Armor Approach

Infrastructure-as-Code (IaC)

Armor uses IaC to manage the setup and ongoing maintenance of your environment – enabling full transparency, quality, and empowering organizations' digital transformations.

Why Armor uses an Infrastructure-as-Code (IaC) Approach

- Allows for security best practices to be built-in, rather than reconfigured for every customer environment
- Modularity ensures that we deploy predictable, repeatable, and thoroughly-tested infrastructure components and configurations
- Integrates well with CI/CD pipelines and promotes DevSecOps culture
- Allows for static analysis and simplified review of the code (as opposed to taxing reviews or audits of infrastructure)
- Ensures complete provider transparency and customer ownership

Cornerstone Technologies

Terraform

The de facto standard for modern cloud-native infrastructure management.

Terragrunt

An open source (MIT) wrapper for Terraform that provides extra tools for keeping Terraform code DRY, working with multiple Terraform modules, and managing remote state.

GitHub

The most widely-used version control and collaboration platform and has a host of useful features for managing and deploying infrastructure code. (optional)

ARMOR

Source Code Ownership Model

Infrastructure-as-Code Library

SIEM Rules, Schemas, and Parsers

Threat Intel & Enrichment

Owned and managed by Armor

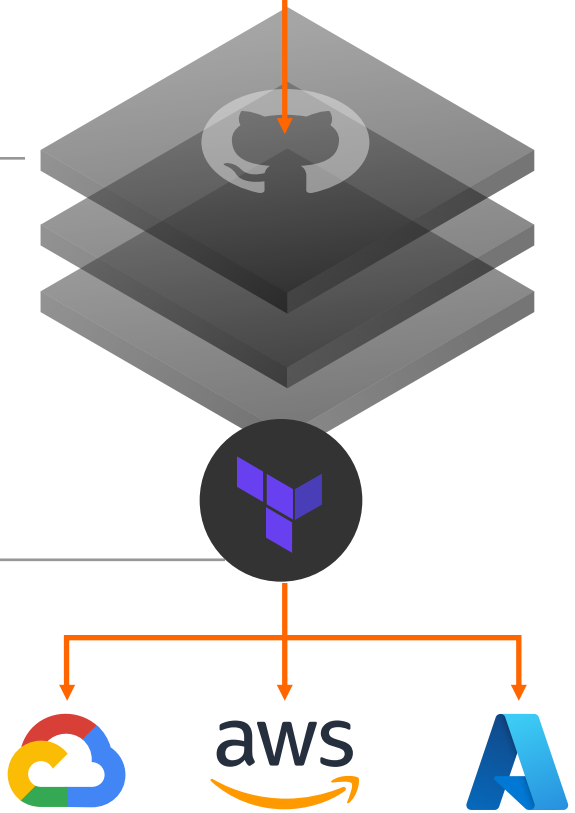
Source Code Ownership

As new or updated content is published by Armor, you'll automatically get updates pushed to your source control system, and you'll retain ownership of this code even if you decide not to renew your subscription.

This is critical if you want to avoid vendor (MSP/MSSP) lock-in, if you're servicing sub-accounts that need severability, or will be in-sourcing SOC capabilities in the future.

Automated Deployments

Stay up-to-date with the latest detection and correlation capabilities while maintaining control over and ownership of your environment – the best of both worlds.



Owned by you — managed by Armor

ARMOR

Security and Quality Controls

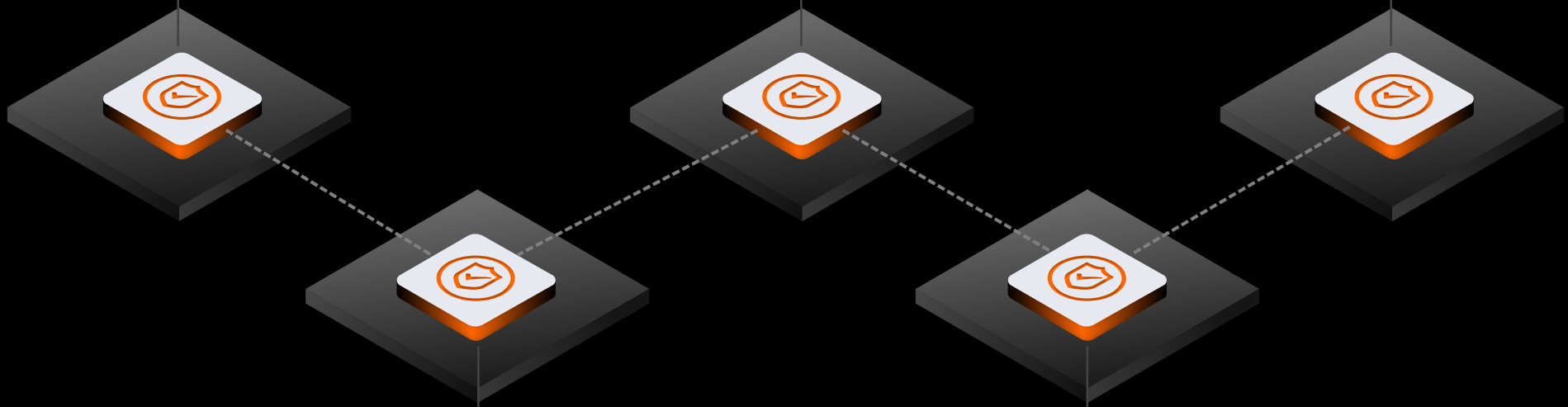
Continuous Integration Checks

Every change is pushed to source control is automatically checked against security best practices and functional tests.

Regression Test Suite

Once infrastructure or content library updates have been reviewed, they are deployed to our regression testing environment and a full suite of automated tests are performed.

Updates Deployed to Your Environment



Human Code Review

Every change set is reviewed by a subject matter expert for security and stability before being merged into the codebase.

Customer Change Management

If required by your internal policies, an additional review step may be added to the workflow to accommodate your change management process.

ARMOR