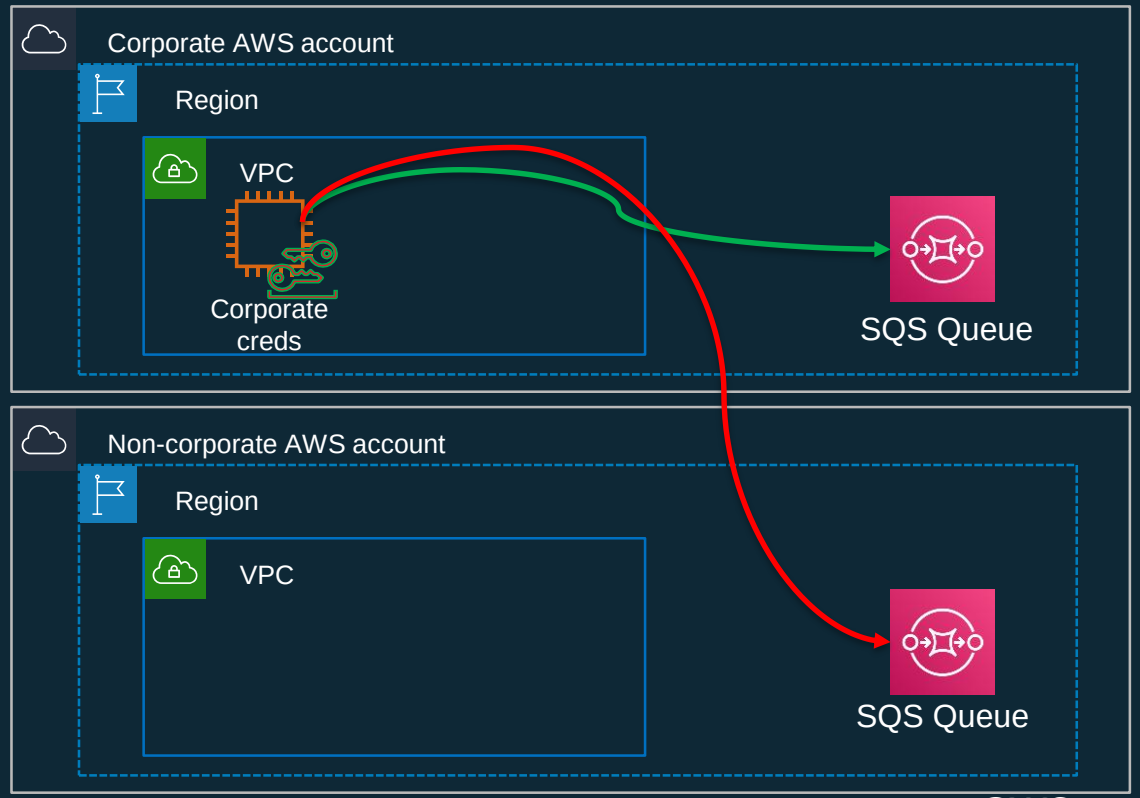
```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": {
        "AWS": "*"
      },
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgID": "o-xxxxxxxx"
        }
      }
    }
  ]
}
```



Resource Perimeter on Identity

My identities can access only trusted resources

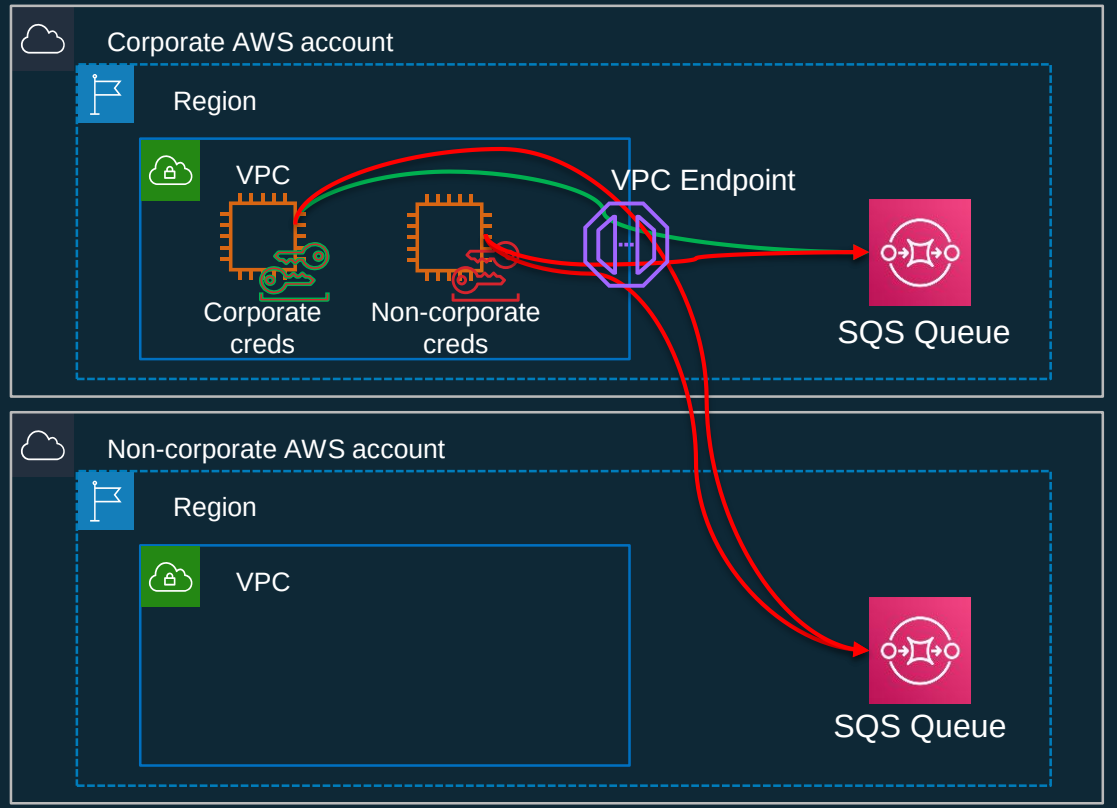
```
……
{
  "Effect": "Deny",
  "Action": [
    "sqs:SendMessage"
  ],
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "aws:ResourceOrgID ": "o-xxxxxxxxxx"
    }
  }
}
……
```



Resource Perimeter on Network

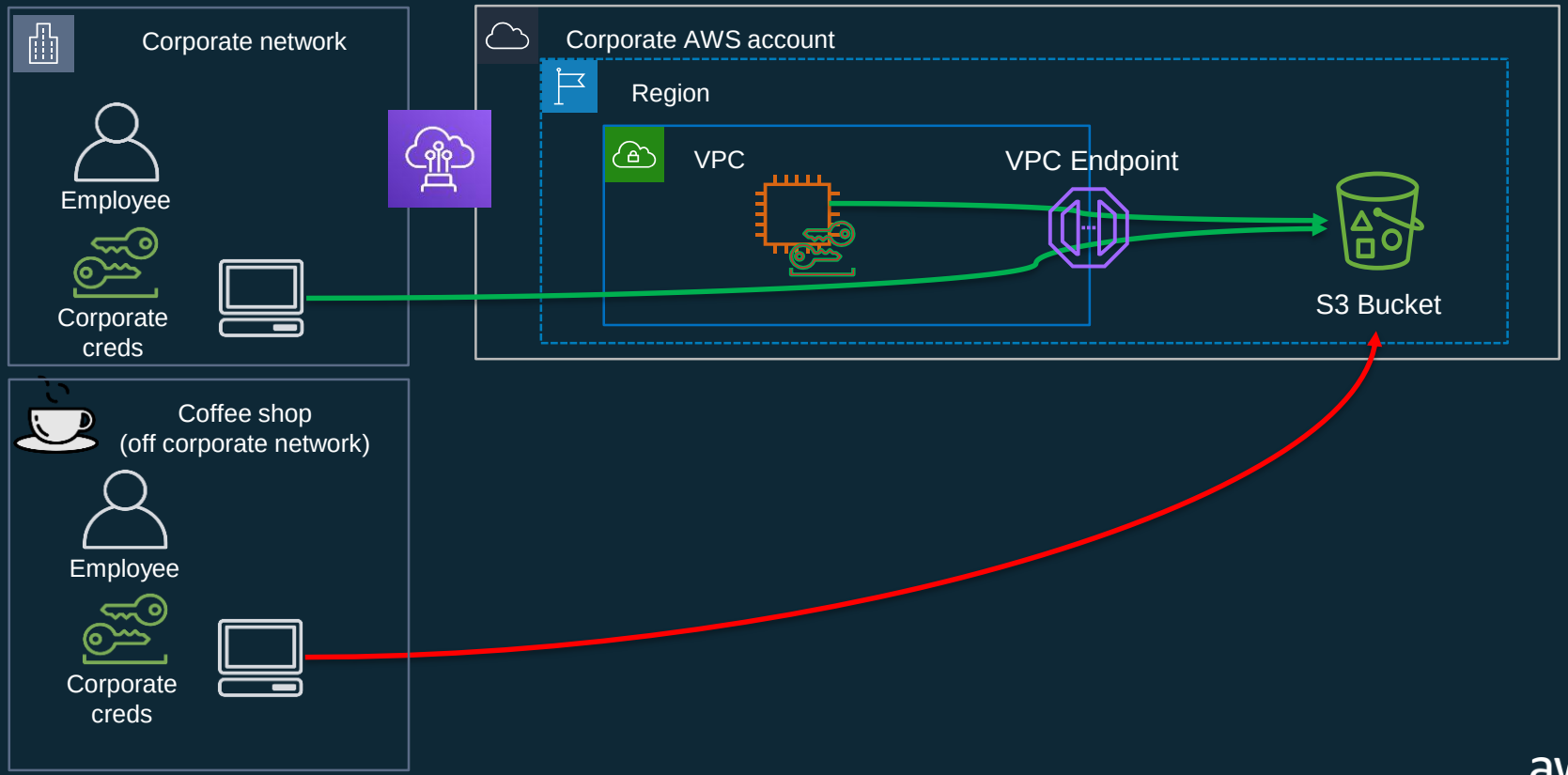
Only trusted resources can be accessed from my network

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": {
        "AWS": "*"
      },
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgID": "o-xxxxxxxxxx",
          "aws:ResourceOrgID": "o-xxxxxxxxxx"
        }
      }
    }
  ]
}
```



Network Perimeter on Resource

My resources can only be accessed from expected networks



Network Perimeter on Resource

My resources can only be accessed from expected networks

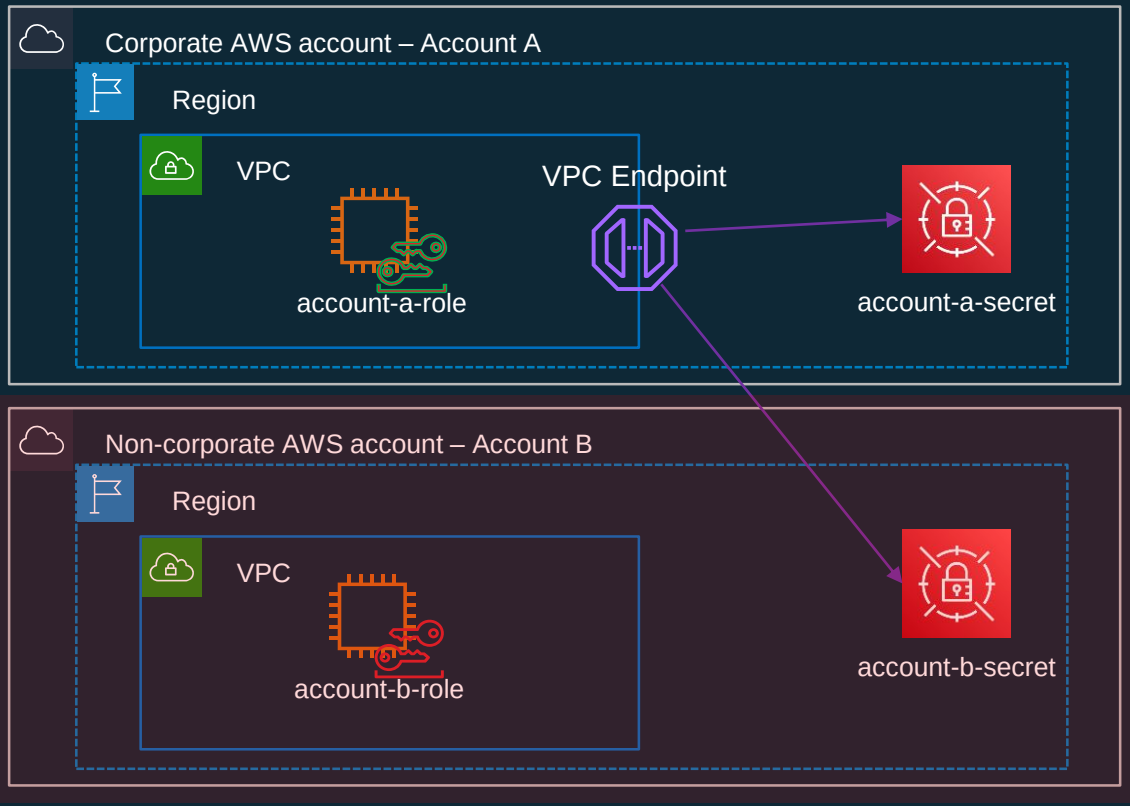
```
......
{
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:*",
  "Resource": [
    "arn:aws:s3:::my-data-bucket",
    "arn:aws:s3:::my-data-bucket/*"
  ],
  "Condition": {
    "NotIpAddressIfExists": {
      "aws:SourceIp": "<cidr>"
    },
    "StringNotEqualsIfExists": {
      "aws:SourceVpc": "<vpc-xxxxxxxx>"
    },
    "BoolIfExists": {
      "aws:PrincipalIsAWSService": "false",
      "aws:ViaAWSService": "false"
    },
    "ArnNotLikeIfExists": {
      "aws:PrincipalArn": "arn:aws:iam::<AccountNumber>:role/aws-service-role/*"
    }
  }
}
......
```

Data perimeter controls

Perimeter	Intent / Control Objective	Applied on	Using	Primary IAM feature
Identity	Only trusted identities can access my resources	**Resources**	Resource-based policy	aws:PrincipalOrgID aws:PrincipalIsAWSService
	Only trusted identities are allowed from my network	**Network**	VPC endpoint policy	aws:PrincipalOrgID
Resource	My identities can access only trusted resources	**Identities**	SCP policy	aws:ResourceOrgID
	Only trusted resources can be accessed from my network	**Network**	VPC endpoint policy	aws:ResourceOrgID
Network	My identities can access resources only from expected networks	**Identities**	SCP policy	aws:SourceIp aws:SourceVpc/SourceVpce aws:ViaAWSService
	My resources can only be accessed from expected networks	**Resources**	Resource-based policy	aws:SourceIp aws:SourceVpc/SourceVpce aws:ViaAWSService aws:PrincipalIsAWSService

Implementing a data perimeter (demo)

Demo setup



account-a-role and account-b-role permissions

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource": "arn:aws:secretsmanager:us-east-1:*:secret:*"
    }
.....
  ]
}
```

Learn more

- Data perimeters on AWS
- Building a data perimeter on AWS whitepaper
- Data perimeter hands-on workshop workshop

Thank you!