Unified Control in Multi-Cloud Environments

Subject: Eliminating Configuration Drift via Immutable Infrastructure

1. Summary

As enterprises scale across AWS, Azure, and GCP, managing different security models leads to Configuration Drift. This whitepaper advocates for a Cloud-Agnostic Abstraction Layer to eliminate drift by enforcing immutable Infrastructure as Code (IaC) and global policy synchronization. This ensures compliance and 99.99% consistency across environments.

2. The Infrastructure Problem: The "Drift" Trap

Multi-cloud strategies offer redundancy and flexibility, but they introduce a "Tower of Babel" problem. Each cloud provider uses different APIs, security primitives, and IAM structures.

When operations teams manually tweak settings or use disparate tools for each cloud, **Configuration Drift** inevitably occurs. This drift creates two severe risks:

- **Security Gaps:** A firewall rule patched in AWS might be missed in Azure, leaving a silent vulnerability open to attackers.
- **Downtime:** Inconsistent configurations between primary and failover regions lead to deployment failures during critical recovery moments.

Legacy tools that rely on "post-deployment scanning" are insufficient; they detect the problem only *after* the vulnerability is already live.

3. Senrysa Solution: A Cloud-Agnostic Abstraction Layer