Safe Terraform auto-apply with conftest



Josep Medialdea
Senior Site Reliability Engineer

Ricard Bejarano
Lead Site Reliability Engineer

SREday London 2026 Q3

A day in the life of a Terraform change

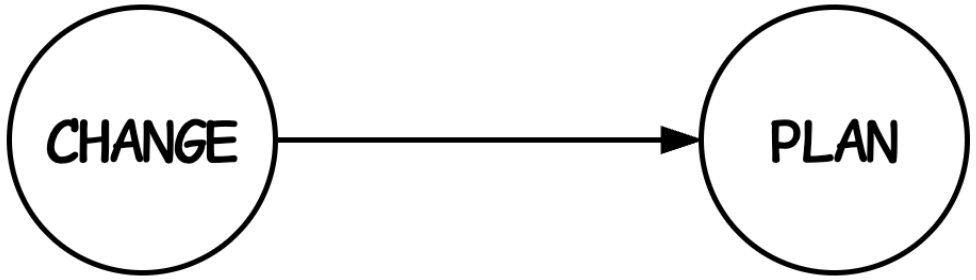
© 2026 Cisco and/or its affiliates. All rights reserved.

A day in the life of a Terraform change



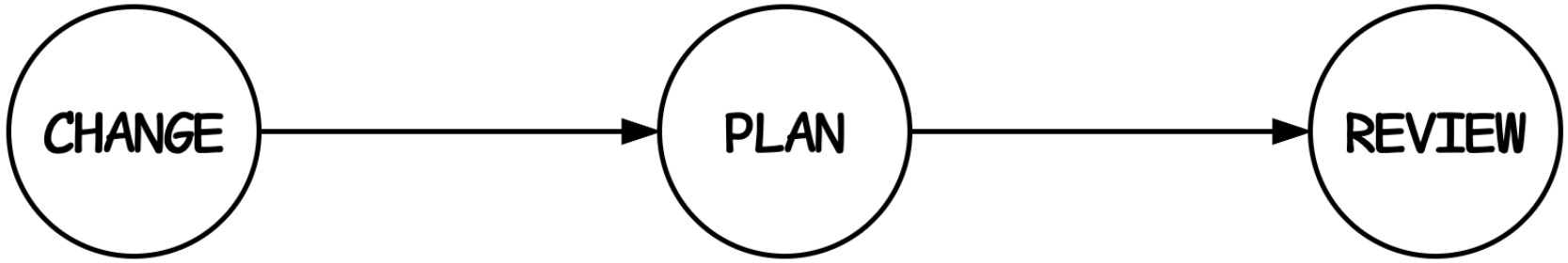
© 2026 Cisco and/or its affiliates. All rights reserved.

A day in the life of a Terraform change



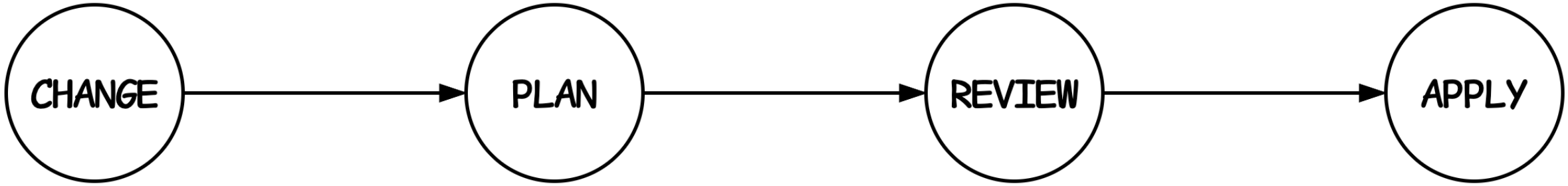
© 2026 Cisco and/or its affiliates. All rights reserved.

A day in the life of a Terraform change



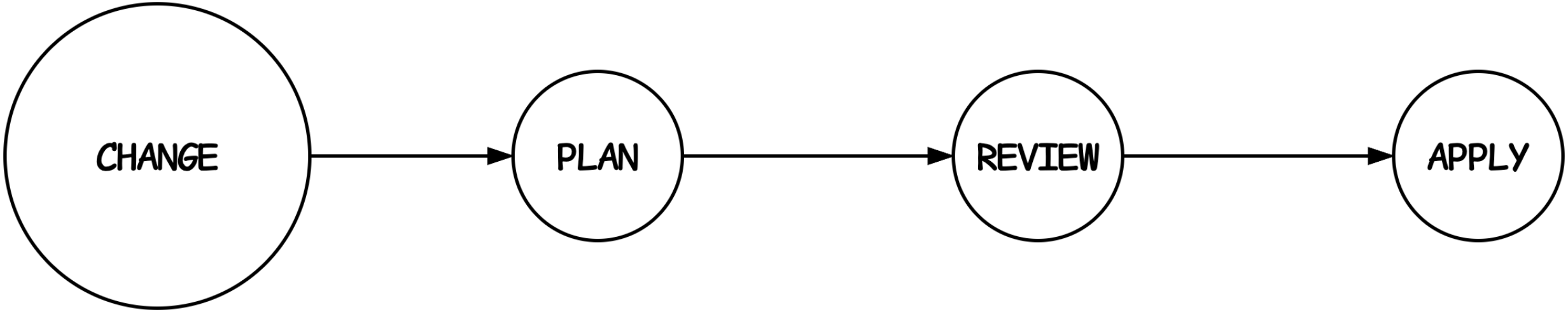
© 2026 Cisco and/or its affiliates. All rights reserved.

A day in the life of a Terraform change



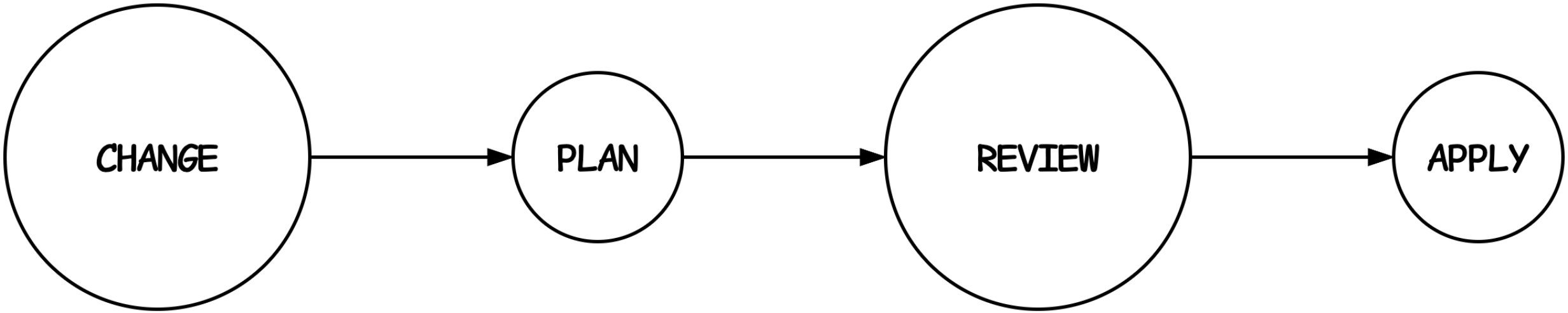
© 2026 Cisco and/or its affiliates. All rights reserved.

A day in the life of a Terraform change



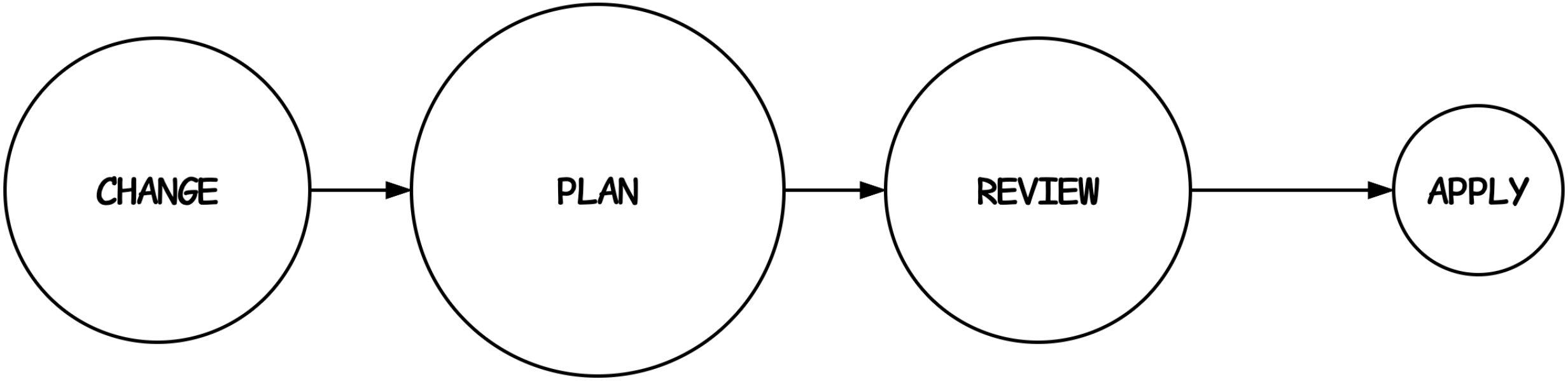
© 2026 Cisco and/or its affiliates. All rights reserved.

A day in the life of a Terraform change



© 2026 Cisco and/or its affiliates. All rights reserved.

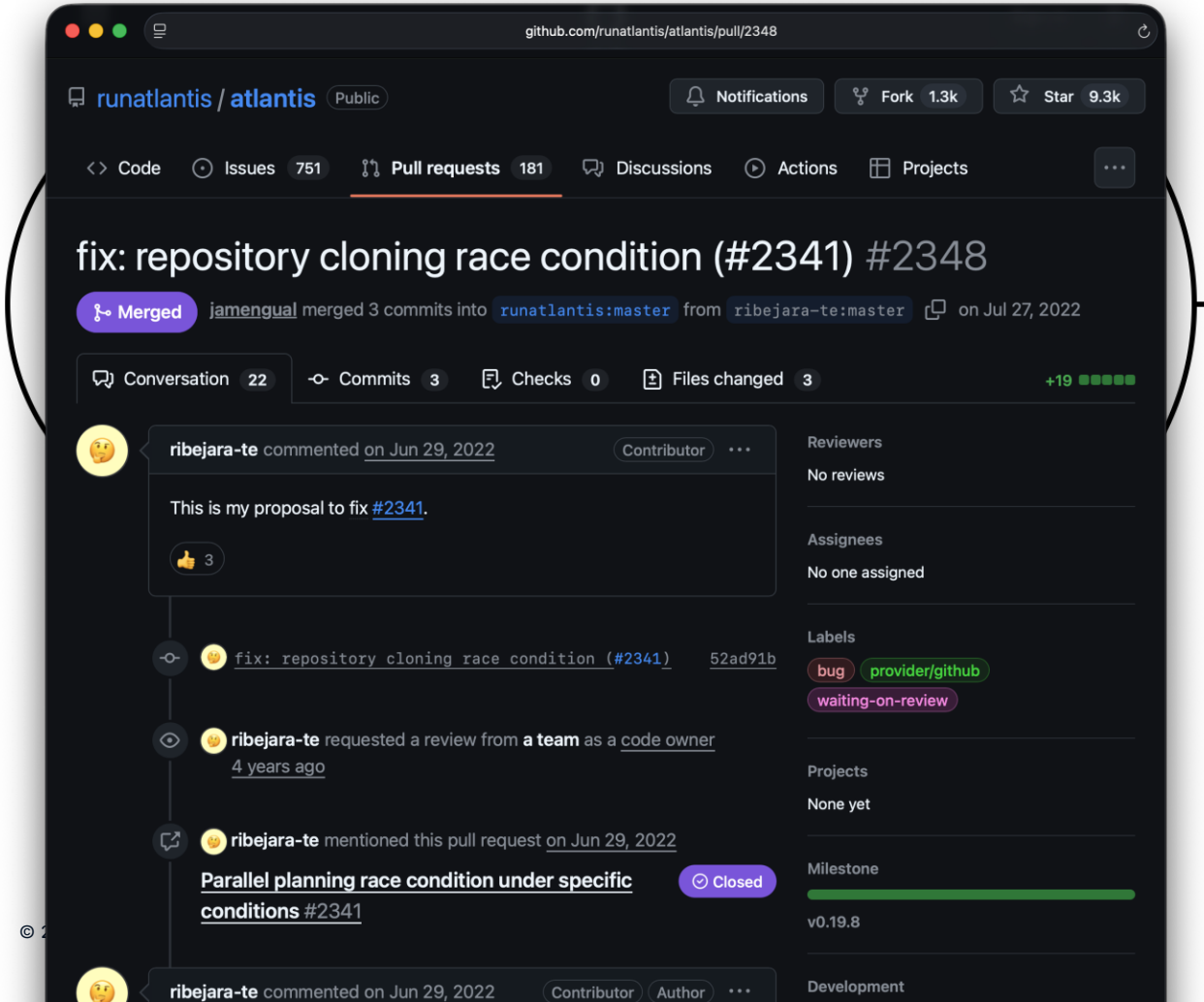
A day in the life of a Terraform change

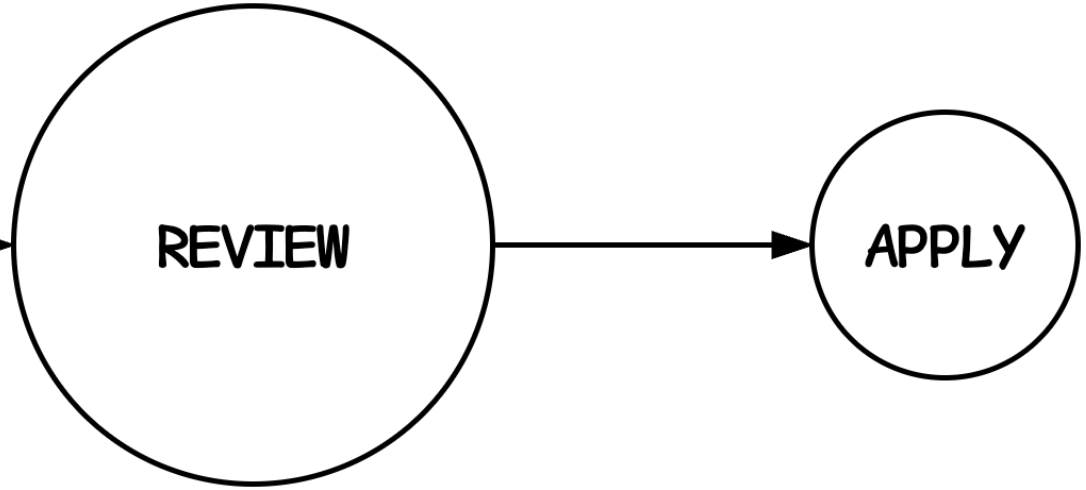


© 2026 Cisco and/or its affiliates. All rights reserved.

The problem

A day in the life of a Terraform change

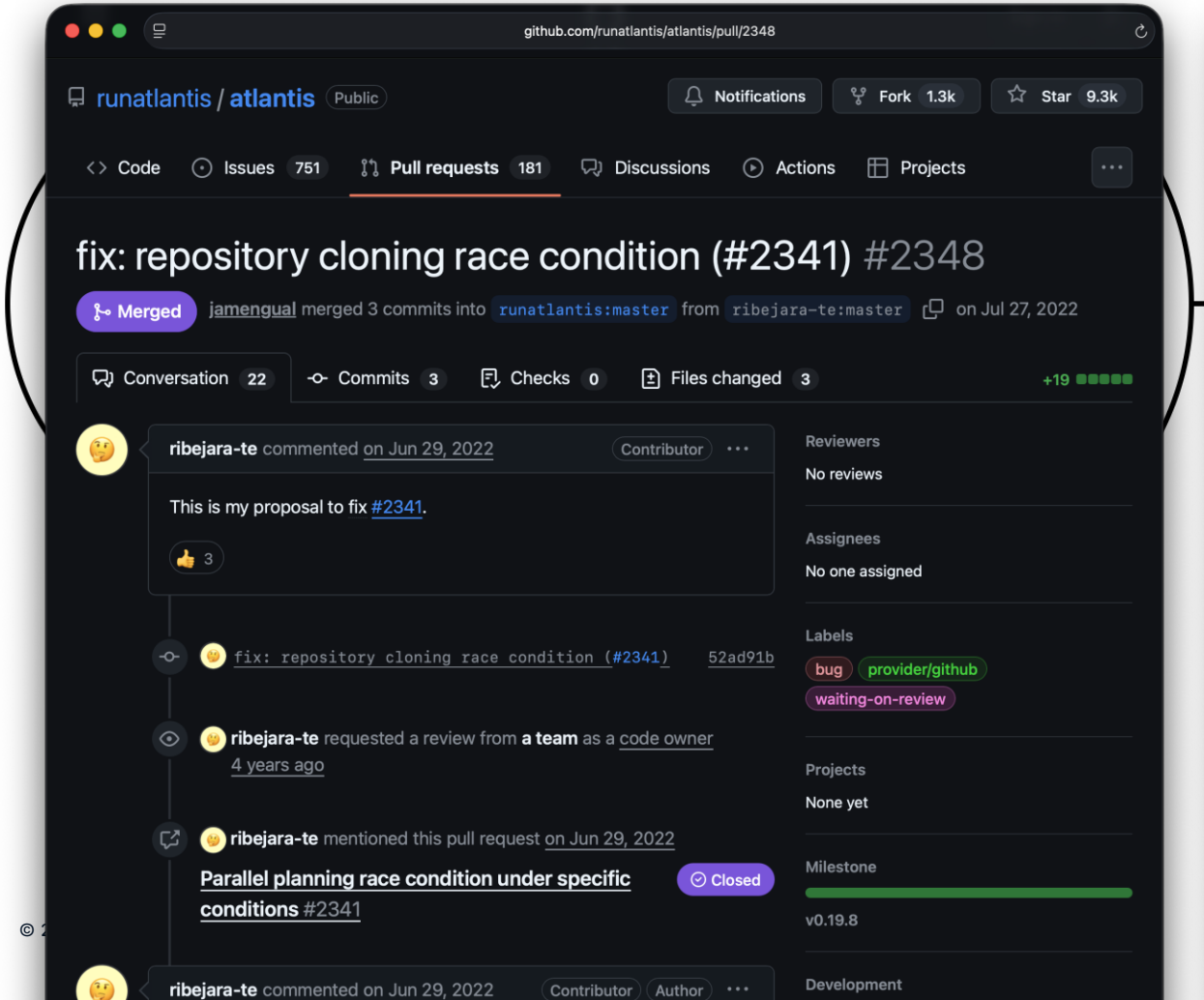


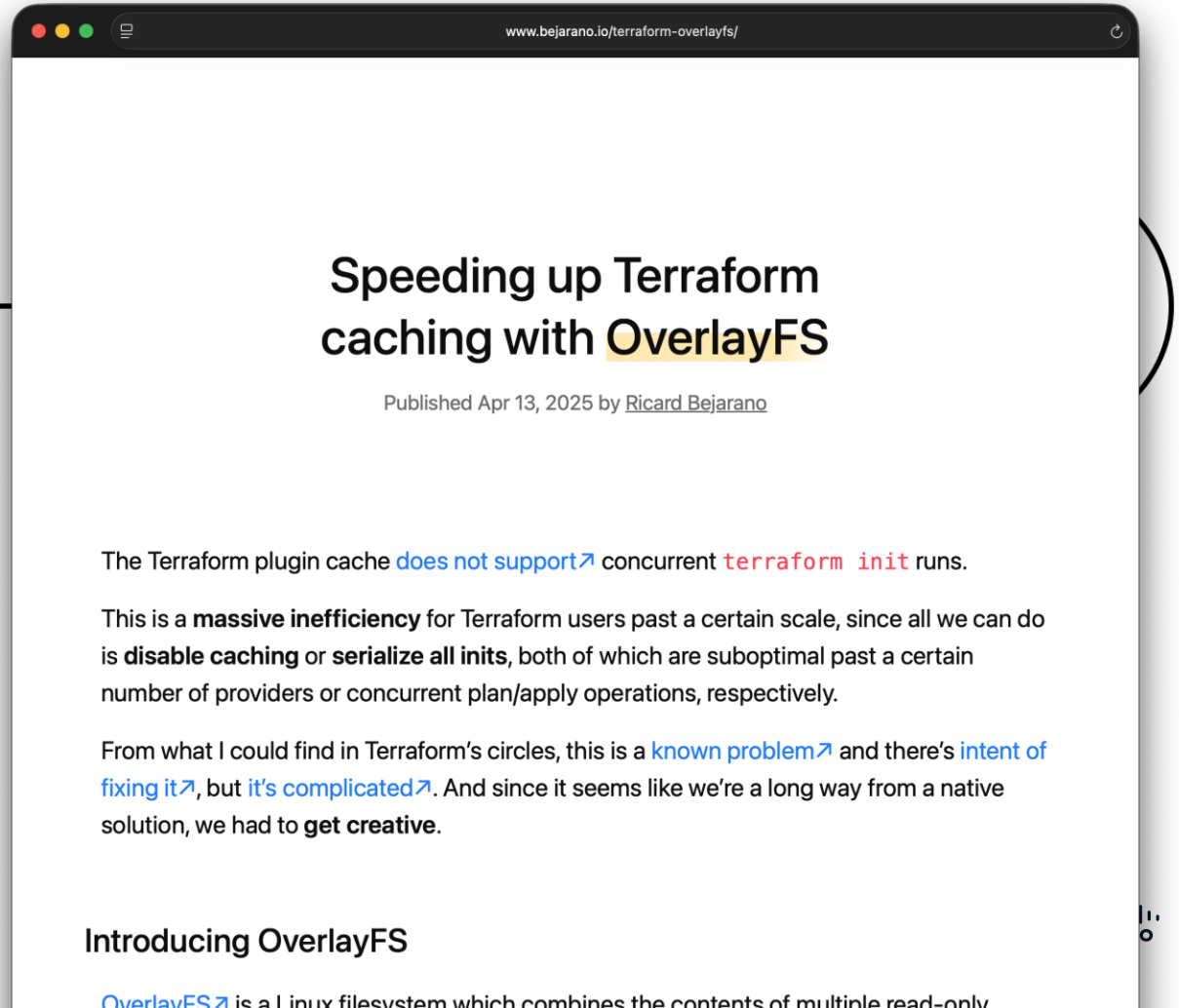


© 2

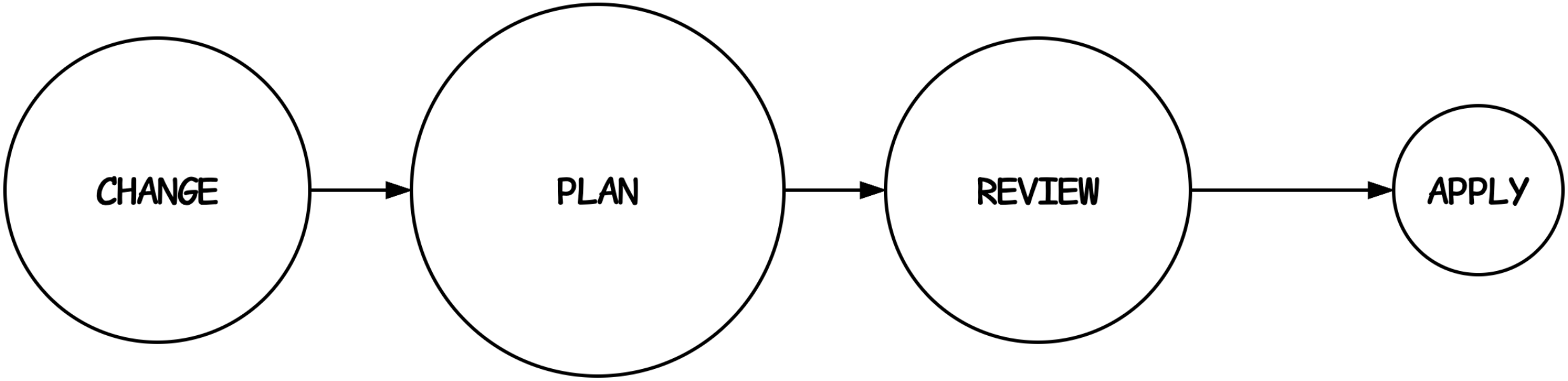
The problem

A day in the life of a Terraform change



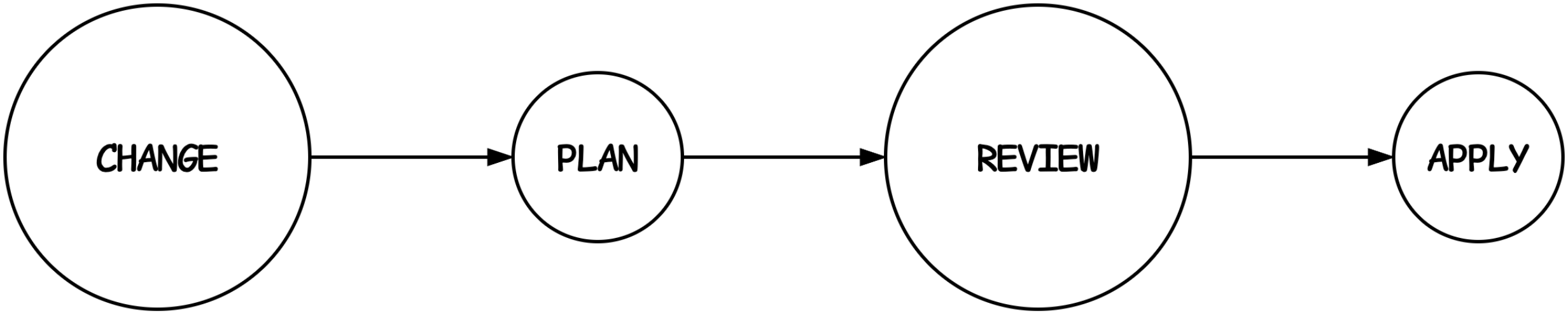


A day in the life of a Terraform change



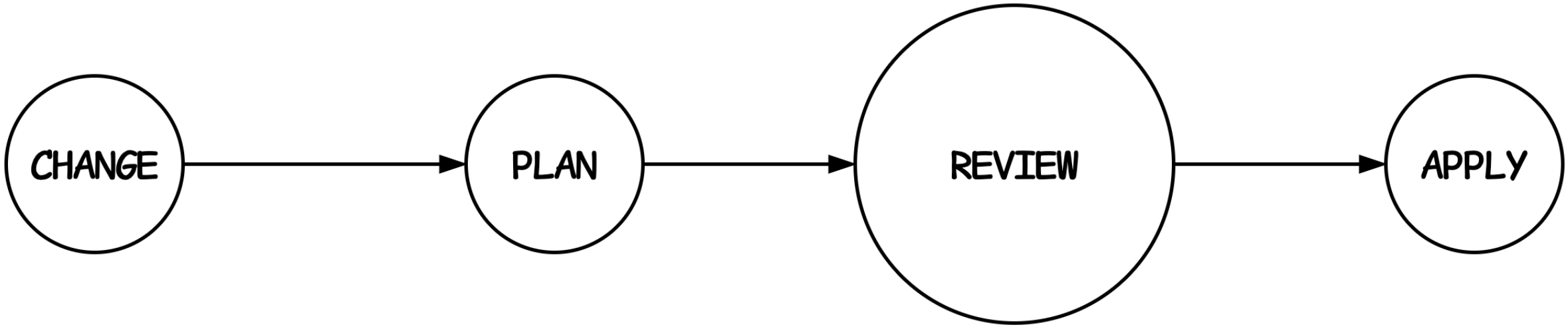
© 2026 Cisco and/or its affiliates. All rights reserved.

A day in the life of a Terraform change



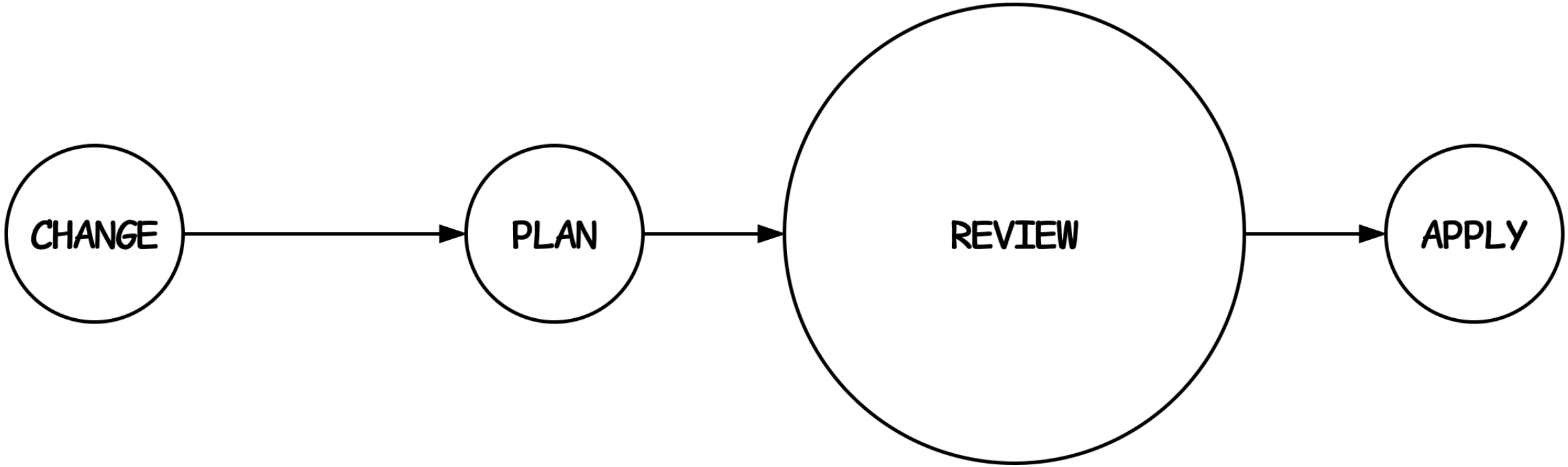
© 2026 Cisco and/or its affiliates. All rights reserved.

A day in the life of a Terraform change



© 2026 Cisco and/or its affiliates. All rights reserved.

A day in the life of a Terraform change



© 2026 Cisco and/or its affiliates. All rights reserved.

AI is not the answer

© 2026 Cisco and/or its affiliates. All rights reserved.

AI is not the answer

Stakes are too high

© 2026 Cisco and/or its affiliates. All rights reserved.

AI is not the answer

Stakes are too high

Nondeterministic

© 2026 Cisco and/or its affiliates. All rights reserved.

AI is not the answer

Stakes are too high

Nondeterministic

No accountability

© 2026 Cisco and/or its affiliates. All rights reserved.

AI is not the answer

Stakes are too high

Nondeterministic

No accountability

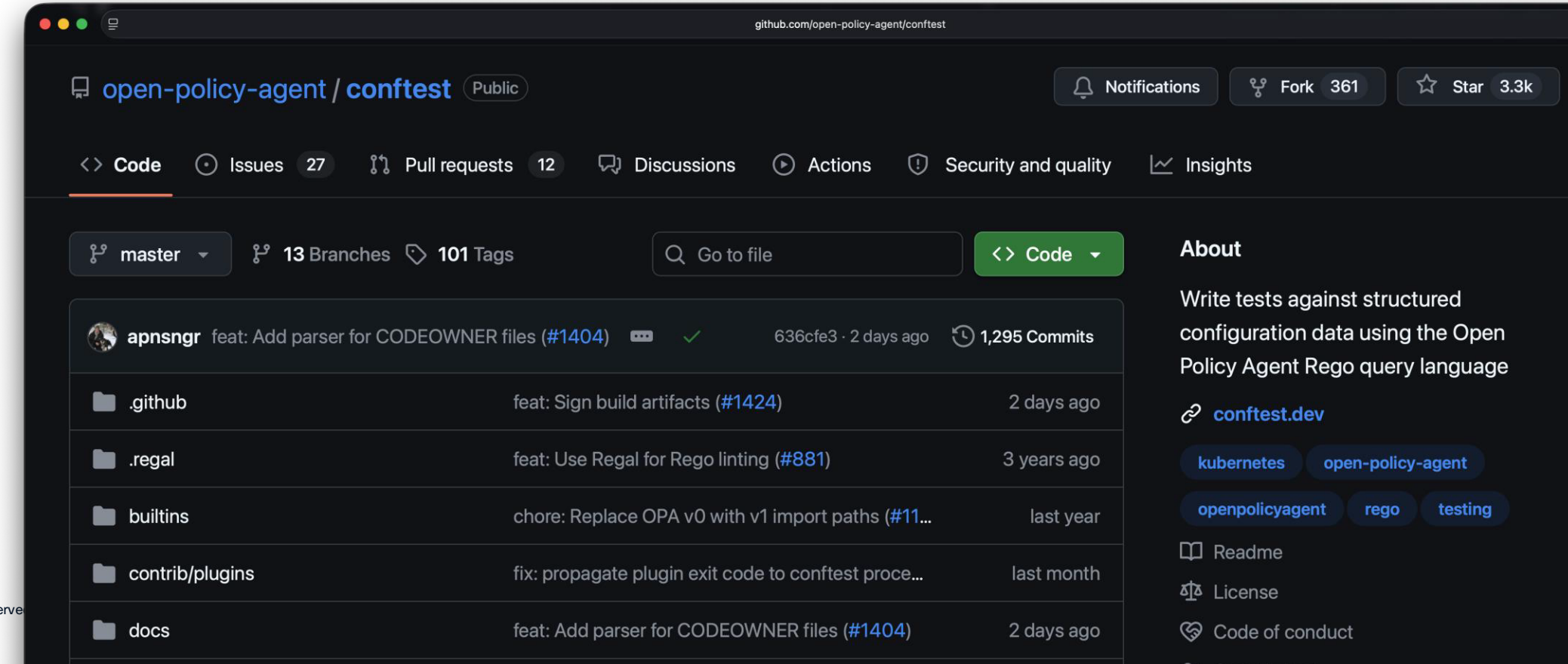
Can be fooled

© 2026 Cisco and/or its affiliates. All rights reserved.

The solution

Introducing: conftest

github.com/open-policy-agent/conftest



© 2026 Cisco and/or its affiliates. All rights reserve

What is conftest?

© 2026 Cisco and/or its affiliates. All rights reserved.

The solution

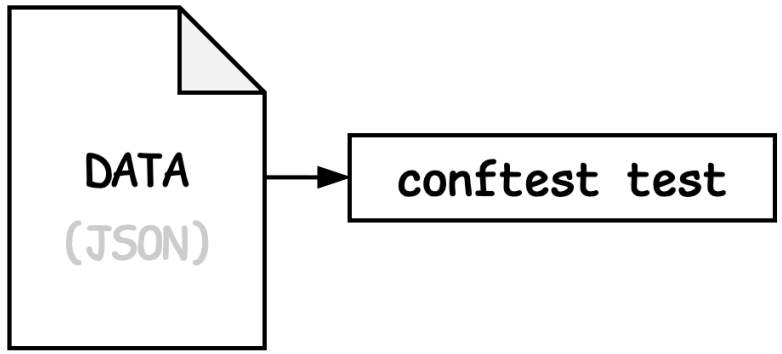
What is conftest?

```
conftest test
```

© 2026 Cisco and/or its affiliates. All rights reserved.

The solution

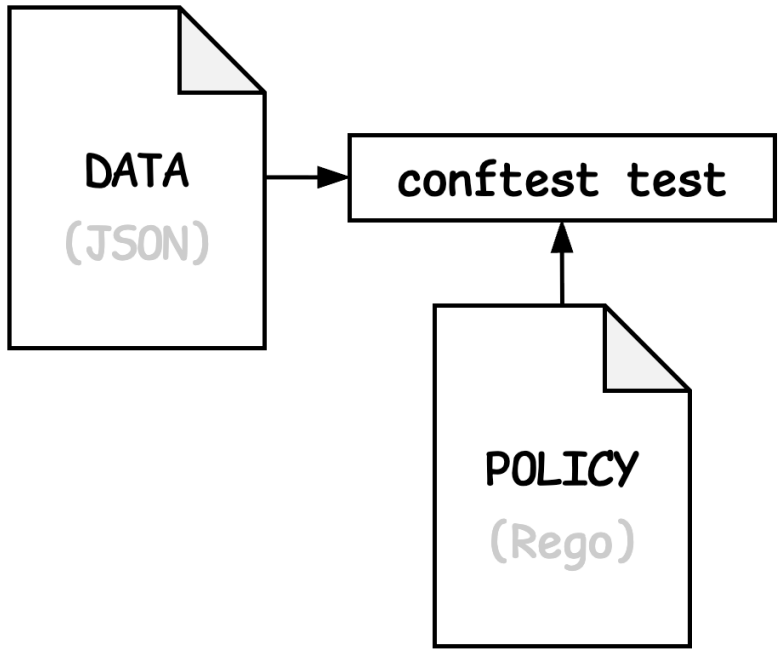
What is conftest?



© 2026 Cisco and/or its affiliates. All rights reserved.

The solution

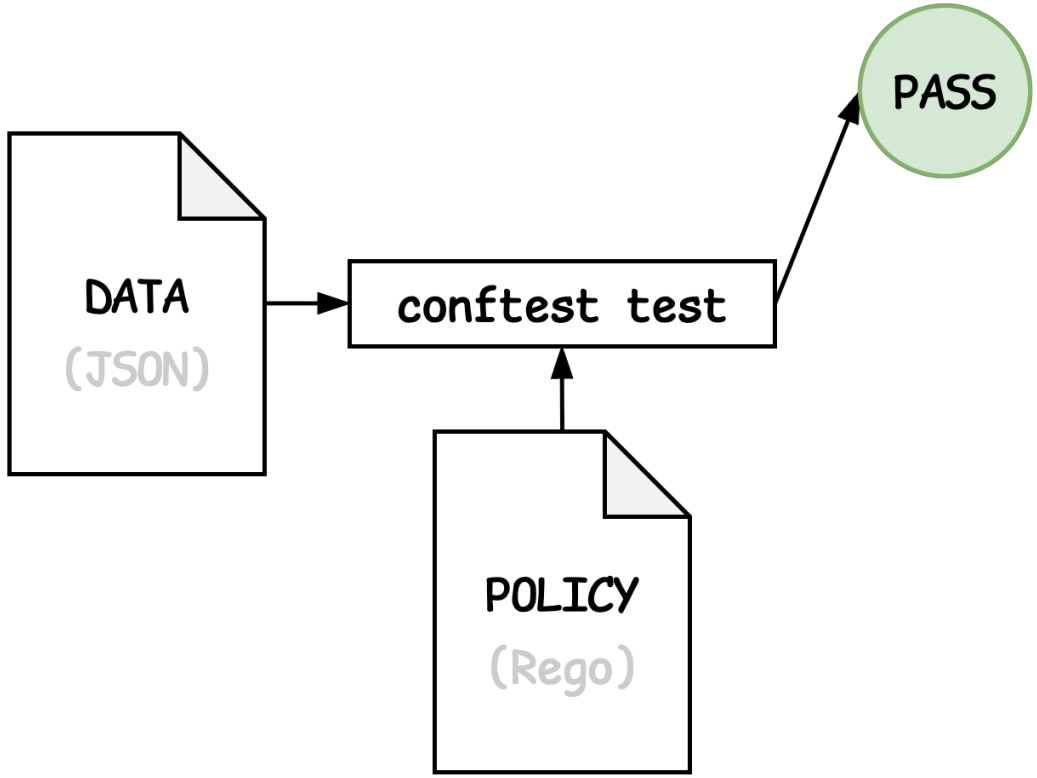
What is conftest?



© 2026 Cisco and/or its affiliates. All rights reserved.

The solution

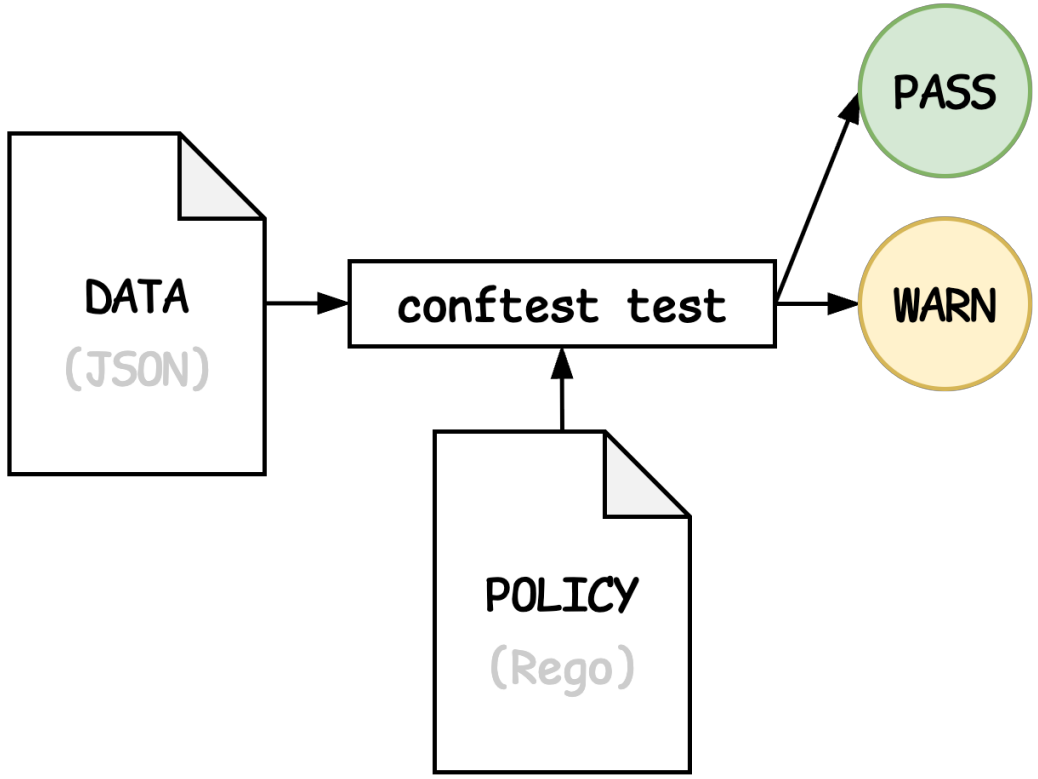
What is conftest?



© 2026 Cisco and/or its affiliates. All rights reserved.

The solution

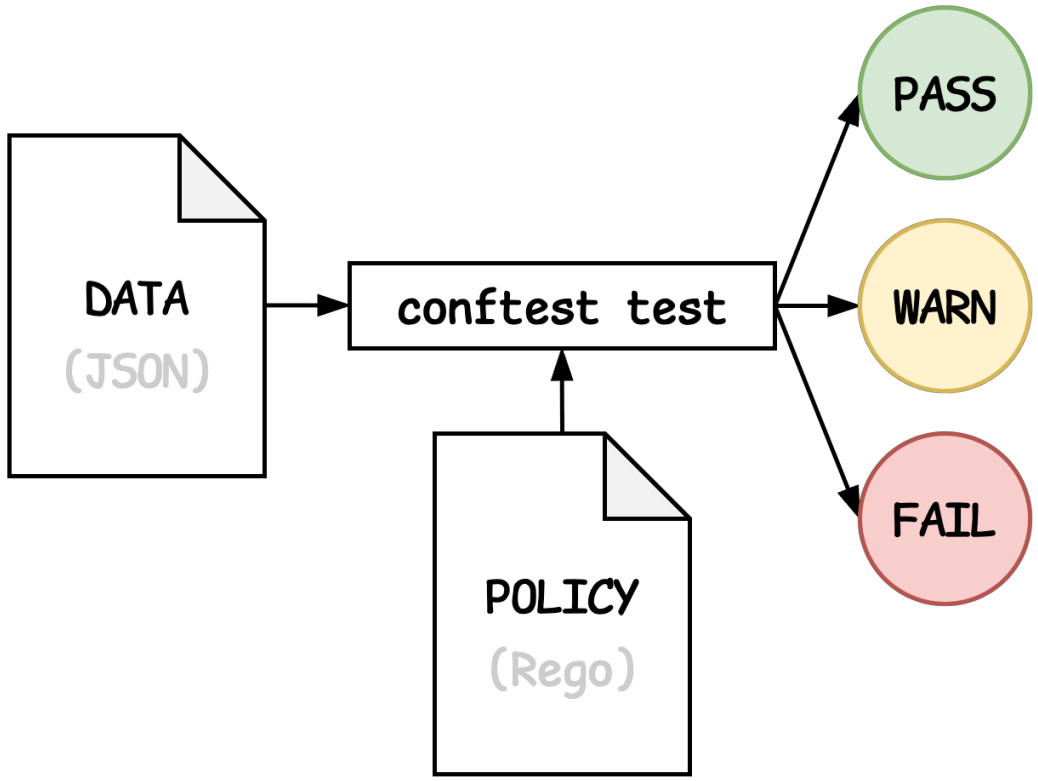
What is conftest?



© 2026 Cisco and/or its affiliates. All rights reserved.

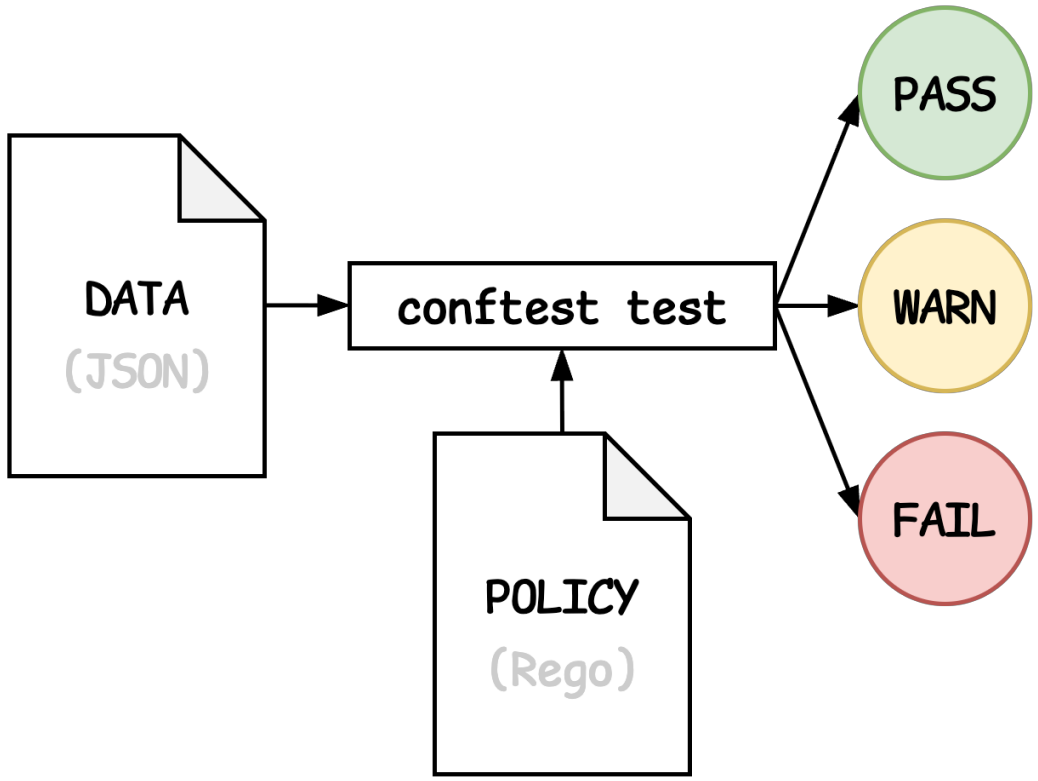
The solution

What is conftest?



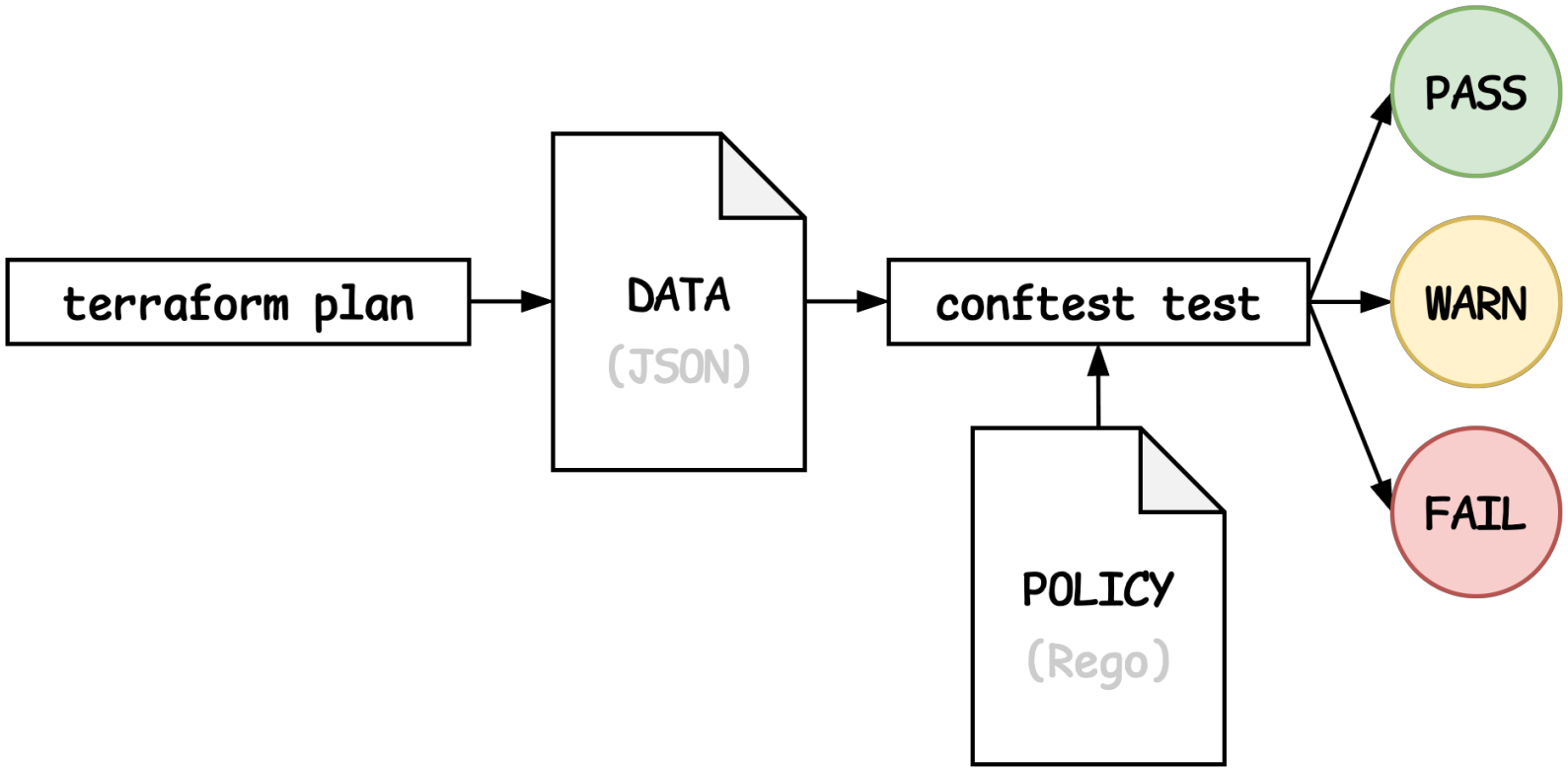
© 2026 Cisco and/or its affiliates. All rights reserved.

Putting it all together



© 2026 Cisco and/or its affiliates. All rights reserved.

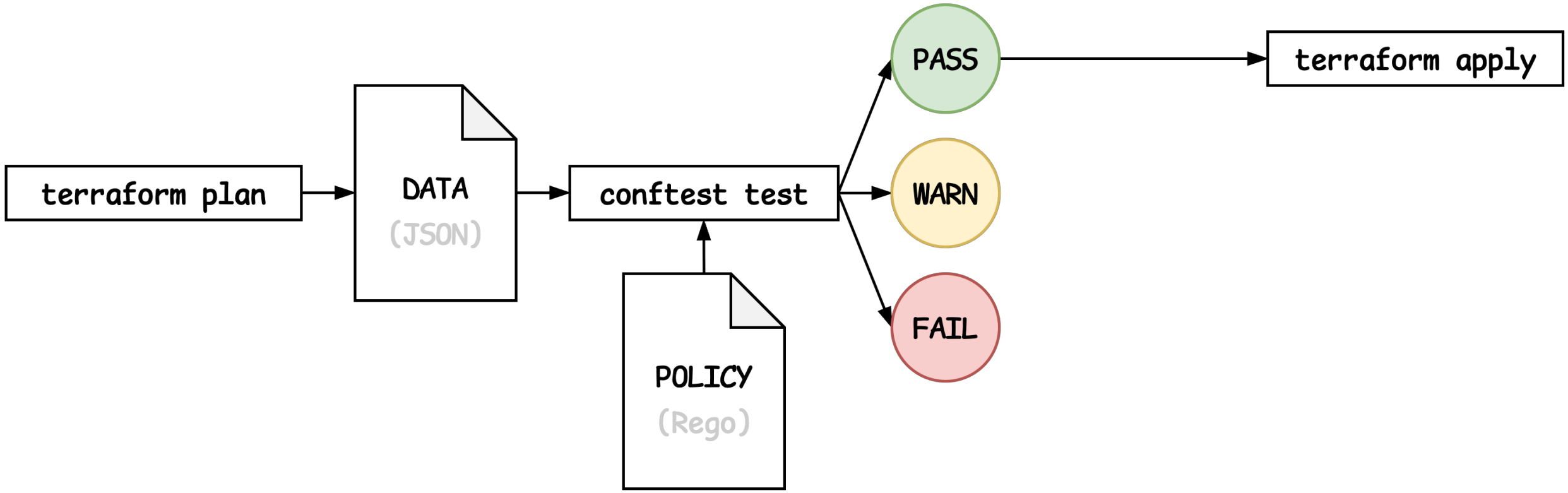
Putting it all together



© 2026 Cisco and/or its affiliates. All rights reserved.

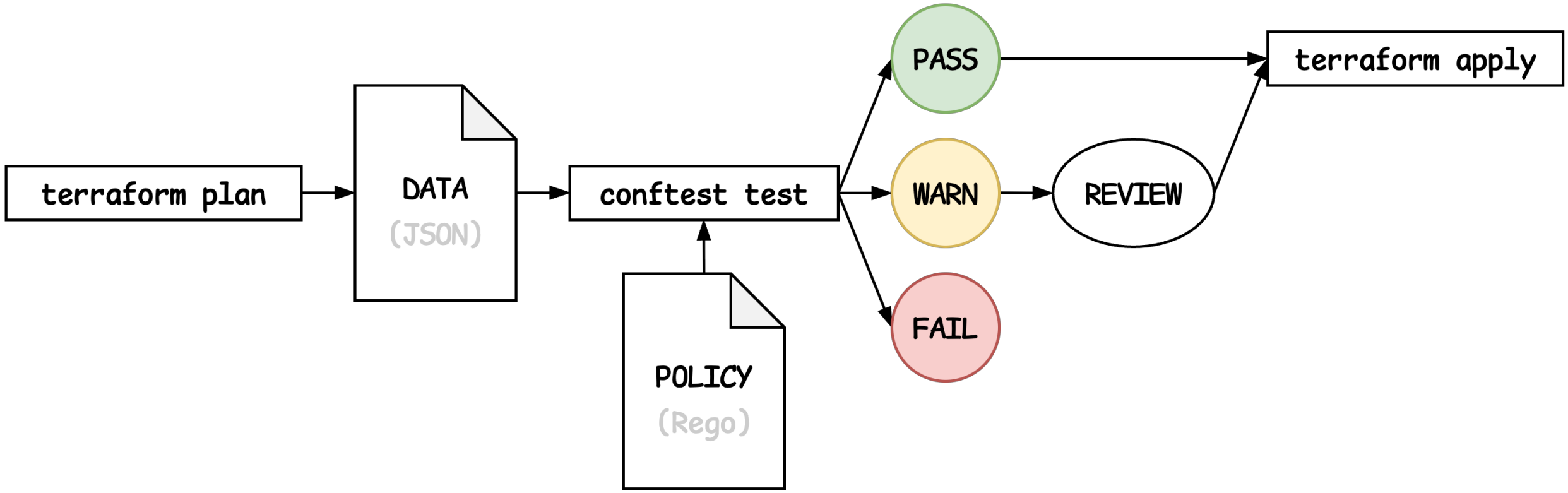
The solution

Putting it all together



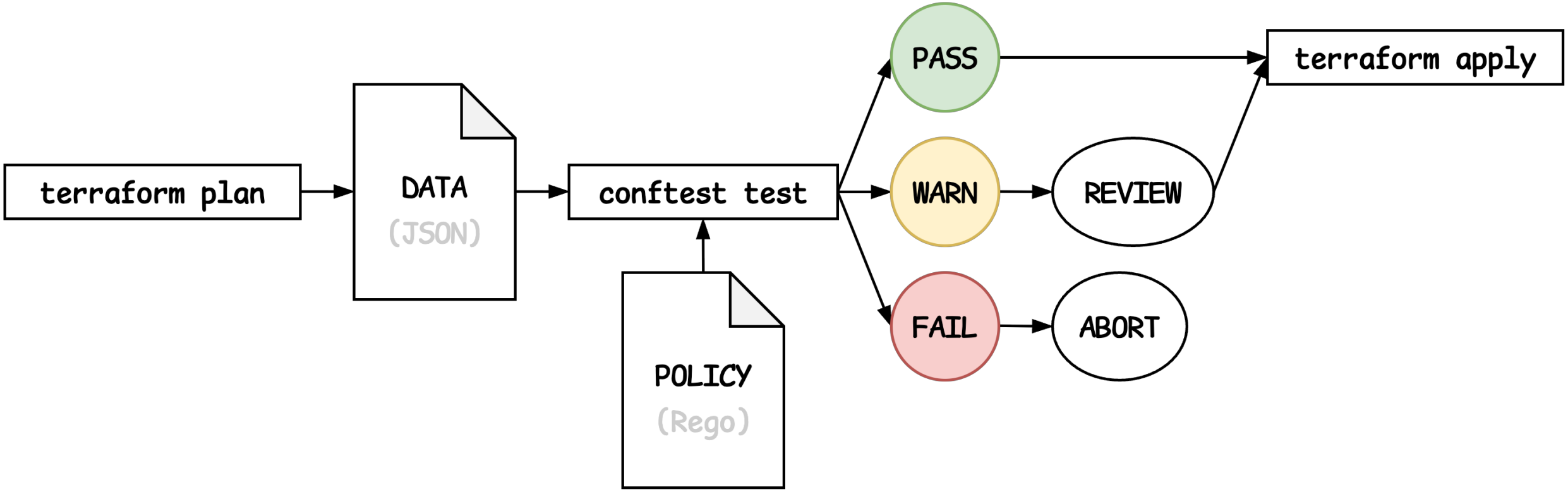
© 2026 Cisco and/or its affiliates. All rights reserved.

Putting it all together



© 2026 Cisco and/or its affiliates. All rights reserved.

Putting it all together



© 2026 Cisco and/or its affiliates. All rights reserved.

Terraform & conftest in action

Terraform plan

```
$ terraform plan -out terraform.tfplan

Terraform will perform the following actions:

  # aws_s3_bucket.one will be created
  + resource "aws_s3_bucket" "one" {
      + acl    = "private"
      + bucket = "one"
      + tags   = {
          + "Name"   = "one"
          + "Region" = "eu-west-2"
        }
        [...]
    }

Plan: 1 to add, 0 to change, 0 to destroy.
```

© 2026 Cisco and/or its affiliates. All rights reserved.

Terraform plan files are not JSON

```
$ file terraform.tfplan

terraform.tfplan: Zip archive data
```

© 2026 Cisco and/or its affiliates. All rights reserved.

Terraform plan files are not JSON but they can be

```
$ file terraform.tfplan

terraform.tfplan: Zip archive data

$ terraform show -json terraform.tfplan > terraform.tfplan.json
```

© 2026 Cisco and/or its affiliates. All rights reserved.

Terraform plan files are not JSON but they can be

and this is what they look like

```
$ file terraform.tfplan

terraform.tfplan: Zip archive data


$ terraform show -json terraform.tfplan > terraform.tfplan.json

$ jq keys < terraform.tfplan.json

[
  "applyable",
  "checks",
  "complete",
  "configuration",
  "errored",
  "format_version",
  "output_changes",
  "planned_values",
  "prior_state",
  "relevant_attributes",
  "resource_changes",
  "resource_drift",
  "terraform_version",
  "timestamp",
  "variables"
]
```

© 2026 Cisco and/or its affiliates. All rights reserved.

Terraform plan files are not JSON but they can be

and this is what they look like

```
$ jq .resource_changes < terraform.tfplan.json
[
  {
    "address": "aws_s3_bucket.one",
    "type": "aws_s3_bucket",
    "name": "one",
    "provider_name": "registry.terraform.io/hashicorp/aws",
    "change": {
      "actions": ["create"],
      "before": null,
      "after": {
        "acl": "private",
        "bucket": "one",
        "tags": {
          "Name": "one",
          "Region": "eu-west-2"
        }
      },
      "before_sensitive": false,
      "after_sensitive": false
    }
  }
]
```

© 2026 Cisco and/or its affiliates. All rights reserved.

Rego policy

```
$ cat policy.rego

package main

warn contains "The plan contains actions other than create" if {
    some resource in input.resource_changes
    some action in resource.change.actions

    not action in ["no-op", "create"]
}

deny contains "AWS S3 buckets must be created with acl = private" if {
    some resource in input.resource_changes

    resource.type == "aws_s3_bucket"
    "create" in resource.change.actions
    resource.change.after.acl != "private"
}
```

© 2026 Cisco and/or its affiliates. All rights reserved.

Example 1

```
$ terraform show terraform.tfplan

Terraform will perform the following actions:

  # aws_s3_bucket.one will be created
  + resource "aws_s3_bucket" "one" {
      + acl    = "private"
      + bucket = "one"
      + tags   = {
          + "Name"   = "one"
          + "Region" = "eu-west-2"
        }
        [...]
    }

Plan: 1 to add, 0 to change, 0 to destroy.
```

© 2026 Cisco and/or its affiliates. All rights reserved.

Terraform & conftest in action

Pass!

(safe to auto-apply)

```
$ terraform show terraform.tfplan

Terraform will perform the following actions:

  # aws_s3_bucket.one will be created
  + resource "aws_s3_bucket" "one" {
      + acl    = "private"
      + bucket = "one"
      + tags   = {
          + "Name"   = "one"
          + "Region" = "eu-west-2"
        }
        [...]
    }

Plan: 1 to add, 0 to change, 0 to destroy.

$ conftest test --policy policy.rego terraform.tfplan.json

2 tests, 2 passed, 0 warnings, 0 failures, 0 exceptions
```

© 2026 Cisco and/or its affiliates. All rights reserved.

Example 2

```
$ terraform plan -out terraform.tfplan

Terraform will perform the following actions:

  # aws_s3_bucket.one will be updated in-place
  ~ resource "aws_s3_bucket" "one" {
      ~ object_lock_enabled = false -> true
        [...]
    }

  # aws_s3_bucket.two will be created
  + resource "aws_s3_bucket" "two" {
      + acl    = "private"
      + bucket = "two"
      + tags   = {
          + "Name"   = "two"
          + "Region" = "eu-west-2"
        }
        [...]
    }

Plan: 1 to add, 1 to change, 0 to destroy.
```

© 2026 Cisco and/or its affiliates. All rights reserved.

Warn!

(review before apply)

```
$ terraform plan -out terraform.tfplan

Terraform will perform the following actions:

  # aws_s3_bucket.one will be updated in-place
  ~ resource "aws_s3_bucket" "one" {
      ~ object_lock_enabled = false -> true
        [...]
    }

  # aws_s3_bucket.two will be created
  + resource "aws_s3_bucket" "two" {
      + acl    = "private"
      + bucket = "two"
      + tags   = {
          + "Name"   = "two"
          + "Region" = "eu-west-2"
        }
        [...]
    }

Plan: 1 to add, 1 to change, 0 to destroy.

$ conftest test --policy policy.rego terraform.tfplan.json

WARN - The plan contains actions other than create

2 tests, 1 passed, 1 warnings, 0 failures, 0 exceptions
```

© 2026 Cisco and/or its affiliates. All rights reserved.

Example 3

```
$ terraform plan -out terraform.tfplan

Terraform will perform the following actions:

  # aws_s3_bucket.three will be created
  + resource "aws_s3_bucket" "three" {
      + acl    = "public-read"
      + bucket = "three"
      + tags   = {
          + "Name"   = "three"
          + "Region" = "eu-west-2"
        }
        [...]
    }

Plan: 1 to add, 0 to change, 0 to destroy.
```

© 2026 Cisco and/or its affiliates. All rights reserved.

Fail!

(not safe to apply)

```
$ terraform plan -out terraform.tfplan

Terraform will perform the following actions:

  # aws_s3_bucket.three will be created
  + resource "aws_s3_bucket" "three" {
      + acl    = "public-read"
      + bucket = "three"
      + tags   = {
          + "Name"   = "three"
          + "Region" = "eu-west-2"
        }
        [...]
    }

Plan: 1 to add, 0 to change, 0 to destroy.

$ conftest test --policy policy.rego terraform.tfplan.json

FAIL - AWS S3 buckets must be created with acl = private

2 tests, 1 passed, 0 warnings, 1 failures, 0 exceptions
```

© 2026 Cisco and/or its affiliates. All rights reserved.

Our setup

© 2026 Cisco and/or its affiliates. All rights reserved.

Our setup



Scaling Terraform at ThousandEyes (2023)

© 2026 Cisco and/or its affiliates. All rights reserved.

Our setup



165k resources

2.9k states

10k ops/day

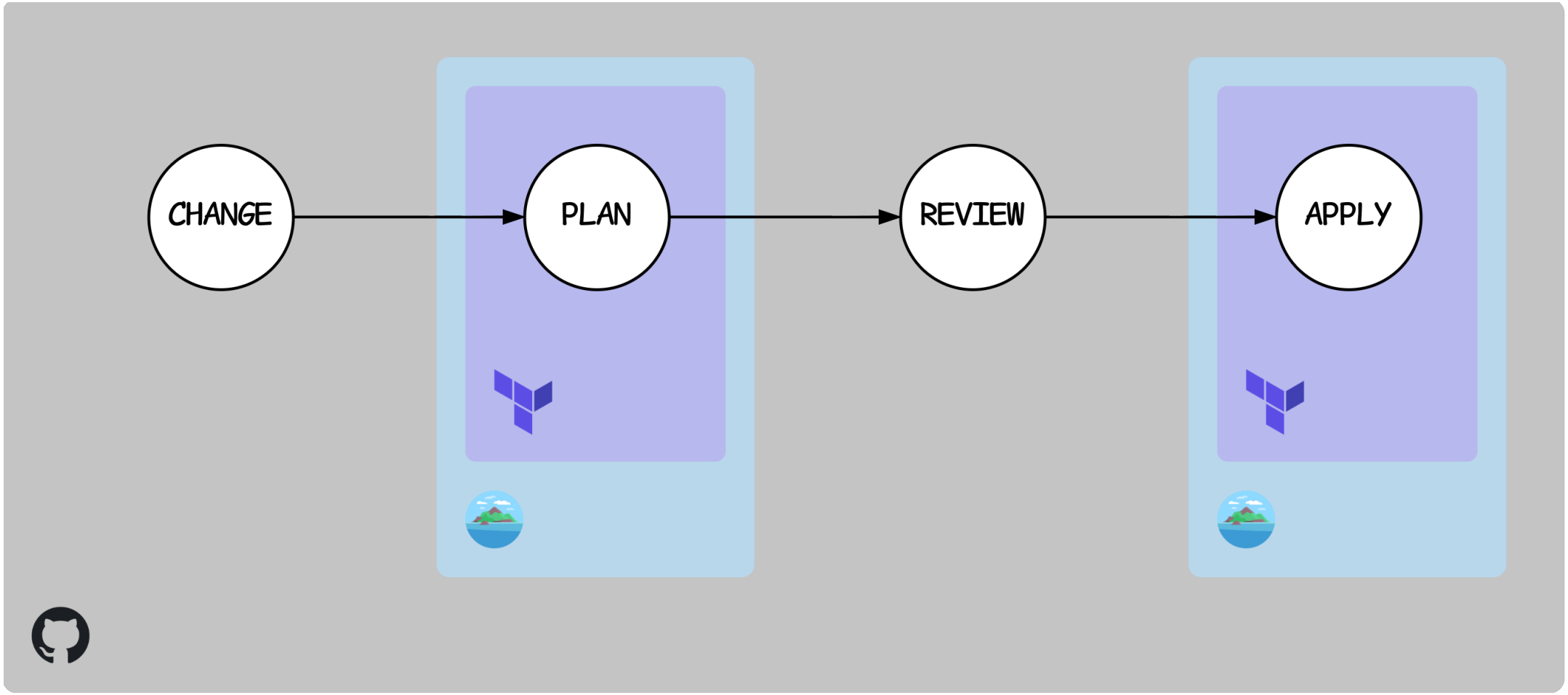
Scaling Terraform at ThousandEyes (2023)

© 2026 Cisco and/or its affiliates. All rights reserved.

Our workflow

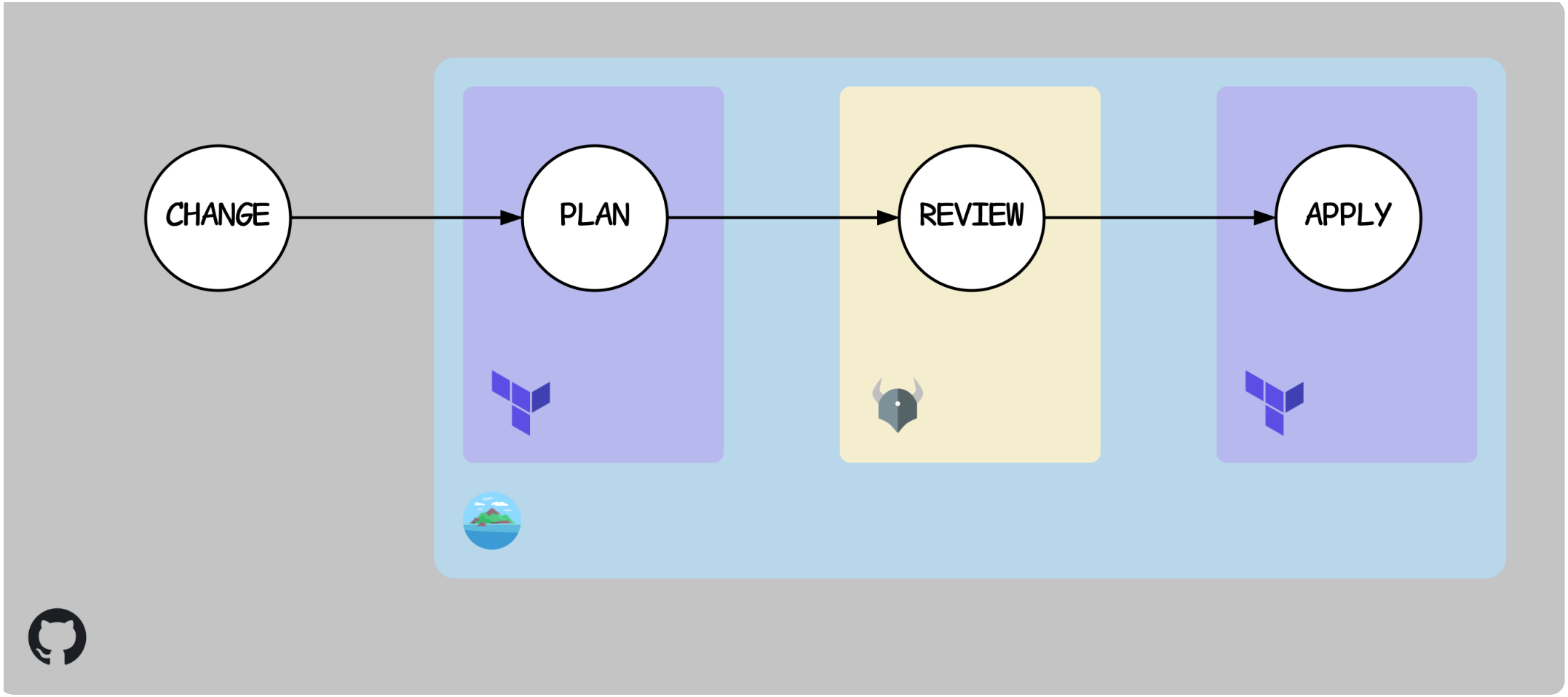
© 2026 Cisco and/or its affiliates. All rights reserved.

Our workflow



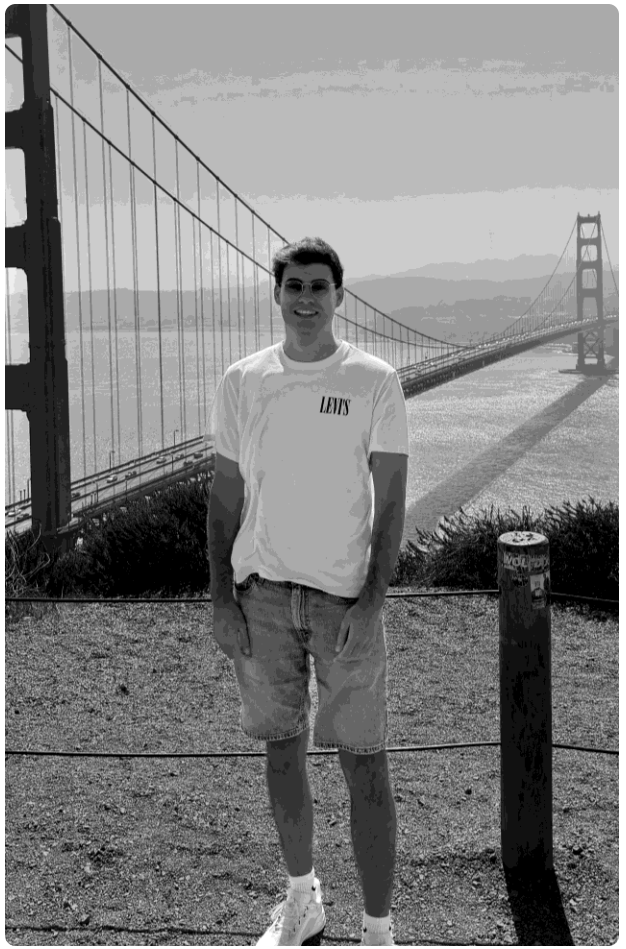
© 2026 Cisco and/or its affiliates. All rights reserved.

Our workflow with conftest



© 2026 Cisco and/or its affiliates. All rights reserved.

Safe Terraform auto-apply with conftest





Join our team!

careers.cisco.com

Josep Medialdea
Senior Site Reliability Engineer

linkedin.com/in/josepmedialdea

Ricard Bejarano
Lead Site Reliability Engineer

linkedin.com/in/ricardbejarano

© 2026 Cisco and/or its affiliates. All rights reserved.