Cyber Security

2024

Securing Your Cloud

Vathna.lay@cadt.edu.kh

Cloud Aren’t Bulletproof

- **The Importance of Security:** Cloud computing brings numerous benefits, but security management is a vital responsibility.
- **Clouds as Infrastructure Elsewhere:** Clouds are essentially remote infrastructure, requiring security measures akin to on-premises infrastructure.
- Focus on Public Clouds: This discussion primarily concerns public cloud providers like
  - AWS
  - Google Cloud.

Cloud Aren’t Bulletproof

- **Creating a Security Plan:** A solid security plan is the first step towards optimal security in the cloud.
- **Understanding Your Business:** In-depth knowledge of your business operations is crucial for effective security planning.
- **Innovation Through Understanding:** A deep understanding of your business can lead to innovative improvements.
- **Identifying Assets to Protect**: The initial step in security planning is to determine which assets require protection.

Identifying Your Cyber Assets

- **From Throught to Action:** Translate your initial cloud security concern into a practical strategy by pinpointing the assets you need to protect.
- **Asset Inventory: The Cornerstone of Your plan:** Knowing what you need to safeguard is the most crucial aspect of your security plan
- **Cybersecurity is Cybersecurity:** A comprehensive plan considers all cyber assets, regardless of their location or operational environment.
- **Cyber Assets Everywhere**
- **Building a Team Effort**

Initiating your Cloud Security plan

- **Start Simple, But Shareable:** Small companies can begin with spreadsheets or databases to list all company applications.
- **Hidden Silo Challenge:** Many departments use applications unknown to IT, creating isolated "siloes" of data.
- **The Eye-Opener:** Listing applications reveals the extent of software and data usage, raising the question of oversight.
- **Data Awareness:** Each application listing should include information about the types of data it creates or uses.

Automating Discovery

- **Automated Discovery:** larger organizations can leverage automated tools to efficiently generate a list of applications, networks and data
- **Migration Planning aid:** This process is especially valuable when planning a migration to the cloud

- Amazon Discovery Service
- Google Cloud Discovery Service

Amazon Discovery Service

- **Data Collection and Storage:** AWS Discovery Service Identifies applications used within your computer and stores the data in the AWS Migration Hub
- **Data Export and Analysis:** This information can be exported to Excel or used with AWS analysis tools for deeper insights.
- **Performance Data via APIs:** AWS APIs allow you to store performance data for each application , aiding in risk assessment
- **Agent-less Discovery:** Gather data from your VMware environment.
- **Agent-based Discovery:** Deploys agents on each server to collect more detail info..

Google Cloud Discovery Service

- **Built-in Discovery:** Google Cloud offer a native discovery service to help you manage your cloud resource
- **Instance Metadata:** Easily obtain information like IP address, machine types, and network details for application running in Google Cloud.
- **Project Metadata:** Tracks similar information for applications running in physical data center
- **Centralized Resource Management:** Get a unified view of your entire cloud environment for streamlined management.

Your Service Level Agreements (SLAs)

- **SLA Defined:** An SLA outlines performance and reliability levels promised by your cloud service provider
- **Impact on Availability:** While not stricty security, SLA performance affects the availability of your application and data.
- **Internal vs. External SLAs:** IT departments often have internal SLAs with departments, dependent on cloud providers' SLAs.
- **Shared Security Responsibility:** Cloud providers typically handle physical security and some antimalware, but may offer additional security service

Your Service Level Agreements (SLAs)

- **SLA Examples:**
  - **Amazon: https://aws.amazon.com/legal/service-level-agreements**
  - **Google: https://cloud.google.com/terms/sla**
  - **Oracle: www.oracle.com/cloud/sla**
- **SLA Coverage**: SLAs typically cover uptime, disk efficiency, DNS integrity, email delivery, etc., often with guarantees near 100%.
- **Imperfect but Reliable:** Most SLAs guarantee around 99.99% or 99.95% due to potential failures, but these services are statistically safe.

Where is the Security?

- **Security is implied, Not Guaranteed: SLAs** rarely explicitly guarantee security; it's a shared responsibility.
- **Provider's Role**: Cloud Providers focus on physical security, some malware detection, and 24/7 networking operations.
- **Shared Responsibility Model:** Security is a joint effort. Providers offer tools and service to help you secure your cloud environment
- **Provider Security Tools**: (Data Encryption, Malware Monitoring, Catastrophic failture remediation)
- **Third-Party Integrations:** Many security tools are offered by partners that seamlessly integrate with the cloud provider's platform

Knowing Your Part

- **The ball is in Your court:** You are primarily responsible for your cloud security
- **Company Resource Assessment:** Evaluate if you have the internal resource to provide the necessary security services.
- **Third-Party options:** Consider contracting with third-party security providers for monitoring, identity management, and other service.
- **AI-Powered Security (AIOps):** Explore using AI frameworks to integrate cloud security into your overall cybersecurity strategy. AIOps can utilize big data to detect intrusions and accelerate threat resolution.

Question

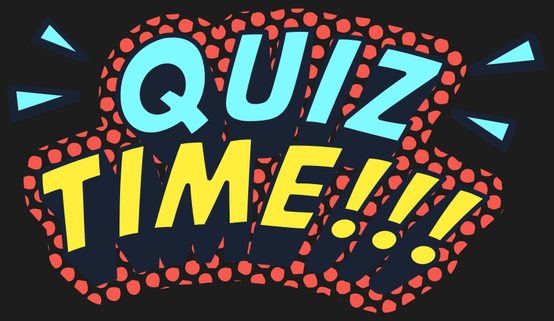
What is the primary focus when starting a cloud security plan?

(A) Implementing encryption

(B) Hiring a third-party security provider

(C) Identifying and inventorying assets

(D) Negotiating Service Level Agreements (SLAs)



Question

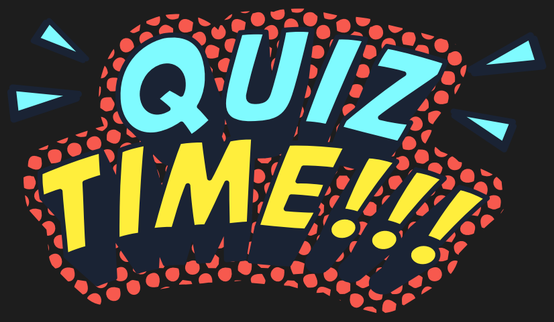
What is a "silo" in the context of cloud security planning?

(A) A type of cloud storage

(B) A department isolated from IT with its own applications and data

(C) A specific security protocol

(D) A type of malware attack



Question

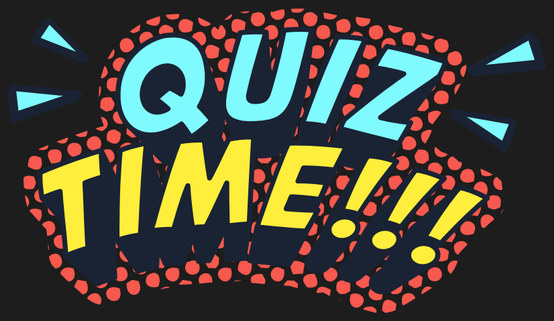
Which of the following is NOT a typical method for automated asset discovery in larger organizations?

(A) AWS Application Discovery Service

(B) Manual spreadsheet creation

(C) Google Cloud Discovery Service

(D) Third-party discovery tools



Question

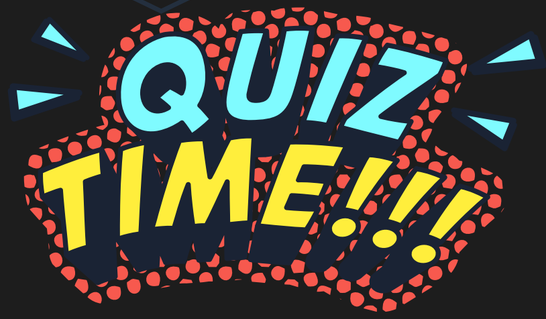
What kind of information does AWS Discovery Service collect?

(A) Employee salaries

(B) Customer purchase history

(C) Application usage, network connections, & performance metrics

(D) Social media engagement data



Question

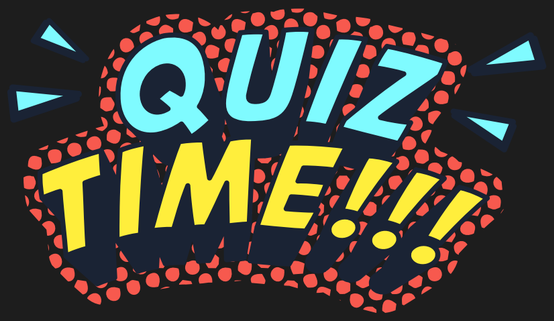
What is a Service Level Agreement (SLA)?

(A) A contract detailing the security measures a cloud provider will implement

(B) A document outlining the performance and reliability a cloud provider promises

(C) An agreement between a company and its IT department regarding internal service levels

(D) A set of security standards for cloud applications



Question

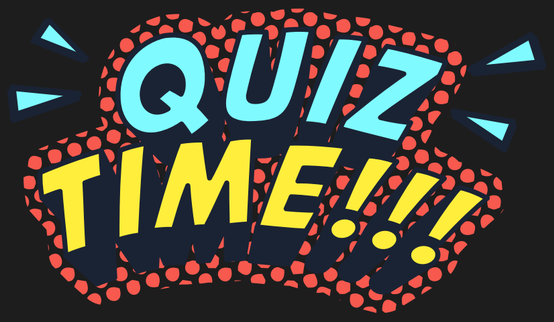
What is the "shared responsibility" model in cloud security?

(A) The cloud provider is fully responsible for security

(B) The customer is fully responsible for security

(C) Security is a joint effort between the customer and the cloud provider

(D) Security is not a concern in the cloud



Question

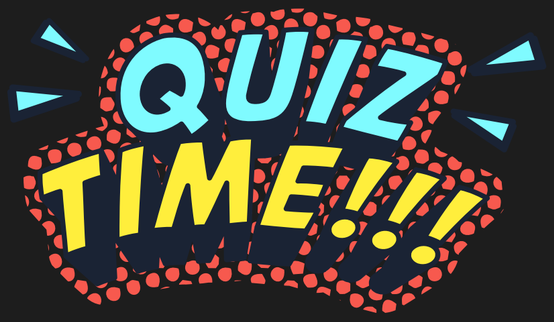
Which of these is NOT a common security tool offered by cloud providers?

(A) Data encryption

(B) Malware monitoring

(C) Guaranteed financial compensation for data breaches

(D) Disaster recovery services



Question

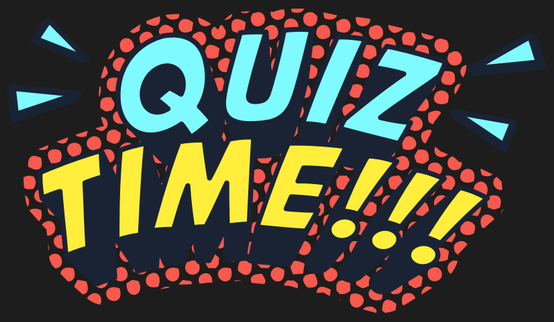
What is AIOps?

(A) Artificial Intelligence for Illegal Operations

(B) All-In-One Operations for Security

(C) Artificial Intelligence for IT Operations

(D) Advanced Internet Optimization Protocols



Question

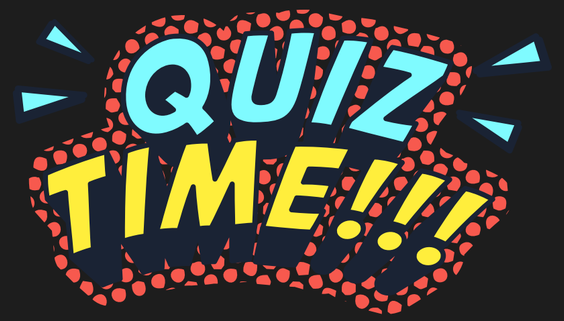
Which Google Cloud feature provides information about applications running in the cloud?

(A) Google Cloud Vision

(B) Instance metadata.

(C) Project metadata

(D) Google Cloud Storage



Question

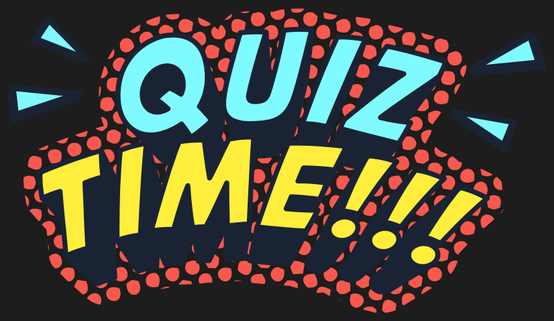
What is the first step to take when considering third-party cloud security providers?

(A) Immediately sign a contract

(B) Explore the offerings of certified partners listed on the cloud provider's website.

(C) Ask for recommendations on social media

(D) Base your decision solely on price



Building Your Cloud Security Dream Team

- **The Importance of Teamwork**
- **Diverse Skillsets, Not Experts**
- **Bridging Departmental Boundaries**
- **Understanding Security Requirements**
- **Responsibility and Ownership:** the team is responsible for building and implementing the security plan, ensuring that it's followed throughout the organization.
- **Education and Enforcement:** Team members educate colleagues on best security practices and help ensure compliance.

Involving stakeholders

- **Stakeholders Beyond the Boardroom:** Cloud security involves a diverse group, including providers, carriers, brokers,auditors, and end-users.
- Key Stakeholder Roles:
  - **Cloud Service Providers**: Deliver the cloud infrastructure, software, or platforms.
  - **Cloud Carriers:** Provide network connectivity to access cloud services.
  - **Cloud Brokers:** Offer value-added services, including security and identity management.
  - **Cloud Auditors:** Verify compliance with SLAs and data protection regulations.
  - **Cloud Consumers:** Your employees, the end-users of cloud applications and data.

Involving stakeholders

- **Involving Internal Experts**
- **The power of Personal stake:** Involving users in the planning process fosters a sense of ownership and commitment to security.
- **Insider Knowledge:** Front-line employees understand the nuances of application use, data access needs, and potential vulnerabilities.
- **Building the Team**: Hold group meetings (virtual or in-person) to gauge interest, enthusiasm, and knowledge to select the best team members.

Restricting Access

- **Obvious yet crucial:** restricting data access is a fundamental principle of cloud security.
- **The compliance correction:** Access restrictions are a major component of many compliance regulations
- **Modern Methods:** while the principle remains the same, the methods for user validation have evolved significantly.
- **Determining Access Level:** it's essential to define who has access to what type of data and applications

Determining Access Levels: A Balancing Act

- **Complexity of Access Control:** Properly configuring access can be challenging due to varying data sensitivity and user needs
- **Subjective Decisions:** Determining access levels often involves subjective judgements, except when compliance regulations are involved
- **Identifying Legitimate Users**: Start by knowing who should have access, but be aware unauthorized access can be difficult to detect.
- **The Insider Threat:** Even legitimate users can misuse their access, posing a risk to data security
- **AI for Anomaly Detection**

Catching Flies with Honey: Honeypotting in the Cloud

- **Honeypot Strategy:** Honeypots are decoy resources used to detect unauthorized access and potential breaches.
- **Types of Honeypots**
  - **High Interaction:** VM with full service
  - **Low Interaction:** VM with limited service
  - **Canary:** Cloud-based honeypots for easy deployment and flexibility

Advantage of cloud Honeypot

- **Cost-Effective:** No physical hardware needed, and cloud resources are often inexpensive when idle.
- **Geographic Flexibility**: Easy to deploy and relocate to high-risk areas.
- **Rapid Deployment:** New cloud instances can be spun up quickly.
- **Risks and Rewards:** Honeypots can be risky if not carefully managed, as they can potentially provide hackers with network access.
- **Honeypot Variations**: Can also involve fake data, documents, and accounts to trigger alerts when accessed.

Least Privilege Policy & Access Restriction

- **Least Privilege Principle:** Grant only the minimum necessary privileges to users, programs, and processes.
- **Database Over-Privileging:** Avoid granting excessive permissions in databases, especially in web development.
- **Limiting Roles:** Restrict the number of roles with unrestricted access to sensitive data and applications.
- **Malware Considerations**: Malware can exploit even low-level accounts, so least privilege applies to all users.
- **Data Value vs. Sensitivity**: Even seemingly unimportant data can be valuable to attackers, so limit access to minimize risk.

Implementing Zero Trust

- **Zero Trust Core Principle:** Trust no one by default.
- **Shift from Perimeter Security:** Traditional parameter security is insufficient in the Cloud era.
- **Authentication, Validation, Continuous Checking:** Zero trust requires a multi-layered approach to ensure only authorized access.
- The "**Who goes there**" mentality: Adopt a mindset of constant vigilance and assume every access request could be a threat.
- **From the "once you're in, you're trusted" model:** each resource is responsible for its own security
- **The need for unified Security:** cloud environment introduce complexity and multiple perimeters, necessitating a unified security policy like zero trust.

The Foundations of Zero Trust Philosophy

- **Core Philosophy:** Zero trust shifts security focus from perimeter defenses to individual resource.
- **Five Essential Features:**
  - **Two-Way Authentication (MFA)**
  - **Endpoint Device management:** Secure communication depends on trusted hardware
  - **End-to-end encryption:**
  - **Public Key/ Private Key:** Secure Communication by using paired keys. (SSL/TLS certificates)
  - **Micro-segementation:** devide networks into smaller zones to limit the impact of the breach

Challenges in Implementing Zero trust

- **The Inevitability of Change:** The threat landscape constantly evolves, requiring a fluid and adaptable zero trust approach
- **Legacy System Integration**: Older systems may not be compatible with zero trust principles, posing a challenge for integration.
- **Achieving Full Visibility:** Ensuring complete visibility across all IT assets, including shadow IT and mobile devices, is difficult but necessary.
- **Building DIY Solutions:** Cloud environments weren't inherently designed for zero trust, necessitating custom solutions or third-party tools.

Challenges in Implementing Zero trust

- **Business Collaboration:** Collaboration across departments and with vendors is essential for successful zero trust implementation.
- **Zero Trust Agility:** An agile approach allows for quick adaptation to changes and continuous improvement of security measures.
- **The Right Team**: Building a knowledgeable and empowered team is crucial for overcoming challenges and maintaining zero trust principles.

MFA & OTP in Zero Trust

- **MFA for Enhanced Security:** Multifactor authentication (MFA) is a standard for authenticating users, especially in cloud SaaS applications.
- **SurePassID:** A popular MFA system offering features like hybrid deployment, offline login, firewall configurations, and audit capabilities. It integrates with SIEM systems and supports compliance.
- **Vulnerability of SMS OTPs**: SMS-based one-time passwords (OTPs) are no longer considered secure due to susceptibility to man-in-the-middle attacks.
- **Four type of OTPs**
  - **Soft Tokens:** Deliver through mobile apps
  - **Hard Tokens:** Physical device (key fobs) that generate codes
  - **On-Demand Tokens:** sent via SMS or email for initial logins
  - **FIDO U2F Tokens:** USB fobs providing strong authentication with public key cryptography

Question

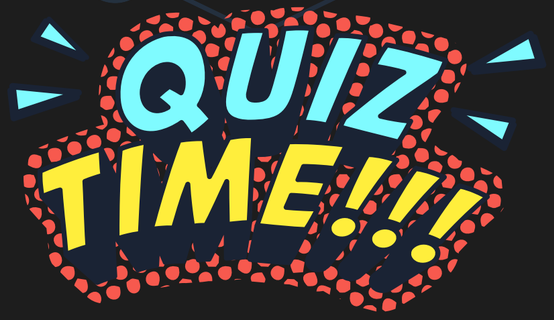
What is the core principle of least privilege policy?

A. Grant all users maximum access for efficiency.

B. Restrict access to only what is absolutely necessary for a user's role.

C. Prioritize senior employees' access over others.

D. Focus security efforts on external threats only.



Question

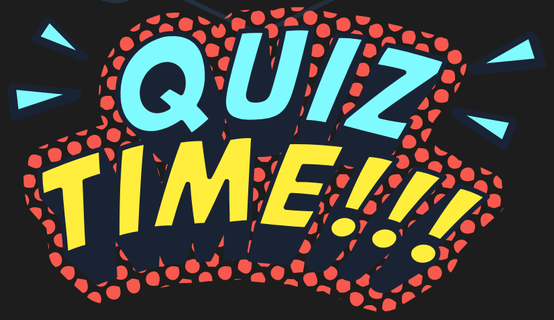
Which of the following is NOT a type of honeypot?

A. High interaction

B. Low interaction

C. Canary

D. Honeybee



Question

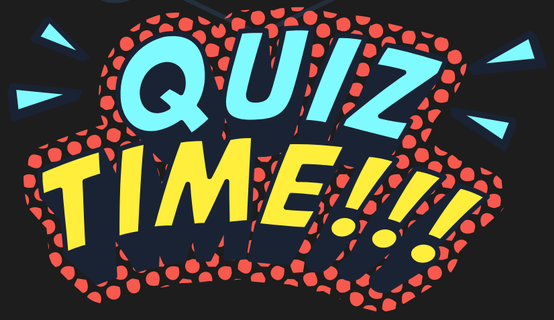
What is the primary goal of a zero trust framework?

A. To eliminate the need for passwords.

B. To shift security focus from perimeter defenses to individual resources.

C. To rely solely on firewalls for protection.

D. To grant all users unrestricted access for collaboration.



Question

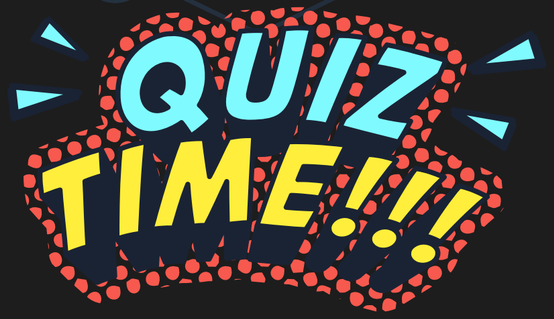
Which of the following is NOT a core feature of zero trust?

A. Two-way authentication

B. Endpoint device management

C. End-to-end encryption

D. Unlimited user privileges



Question

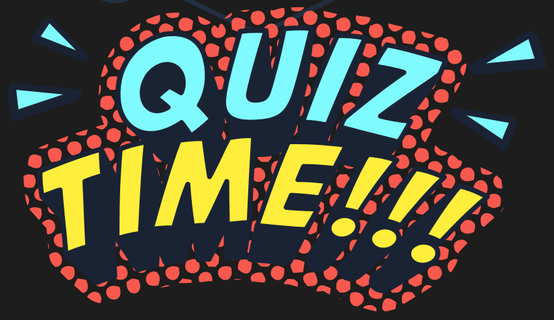
What is the purpose of SSL/TLS certificates in the context of public key cryptography?

A. To encrypt emails.

B. To store user passwords securely.

C. To verify the identity of websites and prevent spoofing attacks.

D. To generate one-time passwords.



Question

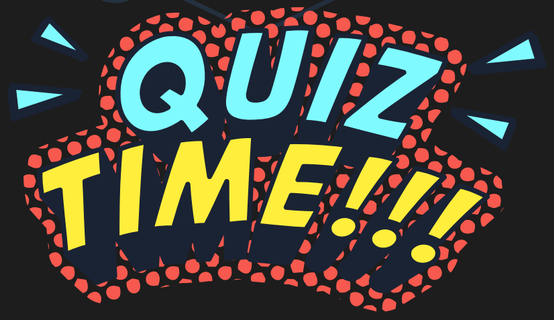
Which of the following is a challenge in implementing zero trust?

A. The static nature of technology

B. The simplicity of integrating legacy systems

C. The abundance of complete, off-the-shelf solutions

D. The need for continuous adaptation to changes



Question

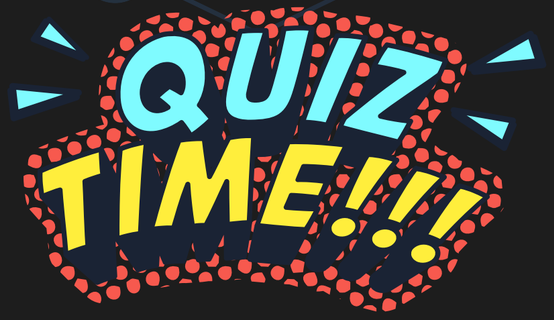
What does "air gapped" mean in the context of security?

A. A device connected to a public Wi-Fi network.

B. A device isolated from unsecured networks.

C. A device that requires two-factor authentication.

D. A device with end-to-end encryption enabled.



Question

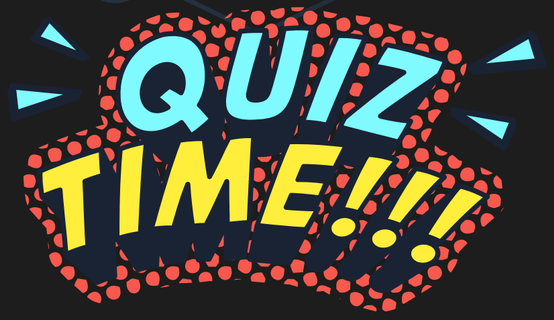
What is the main disadvantage of on-demand tokens?

A. They require specialized hardware.

B. They are time-based and expire quickly.

C. They are not as secure as other token types due to potential interception during delivery.

D. They require users to have smartphones.



Question

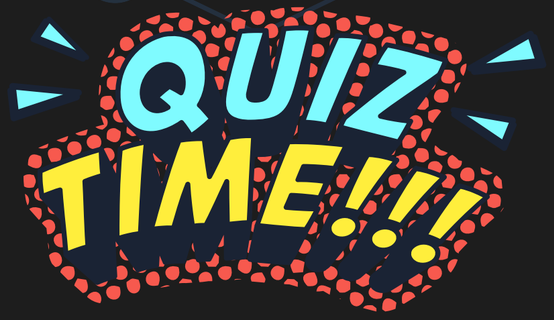
What is the advantage of FIDO U2F tokens over other types of tokens?

A. They are the cheapest option.

B. They have the widest industry support.

C. They are the most resistant to phishing, session hijacking, and man-in-the-middle attacks.

D. They are fully supported on all mobile devices.



Question

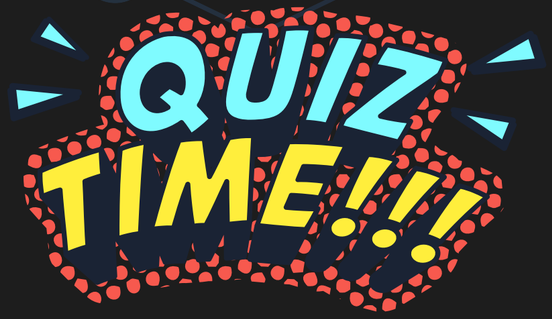
What are the two main methods used by AWS Discovery Service to collect information about applications?

A. Active and passive scanning

B. Agentless and agent-based discovery

C. Public and private key encryption

D. Deep packet inspection and network flow analysis




?
Q&A