Secure Cloud Foundation for AWS

ADVISORY | IMPLEMENTATION

Cloud adoption creates security and compliance challenges

In today's increasingly digital world, the way a business approaches its cloud computing strategy is paramount. As an enterprise's cloud footprint grows rapidly, numerous challenges are created including:

- Storing data in a secure managed environment
- Complying with information security policies
- Maintaining central visibility and governance over data and assets
- Fulfilling compliance requirements
- Enforcing least privilege in terms of where, when and who can access data
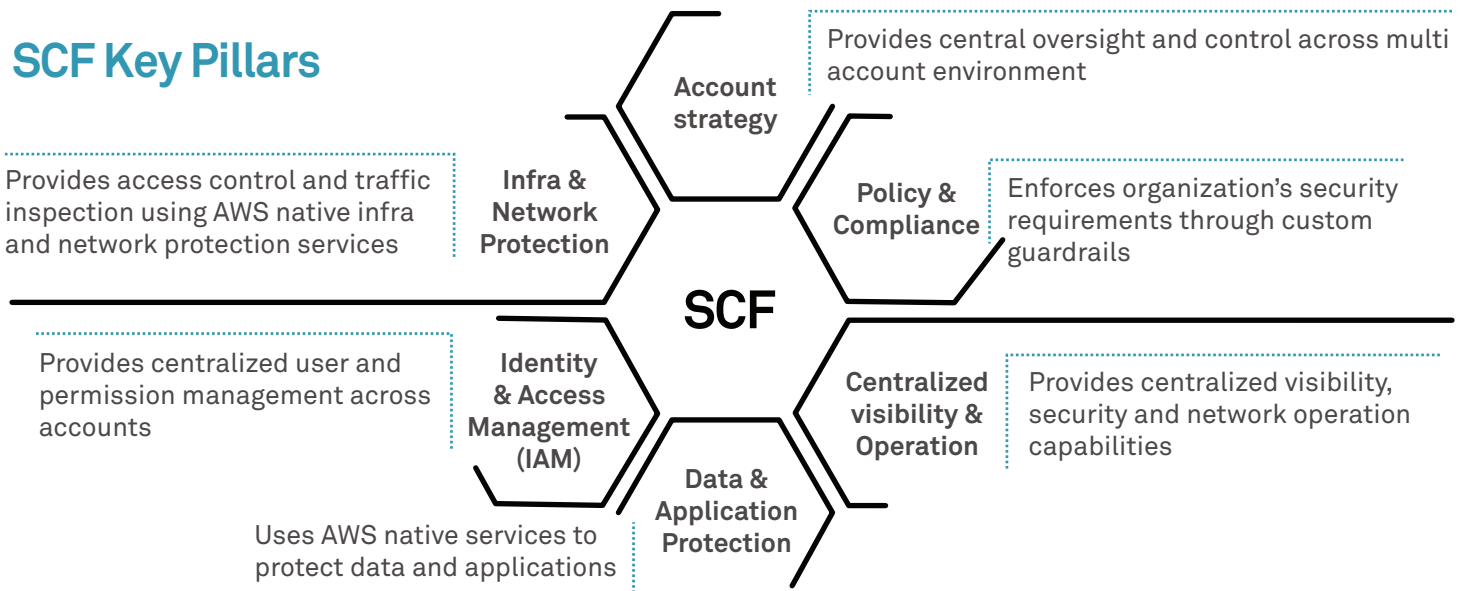
The cloud is a key enabler for business growth. In this new environment, security and compliance cannot be an afterthought.

- More than **72%*** of enterprises confirm risks due to misconfigurations or wrong setup.
- More than **46%*** of enterprises cannot validate cloud compliance. PCI DSS, HIPAA, NIST, SOC2 have penalties associated with violations.

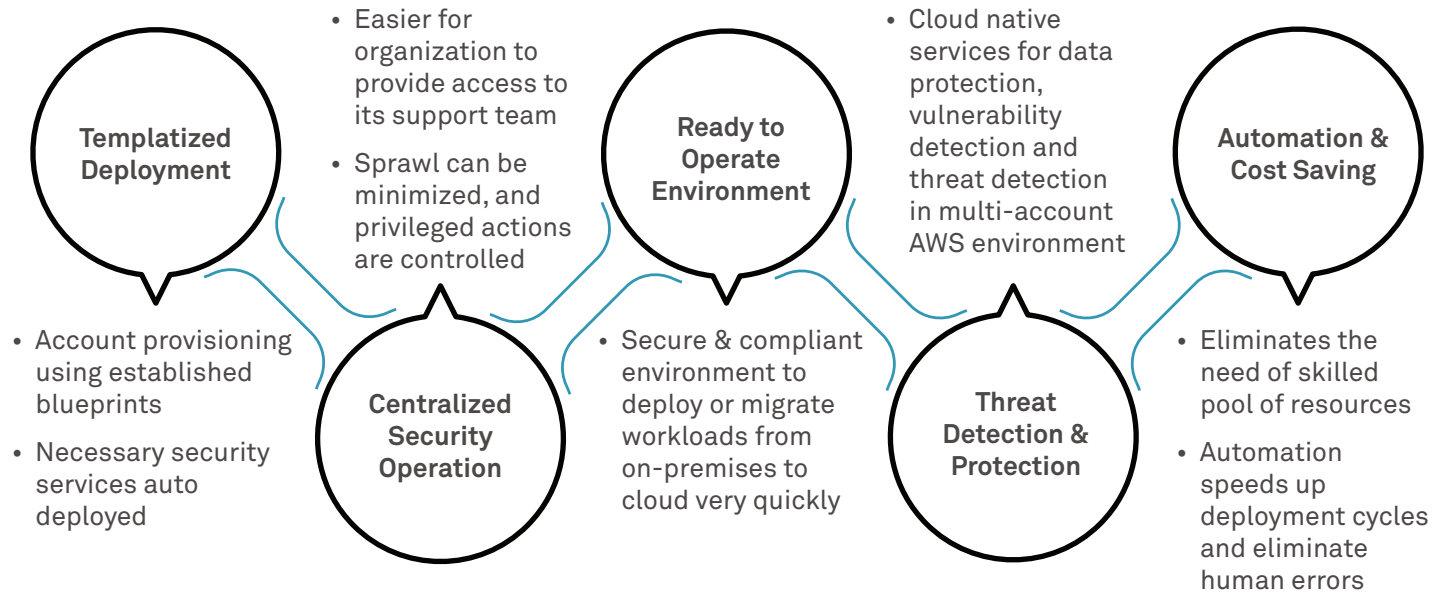## Wipro's Secure Cloud Foundation (SCF) for AWS speeds up cloud migration

Wipro's Secure Cloud Foundation for AWS accelerates the cloud adoption journey by providing a secure environment with data, application, network and infra protection capabilities. It creates a Landing Zone for the enterprise to securely deploy or migrate workloads and data. The SCF addresses the security, compliance, and identity and access requirements of an enterprise operating in an AWS multi-account environment.

SCF Key Pillars

Provides central oversight and control across multi account environment

Account strategy

Provides access control and traffic inspection using AWS native infra and network protection services

Infra & Network Protection

Policy & Compliance

Enforces organization's security requirements through custom guardrails

SCF

Provides centralized user and permission management across accounts

Identity & Access Management (IAM)

Centralized visibility & Operation

Provides centralized visibility, security and network operation capabilities

Data & Application Protection

Uses AWS native services to protect data and applications

*Source: Lacework Cloud Threat Report Vol 4

Secure Cloud Foundation (SCF) for AWS - Business benefits

Templatized Deployment

- Easier for organization to provide access to its support team
- Sprawl can be minimized, and privileged actions are controlled

- Account provisioning using established blueprints
- Necessary security services auto deployed

Centralized Security Operation

Ready to Operate Environment

- Cloud native services for data protection, vulnerability detection and threat detection in multi-account AWS environment

- Secure & compliant environment to deploy or migrate workloads from on-premises to cloud very quickly

Threat Detection & Protection

Automation & Cost Saving

- Eliminates the need of skilled pool of resources
- Automation speeds up deployment cycles and eliminate human errors

Secure Cloud Foundation (SCF) for AWS - key differentiators

- Customized preventive guardrails (20+) and detective guardrails (180+) for specific security needs
- Deployment of compliance packs in the form of config checks (PCI DSS, HIPAA, FedRAMP, CIS) to quickly adhere to compliance standards
- Customized permission sets deployment and integration with third party identity stores for access provisioning to AWS multi-account environment
- Deployment of AWS native security services for sensitive data identification, threat detection, vulnerability management
- Centralized east-west and north-south traffic inspection capabilities

Connect with us to get started

To learn more about how Wipro can help your organization attain a secure cloud foundation, please contact us at: **wipro.com/cybersecurity/#contact-us**

Siva VRS
Vice President & Global Head
Cloud & Infra Security

Bhaveshkumar Bhatt
General Manager & Practice Head
Cloud Security

wipro | CyberSecurity by CyberSecurists.