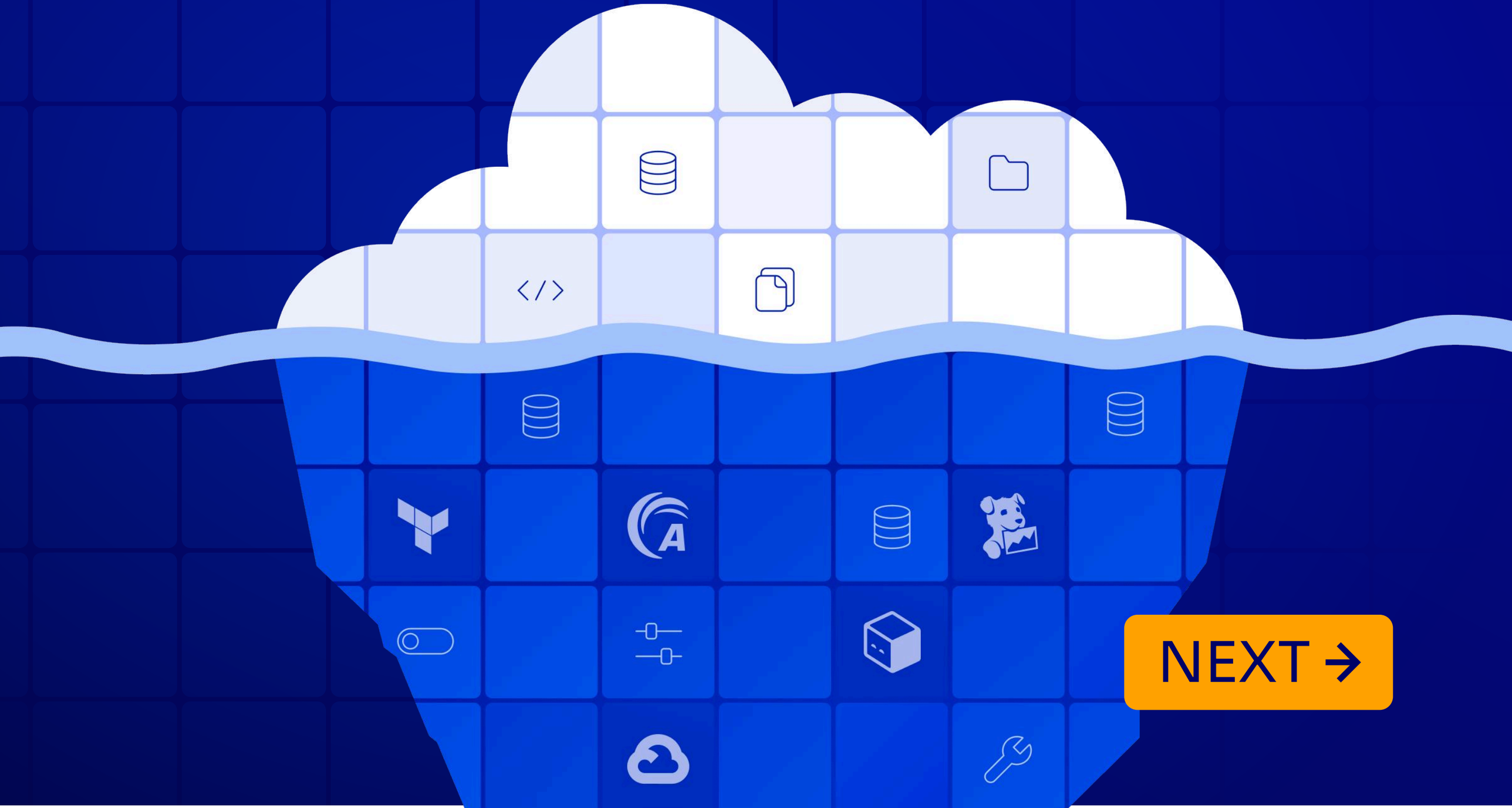
Control Monkey

The Disaster Recovery Iceberg

What your DR plan protects vs. what recovery actually requires



NEXT →

What most DR plans protect

- Data
- VM snapshots
- Storage replication
- Application failover

This is the part most teams can see, measure, and test.

NEXT →

But DR often misses configuration

- Cloud configuration
- IAM policies
- DNS records
- Network routing
- Load balancer settings
- Security groups

Your data can be safe.

But the environment needed to run it may not be **recoverable.**

NEXT →

Why DR visibility breaks

- Changes happen outside backup tools
- Resources are created manually
- SaaS settings drift over time
- DNS, IAM, and network rules change constantly
- No known-good restore point

When configuration changes everywhere, DR plans lose track of what needs to be restored.

NEXT →

Where recovery slows down

Incident

Configuration lost or changed

DNS

IAM

DB

Routes

?

Known-Good State

Back to operations

```
$ restore config
$ validate dependencies
$ recover
```

What changed?

What should be restored first?

What depends on it?

NEXT →

Most DR plans protect the visible layers

Traditional DR protects:
Data ▪ Apps

But operations also depend on:

- Identity
- Networking
- SaaS
- Dependencies
- More

Traditional backup restores data.

ControlMonkey restores the configuration required for operations.

NEXT →

Where does your DR visibility end?

ControlMonkey brings disaster recovery to Cloud and SaaS configuration.

- Discover what's missing
- Back up configuration continuously
- Version every change
- Restore known-good states
- Track DR readiness