PassQueen
a.k.a dumpsqueen.com

Advanced Security Architecture for Account Managers

Cisco 700-265

Version Demo

Total Demo Questions: 16

Total Premium Questions: 165

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Security Solutions	75
Topic 2, Security Architecture	11
Topic 3, Security Operations	3
Topic 4, Security Sales Strategies	76
Total	165

QUESTION NO: 1

Which zero-trust principle limits a user or device to only the applications and resources required for its approved role?

A. least-privilege access

B. open network access

C. permanent trust

D. unrestricted lateral movement

E. shared administrator credentials

ANSWER: A

Explanation:

Least-privilege access is correct because it limits access rights to the minimum resources and actions needed for an authorized task. Rather than providing broad network access after authentication, a zero-trust architecture uses identity, device posture, application requirements, and policy to restrict access appropriately.

Applying least privilege reduces the impact of compromised credentials or devices because an attacker cannot automatically access unrelated systems and sensitive data. Cisco's zero-trust approach emphasizes continuous verification and granular access controls to reduce implicit trust. See the Cisco Zero Trust overview.

QUESTION NO: 2

Which three options are Cisco Advanced Threat Solutions? (Choose three.)

A. Next-Generation Intrusion Prevention System

B. Stealthwatch

C. remote access VPN

D. identity and access control

E. web security

F. cognitive Threat analytics

ANSWER: B D F

Explanation:

Stealthwatch, identity and access control, and cognitive Threat analytics are the three Cisco Advanced Threat Solutions in the portfolio terminology used by this question. Stealthwatch provides network-wide visibility and behavioral analytics, enabling security teams to identify suspicious activity, investigate it using network telemetry, and respond to threats that may evade signature-based controls. Cisco has since renamed this product Cisco Secure Network Analytics, while retaining its network-detection-and-response role. See the Cisco Secure Network Analytics product page.

Identity and access control supplies the trusted user, device, and access context needed to make effective threat decisions and to contain an incident through policy enforcement. Cisco Identity Services Engine is Cisco's central platform for this identity-based access control and contextual visibility. Its role is described on the Cisco Identity Services Engine product page.

Cognitive Threat Analytics applies cloud-based behavioral analysis and machine learning to telemetry to uncover malicious behavior, particularly threats that can be difficult to detect through conventional alerts alone. Together, network behavioral visibility, identity context and control, and cognitive analytics support the detection, investigation, and containment objectives of Cisco's advanced-threat architecture.

QUESTION NO: 3

Which two attack vectors are protected by malware protection? (Choose two.)

A. mobile

B. campus and branch

C. email

D. cloud apps

E. voicemail

ANSWER: A D

Explanation:

Malware protection applies to **mobile** and **cloud apps** because users and data can be exposed to malicious files, applications, links, and payloads through both mobile-device activity and software-as-a-service environments. Mobile protection extends malware defense to devices operating outside the traditional enterprise perimeter, helping organizations detect and prevent threats delivered through mobile applications, web activity, or files. Cisco's security portfolio emphasizes extending protection to users and endpoints wherever they connect.

Cloud applications are also a significant malware delivery and storage channel. Files shared through sanctioned or unsanctioned SaaS services can contain malicious content, and malware protection capabilities can inspect activity and files associated with cloud-app use to identify threats and support remediation. This aligns with Cisco's cloud security approach, which provides visibility and protection for SaaS applications and their data. Together, protection for mobile and cloud apps addresses modern attack paths created by distributed users, unmanaged locations, and cloud-based collaboration. See Cisco's Secure Endpoint overview and Cisco Cloudlock overview.

QUESTION NO: 4

Which three main points of the Cisco Security & Threat Landscape module are true? (Choose three.)

A. An effective security solution provides customers with the necessary tools and resources to overcome their ever-growing security challenges.

B. The Cisco Security Solutions Portfolio drives customer business outcomes.

C. The business case for security is defined in the threat landscape.

D. The threat landscape is expanding and increasing costs for customers.

E. Customers need an easy to manage and fully integrated solution.

F. Customers must understand how vulnerable they are.

ANSWER: B D E

Explanation:

The central message is that the threat landscape is expanding and increasing costs for customers, making security a business issue as well as a technical one. Organizations face a growing volume of attacks, more sophisticated adversaries, and operational complexity across users, applications, networks, endpoints, and cloud environments. Cisco describes this need as requiring stronger security resilience and protection that can operate across a distributed environment.

Customers need an easy to manage and fully integrated solution because disconnected point products can create operational silos, inconsistent policy enforcement, and excessive alert volume. A unified approach helps security teams gain better visibility, correlate telemetry, automate responses, and manage risk more efficiently. Cisco's security platform strategy emphasizes integrated capabilities and shared intelligence across the security estate.

The Cisco Security Solutions Portfolio drives customer business outcomes by connecting security investments to resilience, operational efficiency, reduced risk, protected productivity, and business continuity. Rather than treating security as an isolated control, the portfolio supports secure transformation while helping organizations simplify operations and defend their business. See Cisco's Security portfolio overview and its secure access service edge resources.

QUESTION NO: 5

Which three options are solutions and features of the cloud apps threat-centric solution? (Choose three.)

A. Cloud App Security

B. CTD and Network Analytics

C. remote access VPN

D. accelerated threat response

E. complete policy management

F. cloud data loss prevention

ANSWER: A D F

Explanation:

Cloud App Security, accelerated threat response, and cloud data loss prevention are the core capabilities represented by a threat-centric approach for cloud applications. Cloud App Security provides visibility into sanctioned and unsanctioned cloud-app usage and applies security controls to protect users, applications, and data in software-as-a-service environments. Cisco's Cloudlock capabilities were designed to provide cloud access security broker functions, including activity visibility, policy enforcement, and threat detection across cloud applications. Cloud data loss prevention extends that protection to sensitive information by discovering data in cloud services and applying policies to prevent inappropriate exposure or sharing. Accelerated threat response is essential because cloud-app incidents require rapid investigation and coordinated action across security telemetry and enforcement points; Cisco threat-response workflows bring context together to help security teams investigate and remediate incidents faster. Together, these capabilities address cloud adoption with visibility, data protection, and a response process that is aligned with a threat-centric security architecture. See Cisco's Cloudlock overview and Threat Response overview for Cisco's descriptions of cloud security controls and incident-response workflows.

QUESTION NO: 6

Which NGIPS appliance do you use if yourcustomer is at the enterprise level and requires modular architecture that Is scalable?

A. Cisco 4000 Senes ISR

B. Cisco 300 SenesISR

C. RrePOWER 2100 Series

D. RrePOWER 8000 Series

E. ASA 7000 Series

ANSWER: D

Explanation:

RrePOWER 8000 Series is the correct choice because the Cisco FirePOWER 8000 Series was designed for large enterprise and service-provider deployments that need high-capacity, scalable next-generation intrusion prevention. Its modular chassis architecture supports interchangeable network modules and security processing modules, allowing an organization to select interface density and inspection performance appropriate to its deployment. This modularity also enables growth without replacing the complete platform: capacity can be expanded as traffic volumes, segment counts, and inspection requirements

increase. The platform was positioned for demanding environments requiring high throughput while applying NGIPS controls, application visibility, and advanced threat protection across many network links. Cisco's FirePOWER 8000 Series documentation describes the appliance family as a modular platform with multiple chassis and module choices for scaling performance and connectivity. This makes it suitable where enterprise architecture requirements emphasize resilience, expansion, and high-density deployment rather than a fixed-form-factor appliance. See the Cisco FirePOWER 8000 Series data sheet and Cisco's FirePOWER 8000 Series product page for platform details.

QUESTION NO: 7

How does the Cisco policy and access solution handle a changing user base in growing company?

A. Cisco delivers a flexible and scalable security solution framework that can adapt to changing customer needs

B. Ciscoarchitecture offers the lowest TCO by providing product that integrate, which lowers the cost of IT setup, management, and maintenance.Cï¼ŽCisco Talos Security Intelligence and Research Group integrates into all security solutions, which provides advancedprotection against new threats.

C. Cisco provides you the ability to monitor and restrict application usage. As applications become more complex, Cisco provides the flexibility to control all or subsets of the application.

ANSWER: A

Explanation:

Cisco delivers a flexible and scalable security solution framework that can adapt to changing customer needs. This is the correct answer because a growing organization must be able to extend identity-based access controls, enforcement points, user and device visibility, and policy administration without replacing its security architecture. Cisco's policy-and-access approach is designed to apply consistent access policy as the number of employees, contractors, endpoints, locations, and applications changes. Centralized identity and access policy enables administrators to define who may connect, which devices meet security requirements, and what level of network access is appropriate. This supports operational growth while maintaining governance and reducing the need to manage separate, disconnected access-control systems. Cisco Identity Services Engine is a core component of this approach: it provides centralized policy administration and context-aware access control across wired, wireless, and VPN connections. Its architecture can scale through distributed deployment models as organizational requirements expand. Cisco also frames secure access as an adaptable zero-trust capability, where access decisions can continuously use identity, device, and contextual signals. These capabilities directly address a changing user base by allowing policies and enforcement to evolve with business needs. See Cisco Identity Services Engine and Cisco Zero Trust.

QUESTION NO: 8

Which two options are benefits of the web threat-centric solution? (Choose two.)

A. data loss prevention with NGFW

B. malware blocking with AMP

C. email encryption with CRES

D. policy-driven URL filtering

E. rogue web filtering protection through CTA

ANSWER: B D

Explanation:

Malware blocking with AMP is a core benefit of Cisco's web threat-centric security approach. Advanced Malware Protection for web traffic extends protection beyond a single point-in-time file inspection: it uses threat intelligence and file analysis to identify and block malicious content delivered through web browsing. This helps organizations protect users from web-based malware, including threats that may be identified after initial observation.

Policy-driven URL filtering is also a foundational web-security capability. Cisco web security products apply organizational browsing policies using URL categories, reputation, and identity-aware controls. This enables administrators to consistently permit business-appropriate access while restricting risky or unacceptable web destinations, reducing exposure to malware, command-and-control communications, and other internet-borne threats. These controls combine preventative policy enforcement with advanced threat protection, which is central to a threat-centric web-security architecture. Cisco describes the relevant secure web gateway and URL-filtering capabilities in its Web Security Appliance documentation and explains AMP's malware-detection and protection model in its Advanced Malware Protection overview.

QUESTION NO: 9

Which three options are main areas of the Cisco Security Portfolio? (Choose three.)

A. cloud security

B. ASA and NGIPS

C. policy and entry

D. roaming security

E. advanced threat

F. web and email security

ANSWER: A E F

Explanation:

Cisco's security portfolio is organized around protecting users, workloads, applications, and data across the places where organizations operate. **cloud security** is a principal portfolio area because Cisco provides capabilities for securing cloud access, cloud applications, and cloud workloads while applying consistent protection across hybrid and multicloud environments. Cisco describes its cloud-security approach as helping organizations protect cloud environments and simplify security operations.

advanced threat is also a core area because identifying, investigating, containing, and responding to sophisticated attacks is central to an effective security architecture. Cisco's extended detection and response capabilities correlate security telemetry and help teams prioritize and remediate threats across their environment.

web and email security is a main area because web browsing and email are common delivery channels for phishing, malicious links, malware, and credential theft. Cisco's secure email and web protections are designed to prevent these threats before they reach users or cause broader compromise. Together, these areas represent complementary layers of Cisco security coverage: cloud environments, advanced threat defense and response, and protection for prominent user-facing attack vectors. See Cisco's Cloud Security overview and its Email Security overview.

QUESTION NO: 10

Which two options are products and benefit of email threat-centric solution? (Choose two)

A. Meraki

B. Cloudlock

C. Cisco Registered Envelope Service

D. Cisco Umbrella

E. Web Filtering

F. AMP for Endpoints

ANSWER: D F

Explanation:

Cisco Umbrella and AMP for Endpoints are correct because they extend email security into the broader threat-centric security architecture. Email is a common initial delivery channel for malicious URLs and attachments, so protection must continue after a message reaches the user. Cisco Umbrella supplies DNS-layer protection that can block users from connecting to malicious domains, including destinations reached through links in email. This reduces the chance that a phishing or malware campaign succeeds when a recipient clicks a malicious URL. Cisco documents this DNS-layer security capability and its protection against threats across users and devices at Cisco Umbrella.

AMP for Endpoints, now part of Cisco Secure Endpoint, provides endpoint-based malware prevention, detection, investigation, and response. When a malicious attachment or payload reaches an endpoint, its telemetry and retrospective security capabilities help identify affected devices and support containment and remediation. Integrating email protection with endpoint visibility enables security teams to correlate the original email event with endpoint activity and respond across the attack lifecycle. Cisco describes Secure Endpoint's prevention, detection, and response capabilities at Cisco Secure Endpoint. Together, these products support layered protection for threats delivered through email links and attachments.

QUESTION NO: 11

Which CiscoSecurity benefit is a differentiator that allows partners to plan and model their business?

A. one solution to fit every need

B. comprehensive vision for security

C. lowest price points

D. unparalleled commitment

E. best-in-class technologies

ANSWER: D

Explanation:

unparalleled commitment is the Cisco Security differentiator that enables partners to plan and model their business. A sustained commitment to the security market gives partners greater confidence that Cisco will continue investing in its portfolio, platforms, partner ecosystem, training, and routes to market. That predictability matters when a partner is deciding where to develop technical skills, build managed services, make sales investments, and create recurring-revenue offers. Cisco's security strategy is designed around helping partners deliver integrated security outcomes while expanding their practices over time. The resulting long-term alignment supports practical business planning: partners can forecast demand, align resources with Cisco programs, and develop service capabilities around an ongoing relationship rather than a short-lived product opportunity. Cisco describes its partner ecosystem as a central element of how customers access expertise, solutions, and lifecycle value, while its security portfolio emphasizes continued innovation and broad platform integration. These commitments provide the stable foundation that partners need for investment and growth planning. See Cisco's Partner ecosystem overview and Security portfolio overview.

QUESTION NO: 12

Which component of Stealthwatch uses sophisticated security analytics to accelerate threat response time?

A. threat protection

B. investigation

C. granular visibility

D. network control

E. anomaly detection

ANSWER: B

Explanation:

investigation is the Stealthwatch capability that applies sophisticated security analytics to help security teams rapidly understand and respond to suspected threats. After Stealthwatch identifies concerning network behavior, its investigation workflow brings relevant context together, such as affected hosts, communications, behavioral observations, and associated flow telemetry. This reduces the manual effort required to correlate network activity across systems and enables analysts to move more quickly from an alert to a validated incident and an appropriate response.

In Cisco's Secure Network Analytics portfolio, formerly known as Stealthwatch, network-derived telemetry is analyzed to provide actionable insight into threats and anomalous behavior across the environment. Investigation is therefore the component focused on accelerating the analyst's response process through contextualized security analytics rather than merely collecting visibility data. Cisco describes Secure Network Analytics capabilities and its use of network telemetry for threat detection and investigation at Cisco Secure Network Analytics. Additional Cisco guidance on using network visibility and analytics to investigate security events is available in the Secure Network Analytics solution overview.

QUESTION NO: 13

Which three issues do customers with limited mobility issues deal with? (choose three)

A. Remote workers that compromise security

B. Solutions that do not extend off network

C. Complex mobile management

D. Complex mobile management

E. Big data center vulnerability

F. Expensive malware attacks

ANSWER: A B C

Explanation:

Customers operating with limited mobility commonly face a security and operational gap when people, devices, and applications move beyond the traditional office network. **Remote workers that compromise security** identifies the need to protect access by users working from unmanaged or less-trusted locations without weakening policy enforcement. **Solutions that do not extend off network** captures the limitation of security architectures designed mainly for an on-premises perimeter; users require consistent protection and access controls whether they connect from a branch, home, or public network. **Complex mobile management** reflects the administrative burden of applying device, identity, connectivity, and security policies across a changing mobile workforce. Cisco's secure-access approach is designed to extend policy-based access and protection to users regardless of location, while centralized cloud-delivered security reduces operational complexity. This aligns with the Cisco focus on providing secure, seamless access for hybrid work and on protecting users and devices both on and off the corporate network. See Cisco Secure Access and Cisco Hybrid Work solutions.

QUESTION NO: 14

Which Cisco security technology delivers the best real-time threat intelligence?

A. Identity Services Engine

B. Cisco Talos Security

C. Cisco Security Manager

D. Next Generation Firewall

E. TrustSec

ANSWER: B

Explanation:

Cisco Talos Security is correct because Talos is Cisco's global threat-intelligence organization. It continuously collects and analyzes telemetry, malware samples, DNS activity, email and web threats, vulnerabilities, and attacker infrastructure from a broad range of Cisco security products and internet-scale sensors. The resulting intelligence is used to produce timely threat research, indicators of compromise, detection content, reputation data, and protections that are delivered across the Cisco Security portfolio. This enables security controls to identify emerging malicious activity and apply updated defenses with minimal delay, which is the core value of real-time threat intelligence.

For an account-manager security architecture discussion, Talos represents the intelligence foundation that strengthens prevention, detection, and response capabilities across products and services. Cisco describes Talos as one of the largest commercial threat-intelligence teams, combining human research with large-scale telemetry and automated analysis. Its intelligence informs protections for threats such as phishing, malware, malicious domains, and network-based attacks. More information is available from Cisco Talos Intelligence Group and Cisco's overview of Cisco Talos threat intelligence.

QUESTION NO: 15

Which application works with Cisco NGFW to provide administrators powerful application and usage controls over mobile users?

A. TrustSec

B. Cloudlock

C. Stealthwatch

D. Next Generation Firewall

E. AnyConnect

F. AMP Threat Grid

ANSWER: E

Explanation:

Cisco AnyConnect is correct. AnyConnect, now branded Cisco Secure Client, is Cisco's endpoint client for providing secure remote connectivity for mobile users through Cisco security gateways, including Cisco NGFW platforms. It establishes authenticated, encrypted remote-access VPN connectivity and can deliver identity, device, posture, and connection context to the security policy decision process. This allows administrators to extend centralized security policy to users who are off the corporate network rather than treating remote access as a separate, unmanaged service.

When used with Cisco NGFW capabilities, AnyConnect supports controlled access to internal resources and consistent enforcement of application-aware security policies for remote users. Administrators can apply access controls based on the authenticated user and connection context, while the firewall inspects and controls traffic using its next-generation security functions. The client also supports related endpoint-security functions, such as posture assessment and secure access workflows, which helps maintain visibility and policy enforcement for a mobile workforce. Cisco's documentation describes Secure Client as the client used for secure remote access and identifies its integration with Cisco security infrastructure: Cisco Secure Client and Cisco Secure Firewall.

QUESTION NO: 16

WhichCisco business value is represented by features of automatic updates and post-attack guidance?

A. cost effectiveness

B. flexibility

C. protection

D. completeness

E. control

ANSWER: C

Explanation:

protection is the Cisco business value represented by automatic updates and post-attack guidance. Effective protection is not limited to blocking a threat at a single point in time; it depends on maintaining current defenses as adversaries, vulnerabilities, indicators, and attack techniques change. Automatic updates help ensure that security controls receive current threat intelligence, detections, and protective capabilities without relying on delayed manual intervention. This supports continuous prevention and detection across the environment.

Post-attack guidance extends that protection outcome beyond initial detection. It helps security teams understand the scope and relevance of an event, prioritize response actions, investigate what occurred, and take steps to contain and remediate the threat. This is consistent with Cisco's threat-focused security approach, which emphasizes visibility and response throughout an attack lifecycle rather than treating security as a purely preventive function. Cisco describes its security portfolio as helping organizations prevent, detect, and respond to threats, while Cisco Talos provides the threat intelligence that informs protective capabilities and updates. See Cisco Security and Cisco Talos Intelligence Group.