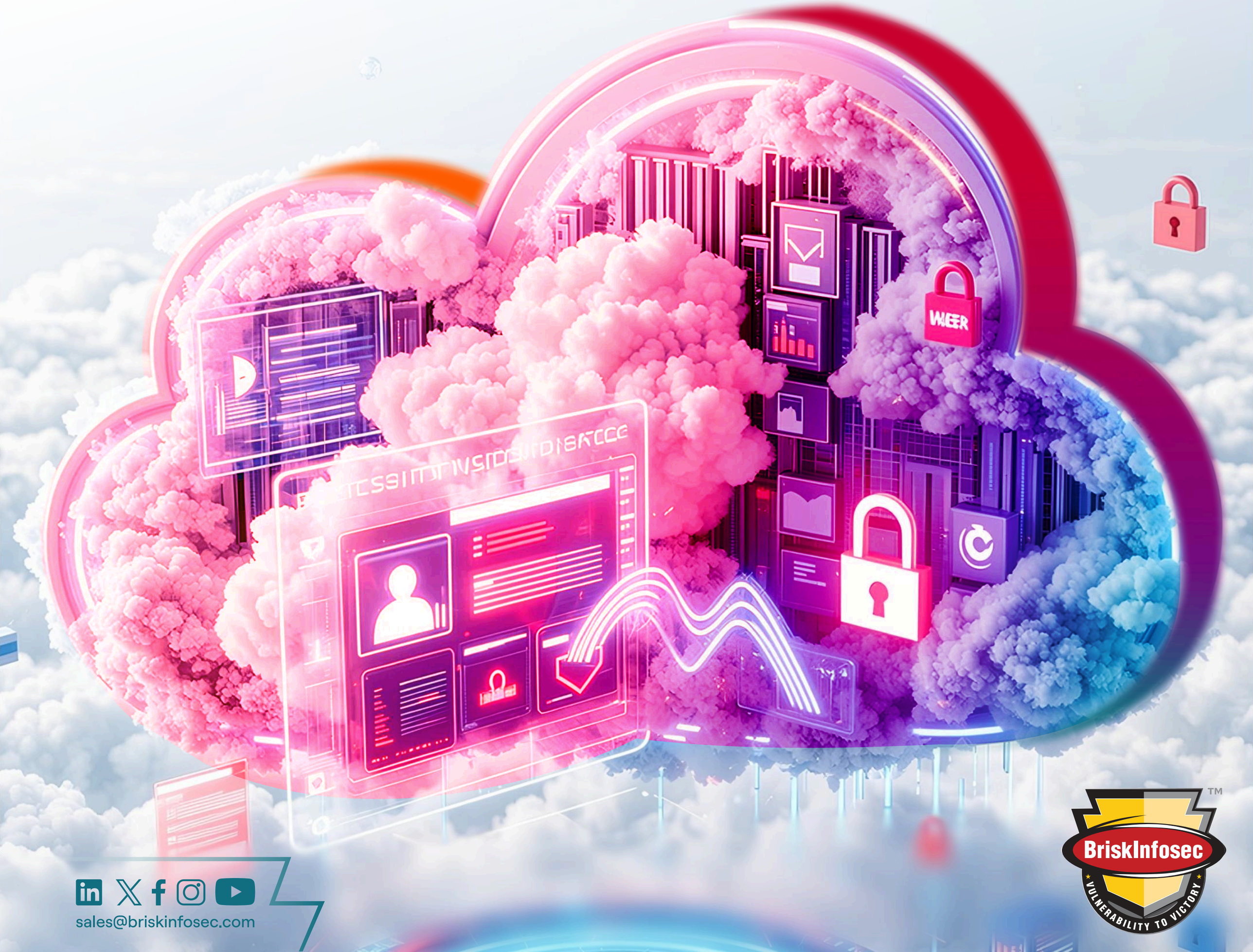
5 Things to Follow When Using Multi-Cloud Security

CREST Accredited

certin Empanelled



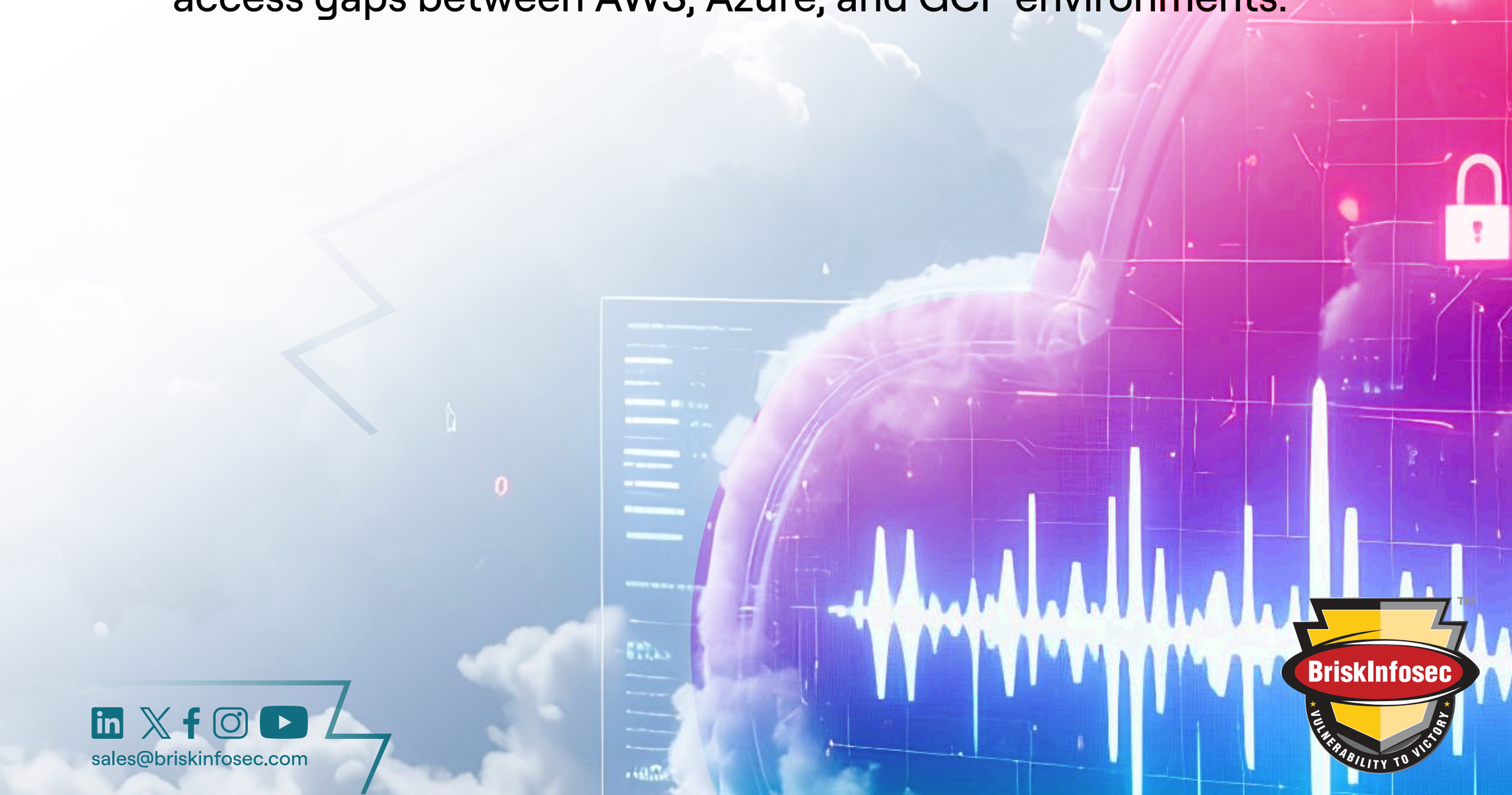
sales@briskinfosec.com

BriskInfosec™

VULNERABILITY TO VICTORY

Establish Unified Identity & Access Management (IAM)

- Implement a centralized IAM strategy across all cloud platforms.
- Use single sign-on (SSO) and multi-factor authentication (MFA) consistently.
- Map user roles and permissions uniformly to prevent access gaps between AWS, Azure, and GCP environments.



sales@briskinfosec.com

Deploy Cloud Security Posture Management (CSPM)

- Continuously monitor misconfigurations across all cloud environments.
- Automate compliance checks for standards like SOC 2, ISO 27001, and regulatory frameworks.
- Set up real-time alerts for policy violations and drift detection.

sales@briskinfosec.com

Implement Data Classification & Encryption Standards

CREST Accredited

certin Empanelled

- Classify data based on sensitivity levels before it moves between clouds.
- Enforce encryption-in-transit and at-rest policies uniformly.
- Maintain consistent key management practices across all platforms using cloud-native or third-party solutions.

sales@briskinfosec.com

BriskInfosec™ VULNERABILITY TO VICTORY

Create Cross-Cloud Incident Response Procedures

- Develop standardized playbooks that work across multiple cloud providers.
- Develop standardized playbooks that work across multiple cloud providers.
- Practice tabletop exercises that simulate multi-cloud security incidents to test response times and coordination.

sales@briskinfosec.com

Monitor with Centralized Security Analytics

- Deploy SIEM/SOAR solutions that aggregate logs from all cloud environments.
- Create unified dashboards for threat detection and compliance reporting.
- Establish baseline behaviors for each cloud workload to identify anomalies effectively.

sales@briskinfosec.com

Talk to Our
Security Experts

Book a Meeting

CREST. Accredited

certin Empanelled

BriskInfosec™

VULNERABILITY TO VICTORY

sales@briskinfosec.com