DUMPSARENA

Cisco Small and Medium Business Sales (SMBS)

Cisco 700-250

Version Demo

Total Demo Questions: 6

Total Premium Questions: 69

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, SMB Market	13
Topic 2, Cisco SMB Architecture	6
Topic 3, Cisco SMB Products	40
Topic 4, Selling Cisco SMB Solutions	10
Total	69

QUESTION NO: 1

Which Cisco product is part of the smart experience for empowering IT?

A. Meraki Sensors

B. Meraki Insight

C. Umbrella

D. Meraki Cameras

ANSWER: B

Explanation:

Meraki Insight is the Cisco Meraki solution that supports a smart experience for empowering IT because it gives IT teams end-to-end visibility into how users experience critical network applications. It extends monitoring beyond basic device availability by measuring application performance across the LAN, WAN, and Internet, helping administrators distinguish among network, server, and application-related causes of poor performance. This context enables faster, more informed troubleshooting from the Meraki dashboard and helps IT teams prioritize issues that affect users and business services.

Meraki Insight is particularly relevant to an IT-empowerment experience because it combines performance analytics, health metrics, and actionable troubleshooting workflows in a cloud-managed interface. IT personnel can use it to observe web-application response behavior, WAN performance, and connectivity paths without deploying separate traditional monitoring platforms. The resulting visibility reduces operational complexity and supports proactive maintenance of the digital services on which employees and customers depend. Cisco describes Meraki Insight as a solution for assuring and optimizing application experience, including visibility into application performance and network conditions. See the Cisco Meraki Insight data sheet and the Meraki Insight product overview.

QUESTION NO: 2

Which Cisco product features Integrated Mobile Device Mana,gement?

A. Duo

B. Umbrella

C. Meraki

D. Webex

ANSWER: C

Explanation:

Meraki is correct because Cisco Meraki Systems Manager is Cisco’s cloud-managed endpoint-management platform and includes mobile device management capabilities. Through the Meraki dashboard, an organization can enroll, configure, monitor, and secure managed mobile devices from a centralized interface. Systems Manager supports common device-management activities such as applying configuration profiles and restrictions, distributing applications, inventorying hardware and software, enforcing security policies, and remotely locking or erasing devices when needed. This makes it appropriate for small and medium businesses that need consistent visibility and policy enforcement across employee-owned or company-owned phones and tablets without deploying complex on-premises management infrastructure. Meraki also integrates endpoint-management information with the broader Meraki cloud platform, helping administrators use device context when managing network access and security. Cisco describes Systems Manager as endpoint management delivered through the Meraki dashboard, with support for mobile-device management workflows and device enrollment. See the Cisco Meraki Systems Manager overview and Cisco’s Systems Manager product page for product capabilities and deployment details.

QUESTION NO: 3

Which Cisco solution should an SMB IT support company adopt lo help mitigate network vulnerabilities?

A. CML

B. Catalyst Access Points

C. Webex Control Hub

D. FirePower Firewalls

ANSWER: D

Explanation:

FirePower Firewalls is the appropriate solution because Cisco Secure Firewall, formerly Cisco Firepower, is designed to reduce network exposure through integrated next-generation firewall and threat-defense capabilities. For an SMB IT support company, this provides a practical security control at the network perimeter and between internal network segments, where it can inspect traffic and enforce policies before threats reach users, applications, or critical systems. Cisco's firewall platform combines stateful firewalling with application visibility and control, intrusion prevention, URL filtering, and malware-defense integrations. These capabilities help identify exploit attempts, suspicious connections, and access to known malicious destinations, enabling the company to mitigate vulnerabilities that could otherwise be used to compromise the customer network. Cisco Talos threat intelligence also supplies continuously updated intelligence that helps the platform recognize emerging threats and indicators of compromise. Centralized security policy and event visibility further allow an IT provider to operate consistent protections across SMB environments while monitoring and responding to security events. Cisco describes Secure Firewall as delivering threat-focused protection with firewall, intrusion prevention, and advanced malware-defense capabilities. See the Cisco Secure Firewall product page and the Cisco Secure Firewall 1000 Series data sheet.

QUESTION NO: 4

Which Cisco product is part of the smart experience for enabling workspaces?

A. Cisco Secure Email

B. Meraki insight

C. Meraki Systems Manager

D. Meraki Camera

ANSWER: D

Explanation:

Meraki Camera is part of Cisco's smart-workspace experience because Cisco Meraki MV smart cameras provide the environmental visibility and operational data needed to manage physical workplaces intelligently. In addition to supporting physical security, MV cameras can use on-camera analytics to identify people and support occupancy-oriented insights. These capabilities help organizations understand how spaces are being used, assist with workplace planning, and make operational decisions based on near-real-time observations. The cloud-managed Meraki dashboard centralizes camera configuration, video access, and analytics, allowing an IT team to operate workspace technology without deploying separate, complex video-management infrastructure. Cisco positions its smart-building and smart-workspace capabilities around connecting physical-space data with workplace operations; MV cameras are an important source of that data. For example, Cisco Meraki documents people detection and related camera analytics in its MV documentation, while Cisco Spaces describes using location and occupancy intelligence to improve workplace experiences and space utilization. Together, these capabilities illustrate why a Meraki camera belongs in an offering focused on enabling smart workspaces. See Cisco Meraki MV People Detection and Cisco Spaces.

QUESTION NO: 5

Which feature was designed for Cisco partners to co-brand and embed on their websites?

A. SMB Services Portal

B. SMB Experience Explorer

C. SMB Portfolio Explorer

D. Select Solutions Portal

ANSWER: B

Explanation:

SMB Experience Explorer is the Cisco partner-facing digital experience designed to be co-branded and embedded within a partner's website. It gives partners an interactive way to present Cisco solutions relevant to small and midsize businesses, helping prospective customers explore business needs, solution areas, and the value that Cisco technologies can provide. Rather than requiring a customer to navigate a separate Cisco destination, the co-brandable experience lets the partner maintain its own web presence and customer relationship while incorporating Cisco messaging and solution guidance. This supports a scalable marketing motion: partners can use Cisco-developed content and interactive solution discovery in their own demand-generation activities, while aligning the experience to their brand. The feature therefore fits Cisco's broader small-business strategy of enabling partners to deliver solution-led customer conversations and digital engagement. Cisco's small-business solution resources are available at Cisco Small Business Solutions, and Cisco partner resources and programs are available through the Cisco Partner site.

QUESTION NO: 6

Which feature results in fewer cyberattacks and breaches for an organization?

A. security products from multiple vendors

B. large cybersecurity team

C. proactive security strategy

D. multi-cloud security platform

ANSWER: C

Explanation:

proactive security strategy is correct because it shifts an organization from reacting after an incident occurs to continuously reducing the likelihood and impact of successful attacks. A proactive approach combines ongoing risk assessment, security controls, threat intelligence, vulnerability management, timely patching, monitoring, and practiced incident-response processes. These activities identify exposures and suspicious behavior early, allowing the organization to remediate weaknesses or contain threats before they develop into material breaches.

For small and medium businesses, this strategy is especially valuable because security resources are often limited. A risk-based, proactive program helps prioritize the most consequential assets, identities, applications, and vulnerabilities rather than relying solely on ad hoc responses after an alert or compromise. It also supports consistent security hygiene, including multifactor authentication, employee awareness, secure configuration, backups, and verification that controls are functioning as intended.

Cisco describes security resilience as the ability to protect business operations before, during, and after adverse events; this depends on anticipating threats and building protective and recovery capabilities into normal operations. Cisco's guidance on extended detection and response likewise emphasizes continuous visibility, detection, investigation, and response across the environment. These practices make a proactive security strategy the feature most directly associated with reducing cyberattacks and breaches. See Cisco: What Is Security Resilience? and Cisco: What Is XDR?.