Data Perimeters on AWS

Archived: 2026-04-05 15:48:52 UTC

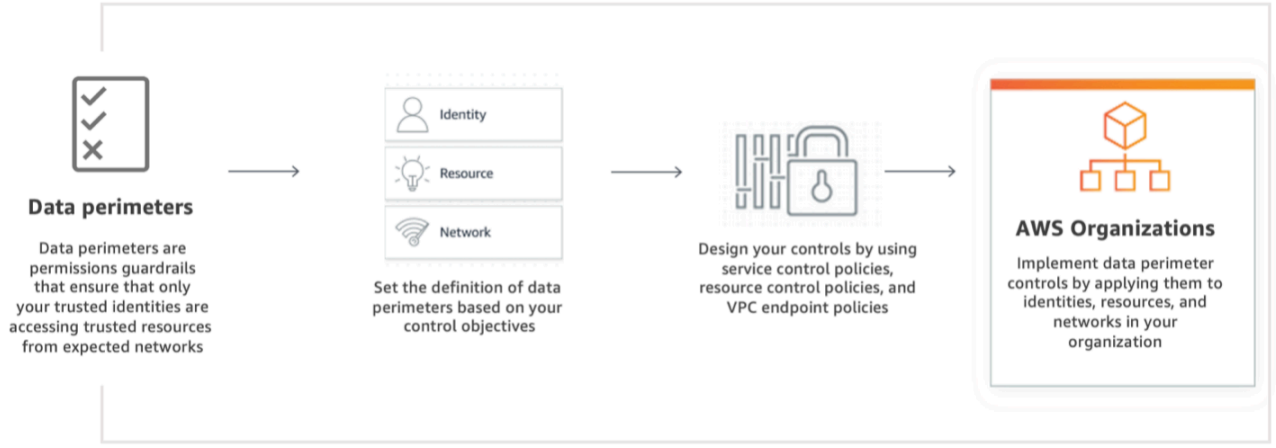
What is a data perimeter?

A data perimeter is a set of permissions guardrails in your AWS environment you use to help ensure that only your trusted identities are accessing trusted resources from expected networks. Data perimeter guardrails are meant to serve as always-on boundaries to help protect your data across a broad set of AWS accounts and resources. These organization-wide guardrails do not replace your existing fine grained access controls. Instead, they help improve your security strategy by ensuring that all AWS Identity and Access Management (IAM) users, roles, and resources adhere to a set of defined security standards. Data perimeter guardrails work alongside AWS Well-Architected Framework security design principles and other security best practices to strengthen your overall security posture.

- Explore data perimeters in AWS Identity and Access Management (IAM) documentation.
- Consult the Data perimeter policy examples GitHub repo for service specific considerations when implementing data perimeters in your environment.
- Learn from customers implementations of data perimeter controls for specific use cases.

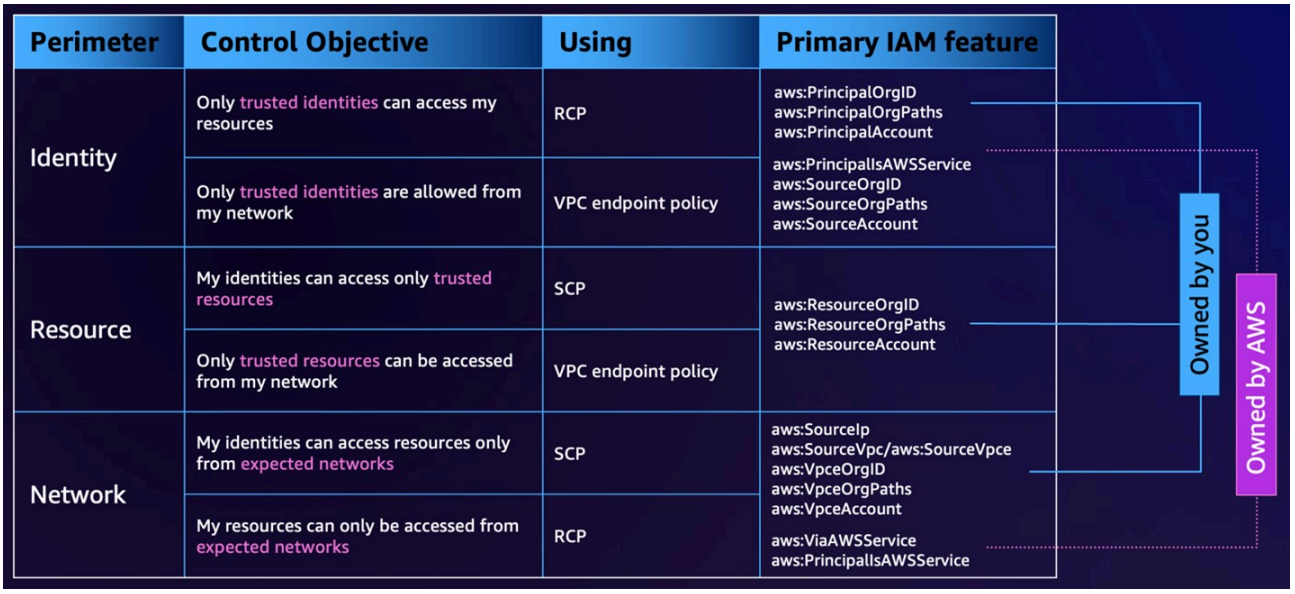
How it works

To establish data perimeters, define your control objectives first and implement those objectives by using service control policies (SCPs), resource control policies (RCPs), and VPC endpoint policies. Then, apply these policies as data perimeter guardrails in your AWS organization.



Data perimeter control objectives and capabilities

Data perimeter coarse-grained controls help you achieve six distinct security objectives through the implementation of different combinations of IAM policy types and condition keys.



Benefits

Meet security and compliance requirements

Implement organization-wide permissions guardrails that help prevent AWS accounts, organizational units, or an entire organization from taking actions that do not meet your security and compliance policies. By using preventive controls, you can establish that only your trusted identities are accessing trusted resources from expected networks.

Improve your data loss prevention strategies

Use data perimeters in your data loss prevention strategies to detect and help prevent intentional or unintentional transfers of sensitive information for unauthorized use. Data perimeters provide cloud-native preventive controls to restrict access to trusted identities accessing sensitive data as you intend.

Establish an organization-wide data perimeter

With an organization-wide data perimeter in place, you can start by granting broader permissions to developers to get them started quickly on their projects. After the workload is well defined, work your way toward specific permissions and least privilege.

Use cases

Allow data access to only those you want to have access

Establish an organization-wide data perimeter to allow data access to only those you want to have access. For example, they can help you ensure that data is accessed only by your employees and only from your corporate network, including your on-premises data centers or VPCs. Also, they can help prevent resources from being shared with external roles and users.

Help protect sensitive information

Help protect sensitive information with organization-wide data perimeters. Also help prevent employees from using non-corporate credentials to access non-corporate resources, which could lead to intentional or unintentional data loss. Help ensure that your employees can access only company-approved data stores.

Help prevent credential use outside of your corporate environment

Help prevent employees from using corporate credentials outside of your corporate environment, including your on-premises data centers and VPCs. Create an organization-wide perimeter that helps prevent your identities from performing any actions outside of your corporate network.

Resources

Technical documentation

Tech talk

Building a data perimeter on AWS

Watch now »

Whitepaper

Building a data perimeter on AWS

Read now »

GitHub repo

Data perimeter policy examples

Read now »

Blogs

Blog Post Series: Establishing a Data Perimeter on AWS

The purpose of the Data Perimeters Blog Post Series is to provide prescriptive guidance about establishing your data perimeter at scale, including key security and implementation considerations. These blog posts cover in depth

the objectives and foundational elements needed to enforce identity, resource, and network data perimeters and how to use a risk-based approach to apply the relevant controls.

Customer use cases

Video

AWS re:Inforce 2025 - Establishing a data perimeter on AWS, featuring Block, Inc. (IAM305)

Watch now »

Video

AWS re:Inforce 2024 - Establishing a data perimeter on AWS, featuring Capital One (IAM305)

Watch now »

Video

AWS re:Inforce 2023 - Establishing a data perimeter on AWS, featuring USAA (IAM301)

Watch now »

Document

AWS re:Invent 2022 - Establishing a data perimeter on AWS, featuring Goldman Sachs (SEC326)

Read now »

Video

AWS re:Inforce 2022 - Establishing a data perimeter on AWS, featuring Vanguard (IAM304)

Watch now »

Hands-on activities
