Securing the Cloud: A Data-Driven Approach

Data Classification

Organize data based on sensitivity and business impact

Implement appropriate security controls and access restrictions for different data classifications

Ensure compliance with industry regulations

Correctly identify and protect regulated data to avoid penalties and security breaches

Leverage automated classification tools

Scan, tag, and categorize structured and unstructured data based on predefined security policies

Integrate classification with encryption

Apply automated encryption policies to restricted and confidential data

Effective data classification enhances security, optimizes access management, and ensures regulatory compliance in cloud environments.

Identity and Access Management (IAM)

- **Authentication**

  Verification of user identity through passwords, biometrics, tokens, or multi-factor authentication (MFA).

- **Authorization**

  Definition of access rights based on predefined security policies to ensure users only have access to needed resources.

- **User Lifecycle Management**

  Control over user creation, modification, and removal across an organization's IT infrastructure to prevent orphan accounts.

- **Privileged Access Management (PAM)**

  Enhanced controls over high-privilege accounts to prevent exploitation, including monitoring and restricting administrative access.

- **Federated Identity Management**

  Integration with single sign-on (SSO) and identity federation for seamless cross-system authentication.

Access Policies

Discretionary Access Control (DAC)

Users control access permissions to data and resources.

Mandatory Access Control (MAC)

System-enforced access policies based on predefined security rules.

Role-Based Access Control (RBAC)

Access granted based on job roles and responsibilities within the organization.

Attribute-Based Access Control (ABAC)

Access decisions made based on user attributes such as department, location, and time.

Access policies are critical for preventing unauthorized access and ensuring regulatory compliance in cloud environments.

Encryption and Key Management

- **Data Encryption**

  Transforming data into unreadable format to ensure confidentiality

- **Encryption at Rest**

  Protecting stored data with encryption

- **Encryption in Transit**

  Securing data during transmission

- **End-to-End Encryption (E2EE)**

  Ensuring data remains encrypted from sender to recipient

- **Cloud-native Key Management**

  Using cloud services to securely store and manage cryptographic keys

- **Key Rotation Policies**

  Automatically rotating encryption keys on a regular basis

- **Restricted Key Access**

  Controlling access to cryptographic keys using IAM policies and Hardware Security Modules (HSMs)

Data Loss Prevention (DLP)

- **Content Inspection**

  Detect and identify sensitive data within documents, emails, and other content

- **Endpoint DLP**

  Prevent data leaks and unauthorized transfers from employee devices

- **Cloud DLP**

  Monitor and protect data stored in cloud environments

- **Automated Scanning**

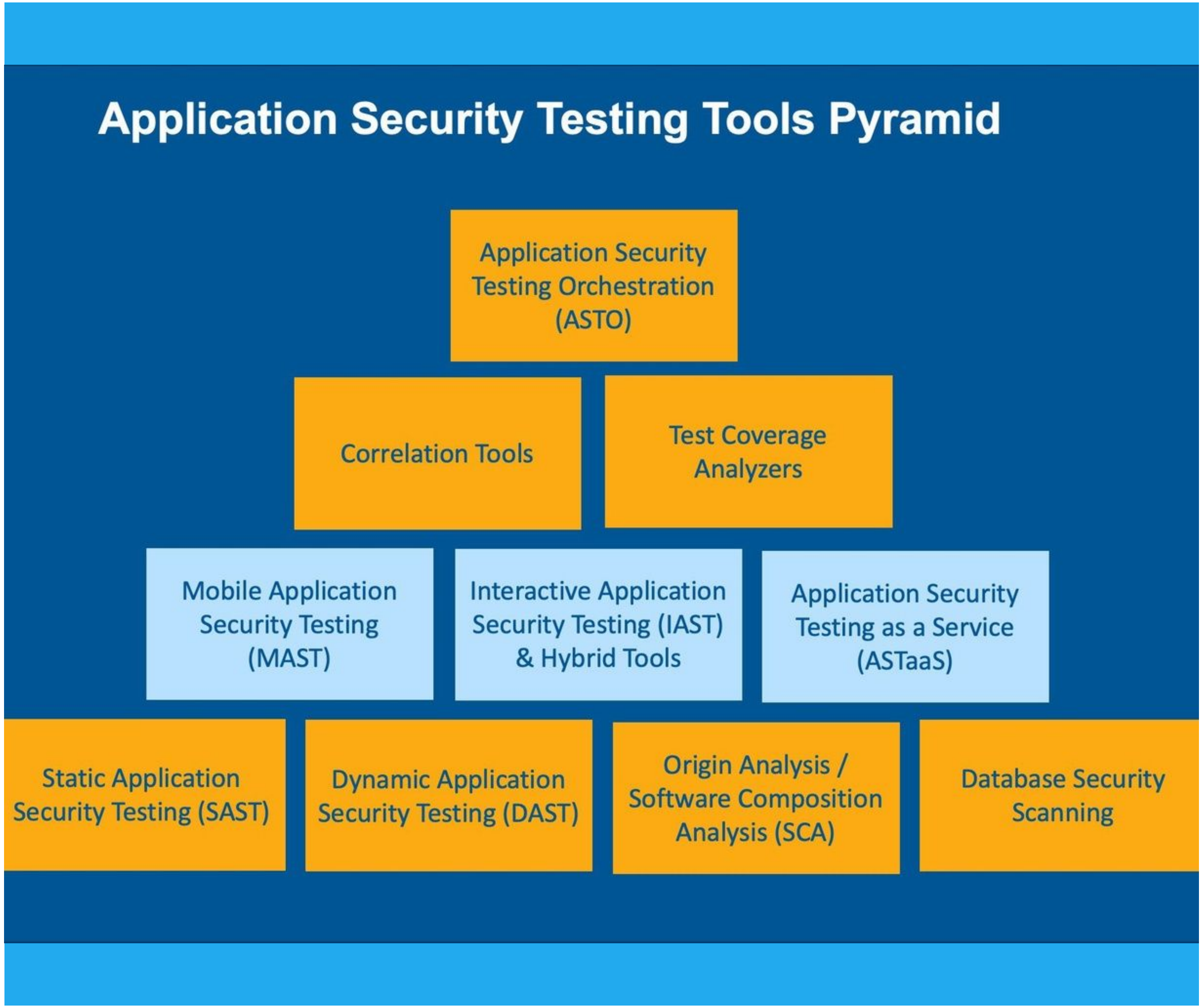
  Deploy tools to continuously scan for sensitive data and policy violations

- **Clear DLP Policies**

  Establish well-defined data loss prevention policies to guide employee behavior

- **Real-time Monitoring**

  Implement real-time monitoring and alerting to detect and respond to potential data leaks



Application Security Testing Tools Pyramid

Application Security Testing Orchestration (ASTO)

Correlation Tools

Test Coverage Analyzers

Mobile Application Security Testing (MAST)

Interactive Application Security Testing (IAST) & Hybrid Tools

Application Security Testing as a Service (ASTaaS)

Static Application Security Testing (SAST)

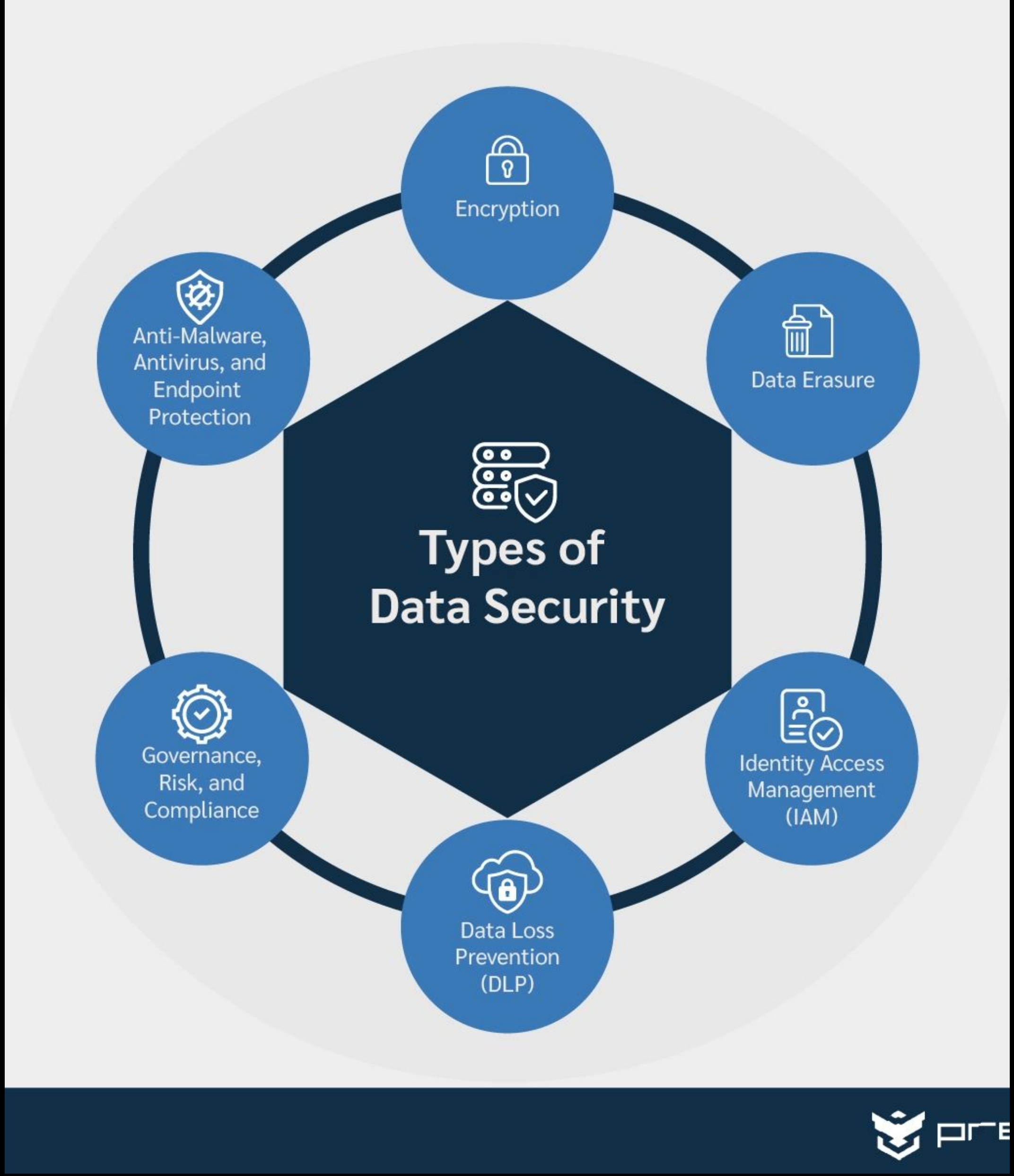
Dynamic Application Security Testing (DAST)

Origin Analysis / Software Composition Analysis (SCA)

Database Security Scanning

Conclusion

Data security is a critical aspect of cloud computing, involving various tools and techniques to protect digital information from unauthorized access, corruption, theft, and loss. These measures aim to maintain confidentiality, integrity, and availability (CIA) while ensuring compliance with industry regulations.



Securing the Cloud: A Data-Driven Approach

Data security is a critical component of cloud computing, involving various tools and techniques to protect digital information from unauthorized access, corruption, theft, and loss. These measures aim to maintain the confidentiality, integrity, and availability (CIA) of data while ensuring compliance with industry regulations such as GDPR, HIPAA, and PCI DSS.