

Codified cloud security platform



Bridgecrew's developer-first platform provides security and compliance coverage for infrastructure as code (IaC) as well as cloud resources and workloads in runtime.

Run #65421 Failed!
Scanned 3 resources, 3 errors were found.

COMMIT FIXES

BACK feature-24 > master #284 3e859e8 N.Uhura 30 Jan 2021 4:43 PM

/s3.tf MORE SUPPRESS FIX

```

resource "aws_s3_bucket" "b" {
  5 5   versioning {
  6 6     enabled = false
  7 7   }
  8 +   server_side_encryption_configuration {
  9 +     rule {
 10 +       apply_server_side_encryption_by_default {
 11 +         sse_algorithm = "AES256"
 12 +       }
 13 +     }
 14 +   }
 15 }
  
```

HIGH Ensure all data stored in the S3 bucket have versioning enabled

/s3.tf MORE SUPPRESS FIX

```

resource "aws_s3_bucket" "b" {
  5 5   acl = "private"
  6 6
  7 7   versioning {
  8 +     enabled = false
  9 +     enabled = true
  
```

HIGH Ensure all data stored in the S3 bucket have versioning enabled

Errors by Benchmark

Benchmark	Failed	Passed	Suppressed
NIST-800-53	141	248	3
SOC2	97	124	4
CIS KUBERNETES	93	54	23
PCI-DSS V3.2	81	24	12
HIPAA	80	29	0

aws:ec2:us-west-2:563645614897:security-group/sg-03bcf...

Name "eksctl-eks1-node-... Description "Communication... VPC Id "vpc-...

Ingress [{"cidr_blocks":["0... Egress [{"cidr_blocks":["0.0.0... Partition

Related Resources:

Dependents

aws:ec2:us-west-2:563645614897:instance/i-00e78c6054dbf34c1 vpc-sec...

Depends on

aws:eks:us-west-2:563645614897:cluster/eks1 tags.alpha.eksctl.io/ci/...

Resource History:

- bc Error Detected Ensure security groups have an owner tag
- bc Resource Modified _partition
- bc Error Suppressed Ensure taggable resources are tagged
- bc Error Detected Ensure taggable resources are tagged
- bc Initial scan egress ingress name +5



100s of built-in policies

Powered in-part by Checkov, our open-source IaC static analysis tool, Bridgecrew comes pre-built with 500+ community-backed policies across the major cloud providers.

With Bridgecrew, policies can be enforced throughout the development lifecycle, from development on local workstations to running resources in production.



Security and beyond

Policies map to security best practices as defined by the Center for Internet Security (CIS) as well as compliance benchmarks such as SOC 2, HIPAA, GDPR, and more.

In addition to providing security and compliance guardrails, policies also help teams enforce infrastructure development best practices such as resource versioning and logging.



Security-as-code fixes

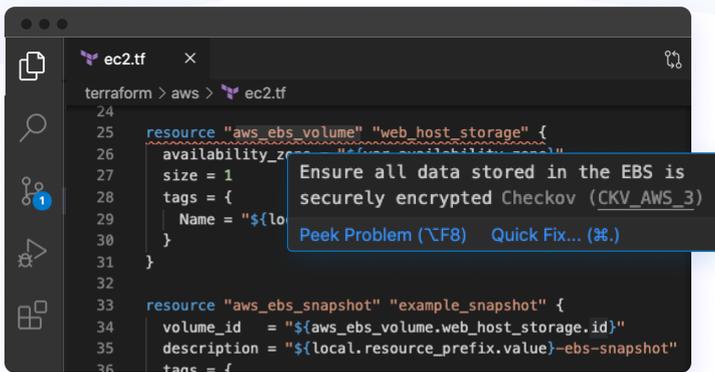
For each policy violation, Bridgecrew provides context-aware insight into its potential impact as well as rationale and documentation behind the error.

To make feedback as actionable as possible, Bridgecrew also provides security-as-code fixes via pull requests in build-time and automated remediations in runtime.

Embedded DevSecOps workflows



For automated and continuous feedback, Bridgecrew embeds into the tools and processes you already depend on to write, manage, test, and deploy your infrastructure.



Fast, pre-commit feedback

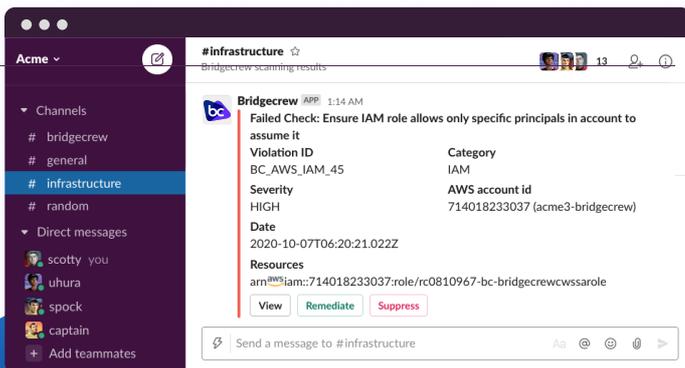
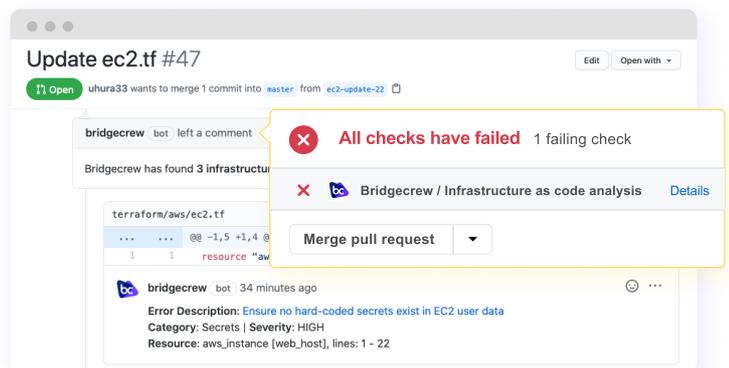
Scan IaC files and directories for misconfigurations pre-commit with Bridgecrew CLI or enforce guardrails as you code with Bridgecrew's IDE extensions.

Bridgecrew empowers developers to move fast by surfacing security and compliance feedback before code gets integrated into shared repositories.

Continuous code reviews

Prevent misconfigurations from being deployed by getting feedback on each commit, pull/merge request, or as part of your CI/CD pipeline.

Bridgecrew integrates with version control systems and CI/CD providers to continuously and automatically scan all IaC changes for errors.



Real-time notifications

Get alerted as soon as new errors are identified with real-time notifications and get a birds-eye view of your cloud security posture with weekly email updates.

Bridgecrew also integrates with tools such as Jira to open tickets that include the metadata, rationale, and code needed to fix errors wherever they are.



Cloud drift detection

Monitor cloud resources in runtime for drift from pre-defined IaC configuration.



IAM right-sizing

Analyze IAM for overly permissive roles and implement right-sized configuration.



Custom policies

Define and enforce your own infrastructure policies with Bridgecrew's no-code or YAML policy creator.



Security-as-code fixes

Transform runtime errors into secure and compliant infrastructure configuration.