INFOGRAPHIC

DevOps Teams: Beware the Security Risk of CLOUD ZOMBIES

The number one cause of data breaches in the cloud is misconfiguration. Yet, zombie cloud resources, by definition, are not tracked by cloud and security teams, posing real security misconfiguration risk.

WHAT ARE CLOUD ZOMBIES?
(or should we say what are they *not?*)

Zombie cloud resources are:

- not included in your management and security tools
- not scanned for misconfiguration vulnerabilities
- not patched with the latest security updates
- not validated for compliance
- not cycled out via immutable infrastructure practices

SO, HOW DO YOU FIX THEM?

1. ESTABLISH VISIBILITY

Find a tool that gives you full and continuous cloud visibility.

Utilize visual diagrams of your environments to help identify zombies.

2. IDENTIFY AND TERMINATE

3. ENFORCE TAGS

Use tags to track and manage cloud resources and establish effective tagging conventions to enforce them.

Adopting an infrastructure as code tool and automated pipelines will track resource modifications, even outside of your pipeline.

4. EMBRACE INFRASTRUCTURE AS CODE & AUTOMATED PIPELINES

5. INCLUDE DEV INTO YOUR SECURITY

Dev environments can pose a security risk to production infrastructure and data, so build them into security plans without undue restrictions.

Perform steps 1 through 5 (including orphaned/zombie resources) and the audits and compliance reporting you're already doing will be much easier.

6. CONDUCT AUDITS AND REPORTING

BOTTOM LINE:

If you have AWS, Azure, or GCP environments running at scale, you should assume the presence of zombie resources. Eliminating and preventing them will improve your security posture and save you money, not to mention when cloud security is done correctly, it usually improves your bottom line.

Learn how Fugue provides autonomous cloud security and compliance to protect against cloud misconfiguration at www.fugue.co.