



Cisco 700-250

Cisco Small and Medium Business Sales (SMBS)

Thank You for Downloading 700-250 Updated Exam Questions

<https://certs4sale.com/cisco/700-250-pdf-exam-dumps>

Product Questions: 53

Version: 4.1

Question: 1

How are Cisco's SMB experiences designed to cater to the unique challenges and needs of SMBs?

- A. providing generalized training and support
- B. offering dedicated support lines and training modules specifically for SMB customers
- C. reducing confusion by limiting deployment options
- D. building SMB experiences around on-premises devices so internet outages do not affect productivity

Answer: B

Explanation:

Cisco's SMB experiences are tailored to address the unique challenges faced by small and medium businesses. These include limited IT resources, budget constraints, and the need for efficient and easy-to-manage solutions. To cater to these needs, Cisco provides dedicated support lines and training modules specifically designed for SMB customers. This approach ensures that SMBs receive focused and specialized assistance, which helps them effectively utilize Cisco's technology and

maximize their investment. By offering these dedicated resources, Cisco enhances the overall experience for SMBs, enabling them to deploy and manage their IT infrastructure with greater confidence and efficiency.

Reference:

- Cisco SMB Solutions Overview
- Cisco SMB Support and Resources Documentation

Question: 2

With technological advancements progressing faster than ever, privacy has become a significant concern. What is Cisco's belief about privacy?

- A. It is a fundamental human right.
- B. It's important to security.
- C. It is optional.
- D. It is a business strategy.

Answer: A

Explanation:

Cisco firmly believes that privacy is a fundamental human right. This belief underpins their approach to developing and implementing security measures across their products and services. Cisco is committed to protecting the privacy of individuals and organizations by ensuring that their data is handled with the utmost care and in compliance with global privacy regulations. This stance on privacy drives Cisco to design their technologies with robust security features that safeguard user information and promote trust.

Reference:

- Cisco Trust Center
- Cisco Privacy Data Sheets and Policies

Question: 3

Which devices are considered cloud-first technology?

- A. Catalyst devices
- B. IP video endpoints
- C. Meraki devices
- D. HVAC Sensors

Answer: C

Explanation:

Meraki devices are considered cloud-first technology because they are designed to be managed through the cloud, providing centralized control and visibility over the network. This cloud-based approach simplifies the management of network infrastructure, making it more accessible and efficient for SMBs and enterprises alike. Meraki's cloud-first design allows for seamless updates, scalability, and real-time monitoring, which are crucial for modern IT environments. This contrasts with traditional on-premises devices that require more manual management and maintenance.

Reference:

- Cisco Meraki Product Overview
- Cisco Meraki Cloud Management Documentation

Question: 4

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:

A proactive security strategy is essential for reducing the number of cyberattacks and breaches an organization faces. This approach involves anticipating potential security threats and taking measures to prevent them before they can cause harm. Elements of a proactive security strategy include continuous monitoring, regular vulnerability assessments, timely patching of software, employee training on cybersecurity best practices, and the implementation of advanced security technologies such as intrusion detection systems and automated threat response. By staying ahead of potential threats, organizations can significantly reduce their risk of cyberattacks and breaches.

Reference:

- Cisco Security Strategy Documentation
- Cisco Cybersecurity Reports

Question: 5

How are customers who have not spent any money in the last 12 quarters classified?

- A. Renewed Logo
- B. Stable Logo
- C. New Logo

D. Dormant Logo

Answer: D

Explanation:

Customers who have not spent any money in the last 12 quarters are classified as "Dormant Logo." This classification helps businesses identify customers who have become inactive over a significant period. Understanding which customers fall into this category allows companies to develop targeted re-engagement strategies to win back their business. By identifying and addressing the needs of dormant customers, businesses can potentially reactivate these accounts and improve their overall customer retention rates.

Reference:

- Cisco Customer Classification Guidelines
- Cisco Sales Strategies Documentation

Question: 6

Which solution is recommended for SMBs seeking to optimize and automate?

A. platform-as-a-service

B. AI powered applications

C. business intelligence

D. Generative Ai

Answer: B

Explanation:

For SMBs looking to optimize and automate their operations, AI-powered applications are highly recommended. These applications leverage artificial intelligence to streamline business processes, enhance decision-making, and improve efficiency. Examples of AI-powered applications include automated customer service chatbots, predictive analytics tools, and intelligent automation systems for tasks like invoicing and inventory management. By adopting AI-powered solutions, SMBs can achieve greater productivity, reduce operational costs, and stay competitive in their market.

Reference:

- Cisco AI Solutions for SMBs
- Cisco Automation and Optimization Technologies

Question: 7

Environmental sustainability is very important to Cisco. What is Cisco's goal regarding net zero emissions?

- A. achieve it by 2025
- B. achieve it by 2030
- C. achieve it by 2040
- D. has already been achieved

Answer: C

Explanation:

Cisco has set a goal to achieve net zero emissions by 2040. This ambitious target reflects Cisco's commitment to environmental sustainability and its recognition of the urgent need to address climate change. Achieving net zero emissions means that Cisco aims to balance the amount of greenhouse gases emitted with an equivalent amount being removed from the atmosphere, resulting in a net zero carbon footprint. This goal involves reducing emissions across its operations

and supply chain and investing in renewable energy and carbon offset projects.

Reference:

- Cisco Environmental Sustainability Goals
- Cisco CSR Reports

Question: 8

Which Cisco solution should a community college implement to fortify DNS requests?

- A. Umbrella
- B. DNS redundancy
- C. Cisco Secure Email
- D. Duo

Answer: A

Explanation:

Cisco Umbrella is the recommended solution for a community college looking to fortify DNS requests. Cisco Umbrella provides secure DNS-layer protection, blocking malicious domains, IP addresses, and cloud applications before they can reach the network. This helps prevent phishing, malware, and other cyber threats, ensuring a safer online environment for students, faculty, and staff. The solution is cloud-based, making it easy to deploy and manage without requiring additional hardware.

Reference:

- Cisco Umbrella Product Overview
- Cisco DNS Security Solutions

Question: 9

Which Cisco product is part of the Secure SMB experience for enhancing workspaces?

- A. Duo
- B. Umbrella
- C. DNA Center
- D. Meraki Cameras

Answer: D

Explanation:

Meraki Cameras are part of the Secure SMB experience, designed to enhance workspaces by providing advanced security and surveillance capabilities. These cloud-managed smart cameras offer high-definition video monitoring, analytics, and easy integration with other security systems. Meraki Cameras help SMBs improve physical security, monitor business operations, and ensure the safety of their employees and assets. The simplicity of deployment and management through the Meraki Dashboard makes them a suitable choice for SMBs looking to bolster their security infrastructure.

Reference:

- Cisco Meraki Cameras Product Information
- Cisco Secure SMB Solutions

Question: 10

Technology takes many different forms and impacts every aspect of our lives. In Cisco's view, what is the role of technology?

- A. to increase costs for businesses
- B. to limit global connectivity
- C. to complicate processes
- D. to change lives and empower people

Answer: D

Explanation:

Cisco believes that the role of technology is to change lives and empower people. This perspective underscores Cisco's commitment to developing innovative solutions that enhance connectivity, productivity, and overall quality of life. By leveraging technology, Cisco aims to bridge digital divides, enable global communication, and provide tools that help individuals and organizations achieve their full potential. Technology is seen as a positive force that drives progress and creates opportunities for personal and professional growth.

Reference:

- Cisco Corporate Social Responsibility Report
- Cisco Vision and Mission Statements

Question: 11

What is a quality requirement for a secure SMB?

- A. endpoint security with threat hunting and vulnerability management

- B. cloud-delivered security to all devices
- C. low friction secure access process
- D. zero trust identity-based access to every application

Answer: D

Explanation:

A key quality requirement for a secure SMB is implementing zero trust identity-based access to every application. This security model ensures that only authenticated and authorized users can access applications, regardless of their location or device. By adopting a zero trust approach, SMBs can significantly reduce the risk of unauthorized access and data breaches. This involves continuous verification of user identities, strict access controls, and monitoring of all network activities. The zero trust framework is essential for maintaining robust security in an environment where remote work and cloud applications are prevalent.

Reference:

- Cisco Zero Trust Security Solutions
- Cisco Secure SMB Guidelines

Question: 12

Where do SMB partners find free-to-use customizable campaigns and assets?

- A. Cisco Solutions Velocity Central
- B. The Life Cycle Advantage Portal
- C. Cisco Velocity Advantage Portal
- D. Cisco Marketing Velocity Central

Answer: D

Explanation:

SMB partners can find free-to-use customizable campaigns and assets on Cisco Marketing Velocity Central. This platform offers a wide range of marketing resources tailored to help Cisco partners create effective campaigns, promote their services, and drive customer engagement. These resources include templates, guides, and tools that partners can customize to suit their specific needs, making it easier to market Cisco products and solutions effectively.

Reference:

- Cisco Marketing Velocity Central Overview
- Cisco Partner Marketing Resources

Question: 13

What is a functional requirement for a secure SMB?

- A. high-quality, seamless, and resilient capture capabilities
- B. a holistic view of all data
- C. low friction secure access process
- D. zero trust identity-based access to applications with multifactor authentication

Answer: D

Explanation:

A functional requirement for a secure SMB includes implementing zero trust identity-based access to applications with multifactor authentication (MFA). This approach ensures that only verified users can access sensitive data and applications, adding an extra layer of security through MFA. By requiring multiple forms of verification, SMBs can protect against unauthorized access and reduce the risk of security breaches, ensuring that their data and applications remain secure even if user

credentials are compromised.

Reference:

- Cisco Zero Trust Security Solutions
- Cisco Multifactor Authentication Best Practices

Question: 14

What is a benefit of using Meraki in retail SMB?

- A. quickly troubleshoot issues
- B. decentralized security
- C. manage each store's devices independently
- D. monitor performance after data has been stored in the cloud

Answer: A

Explanation:

One of the key benefits of using Meraki in retail SMBs is the ability to quickly troubleshoot issues. Meraki's cloud-based management platform provides centralized visibility and control over the entire network, enabling IT administrators to identify and resolve problems efficiently. This rapid troubleshooting capability helps minimize downtime, maintain a high level of customer service, and ensure that the retail operations run smoothly. Additionally, Meraki's intuitive dashboard simplifies network management, making it easier for retail SMBs to manage their IT infrastructure.

Reference:

- Cisco Meraki for Retail Solutions

- Cisco Meraki Dashboard Features

Question: 15

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: B

Explanation:

Meraki Insight is a Cisco product that is part of the smart experience for enabling workspaces. It provides deep visibility into network and application performance, allowing organizations to proactively identify and troubleshoot issues that could impact user experience. By leveraging Meraki Insight, businesses can optimize their network performance, ensure seamless application delivery, and enhance overall productivity in the workspace.

Reference:

- Cisco Meraki Insight Product Overview
- Cisco Smart Workspaces Solutions

Question: 16

Which features are managed in the Cisco Control Hub?

- A. Catalyst Switches

B. Meetings and Messagin91

C. Meraki Cameras

D. Cisco IP Phones

Answer: B

Explanation:

The Cisco Control Hub is a centralized management platform used to manage features related to meetings and messaging. It allows administrators to configure, monitor, and troubleshoot Cisco Webex services, ensuring effective communication and collaboration across the organization. The Control Hub provides analytics, security settings, and user management tools, making it an essential part of managing Cisco's collaboration suite.

Reference:

- Cisco Control Hub Documentation
- Cisco Webex Meetings and Messaging Management

Question: 17

Which segment presents the largest opportunity for managed services?

A. Collaboration

B. Security

C. Data Center

D. Observability

Answer: B

Explanation:

The segment that presents the largest opportunity for managed services is Security. With the increasing complexity of cyber threats and the growing need for robust security measures, businesses are turning to managed security services to protect their networks and data. Managed security services offer comprehensive solutions, including threat detection and response, vulnerability management, and compliance monitoring, providing businesses with the expertise and resources needed to maintain a secure environment.

Reference:

- Cisco Managed Security Services Overview
- Market Analysis Reports on Managed Security Services

Question: 18

Which product enhances workspaces for SMBs by accelerating the Webex platform experience?

A. Webex Breakout Rooms

B. Webex Control Hub

C. Webex Boards

D. Webex Polls

Answer: C

Explanation:

Webex Boards enhance workspaces for SMBs by accelerating the Webex platform experience. These

interactive touchscreens integrate with the Webex platform, enabling seamless collaboration through video conferencing, digital whiteboarding, and content sharing. Webex Boards create an engaging and productive environment for meetings, brainstorming sessions, and team collaboration, making them a valuable tool for SMBs looking to optimize their workspace experience.

Reference:

- Cisco Webex Boards Product Information
- Cisco Collaboration Solutions for SMBs

Question: 19

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:

The SMB Experience Explorer is designed for Cisco partners to co-brand and embed on their websites. This feature allows partners to showcase Cisco's SMB solutions, providing an interactive way for potential customers to explore the offerings and benefits. By co-branding the SMB Experience Explorer, partners can enhance their marketing efforts and demonstrate the value of Cisco's SMB solutions to their clients.

Reference:

- Cisco Partner Marketing Tools

- Cisco SMB Experience Explorer Overview

Question: 20

For which portfolio is Cisco a global leader?

- A. security
- B. cloud security
- C. networking
- D. data monitoring

Answer: C

Explanation:

Cisco is a global leader in networking. The company's extensive portfolio includes solutions for enterprise networking, data center networking, cloud networking, and more. Cisco's networking products and technologies are known for their reliability, scalability, and innovation, making them a top choice for businesses worldwide. Cisco's leadership in networking is supported by a strong ecosystem of partners and a commitment to continuous improvement and adaptation to emerging trends.

Reference:

- Cisco Networking Solutions
- Industry Reports on Networking Leaders

Question: 21

Which Cisco product secures the perimeter less, work-from-anywhere world with Zero Trust?

- A. Duo

B. Meraki MX

C. Umbrella

D. Meraki Insight

Answer: A

Explanation:

Cisco Duo is designed to secure the perimeter-less, work-from-anywhere world with a Zero Trust approach. Duo ensures that only authenticated and authorized users can access applications and data, regardless of their location. It provides multi-factor authentication (MFA), device visibility, and adaptive access policies to protect against unauthorized access and enhance security in a distributed workforce environment.

Reference:

- Cisco Duo Security Overview
- Cisco Zero Trust Security Solutions

Question: 22

Which Cisco product is part of Remote SMB for empowering IT management?

A. ThousandEyes

B. Umbrella

C. Cisco Secure Endpoint

D. Duo

Answer: B

Explanation:

Cisco Umbrella is part of the Remote SMB solutions, empowering IT management by providing cloud-delivered security that protects users both on and off the network. Umbrella offers DNS-layer security, secure web gateway capabilities, and cloud-delivered firewall features, ensuring comprehensive protection and visibility across the entire network. It simplifies security management and enhances the ability of IT teams to protect remote workers effectively.

Reference:

- Cisco Umbrella Product Information
- Cisco Remote Work Solutions

Question: 23

Which marketing asset educates partners about Cisco's overarching SMB strategy?

A. SMB Partner Campaign Kit

B. Select SMB Assets

C. SMB Marketing Toolbox

D. SMB Marketing Kit

Answer: C

Explanation:

The SMB Marketing Toolbox is designed to educate partners about Cisco's overarching SMB strategy. This comprehensive toolkit provides resources, insights, and materials that help partners understand and effectively communicate Cisco's strategic vision for the small and medium business segment. It includes various marketing assets that detail the unique value propositions, competitive differentiators, and go-to-market strategies tailored for SMB customers, thereby enabling partners to

align their sales and marketing efforts with Cisco's SMB objectives.

Question: 24

What does the hybrid SMB experience deliver to the customer?

- A. cloud security
- B. secure Connectivity and dynamic collaboration
- C. zero trust identity-based access
- D. less distributed applications

Answer: B

Explanation:

The hybrid SMB experience delivered by Cisco focuses on providing secure connectivity and dynamic collaboration. This approach ensures that SMBs can maintain secure connections across various environments, whether in-office or remote, and leverage dynamic collaboration tools that enhance productivity and communication. This experience integrates Cisco's robust security protocols and collaboration solutions, such as Webex, to support a seamless and efficient work environment for SMBs, adapting to the hybrid work model that combines both remote and in-person work.

Reference: Cisco Small and Medium Business Sales Documentation

Question: 25

Which device connects remote SMB workers with power collaboration solutions and award-winning devices?

- A. Meraki Insight

B. Cloud Meeting Solutions

C. WebEX

D. Meraki Systems Manager

Answer: C

Explanation:

Webex is the device that connects remote SMB workers with powerful collaboration solutions and award-winning devices. As a leading solution in video conferencing and online meetings, Webex provides a platform for secure and effective communication and collaboration. It integrates seamlessly with various devices and applications, offering features like video conferencing, screen sharing, and real-time messaging. This makes it an ideal tool for remote SMB workers who need to stay connected and collaborate efficiently, no matter their location.

Question: 26

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

A. CML

B. Catalyst Access Points

C. Webex Control Hub

D. FirePower Firewalls

Answer: D

Explanation:

Cisco FirePower Firewalls are specifically designed to provide advanced threat protection and mitigation of network vulnerabilities. These firewalls offer next-generation features, such as intrusion prevention systems (IPS), advanced malware protection (AMP), and URL filtering, which are crucial for securing SMB networks against various threats. FirePower Firewalls can detect and block sophisticated threats in real-time, offering comprehensive security solutions that protect network assets from attacks.

1. Advanced Threat Protection: FirePower Firewalls use a combination of deep packet inspection, real-time threat intelligence, and behavior-based analysis to detect and mitigate threats.
2. Intrusion Prevention System (IPS): This feature identifies and stops malicious traffic and known vulnerabilities before they can enter the network.
3. Advanced Malware Protection (AMP): AMP provides continuous analysis and retrospective security, helping to detect, track, and remediate advanced malware.
4. URL Filtering: This feature blocks access to malicious websites and unwanted content, reducing the risk of phishing and other web-based attacks.

Reference:

- Cisco Firepower Next-Generation Firewall Data Sheet
- Cisco Small Business Solutions Guide
- Cisco FirePower Threat Defense Configuration Guide

Question: 27

Which Cisco product features Integrated Mobile Device Management?

A. Duo

B. Umbrella

C. Meraki

D. Webex

Answer: C

Explanation:

Cisco Meraki offers integrated mobile device management (MDM) as part of its cloud-managed networking solutions. The Meraki Dashboard provides centralized management of network devices, including mobile devices, which allows IT administrators to enforce security policies, monitor device compliance, and manage app deployment.

1. Centralized Management: The Meraki Dashboard enables centralized control over all network devices, including mobile endpoints, through a single interface.
2. Device Enrollment: Administrators can enroll mobile devices in the Meraki system for management and monitoring.
3. Security Policies: Meraki allows the application of security policies to mobile devices, ensuring they meet organizational security standards.
4. App Management: IT administrators can deploy, manage, and update applications on enrolled mobile devices remotely.

Reference:

- Cisco Meraki Mobile Device Management Data Sheet
- Cisco Meraki Dashboard Overview
- Cisco Small Business Solutions Guide

Question: 28

Which security challenge do SMBs face?

A. global shortage of security experts

- B. smaller attack surface
- C. lack of security products
- D. lack of knowledge in cloud security

Answer: D

Explanation:

SMBs (Small and Medium Businesses) often face significant challenges regarding cloud security due to a lack of expertise and knowledge in this domain. As many SMBs migrate to cloud services to leverage cost and efficiency benefits, they often do not have the necessary skills or understanding to secure these environments properly. This can lead to misconfigurations, inadequate protection against threats, and potential data breaches.

1. Limited Resources: SMBs typically have fewer resources to dedicate to IT and security, making it challenging to hire or train personnel with cloud security expertise.
2. Complexity of Cloud Security: Cloud environments introduce new security considerations that differ from traditional on-premises infrastructure, requiring specific knowledge and practices.
3. Evolving Threat Landscape: The dynamic nature of cybersecurity threats necessitates ongoing education and adaptation, which can be challenging for SMBs to keep up with.

Reference:

- Cisco Small Business Security Solutions Overview
- Cisco Cybersecurity Reports
- SMB Cloud Security Challenges Whitepapers

Question: 29

Which security challenge do SMBs face?

- A. global shortage of security experts

- B. smaller attack surface
- C. lack of security products
- D. lack of knowledge in cloud security

Answer: D

Explanation:

One of the critical security challenges faced by SMBs is the global shortage of security experts. This shortage affects SMBs more acutely as they compete with larger enterprises for the limited pool of qualified security professionals. The lack of available expertise can hinder an SMB's ability to implement effective security measures, manage security infrastructure, and respond to incidents.

1. High Demand, Low Supply: The cybersecurity field is experiencing a high demand for skilled professionals, but the supply of qualified individuals is insufficient.
2. Recruitment Challenges: SMBs may struggle to attract and retain security experts due to limited budgets and resources compared to larger companies.
3. Impact on Security Posture: Without access to skilled security professionals, SMBs may face challenges in maintaining robust security defenses and addressing vulnerabilities promptly.

Reference:

- Cisco Security Workforce Studies
- Global Information Security Workforce Study (GISWS)
- Cisco Small Business Cybersecurity Report

Question: 30

What will remain a top priority because of the growing number of connected devices and geopolitical issues?

- A. cyber security
- B. collaboration tools

- C. cashflow
- D. AI-powered applications

Answer: A

Explanation:

Cybersecurity will remain a top priority due to the increasing number of connected devices and ongoing geopolitical issues. The proliferation of IoT devices and the interconnected nature of modern networks expand the potential attack surface, making robust cybersecurity measures essential. Additionally, geopolitical tensions can lead to state-sponsored cyber attacks, requiring businesses of all sizes to prioritize their cybersecurity strategies to protect sensitive information and ensure operational continuity.

1. Growth of Connected Devices: The increasing number of IoT and other connected devices introduces new vulnerabilities and attack vectors that need to be secured.
2. Geopolitical Tensions: Geopolitical issues often manifest in the digital realm through cyber espionage, attacks on critical infrastructure, and other malicious activities, highlighting the need for strong cybersecurity defenses.
3. Continuous Threat Evolution: Cyber threats are continuously evolving, necessitating ongoing vigilance, updated security measures, and a proactive approach to cybersecurity.

Reference:

- Cisco Annual Cybersecurity Report
- Cisco Small Business Solutions Guide
- Industry Reports on Cybersecurity Priorities and Trends

Question: 31

Which groundbreaking feature leverages Meraki Cameras?

- A. Smart Health Notifications
- B. Smart Cleaning Notifications
- C. Smart IoT Notifications
- D. Smart Secure Notifications

Answer: C

Explanation:

Meraki Cameras leverage Smart IoT Notifications as part of their innovative features. These notifications are part of the broader Meraki IoT (Internet of Things) ecosystem, enabling advanced capabilities such as detecting unusual activity, monitoring environmental conditions, and integrating with other IoT devices for comprehensive smart management. The cameras provide intelligent alerts and notifications based on various triggers and conditions, enhancing security and operational efficiency.

1. Integration with IoT Ecosystem: Meraki Cameras can integrate with other IoT devices and systems, allowing for comprehensive monitoring and management.
2. Advanced Analytics: The cameras use advanced video analytics to detect unusual patterns and activities, sending smart notifications to administrators.
3. Enhanced Security: By leveraging IoT notifications, Meraki Cameras provide real-time alerts on potential security breaches or anomalies.

Reference:

- Cisco Meraki MV Cameras Data Sheet
- Cisco Meraki IoT Solutions Overview
- Meraki Smart Notifications and Analytics Documentation

Question: 32

Which Cisco product is part of Remote SMB for enabling people?

- A. Meraki Dashboard
- B. Cisco Secure Client
- C. Meraki Smart Cleaning
- D. Meraki MV

Answer: A

Explanation:

The Meraki Dashboard is a critical component of remote SMB solutions, enabling people to manage and monitor their network infrastructure remotely. The cloud-based dashboard provides a centralized platform for network management, configuration, and troubleshooting, making it ideal for remote work environments.

1. Centralized Management: The Meraki Dashboard allows administrators to manage multiple network devices from a single, intuitive interface.
2. Remote Access: IT staff can access the dashboard from anywhere, enabling them to support remote users and troubleshoot issues without needing to be on-site.
3. Comprehensive Monitoring: The dashboard provides detailed insights and analytics, helping businesses ensure network performance and security.

Reference:

- Cisco Meraki Dashboard Overview
- Cisco Remote Work Solutions Guide
- Meraki Cloud Management Documentation

Question: 33

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 a Cisco product designed to empower IT with a smart experience by providing deep visibility and understanding of network and application performance. It helps IT administrators quickly identify and resolve issues that impact user experience, ensuring optimal network performance and reliability.

1. Network and Application Performance Monitoring: Meraki Insight provides insights into both network and application performance, helping IT teams troubleshoot and optimize their infrastructure.
2. Proactive Alerts: The system sends proactive alerts about potential issues, allowing IT to address problems before they impact users.
3. Detailed Analytics: Meraki Insight offers detailed analytics and reporting, enabling IT teams to make informed decisions about network management and optimization.

Reference:

- Cisco Meraki Insight Data Sheet
- Cisco Meraki Insight Overview
- Cisco Smart IT Solutions Documentation

Question: 34

By which margin are MSPs expected to grow in the next year?

- A. 9%
- B. 11%
- C. 15%
- D. 17%

Answer: C

Explanation:

MSPs (Managed Service Providers) are projected to grow by a margin of 15% in the next year. This growth is driven by the increasing reliance of businesses on managed services for their IT needs, as well as the ongoing shift towards digital transformation and cloud adoption. The demand for managed services is rising as SMBs look to outsource their IT management to specialized providers to enhance efficiency, security, and performance.

1. Market Demand: The growing complexity of IT environments and the need for specialized expertise are fueling the demand for MSPs.
2. Digital Transformation: Businesses are increasingly adopting digital tools and cloud services, which MSPs help to manage and optimize.
3. Security Needs: With the rise in cyber threats, SMBs are turning to MSPs for robust security solutions.

Reference:

- Industry Reports on MSP Market Growth
- Cisco Managed Services Overview
- Market Analysis on IT Services and Managed Services Growth

Question: 35

How are customers classified who have spent at least \$1 in each of the four quarters over the last 12 months?

- A. Stable Buyer
- B. Occasional Buyer
- C. Repeat Buyer
- D. Frequent Buyer

Answer: C

Explanation:

Customers who have spent at least \$1 in each of the four quarters over the last 12 months are classified as Repeat Buyers. This classification indicates a level of consistent purchasing behavior,

reflecting customer loyalty and ongoing engagement with the company's products or services.

1. Consistency in Purchases: Spending in each quarter demonstrates regular interaction and reliance on the products or services offered.

2. Customer Loyalty: Regular purchasing behavior suggests a satisfaction with the products and services, indicating loyalty.

3. Engagement Metrics: Repeat buyers are often seen as a key metric for customer retention and long-term business relationships.

Reference:

- Customer Classification and Segmentation Guidelines
- Cisco Customer Relationship Management Strategies
- Industry Standards for Customer Purchasing Behavior

Question: 36

How does Cisco help SMBs to be truly smart?

A. secure connectivity

B. operational inefficiencies

C. employee automation

D. utilities cost control

Answer: A

Explanation:

Cisco helps SMBs to be truly smart through secure connectivity. Secure connectivity is fundamental for SMBs to operate efficiently, protect their data, and ensure that their network infrastructure

supports their business needs. Cisco provides comprehensive solutions that include secure networking, advanced security features, and robust infrastructure management, all designed to help SMBs achieve secure and reliable connectivity.

1. Secure Networking Solutions: Cisco offers a range of networking solutions that provide secure and reliable connectivity for SMBs.

2. Advanced Security Features: These include firewalls, VPNs, and intrusion prevention systems to protect SMB networks from threats.

3. Comprehensive Management: Tools like the Meraki Dashboard allow SMBs to manage their network infrastructure securely and efficiently.

Reference:

- Cisco Secure Connectivity Solutions Overview
- Cisco SMB Networking Solutions Guide
- Cisco Security Products and Services Documentation

Question: 37

Which Cisco solution provides end-to-end visibility from every user to any application?

- A. Cisco Overwatch
- B. ThousandEyes
- C. Meraki Dashboard
- D. Cisco Control Hub

Answer: B

Explanation:

ThousandEyes provides end-to-end visibility from every user to any application, which is crucial for maintaining optimal network performance and user experience. It offers detailed insights into network paths and application delivery, enabling IT teams to monitor and troubleshoot performance issues across the entire network, including the internet, cloud, and enterprise networks.

1. End-to-End Visibility: ThousandEyes provides comprehensive visibility into the entire network path, from the user to the application, regardless of the location or network segments involved.
2. Network and Application Performance Monitoring: It continuously monitors the performance of applications and the underlying network, identifying bottlenecks and issues affecting user experience.
3. Troubleshooting and Analysis: ThousandEyes offers powerful tools for diagnosing and resolving performance issues, providing detailed metrics and analysis to pinpoint the source of problems.

Reference:

- Cisco ThousandEyes Overview
- ThousandEyes Data Sheet
- Cisco Network Performance Monitoring Solutions

Question: 38

Which visibility product empowers IT by providing insight into application performance?

- A. Duo
- B. ThousandEyes
- C. Webex Control Hub
- D. Umbrella

Answer: B

Explanation:

ThousandEyes empowers IT by providing in-depth insights into application performance. It enables IT teams to monitor, troubleshoot, and optimize the performance of applications across the entire network, ensuring a seamless user experience. ThousandEyes offers visibility into the performance of SaaS applications, internal applications, and the underlying network infrastructure.

1. Application Performance Monitoring: ThousandEyes provides detailed metrics on application performance, helping IT teams identify and address issues that impact user experience.
2. Network Path Analysis: It offers visibility into the network paths that applications take, allowing for precise identification of where performance degradation occurs.
3. Proactive Alerts and Reporting: ThousandEyes sends proactive alerts about performance issues and provides comprehensive reports to help IT teams maintain optimal application performance.

Reference:

- Cisco ThousandEyes Data Sheet
- ThousandEyes Application Performance Monitoring Guide
- Cisco IT Performance Management Solutions

Question: 39

Which percent of SMBs are using more SaaS applications?

- A. 39%
- B. 57%
- C. 80%
- D. 100%

Answer: C

Explanation:

80% of SMBs are using more SaaS applications. The adoption of Software as a Service (SaaS) has been

rapidly increasing among SMBs due to its flexibility, scalability, and cost-effectiveness. SMBs find SaaS applications beneficial for enhancing productivity, collaboration, and business operations without the need for extensive on-premises infrastructure.

1. Flexibility and Scalability: SaaS applications allow SMBs to easily scale their usage based on needs without significant upfront investments.
2. Cost-Effectiveness: By using SaaS, SMBs can reduce costs associated with maintaining and updating on-premises hardware and software.
3. Enhanced Productivity: SaaS applications often include features that improve collaboration and efficiency, making them attractive to SMBs.

Reference:

- Industry Reports on SaaS Adoption among SMBs
- Cisco Small Business Solutions Overview
- Market Analysis on Cloud Services and SaaS Usage

Question: 40

According to the IDC, what is the expected spend on Future of Work technology and services in 2025?

- A. \$500 billion
- B. \$1 trillion
- C. \$1.2 trillion
- D. \$2 trillion

Answer: C

Explanation:

According to the IDC, the expected spend on Future of Work technology and services in 2025 is projected to be \$1.2 trillion. This spending encompasses investments in technologies and services that support new ways of working, including remote work infrastructure, collaboration tools,

cybersecurity, and automation.

1. Remote Work Infrastructure: Increased investment in tools and services that support remote work, including secure connectivity and cloud services.

2. Collaboration Tools: Spending on advanced collaboration platforms that facilitate seamless communication and teamwork.

3. Cybersecurity: Enhanced focus on security solutions to protect distributed workforces and data.

4. Automation: Investment in technologies that automate repetitive tasks and improve operational efficiency.

Reference:

- IDC Future of Work Spending Projections
- Cisco Future of Work Technology Reports
- Market Trends and Analysis on Remote Work Technologies

Question: 41

Which Meraki product is used in Remote SMB work from home?

A. Z4 teleworker gateway

B. Meraki Insight

C. Meraki MV

D. Meraki MT

Answer: A

Explanation:

The Meraki Z4 teleworker gateway is specifically designed for remote SMB work-from-home

scenarios. It provides secure connectivity and robust networking features to support employees working remotely, ensuring they have reliable access to corporate resources.

1. Secure Connectivity: The Z4 gateway provides secure VPN connections, ensuring remote workers can access corporate networks securely.
2. Comprehensive Networking: It offers advanced networking features such as traffic shaping, content filtering, and Wi-Fi, which are essential for remote work environments.
3. Easy Management: The Z4 can be managed remotely via the Meraki Dashboard, making it easy for IT teams to deploy and monitor.

Reference:

- Cisco Meraki Z4 Teleworker Gateway Data Sheet
- Meraki Remote Work Solutions Overview
- Cisco SMB Remote Work Product Documentation

Question: 42

Which Meraki product is used in Remote SMB work from home?

- A. Z4 teleworker gateway
- B. Meraki Insight
- C. Meraki MV
- D. Meraki MT

Answer: A

Explanation:

The Meraki Z4 teleworker gateway is designed to support remote work environments for SMBs. It provides secure and reliable connectivity for employees working from home, ensuring they can access corporate resources efficiently and securely.

1. Secure VPN Connectivity: The Z4 teleworker gateway offers secure VPN connections, allowing

remote workers to securely access the corporate network.

2. Comprehensive Features: It includes advanced networking features such as traffic shaping, content filtering, and integrated Wi-Fi, which are essential for home office setups.

3. Remote Management: The Z4 can be easily managed via the Meraki Dashboard, providing IT administrators with the tools to deploy, monitor, and troubleshoot remotely.

Reference:

- Cisco Meraki Z4 Teleworker Gateway Data Sheet
- Meraki Remote Work Solutions Overview
- Cisco SMB Remote Work Product Documentation

Question: 43

Securing the DNS layer means blocking malicious domains, IP addresses, and cloud applications before establishing a connection. Which Cisco solution helps secure

A. Duo

B. ThousandEyes

C. Umbrella

D. Email Threat Defense

Answer: C

Explanation:

Cisco Umbrella secures the DNS layer by blocking malicious domains, IP addresses, and cloud applications before a connection is established. This proactive security measure helps prevent threats from reaching the network and reduces the risk of malware infections and data breaches.

1. DNS-layer Security: Umbrella blocks malicious domains and IP addresses at the DNS layer, preventing users from accessing dangerous websites and applications.
2. Threat Intelligence: Umbrella leverages real-time threat intelligence to identify and block new and emerging threats.
3. Cloud-based Protection: As a cloud-delivered solution, Umbrella is easy to deploy and manage, providing scalable protection for users both on and off the network.

Reference:

- Cisco Umbrella Overview
- Cisco DNS-layer Security Whitepaper
- Cisco Umbrella Product Documentation

Question: 44

What is an important benefit of SMB experiences?

- A. teams should be in the office to be most productive
- B. does not allow for the interaction of multi-vendor collaboration tools
- C. allows a reduction in the number of people responsible for security
- D. by offering integrated solutions that allow SMBs to stay within their budget constraints

Answer: D

Explanation:

An important benefit of SMB experiences is offering integrated solutions that allow SMBs to stay within their budget constraints. SMBs typically have limited resources and need cost-effective solutions that can deliver the necessary functionality without breaking the bank. Integrated solutions help SMBs by combining multiple functions into a single package, reducing the need for multiple vendors and simplifying management.

1. Cost-Effectiveness: Integrated solutions are generally more affordable as they bundle multiple functionalities into one, saving on the costs of purchasing and maintaining separate systems.
2. Simplified Management: Having an integrated solution means that SMBs can manage their IT infrastructure more easily, reducing the complexity and workload for IT staff.
3. Vendor Reduction: By relying on fewer vendors, SMBs can streamline their operations, reduce the need for multiple support contracts, and minimize compatibility issues.

Reference:

- Cisco SMB Solutions Overview
- Benefits of Integrated IT Solutions for SMBs
- Cisco Cost-Effective Solutions for Small Businesses

Question: 45

What is an important benefit of SMB experiences?

- A. teams should be in the office to be most productive
- B. does not allow for the interaction of multi-vendor collaboration tools
- C. allows a reduction in the number of people responsible for security
- D. by offering integrated solutions that allow SMBs to stay within their budget constraints

Answer: D

Explanation:

An important benefit of SMB experiences is offering integrated solutions that allow SMBs to stay within their budget constraints. SMBs often face financial limitations and need efficient solutions that provide essential functionalities without incurring high costs. Integrated solutions help by combining various features and tools into a single, cohesive package, ensuring that SMBs can manage their operations effectively while keeping expenses in check.

1. Affordability: Integrated solutions tend to be more affordable compared to purchasing separate products for each function, helping SMBs manage their budgets more effectively.
2. Ease of Use: These solutions simplify IT management by providing a unified platform, reducing the complexity and effort required to manage multiple systems.
3. Operational Efficiency: Integrated solutions streamline processes and improve productivity by providing seamless interoperability between different tools and systems.

Reference:

- Cisco SMB Solutions Overview
- Integrated IT Solutions for Small Businesses
- Cisco Budget-Friendly IT Solutions for SMBs

Question: 46

Which Cisco solution helps keep a healthcare patient's information secure?

- A. Cisco Care Plus
- B. Duo
- C. Meraki Systems Manager
- D. DNS redundancy

Answer: B

Explanation:

Duo, a Cisco solution, helps keep healthcare patient information secure by providing robust multi-factor authentication (MFA) and secure access controls. Duo ensures that only authorized users can access sensitive healthcare information, thereby protecting patient data from unauthorized access and breaches.

1. Multi-Factor Authentication (MFA): Duo provides an additional layer of security by requiring users to verify their identity through multiple factors before accessing sensitive information.
2. Access Controls: Duo allows healthcare organizations to enforce strict access controls, ensuring that only authorized personnel can access patient information.
3. Compliance: Duo helps healthcare providers meet regulatory compliance requirements, such as HIPAA, by securing patient information and maintaining data privacy.

Reference:

- Cisco Duo Security Overview
- Cisco Solutions for Healthcare
- Healthcare Data Security Compliance Documentation

Question: 47

Which solution allows SMBs flexibility and proper execution without dedicating to expensive IT resources?

- A. cyber security
- B. business intelligence
- C. AI-powered applications
- D. platform-as-a-service

Answer: D

Explanation:

Platform-as-a-service (PaaS) allows SMBs flexibility and proper execution without dedicating to expensive IT resources. PaaS provides a cloud-based environment where SMBs can develop, run, and manage applications without the complexity of building and maintaining the underlying infrastructure.

1. Flexibility: PaaS offers a scalable environment that can be adjusted according to the SMB's needs, allowing for flexibility in application development and deployment.

2. Cost-Effective: By using PaaS, SMBs can avoid the high costs associated with purchasing and maintaining hardware and software infrastructure.
3. Focus on Development: PaaS enables SMBs to focus on developing and delivering applications rather than managing IT infrastructure, thus improving efficiency and innovation.

Reference:

- Cisco Platform-as-a-Service Solutions
- Benefits of PaaS for SMBs
- Cloud Computing and SMB Flexibility Documentation

Question: 48

Which Cisco product is part of the Secure SMB experience for enabling people?

- A. Meraki MX
- B. Cisco Secure Email
- C. Stealthwatch
- D. Umbrella

Answer: D

Explanation:

Cisco Umbrella is a key part of the Secure SMB experience for enabling people. Umbrella provides comprehensive security for SMBs by protecting against internet-based threats, offering DNS-layer security, and blocking malicious domains and IP addresses before they can impact the network. This helps ensure that users can work securely from anywhere, providing a safer and more productive environment.

1. DNS-layer Security: Umbrella blocks requests to malicious domains and IP addresses at the DNS layer, preventing threats before they reach the network.
2. Comprehensive Protection: It provides protection against phishing, malware, and command-and-control callbacks, securing users both on and off the network.
3. Ease of Use: Umbrella is easy to deploy and manage, making it an ideal solution for SMBs with limited IT resources.

Reference:

- Cisco Umbrella Overview
- Cisco SMB Security Solutions
- Umbrella Product Documentation

Question: 49

Which security feature provides insights into Internet activity and facilitates real-time activity search?

- A. Control Hub
- B. Duo
- C. Cloud-Delivered AI
- D. Secure Web Gateway

Answer: D

Explanation:

A Secure Web Gateway (SWG) provides insights into internet activity and facilitates real-time activity search. It monitors and controls web traffic, enforcing security policies to protect against threats and ensuring compliance with corporate policies. SWG solutions offer visibility into user activity on the internet and allow for the analysis and searching of real-time activity data.

1. Internet Activity Monitoring: SWGs provide detailed visibility into web traffic, enabling organizations to monitor user behavior and internet activity.

2. Real-Time Activity Search: They allow IT administrators to search and analyze real-time activity data to identify potential threats and enforce security policies.

3. Threat Protection: SWGs protect users from web-based threats such as malware, phishing, and malicious websites by filtering and blocking harmful content.

Reference:

- Cisco Secure Web Gateway Overview
- Internet Activity Monitoring Solutions
- Cisco Web Security Documentation

Question: 50

Which Cisco product protects against the loss of sensitive data?

- A. Meraki Systems Manager
- B. Meraki MX
- C. DUO
- D. Umbrella

Answer: B

Explanation:

The Cisco Meraki MX series is a comprehensive security and SD-WAN appliance that includes features specifically designed to protect against the loss of sensitive data. It provides robust security measures such as advanced threat protection, content filtering, and intrusion prevention, which help safeguard sensitive data from breaches and unauthorized access.

1. Advanced Threat Protection: The Meraki MX includes features like malware protection and advanced security analytics to detect and prevent data breaches.

2. Content Filtering: It helps in preventing sensitive data from being sent out or accessed by filtering

web content and applications.

3. Intrusion Prevention System (IPS): The built-in IPS provides deep packet inspection to detect and block potential threats, ensuring sensitive data remains secure.

Reference:

- Cisco Meraki MX Security and SD-WAN Overview
- Cisco Meraki MX Data Sheet
- Meraki Security and Threat Protection Documentation

Question: 51

Which challenge do customers face with hybrid work?

- A. hot desking
- B. collaboration spaces
- C. exponential increase in cloud data
- D. non-inclusive experiences

Answer: C

Explanation:

One of the significant challenges customers face with hybrid work is the exponential increase in cloud data. As more employees work remotely and use cloud services, the amount of data stored and processed in the cloud grows dramatically. This increase brings challenges related to data management, security, and compliance.

1. Data Management: Managing the large volumes of data generated by hybrid work environments

can be complex and resource-intensive.

2. Security: Ensuring the security of data across various cloud platforms and services becomes more challenging with the increased data volume.

3. Compliance: Meeting regulatory requirements for data protection and privacy can be more difficult as data spreads across multiple cloud environments.

Reference:

- Cisco Hybrid Work Solutions Overview
- Challenges of Hybrid Work and Cloud Data Management
- Industry Reports on Hybrid Work and Cloud Data Growth

Question: 52

What enables Umbrella to offer unprecedented insight into launched and staged attacks?

- A. data set of multiple geographies and protocols
- B. understanding the types of sensitive data loss by customers
- C. DNS redundancy
- D. Umbrella's geofenced network

Answer: A

Explanation:

Umbrella offers unprecedented insight into launched and staged attacks through its extensive data set of multiple geographies and protocols. This large and diverse data set allows Umbrella to detect and analyze patterns of malicious activity across different regions and protocols, providing early warning and comprehensive understanding of potential threats.

1. Global Data Coverage: Umbrella collects data from a wide range of geographic locations, giving it a broad view of global threat activity.
2. Protocol Analysis: By analyzing traffic across multiple protocols, Umbrella can identify and understand the behavior of different types of attacks.
3. Threat Intelligence: The extensive data set enhances Umbrella's threat intelligence capabilities, enabling it to detect and respond to emerging threats quickly and accurately.

Reference:

- Cisco Umbrella Threat Intelligence Overview
- Cisco Umbrella Data Collection and Analysis Documentation
- Cisco Security Solutions for Threat Detection

Question: 53

What is a crucial concern for Hybrid SMB?

- A. process automation
- B. complexity of applications
- C. more data with too little contextualization
- D. protect employees, devices, and company data

Answer: D

Explanation:

A crucial concern for hybrid SMBs is protecting employees, devices, and company data. The hybrid work model introduces new security challenges as employees access company resources from various locations and devices. Ensuring the security of these elements is paramount to maintaining business continuity and protecting sensitive information.

1. Employee Protection: Implementing security measures to safeguard employees' digital identities and ensuring their safe access to company resources.
2. Device Security: Managing and securing a diverse range of devices used by employees, including laptops, mobile phones, and tablets.
3. Data Security: Protecting sensitive company data from unauthorized access and breaches, especially as data is accessed and shared across different environments.

Reference:

- Cisco Hybrid Work Security Solutions
- Security Challenges for SMBs in Hybrid Work Environments
- Cisco Best Practices for Securing Remote and Hybrid Workforces

THANK YOU FOR DOWNLOADING 700-250 UPDATED EXAM QUESTIONS

Note: Thanks For Trying The Demo Of Our 700-250 Exam Product

Visit Our Site to Purchase the Full Set of Actual 700-250 Exam Questions With Answers.

Money Back Guarantee



Click The Link Below

<https://certs4sale.com/cisco/700-250-pdf-exam-dumps>