

# DYNAMIC PERMISSIONING PLATFORM FOR AMAZON WEB SERVICE (AWS)

## AWS PRIVILEGE SECURITY IS COMPLEX

- Security and administration are not handled by IT or Security
- Missing complete visibility into who has what level of access and how it's being used
- Static privilege levels expose AWS environments to higher risk of security breaches
- Existing privileged access products are unavailable to typical business users
- Existing threat monitoring solutions fall short of providing necessary identity and policy context for user activities



## SECURE AWS WITH CLOUD PRIVILEGE ACCESS GOVERNANCE

### Dynamic Permissioning

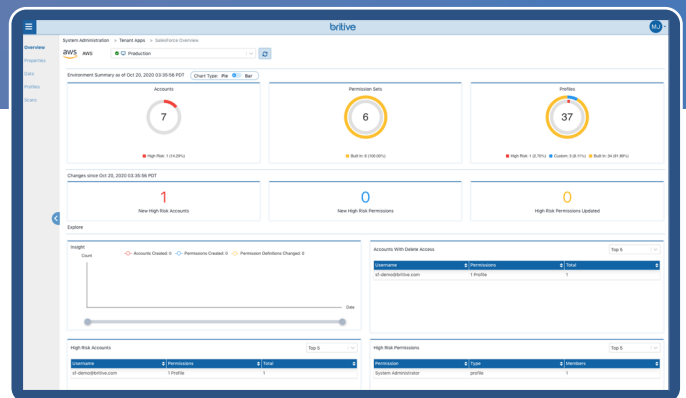
- Automated granting and expiration of Just In Time (JIT) permissions
- Maintenance of Zero Standing Privileges (ZST)
- Centralized and scalable management of human and machine ID's

### Least Privilege Enforcement

- Privilege right sizing
- Discover and elimination of excess privileges
- Reduction of attack surface

### Secrets Governance

- Automated granting of dynamic secrets for human and human and machine processes



### Cross-Cloud Discovery

- Single pane of glass cross cloud (x-cloud)
- Automated discovery and auditing of accounts and privileges
- Reporting from a unified x-cloud access model

### Proactive Monitoring

- Analysis of access changes and policy drift
- Identification of risky behavior
- Post incident investigation of identity-based incidents

